

Evolution of AI-Powered Surveillance and Its Role in Political Control

Munazzah Bukhari¹, Tahira Mumtaz² and Iqra Latif³

<https://doi.org/10.62345/jads.2026.15.2.4>

Abstract

This paper examines the evolution of AI-powered surveillance and its implications for political control. The rapid advancement of Artificial Intelligence (AI) has transformed the landscape of surveillance, enabling governments to monitor and control citizens with unprecedented efficacy. Researchers analyse the development of AI-driven surveillance technologies, including facial recognition, predictive analytics, and social media monitoring, and their deployment in various regimes. This research is conducted under the qualitative research methodology. An analytical approach is used to provide a comprehensive and analytical understanding of AI-powered surveillance technologies. The analysis reveals that AI-powered surveillance has become a crucial tool for governments to suppress dissent, monitor opposition, and maintain social control. Authoritarian regimes leverage AI-driven surveillance to identify and silence critics, while democratic governments use it to monitor citizens under the guise of national security. The use of AI-powered surveillance has significant implications for civil liberties, including the erosion of privacy, freedom of expression, and assembly. It is argued that the unchecked proliferation of AI-powered surveillance technologies poses a significant threat to global democracy and human rights. The paper concludes by highlighting the need for robust regulations, transparency, and accountability mechanisms to prevent the misuse of AI-powered surveillance for political control. By examining the evolution of AI-powered surveillance, this paper sheds light on the emerging challenges to democracy and human rights in the digital age.

Keywords: Technology, Government, Civil Liberties, Freedom of Expression

Introduction

AI technology, which was once only found in science fiction, is now a part of our everyday lives. It powers our smartphones, shapes our musical tastes, and delivers the information we want from our social media accounts. AI would be an integrated system with self-correction capabilities, logical reasoning principles, and goals for information acquisition. One of the most important subfields of artificial intelligence is machine learning, and advancements in this area are being fuelled by a number of factors, including cloud computing, sophisticated microchips, hardware, and market incentives. AI's amazing perspective is also altering governance paradigms, enabling governments to do things they previously could not imagine, such as monitoring citizens, making decisions for them, and influencing election outcomes. AI's flexibility makes it both a powerful

¹Lecturer, Department of Politics & International Relations, Government College Women University, Sialkot.

²Lecturer, Department of Politics & International Relations, Government College Women University, Sialkot.
Email: tahira.mumtaz@gcwus.edu.pk

³Lecturer, Department of Politics & International Relations, Government College Women University, Sialkot.



and ineffective tool of the law. Researchers have also maintained that jurists employ metaphors to explain how the law relates to emerging technologies or new uses of technology. Researcher Robert clarifies, "A metaphor is a way to directly correlate disparate concepts in order to achieve a rhetorical effect, and every metaphor is, in its own way, an argument." "The power of the metaphor is that it colours and controls our subsequent thinking about its subject". According to Michael Fromkin, this power is especially relevant and powerful when the law meets a new technology.

Nevertheless, the law places no blame or accountability on machines, sentient or not; these are issues that should only be taken into account in relation to humans (assuming that legal considerations can be made at all). Unfortunately, people frequently use personifications and metaphors when discussing AI across different legal contexts (the term "AI" itself is a metaphor). As a result, how one names and characterises AI is crucial in determining how it will impact us; the rhetorical framing of what AI is and does will significantly shape what the law and regulations can ever hope to accomplish regarding AI. An important tool for authoritarian governments is China's AI-powered surveillance system, which uses big data analytics and facial recognition. There are issues with privacy, human rights, and civil liberties because this system is used to stifle dissent and strengthen authoritarian control. There has been a significant change in the relationship between technology and political control, with governments now using technology to monitor, control, and manipulate their citizens. Technology can be a powerful tool for authoritarian control, mass surveillance, and the repression of dissent, but it can also open the door to transparency and democratic governance. Artificial intelligence (AI), big data, and digital surveillance have significantly increased the scope and efficacy of political control in recent decades.

Historical Background of Technological Political Control

The use of technology for political control has deep historical roots.

Throughout the 1990s, many governments invested heavily in researching, developing, acquiring, and implementing new technologies for internal security, police, and paramilitary forces. The goal has been to enhance each agency's policing capabilities. This technocratization of policing is based on the premise that it increases response times and cost-effectiveness. Such initiatives aimed to save police resources by automating control processes, speeding up tasks, or reducing the number of personnel required. As a result, advancements in political control technology were designed to expand the scope, effectiveness, and reach of police authority (Wright, 1998).

AI-Powered Control and Digital Surveillance

Artificial intelligence is transforming political systems through digital surveillance and control, while also enhancing resilience in multiple domains. Governments now use AI-enabled surveillance, facial recognition, and big data analytics to monitor citizens and sometimes forecast behaviour. For example, the Chinese Social Credit System uses AI to rate citizen actions and administer rewards or penalties, while Saudi Arabia and Russia employ AI-based monitoring and internet censorship to suppress dissent (Liang et al., 2018). Beyond governance, AI can strengthen resilience in supply chains, cybersecurity, mental health, and urban, ecological, and social systems. Applications such as predictive analytics and machine learning algorithms support resilient infrastructure, business continuity, crisis management, stronger health systems, disaster response, and climate resilience. Real-time AI evaluation and data delivery have become essential during emergencies, improving resource allocation and situational awareness. By enabling better

decision-making and sustainable use, AI contributes to climate resilience, and in healthcare, AI forecasts disease outbreaks, optimises resource allocation, and enhances patient care.

AI technologies strengthen resilience across multiple domains. Security systems with AI reduce the impact of cyberattacks through real-time detection and response. Machine learning enables organisations to maintain secure postures by adapting to new threats. AI also advances social resilience by identifying vulnerabilities and fostering community interventions. Supply chain resilience is strengthened by forecasting demand and optimising logistics. Smart city AI improves quality of life by managing infrastructure, energy, and transportation. In hospitality and tourism, AI enhances operations, customer satisfaction, and environmental sustainability. AI further supports psychological resilience through interventions and mental health resources (Liladhar Rane et al., 2024).

Internet Censorship and Information Control

A lot of their policies use digital media to control political discourse. North Korea, China, and Iran are further examples. They have created intricate systems such as the Great Firewall, an internet censorship tool that stifles dissenting views and limits access to foreign media. Additionally, to disseminate propaganda, sway public opinion, and silence critics, the government developed methods to manage social media nests that used algorithms and AI-powered bots (Creemers, 2018). In what ways does the internet alter state sovereignty, specifically concerning a state's authority to control the dissemination of information across national boundaries? According to one perspective, the internet is a free-flowing, international information space that has enabled both nations and businesses to produce an overwhelming number of filtered segments, frequently with enormously detrimental unintended consequences. National security, cultural sensitivity, and the defence of social values are among the reasons behind such actions, as are monopoly protection and economic rent-seeking. It used to be a technological axiom that the internet's well-known borderless nature was becoming harder to control. In that very endeavour, states and corporations today have risen to a formidable level of technical sophistication and skill. As a result, the internet as it is accessed and experienced in Canada is completely different from that of Iran, China, or Belarus, rather than offering a one-stop international environment. Therefore, using comparative data from more than 22 countries, this chapter explores internet control geopolitics, particularly states' attempts to limit information across international borders.

An online mapping service called Google Earth provided information about the ongoing political situation in Darfur, Sudan, at the beginning of 2007. But shortly after, an aid worker in Sudan complained that he couldn't load the map correctly, and his browser displayed the error message, "This product is not available in your country." Further research confirmed that this specific instance was accurate, as Google filters access to its services based on the "geolocation" of the IP address of the computer submitting the request. In accordance with U.S. export regulations that forbid the sale or export of information products to Sudan, Google was preventing computers with IP addresses situated in that nation from using its services (Deibert, 2008).

Mass Data Collection and Predictive Policing

Predictive policing is becoming more prevalent, primarily through the use of big data and artificial intelligence to foresee criminal activity. Critics claim that predictive policing enables the government to repress populations and disproportionately targets the marginalised, while supporters claim that it improves security. To find and apprehend possible political dissidents,

authorities in some Middle Eastern and Chinese nations use AI-assisted mass data collection (Ferguson, 2017).

Predictive policing is not the only application of AI technology; other emerging technologies linked to the new digital systems may be able to identify individuals based on their appearance, gait, speech patterns, writing, and even typing. They can now identify a person using an AI system that has computer vision capabilities and rules to identify relevant patterns, with some vagueness-in-face-recognition technology based on one's eyes' shape, color, distance between two eyes, and so on in addition to gait movement (walking or running); speech recognition (which emphasizes identifying patterns through pronunciation, intonation, syntax, and accent), identity mood in expressions by identifying emotion through the identification of facial expressions, and their writing styles by identifying patterns that can be gauged writing structures, phrasing, and spelling, for example; and even by reading their lips when conversations are inaudible. (McDaniel, & Pease, K., 2021) Other intelligent systems include smart recognition technologies for identifying knives by their presence within a building, reading license plate numbers on cars, and detecting gunfire. The accuracy of recognition systems, such as facial recognition technologies, has significantly increased over the last five years and often surpasses human recognition skills in head-to-head competitions (Brundage, 2018).

Ethical and Political Concerns

These days, AI Political Control raises significant moral and legal issues. Researchers claim that widespread surveillance leads to totalitarianism and has an impact on freedom of speech and privacy. An international alarm has been raised by organisations like HR Watch and the UN, which have repeatedly warned that uncontrolled AI surveillance will result in human rights violations never seen before. Governments now have more power over their citizens than ever before, thanks to technological advancements. Some argue that these technologies support security and good governance. The challenge ahead is striking a balance among ethical considerations, technological advancement, and regulatory protections (Zuboff, 2019). Digital surveillance, data manipulation efforts, and extremism have largely placed digital media producers and consumers in the dock. Since then, the pendulum has started to swing in favour of thinking about and, in some cases, advocating for the welfare of the digital world, which calls for a much closer examination of the ethical issues surrounding Big Data and ethical AI. In fact, the former is an externality of the BD and AI processes utilised in digital media, which are in opposition to fundamental principles of human rights and democracy (Christodoulou & Lordanou, 2021).

Evolution of Surveillance Technologies

After World War II, the development of electronic surveillance technology began, especially in Europe. We first look at the different origins of surveillance and make the argument that it is a natural part of human societies and has even become a crucial prerequisite for the success of modern industrial societies. The various developments that occurred during the mainframe computer era (1950–1985) either directly or indirectly aided in the automation and sophistication of mass data collection, making it more rationalised but less answerable to the general public. We then move on to video surveillance, one of the most recognisable technologies of the surveillance society era. During the 1990s, its use and growth in the UK and other European countries were influenced by a variety of social and political factors. The use of surveillance technologies by actors such as government agencies, businesses, and individuals has become prevalent in the early 21st-century networked world (Kerstin Goos et al., 2014).

Early Surveillance Methods

In the past, surveillance techniques depended on technological instruments, human intelligence, and physical records. To enhance security in high-risk areas, governments and law enforcement agencies employed wiretapping, closed-circuit television, and third-party informants. Due to their reliance on physical storage and human labour, these techniques were of a smaller scale than contemporary digital surveillance systems (Gill & Phythian, 2018). To track people and uphold social order, early surveillance techniques relied primarily on written records, human informants, and physical monitoring. Spies and messengers were primarily employed by ancient societies, such as Egypt, China, and Rome, to obtain intelligence on internal dissension and adversaries. In the meantime, medieval rulers used secret police and postal inspections to control information. The state's surveillance techniques were improved by the development of bureaucracy and census data, which laid the groundwork for contemporary surveillance technologies (Foucault, 1977).

The Digital Revolution and Surveillance

Many methods have redefined monitoring across all edges, including government monitoring, corporate monitoring, and peer surveillance, thanks to cutting-edge technologies such as CCTV, databases, and internet tracking. While real-time surveillance, big-data aggregation, and predictive policing have been made possible in the modern era, this change presents ethical and privacy concerns because it represents previously unheard-of control over personal data (Goold, 2004). Thus, surveillance targets shifted from state threats to terrorist networks as a result of the global war on terror. Drones became a dual-purpose tool for hunting and collecting in the post-9/11 surveillance environment. Drone use surged during the war in Afghanistan and spread to other countries, such as Iraq, Somalia, and Syria. This coincided with the growth of mass data collection and internet surveillance (Wark, 2021, September 01).

AI's Emergence in Surveillance

At its broadest level, surveillance is defined as the collection or examination of data by an individual or entity relating to other persons, whether acting as individuals or as part of a collective whole. In this AI era, however, surveillance often takes place on an extraordinarily large scale: entities within the reach of minimum visibility utilise big-data techniques and aggregation to actually extend this reach toward unobserved persons, places, or pieces of information. A dramatic example involves the power to surveil, to watch, monitor, track, profile, sort, or discipline individuals and populations in both private and public settings through such environments as CCTV, digital traces on social network sites, or biometric monitoring of bodies. Widely connected networks are used to actively collect, share, and aggregate data. The idea that technologies make it possible to be surveilled somehow fosters fear and self-censorship, and that tracking in and of itself activates a ubiquitous form of social control, is a fundamental idea in surveillance studies. (Kalluri et al., 2017).

Big Data and AI Advancements

The ability of machines or computer programs to perform tasks that a human being can, in areas such as visual perception, audio, text, language, and speech recognition; decision-making; data collection and analysis; and learning, is what we regard as artificial intelligence. As a result, machine learning, a subset of artificial intelligence, is a component of most of what we discuss here. Machine learning is a branch of artificial intelligence that enables machines to perform their jobs effectively through intelligent software. Regression analysis, clustering, classification, and

automated content moderation are just a few of the machine-learning tasks that fall under the umbrella of artificial intelligence. It expands the capabilities of traditional machine learning functions and incorporates expert systems, natural language processing, and symbolic artificial intelligence (Hunter et al., 2024).

AI's integration into Governance and National Security

China has recently focused on developing AI technology, primarily for surveillance. Following the State Council's AI plan, which emphasised AI's significance as a crucial security tool, interest in the technology skyrocketed. Instead of focusing only on research and development, the government has invested significant resources in AI development to see how well it can be applied to improve surveillance capabilities while maintaining mass social control. The development of surveillance technology was further spurred by the COVID-19 pandemic. Artificial intelligence has led the way in surveillance. The implementation of AI-powered facial recognition systems, which keep tabs on people in public areas, follow their whereabouts, and identify those thought to pose a threat to the state, is one well-known example. These systems are frequently combined with China's extensive surveillance camera network to create an extremely intrusive and widespread monitoring infrastructure (Woods, 2025).

Chinese Model of Surveillance in AI: The Roots and Development

The Great Firewall, a complex network of laws and technological tools that blocks foreign websites, filters content, and monitors online activity, is at the heart of China's surveillance system. By limiting citizens' access to politically sensitive or potentially destabilising content, the system effectively establishes a separate Chinese internet where the government can control the narrative. Foreign news websites are severely restricted in China, and Google, Facebook, and Twitter, all widely used abroad, are blocked (Woods, 2025). According to a 2017 report, China spent \$200 billion on domestic security, including projects involving surveillance technology and urban management. An estimated \$20 billion was spent in China in 2018 to buy CCTV cameras and other surveillance equipment for areas within 100 to 300 miles of the country's border, but this amount did not represent a significant share of China's overall investment in this field. Surveillance technology has advanced more quickly as a result of the ongoing COVID-19 pandemic. The Chinese government began widespread surveillance to curb the virus's spread, and the expansion was carried out under the guise of public health and safety.

As part of the measures, security-science technologies like data tracking and facial recognition were used to help enforce quarantine and identify potential virus carriers. But the investments also highlight China's dedication to deploying cutting-edge surveillance technologies to maintain social stability, underscoring the government's strategic priorities and the expanding global influence of Chinese surveillance technology. Artificial intelligence has led the way in surveillance. One well-known example is the use of AI-powered facial recognition software to monitor people in public areas, track their movements, and identify those who may pose a threat to the state. These systems are frequently combined with China's extensive surveillance camera network to create an extremely intrusive and widespread monitoring infrastructure (Woods, 2025).

Use of AI in China in Fast-Growing Industries

The acceleration of scientific and technological advancements, industry optimisation and modernisation, and the general increase in productivity are all fueled by artificial intelligence (AI). The heterogeneity analysis indicates that, while AI is present in strategic emerging industries, the

ownerships that empower it vary across industries. The central and eastern regions are the weakest, while the western region is the strongest in terms of AI empowerment. Furthermore, it was believed that the support for AI was more robust among SOEs than among non-SOEs. An AI technology innovation platform, distinct regulations, and dedicated funds should be established to further leverage AI's role in fostering technological innovation across strategic emerging industries. This combination of low prices, a sizable and rapidly expanding domestic market, and China's most aggressive efforts to attract foreign manufacturers through a range of incentive programs led to the country's rise as the global centre of manufacturing. Although the United States' manufacturing industries have suffered significant harm, the majority of this damage has been in the more established sectors of plastics, metals, textiles and clothing, toys, and furniture. This has had major civilian repercussions for American communities and workers harmed by China, but less so for the pressures on American techno-economic power and dual-use capabilities, particularly in American-headquartered companies. Furthermore, this had nothing to do with a high degree of strategic reliance on China. The elimination of McDonald's Happy Meal toys would be the worst thing that could possibly happen in the event of conflict (Atkinson, 2024).

The 2010s: Expansion of AI Surveillance

There is a growing policy sector and a trade-up of laws and regulations, raising serious questions about whether the concept of privacy and its accompanying policies fairly address the scope of the social problem. The criticisms consist of a number of interconnected components that clarify various conceptual and practical levels. From a philosophical standpoint, privacy is grounded in liberal individualism and may not accurately reflect the diverse and contradictory subjectivities and identities that define the contemporary world (Ennett, 2008). The methods by which people become watchers either through subtle coercion or extremely cunning market manipulation may be more fascinating. Recent empirical research suggests that there are numerous examples of peer-monitoring or lateral surveillance, ranging from neighborhood watch programs to landlord/tenant monitoring, to citizen groups that post the license numbers of people suspected of soliciting prostitutes, to Webcams for the surveillance of children, teenagers, and domestic workers, to locational devices that can be installed in cars to monitor speed, safety protocols, drug and alcohol use, and so forth (Lyon, 2007).

The United States also institutionalised like-for-like monitoring through Operation TIPS, which was launched following an incident. Mail carriers, meter readers, and repair workers whose jobs allow them to do so, as well as anyone else who may have seen or heard of suspicious terrorist activity, could all be considered eligible to serve as informants. The fact that someone had already established a website devoted to "Operation TIPS-TIPS", where people could report suspected informers, was almost thrilling. It should be noted that peer-to-peer monitoring in the US is not particularly new. The American Protective League had about a quarter of a million badge-wearing members between 1915 and 1917, and they proudly reported any suspicious activity to the Justice Department, particularly involving citizens of German descent (Wood, 2004).

Major Policies Enabling AI-Powered Surveillance

Public safety regulations and data privacy laws that exempt surveillance enabled national security laws to permit it with minimal interference. Globally, governments employ artificial intelligence for mass data collection, predictive policing, and facial recognition. Programs like Skynet and Sharp Eyes integrate AI-powered facial recognition into China's national surveillance systems. (Mozur, 2019) Furthermore, the USA PATRIOT Act has transformed government surveillance

capabilities, enabling intelligence services to monitor electronic communications with AI tools. While the General Data Protection Regulation of the European Union places a strong emphasis on data privacy and excludes exceptions for national security and crime prevention, it also makes it easy to facilitate AI-enabled surveillance across European states and further prioritises these benefits over civil liberties (Kuner, 2020).

AI-driven surveillance is being used in smart city projects and private-sector initiatives, with law-enforcement tools provided by corporations such as Google and Amazon. AI is incorporated into urban infrastructure in Singapore and the United Arab Emirates, resolving security issues while posing ethical questions. Future regulations will strike a balance between human rights, privacy, and innovation. For example, under Amazon's Ring Neighbours Program, law enforcement uses AI-generated home surveillance footage, which essentially promotes home surveillance and creates privacy concerns (West, 2020).

Global Trends in AI Surveillance and Political Control

The types of government in the US, China, and Russia affect how AI is applied through Information and War Information Sharing (IWIO). The US gathers a lot of information about domestic security threats, but because their governments are not democratic, China and Russia can gather more information through aggressive means. The information can be used by these states to train AI algorithms for grey zone and IWIO operations. Due to political oversight and democratic principles, the US faces challenges in gathering and utilising large amounts of data. The impact of regime type, AI, and IWIO on these nations' strategies must be taken into account, as surveillance capitalism shapes data collection, AI algorithms, and IWIO (Hunter et al., 2024). Misinformation exacerbated by Gen-AI tools poses a significant threat to democratic epistemic agency. Misinformed individuals can be considered misinformed if they believe incorrect information to be true, but the danger lies in their confidence in its accuracy. Malicious agents, such as political parties, media, or foreign actors, can intentionally spread misinformation to guide people towards specific outcomes. Social media has made it easier for these actors to spread falsehoods, making it harder for them to manipulate public opinion. This issue is particularly concerning in the scenario of democracy. Non-propagandistic disinformation is just as detrimental to democracy as propaganda, and it may be even harder to identify and control (Kuklinski, 2000).

AI Surveillance in Western Democracies

As evidenced by the mass arrest of Japanese citizens following Pearl Harbour, American intelligence has a history of reacting rashly to security threats. Based on rash responses, unprecedented intelligence-gathering operations were launched after 9/11. The Snowden revelations intensified the security and civil rights debate, compelling intelligence services to focus on identifying threats with the least privacy infringement. Analytical skills were enhanced by the introduction of Big Data systems and analyst training. Discussions about striking a balance among civil rights, oversight of counterintelligence authority, and security demands continue (Barnea, 2019). Liberal democracies' responses to the opportunities and challenges posed by AI will depend on how they address internal issues, as well as the increasingly prevalent external phenomenon of the selective, predictive authoritarian alternative. Overall, both situations offer reasons for cautious optimism. Emerging democracies, like the US and the UK, will still need significant concentrated effort, even though they are clearly challenged. To be honest, the challenges do not appear to be more significant than those that have been successfully addressed in the past. The foundation of guarded optimism is a straightforward path dependence. Countries with a long history of individual

liberty will probably adopt the technology in one way, while those in a different situation will probably take a different route. There aren't many differences between the US and China, according to some tech experts, such as Jaron Lanier. This will probably continue with new AI technologies if we remain vigilant. Governments will be extremely uncomfortable with this oligopolistic concentration of power through monopolistic monopolisation of competition and lobbying, just as they were with previous technological revolutions. A third area concerns worries about the state of the media landscape, where tech giants pose a threat to vital public-interest content, effective media plurality, and a Wild West mentality in political advertising. However, all of these new, radical technologies have been used to address these problems. Technology will most likely catch up with regulations governing who owns media, who is a publisher and other issues (Wright, 2019).

AI Surveillance in Other Authoritarian States

Strong countermeasures from the USA and its like-minded partner nations are necessary to stop the negative effects of Russia, China, and other states' use of digital authoritarianism to increase their influence. First of all, if a regime regularly and consciously engages in mass surveillance without protection or safeguards, it should be categorised as a digital authoritarian regime. Businesses that supply digital authoritarian systems should face harsh penalties; this includes businesses based outside both US and Russian jurisdictions, such as those in Europe and Israel. The export of sensitive technologies to China and other digital authoritarians should be severely restricted at the same time (Pokyakova & Meserole, 2019).

Digital authoritarianism is constantly expanding, endangering Internet users' rights and data privacy both nationally and globally. However, the breadth and selection of cases in research on digital authoritarianism remain constrained. These areas of difference are worth considering. According to one viewpoint, the varieties of authoritarianism hypothesis holds that various political systems face a set of enduring and distinctively limiting factors in regulating the digital sphere. Alternatively, according to the development trajectory theory, the technological advancements of a given nation would reflect poorly on the ability of that system to extend governance, govern, or both (Howells & Henry, 2021). Through the use of facial recognition, internet monitoring, and predictive policing, artificial intelligence (AI) surveillance has recently come to light as a means by which Russia may monitor and control its citizens. According to research, predictive policing signals potential opposition targets and counters purported movement or financial transaction patterns. Furthermore, growing concerns about global authoritarianism through digital governance have been exacerbated by Russia's advances in AI surveillance, facilitated by partnerships with Chinese firms such as Huawei. The broader trend of using AI as a weapon against civil liberties and democratic movements worldwide includes these developments (Gelman, 2021).

The Role of International Organisations and Human Rights Concerns

Given the many new threats to human rights on the internet, digital human rights are becoming increasingly important within international organisations that address human rights. These organisations have both global and local operations, and they work with a variety of priorities and strategies. Leading a multi-stakeholder approach that incorporates academia and civil society are the United Nations and the Council of Europe. Regarding the regulation of new and emerging obstacles to the enjoyment of fundamental human rights, such as freedom of expression, privacy, and data protection, they bring together all international organisations under both soft and hard

law. Human rights-centred artificial intelligence regulation receives special attention. The growing need for international cooperation will be addressed by the Global Digital Compact, which the UN is anticipated to adopt in September 2024 (Wagner et al., 2025). According to the provisions of the General Data Protection Regulation (GDPR) in the European Union, this new world, centred entirely on artificial intelligence systems, generates significant controversy, opportunities, and daunting challenges. These ethical standards of lawfulness, justice, transparency, and data minimisation become the yardsticks by which AI applications are evaluated for their adherence to individual rights to privacy and data protection. An analysis of the GDPR's provisions on citizens' rights, profiling, and automated decision-making will show how important they are to the protection of human rights in this increasingly important context for humans and AI. It emphasises the importance of developing and using AI responsibly and in accordance with the GDPR (Hoxhaj et al., 2023).

It aims to protect human rights and dignity in the AI-infused world by highlighting these moral and legal requirements. AI most clearly reveals its true nature as affecting human rights and dignity at the intersection of such ethical and legal requirements, especially those of the GDPR. To ensure the long-term preservation of individual rights in the digital age, our research contributes to this conversation and offers guidance for the creation of future artificial governments that integrate AI with stricter privacy and data protection standards mandated by European privacy laws.

Conclusion

From traditional state control to the high-tech AI systems of today, what has evolved historically as surveillance represents a historic shift? Early techniques relied on manual tracking and human informants, but technological advancements, particularly in the digital age, undoubtedly changed how governments managed their populace. Digital surveillance and mass data collection under the pretext of national security were sanctioned more frequently in the post-9/11 environment. One could argue that each step helped legitimise policies and actions implemented by different corporations and national governments, thereby accelerating the development of the surveillance state. Artificial intelligence has brought autonomy, accuracy, and a deep integration of surveillance into governance. In yet another example of modernisation, China uses AI to create its own sophisticated surveillance state that combines predictive policing, big data analytics, and facial recognition. The early technological investment and legal framework for creating a political control system with AI-driven surveillance, in collaboration with major tech companies, can be attributed to the Chinese model. On a global scale, increasing AI surveillance brings both opportunities and risks. While some democratic governments use AI to prevent crime, others weaponise it to further repress dissent and solidify state power. The UN, human rights organisations, and other relevant institutions should be compelled to issue a warning against the unrestrained integration of AI into governance in response to this ethical crisis. Analysing China's current control system and its global implications for democracy requires some historical background on AI-powered surveillance. In the coming decades, the role of AI in political control will remain crucial to civil liberties and state governance.

References

- Atkinson, R. D. (2024). China is rapidly becoming a leading innovator in advanced industries. *ITIF Hamilton Center on Industrial Strategy*, 134–137.
- Barnea, A. (2019). Big data and counterintelligence in Western countries. *International Journal of Intelligence and Counterintelligence*, 32(3), 433–447.

- Brundage, M. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford.
- Christodoulou, E., & Lordanou, K. (2021). Democracy under attack: Challenges of addressing ethical issues of AI and big data for more democratic digital media and societies. *Frontiers in Political Science*.
- Creemers, R. (2018). China's social credit system: An evolving practice of control. Oxford China Centre, University of Oxford.
- Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.
- Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books.
- Gellately, R. (1990). *The Gestapo and German society: Enforcing racial policy, 1933–1945*. Oxford University Press.
- Gelman, V. (2021). *Authoritarian Russia: Analyzing post-Soviet regime changes*. University of Pittsburgh Press.
- Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (2nd ed.). Polity Press.
- Goold, B. (2004). *CCTV and policing: Public area surveillance and police practices*. Oxford University Press.
- Howells, L., & Henry, L. A. (2021). Varieties of digital authoritarianism: Analyzing Russia's approach to internet governance. *Problems of Post-Communism*, 54(4), 1–27.
- Hoxhaj, O., Halilaj, B., & Harizi, A. (2023). Ethical implications and human rights violations in the age of artificial intelligence. *Balkan Social Science Review*, 22, 153–171.
- Goos, K., Friedewald, M., Webster, C. W. R., & Leleux, C. (2014). Surveillance in Europe. In D. Wright & S. Gutwirth (Eds.), *The co-evolution of surveillance technologies and surveillance practices* (p. 44). Routledge.
- Kuklinski, J. E. (2000). Misinformation and the currency of democratic citizenship. *The Journal of Politics*, 62(3), 790–816.
- Kuner, C. (2020). The European Union and the search for an international data protection framework. *European Journal of International Law*, 31(1), 307–326.
- Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using AI in their information warfare and influence operations. *Defense & Security Analysis*.
- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415–453.
- Rane, N. L., Choudhary, S. P., & Rane, J. (2024). *Artificial intelligence for enhancing resilience*. University of Mumbai.
- McDaniel, J. M. C., & Pease, K. (2021). *Predictive policing and artificial intelligence*. Routledge.
- Mozur, P. (2019). Inside China's dystopian dreams: AI, shame, and lots of cameras. *The New York Times*.
- Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese model*. Brookings Institution.

- Kalluri, P. R., Agnew, W., Cheng, M., Owens, K., & Birhane, A. (2023). *The surveillance AI pipeline*. arXiv.
- Wagner, B., Kettemann, M. C., Dittmann, K. V., & Montgomery, S. (2025). International organizations and digital human rights. In B. Wagner (Ed.), *Research handbook on human rights and digital technology* (pp. 310–324).
- Wark, W. (2021, September 1). The new world of surveillance: The 9/11 effects and the transformation of global security.
- West, S. M. (2020). Amazon, facial recognition, and the rights of the surveilled. *Journal of Business Ethics*, 162(3), 607–623.
- Wood, D. M. (2004). Editorial: A report on the surveillance society. *Surveillance & Society*, 1(3), 1–4.
- Woods, D. (2025). AI as a tool for surveillance: China's concave trilemma. *Journal of Chinese Political Science*.
- Wright, N. D. (2019). *Artificial intelligence and domestic political regimes: Digital authoritarianism, digital hybrid regimes, and digital democracy*. Air University Press.
- Wright, S. (1998). *An appraisal of technologies for political control*. European Parliament, Directorate-General for Research.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.