The Impact of AI-driven Government Surveillance on Democracy and Liberty

Selvahini Kamalarajan
Department of Electrical and Computer Engineering

Toronto, Canada
s5kamala@uwaterloo.ca

***Abstract*— The growing use of artificial intelligence (AI) by repressive regimes for government surveillance remains a topic that is insufficiently addressed in modern discourse, such as politics, technology and culture. AI technologies, such as facial recognition (FR) systems, have emerged as a transformative technology, reshaping our world at an unprecedented pace. These technologies are implemented in diverse consumer industries to collect biometric facial data, including autonomous vehicles, security systems and facial authentication processes on devices, but they are now being weaponized as surveillance tools to repress and erode the democratic freedoms of citizens. FR technologies are contributing to digital authoritarianism where citizens are losing their fundamental democratic rights, freedom of expression and civil liberties. By examining case studies from China and Russia, this paper explores how the deployment of AI-driven surveillance systems poses significant risks to democratic ideals and political freedoms in authoritarian regimes. In these countries, the use of AI for government surveillance squanders political dissent and opposition, threatening other democratic nations. As such, the significance of this topic in contemporary times will be highlighted and proved using credible examples and references. The paper concludes by highlighting how future research will focus on analyzing the continued evolution of AI surveillance and its effects on democracy.**

Keywords—surveillance, government, AI, facial recognition, democracy, liberty, freedom of expression.

I. Introduction

Envision a world where AI is weaponized as a mass surveillance tool and knows us better than we know ourselves. How would AI surveillance erode personal liberties and threaten democratic ideals? In an increasingly digital world, AI has revolutionized industries by enhancing security and optimizing data analysis [1]. AI's ability to process vast amounts of data and detect patterns in datasets based on predictive algorithms through natural language techniques has accelerated its usage across diverse industries [1]. In particular, FR systems involve complex image processing techniques to detect and analyze biometric facial data to verify an individual's identity [2]. Deep learning algorithms trained on millions of facial data help create three-dimensional faceprints with distinct human features [2]. FR technologies also have a wide range of applications in consumer industries [3]. According to "Research on the application of face recognition system" published by the Journal of Physics: Conference Series, face tracking with 3D face recognition algorithms is used to track criminal suspects or find the relatives of missing persons [3]. In the workplace, facial biometrics is used to input staff information at the time of check-in [3]. Customs stations and other places that require the verification of personnel information are other examples where FR is used for identity authentication [4]. FR also offer diverse benefits compared to other verification systems; concurrency enables cameras or other video equipment to capture multiple faces simultaneously, proving to be more efficient than fingerprint, palm print and other identification technologies [4]. However, despite these advantages, the application of FR in government surveillance threatens democratic ideals by providing unprecedented power for authoritarian governments to control and monitor the masses.

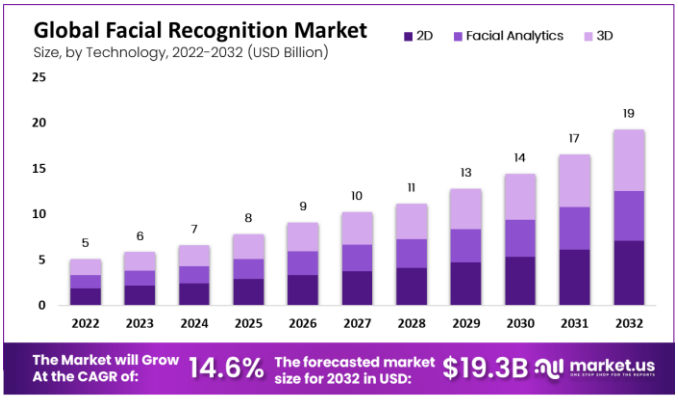

Fig. 1: Global Facial Recognition Market. Adapted from [5].

An ideal democratic world is one where everyone can exercise their rights to freedom of expression, autonomy and privacy. Now more than ever, the advent of AI surveillance can accelerate the potential for authoritarianism in countries wanting greater control through an Orwellian surveillance system. In these regimes, FR systems offer access to the intimate details of citizens' lives where their movements, communication and activities are recorded and monitored to suppress political dissent and individual expression [4]. The use of AI for government surveillance also threatens democratic societies worldwide [4]. Since AI surveillance can perpetuate or even amplify societal biases, authoritarian regimes that aim to enforce

discriminatory practices against certain ethnicities can do so with greater control [4]. As democratic societies enable citizens to live autonomously without state interference—AI-powered surveillance systems, especially FR, present a dystopian reality where democracy and individual autonomy are threatened [4].

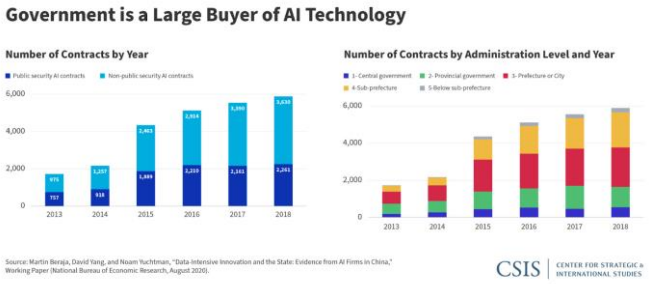

Fig. 2: Purchasers of AI technology. Adapted from [6].

When considering the "world in chains" scenario where a totalitarian government employs novel technology to impose perpetual oppression on the global population [7], AI surveillance serves as a powerful tool to enable such existential risks. Unlike previous authoritarian regimes which were often limited in their ability to rise to power, the capabilities offered by FR technologies—such as predictive policing, real-time monitoring and biometric facial databases—could allow such regimes to achieve indefinite dominance [4]. The effects of deploying AI surveillance technologies to erode democratic freedoms can be better understood by using China and Russia as case studies, which is significant in addressing the risks posed by FR nationwide. Both China's and Russia's AI-driven surveillance systems threaten democratic principles and help to solidify their authoritarian regimes.

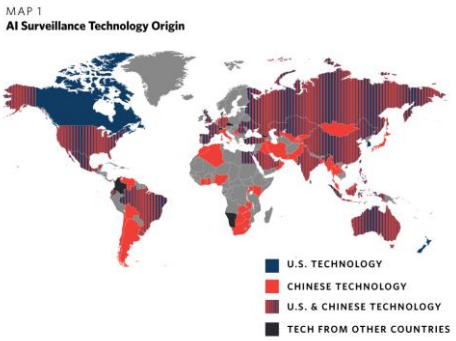

Fig. 3: Surveillance Technology Origin. Adapted from [8].

II. Case Studies

A. China

China's extensive AI-driven surveillance system integrating FR represents a significant violation of democratic principles such as individual privacy, civil liberties, and political freedoms by inducing an authoritative regime. According to "The Road to Digital Unfreedom: President Xi's Surveillance State," researcher Xiao Qiang reports 176 million surveillance cameras, including AI-equipped CCTV cameras, are used to monitor China's 1.4 billion citizens with plans to raise this number to 626 million by the end of the decade [9]. Chinese officials aim to enforce the FR video surveillance system to provide "100 percent coverage" in public spaces, which infringes on the privacy of Chinese citizens [9]. These AI databases are then weaponized for suppressing citizens, including ones with no suspicion of criminal activity, and limiting freedom of speech across mainland China [9]. Furthermore, China's use of AI-based surveillance to repress and target the Uyghur Muslim minority enables them to commit crimes against humanity at an unprecedented level [9]. In Xinjiang, the Chinese Communist Party has established AI databases to spy on political dissidents with the aim of total societal control [10]. The Xianjing authorities have enforced surveillance using CCTV cameras and FR to identify suspicious and threatening behaviour [11]. This data is later used to flag or threaten Uyghur citizens by limiting their liberty and sending them to detention or reeducation camps [12]. The use of such AI surveillance technologies based on racial discrimination threatens the political freedoms and civil liberties of minority populations—infringing on the freedom of religion, autonomy and privacy of citizens [12]. Finally, there is a risk that Chinese mass surveillance technology will become pervasive in other countries as a means of social control [10]. As China is a popular exporter of surveillance technology for more than 80 countries, including 18 countries with poor human rights records, the risk of other countries adopting AI surveillance technology raises privacy, ethical and social concerns according to the Europian Parliament [10]. While China expresses that its AI-powered surveillance system aims to enhance public safety, maintain social stability and promote state-approved behaviour, the reality is that it has been weaponized to monitor, oppress and gain control over its citizens in ways that directly undermine democratic ideals [10].

Fig. 4: The Spread of Surveillance Technology. Adapted from [13].

B. Russia

Russia has deployed FR technology in various public spaces to curb political dissent and limit freedom of speech, thereby eroding democratic freedoms [14]. In 2017, Moscow launched one of the world's largest FR video surveillance networks deploying more than 200,000 cameras across the city [15]. Capable of tracking citizens in real-time, FR technologies enable the Kremlin to target individuals for their political views and participation in protests, signifying an authoritarian regime [15]. For example, during protests in support of the Russian opposition leader Alexei Navalny, Kremlin-controlled Russian

security services used FR to identify and arrest demonstrators in 2021 [16]. This allowed the police to track, arrest, and intimidate opposition leaders and their supporters [14], stifling freedom of speech and assembly. According to a Reuters review of 2,000 court cases, FR cameras have played a fundamental role in the arrests of hundreds of peaceful protestors after they joined anti-government demonstrations [16]. Maria Nemova, a lawyer for the Memorial human rights group, notes, at least 141 people were preventively detained in the Moscow metro after being identified by FR databases [16]. While these people had not committed any illegal activities, they were flagged only because of their previous protest participation [16]. In a democratic society, freedom of expression—including the ability to express political dissent without fear of reprisal—is a fundamental human right. The FR system's ability to track individuals across public spaces without their knowledge or consent undermines this right and exacerbates the issue of reduced civil liberties. Furthermore, leaked government documents reveal that the Kremlin administration plans to fund a comprehensive AI-powered surveillance operation by investing over 11 million euros in advanced surveillance technologies [16]. This disturbing trend of implementing and investing in AI-powered surveillance could potentially lead to AI-based algorithmic authoritarianism through internet censorship, repression and predictive policing [10].

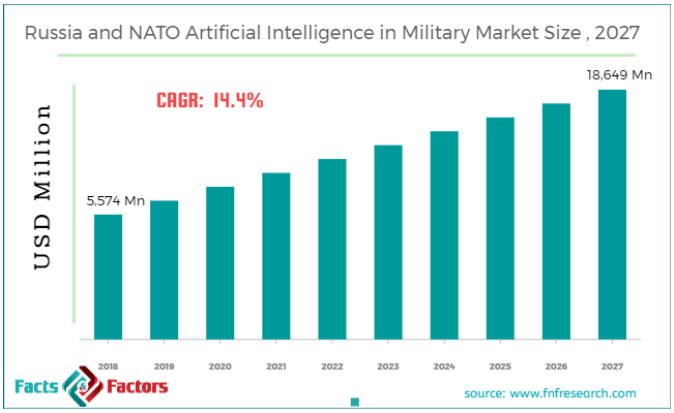

Fig. 5: Military Market Size, 2027. Adapted from [17].

III. Conclusion

In conclusion, AI-based surveillance systems have detrimental consequences on the state of democracy and the civil liberties of citizens today. As freedom of expression and liberty are core values that define democracy, the risks posed by AI deployment in government surveillance for state control raise concerns about the erosion of these democratic ideals. By employing AI surveillance to monitor citizens, especially political dissenters, authoritarian countries create an environment of fear and self-censorship, where individuals may refrain from exercising their rights to free speech, assembly, and protest. For instance, in China, the integration of FR cameras in public spaces violates the privacy of Chinese citizens, who are threatened using AI databases regardless of previous criminal activity [10]. China's surveillance system also enables them to repress ethnic minority populations, namely the Uyghur Muslims by limiting their freedom of expression and liberties, constituting genocide [12]. These actions have broader implications worldwide; Chinese exports of surveillance technologies to countries with poor human rights records mean there is a risk of other nations adopting surveillance technologies to reduce citizens' freedoms on a global scale [10]. Furthermore, Russia deploys FR technology to threaten and punish citizens for their political dissent and protest participation—a clear violation of civil liberties [16]. As FR technologies have been intrusively employed to violate democracy in these countries, there is a need for redirecting future research to focus on the continued usage of AI-powered surveillance systems and their effects.

References

[1] J. Duberry, "AI in public and private forms of surveillance: Challenging trust in the citizen-government relations," *Edward Elgar Publishing eBooks*, pp. 93–125, Jun. 2022, doi: https://doi.org/10.4337/9781788977319.00009.

[2] O. of the P. C. of Canada, "Privacy guidance on facial recognition for police agencies," *www.priv.gc.ca*, May 02, 2022. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/. [Accessed: Nov. 26, 2024].

[3] Chen Mingtsung, W. Qian, J. He, and Zhao zhuomin, "Research on the application of face recognition system," *Journal of physics*, vol. 1684, no. 1, pp. 012126–012126, Nov. 2020, doi: https://doi.org/10.1088/1742-6596/1684/1/012126.

[4] D. Murray, "Facial recognition and the end of human rights as we know them?," *Netherlands quarterly of human rights*, vol. 42, no. 2, May 2024, doi: https://doi.org/10.1177/09240519241253061. [Accessed: Nov. 25, 2024].

[5] *Global Facial Recognition Market By Technology*. 2024. Accessed: Nov. 27, 2024. [Online]. Available: https://market.us/report/facial-recognition-market/

[6] I. Mazzocco, *The AI-Surveillance Symbiosis in China*. 2022. Accessed: Nov. 27, 2024. [Online]. Available: https://bigdatachina.csis.org/the-ai-surveillance-symbiosis-in-china/

[7] D. Minardi, "The grim fate that could be 'worse than extinction,'" *www.bbc.com*, Oct. 16, 2020. https://www.bbc.com/future/article/20201014-totalitarian-world-in-chains-artificial-intelligence. [Accessed: Nov. 25, 2024].

[8] S. Feldstein, Ed., *The Global Expansion of AI Surveillance*. 2019. Accessed: Nov. 27, 2024. [Online]. Available: https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

[9] X. Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State | Journal of Democracy," *Journal of Democracy*, 2019. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/

[10] R. Kaskina and A. Cvetkovska, "Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights," 2024. Available: https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450(SUM01)_EN.pdf. [Accessed: Nov. 27, 2024].

[11] S. Chestnut, "DEALING WITH DEMAND FOR CHINA'S GLOBAL SURVEILLANCE EXPORTS," 2020. Available: https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf. [Accessed: Nov. 25, 2024].

[12] A. Anand, "Repression of Uyghur Muslims and the Freedom of Religious Beliefs in China," *Journal of Social Inclusion Studies*, vol. 8, no. 1, pp. 23–36, May 2022, doi: https://doi.org/10.1177/2394481221085680 [Accessed: Nov. 25, 2024].

[13] J. Cohen, Ed., *The World Relies on China's Surveillance Technology*. 2019. Accessed: Nov. 27, 2024. [Online]. Available: https://www.pcmag.com/news/the-world-relies-on-chinas-surveillance-technology

[14] L. Masri, "How facial recognition is helping Putin curb dissent," *Reuters*, Mar. 28, 2023. Available:

https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/. [Accessed: Nov. 25, 2024].

[15] T. M. Times, “Mass Survellience in Russia Expands Rapidly Since Ukraine Invasion – MT Russian,” *The Moscow Times*, Aug. 17, 2023. https://www.themoscowtimes.com/2023/08/17/mass-survellience-in-russia-expands-rapidly-since-ukraine-invasion-mt-russian-a82151. [Accessed: Nov. 27, 2024].

[16] A. Gielewska, “Kremlin Leaks: How Putin’s Regime is Building AI Surveillance Operations - VSquare.org,” *VSquare.org*, Mar. 27, 2024. https://vsquare.org/kremlin-leaks-russia-putin-ai-surveillance-facial-recognition-ntechlab/ [Accessed: Nov. 27, 2024].

[17] *Russia and NATO Artificial Intelligence in Military Market Size, Share Global Analysis Report, 2019–2027*. 2019. Accessed: Nov. 29, 2024. [Online]. Available: https://www.fnfresearch.com/russia-and-nato-artificial-intelligence-in-military-market