AI and Ethics (2023) 3:369–379
https://doi.org/10.1007/s43681-022-00196-y

REVIEW

"Ethically contentious aspects of artificial intelligence surveillance: a social science perspective"

Tahereh Saheb[1]

Received: 20 May 2022 / Accepted: 29 June 2022 / Published online: 19 July 2022

Abstract
Artificial intelligence and its societal and ethical implications are complicated and conflictingly interpreted. Surveillance is one of the most ethically challenging concepts in AI. Within the domain of artificial intelligence, this study conducts a topic modeling analysis of scientific research on the concept of surveillance. Seven significant scholarly topics that receive significant attention from the scientific community were discovered throughout our research. These topics demonstrate how ambiguous the lines between dichotomous forms of surveillance are: public health surveillance versus state surveillance; transportation surveillance versus national security surveillance; peace surveillance versus military surveillance; disease surveillance versus surveillance capitalism; urban surveillance versus citizen ubiquitous surveillance; computational surveillance versus fakeness surveillance; and data surveillance versus invasive surveillance. This study adds to the body of knowledge on AI ethics by focusing on controversial aspects of AI surveillance. In practice, it will serve as a guideline for policymakers and technology companies to focus more on the intended and unintended consequences of various forms of AI surveillance in society.

Keywords Artificial intelligence · Ethic · Surveillance · Topic modeling

1 Introduction

Artificial intelligence has had a substantial influence on civilization, whether in the form of algorithms and machine learning models, or robots and autonomous systems. Enhancing surveillance and monitoring is one of the most critical uses of artificial intelligence. At least 75 of the world's 176 countries, according to the Global Surveillance Index (GSI), are actively investing in and deploying artificial intelligence (AI) for surveillance purposes, primarily in smart cities, facial recognition, and smart police [17]. Governments have integrated artificial intelligence into cameras, video management software, and mobile phones in collaboration with technology corporations [35] and normalized biometric surveillance in the control of pandemics, such as the current global COVID pandemic [4], Saheb et al., 2021c). According to the GS Index, Chinese and American technology companies are the world's leading providers of artificial intelligence (AI) surveillance technologies (Fig. 1). However, incorporating AI-based surveillance technologies has been a game changer in advancing effective measures in a variety of industries, including healthcare, transportation, and manufacturing. Others, on the other hand, condemn artificial intelligence-based surveillance technologies for their unexpected or intended harmful implications, particularly in the lives of citizens, and their potential to support anti-democratic policies and violations of privacy and human rights principles [25, 48]. The studies express outrage at governments for violating human rights through the use of surveillance technologies for pandemic management [48, 52].

As global concerns about the battle between digital authoritarianism and liberal democracy sprout [67], academic researchers from diverse backgrounds address various dimensions of artificial intelligence for surveillance; as there are conflicting and perplexing perspectives on the consequences of artificial intelligence for surveillance. While some studies focus exclusively on the good effects of AI on surveillance, others emphasize the negative aspects of AI on surveillance.

✉ Tahereh Saheb
t.saheb@modares.ac.ir

[1] Management Studies Center, Tarbiat Modares University, Tehran, Iran

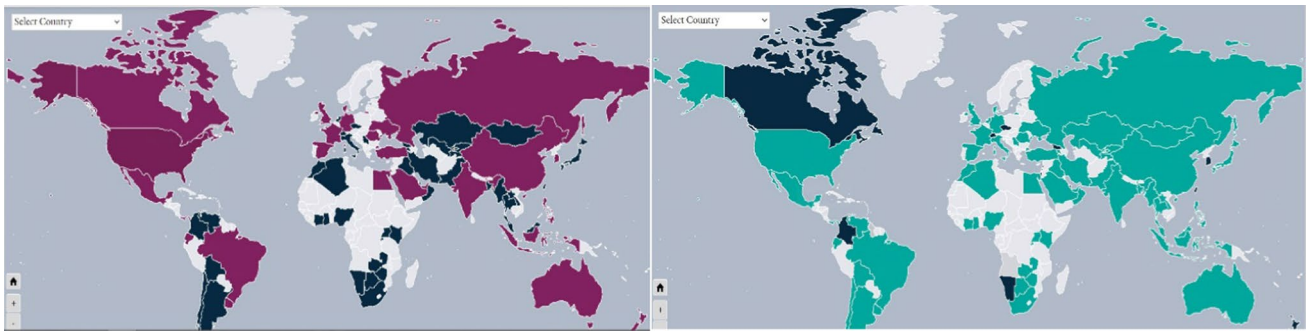

Fig. 1 Countries use American (left) and Chinese (right) Tech companies to supply their AI surveillance technology [17]

As of March 10th, 2022, about 3556 scholarly papers with the keywords artificial intelligence and surveillance were indexed in the Scopus database. As illustrated in Fig. 2, the number of scholarly research on this subject has increased dramatically since 2017 and peaked in 2021. As illustrated in the figure, the subject is an interdisciplinary one that has attracted the interest of scientists from a variety of fields, including computer science, engineering, mathematics, medicine, physics and astronomy, and social sciences. This paper, on the other hand, intends to map the scholarly endeavors of social scientists and humanities working on AI and surveillance to further non-technical discourse about surveillance and AI and to distinguish conflicting perspectives on AI for surveillance. The recent upsurge of interest in ethical AI to emphasize the transparency and accountability of artificial intelligence has enhanced social scientists' scholarly endeavors [33] to underscore both advantages and disadvantages of AI surveillance by governments, industries, and corporations. This study intends to map new scholarly efforts by social sciences and humanities scholars to comprehend the most frequently addressed issues, thereby discovering neglected and overlooked research streams. Theoretically, this study will contribute to the growing body of knowledge regarding social science studies of technology and the ethics of artificial intelligence. Practically, this study will serve as a guide for policymakers and technology corporations interested in gaining a better understanding of the societal consequences of surveillance using artificial intelligence technologies and techniques.

This study will attempt to address the following research questions:

- What is the social science and humanities perspective on the knowledge structure of AI surveillance? What scientific discourse exists around the controversial utilization of artificial intelligence for unethical surveillance purposes?
- How has social science research on artificial intelligence and surveillance evolved over time?
- What are the under-researched and marginalized areas within social science studies of AI and surveillance, as well as the potential research strands?

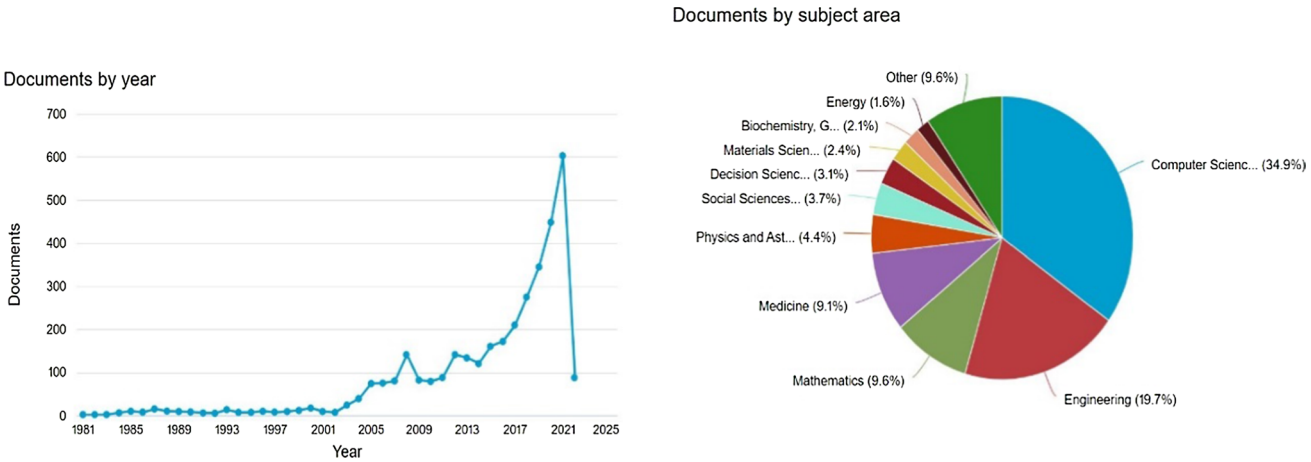

Fig. 2 The evolution of scholarly growth over the interdisciplinary topic of artificial intelligence for surveillance based on papers indexed in Scopus database

2 Methodology

On March 9th, 2022, we extracted data from the SCOPUS database. We searched the abstract, title, and keyword for the terms artificial intelligence AND surveillance. We limited our study to disciplines in the social sciences and humanities and omitted review articles. Only English-language articles, conference papers, books, and book chapters were included. We imposed no further restrictions. This search resulted in the retrieval of 293 documents. After screening the titles and abstracts of the papers, we determined that 14 were irrelevant. Thus, we did topic modeling analysis on 279 papers at the end.

We employed keyword co-occurrence analysis as a bibliometric technique to identify the most influential scholarly topics. We next conducted a content analysis of relevant publications to each topic to complement the bibliometric analysis findings. We analyzed the 279 publications for content analysis. Co-occurrence analysis is a widely used quantitative technique for determining the structure of research and its possible academic relevancy [29, 44]. We analyzed and visualized networks using the VOSviewer software. This software is a widely utilized tool for analyzing and visualizing scientific literature, as well as tracing the evolution and knowledge structure of scientific topics [62, 64]. We displayed the analysis in two ways: one to depict the themes whose normalization was based on modularity, and another to depict the evolution of keywords using overlay visualization. The items were represented according to their total link strength, or TLS score. The modularity algorithm provides significantly more strongly related keywords and sheds light on the strength of networks [46]. Additionally, the TLS score considers the number of connections an object has to other objects as well as the strength of those connections [48].

3 Results

As a consequence of the co-occurrence analysis of keywords, seven main scholarly subjects were identified, as illustrated in Fig. 3. According to the analysis, the first highly addressed topic is public health surveillance and the privacy of contact tracing apps during pandemics, notably the COVID-19. The second topic discusses video surveillance and facial recognition technologies, mostly in the transportation industry. Topic 3 refers to studies on military surveillance and artificial intelligence in its physical forms, such as drones, robots, and autonomous vehicles. Topic 4 pertains to studies on surveillance capitalism and disease surveillance. Subject five is about smart cities, while topic six is about computational surveillance. Additionally, the final topic discusses security surveillance. Noteworthy is the fact that essentially, the majority of the topics have overlapping discussions, but their primary focus is distinct. For

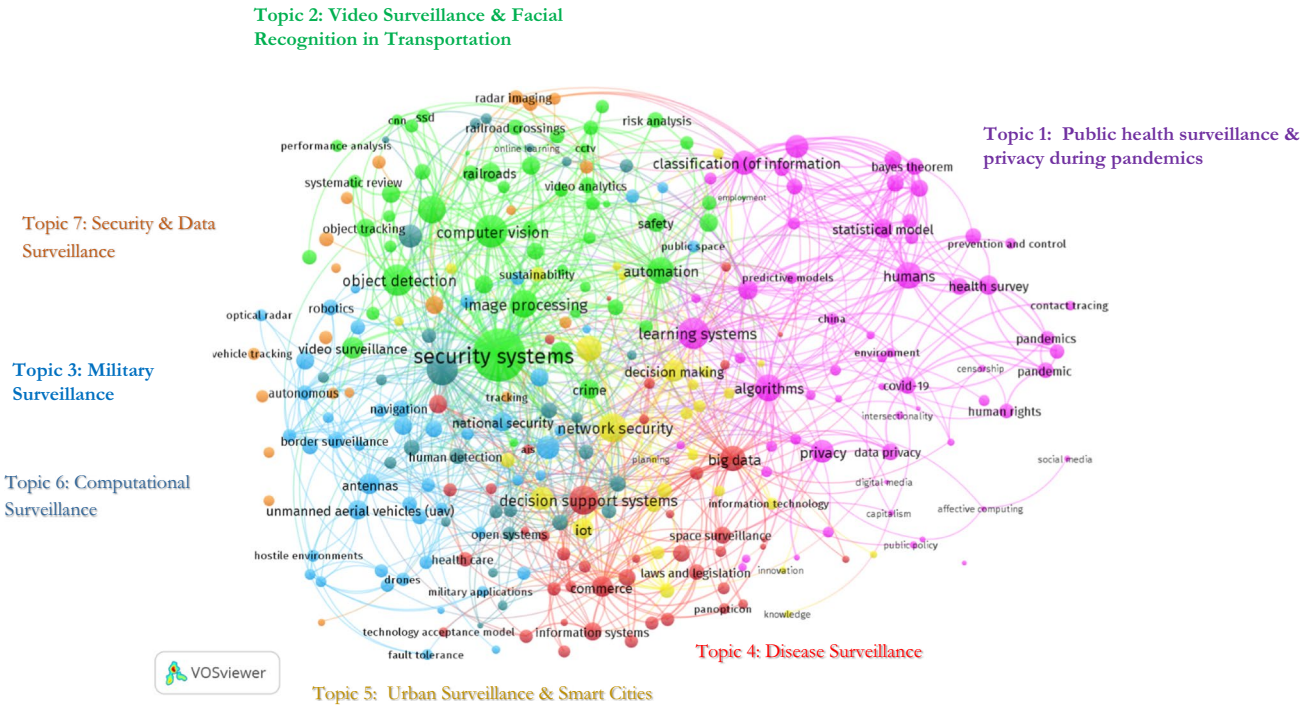

Fig. 3 Co-occurrence analysis of papers yielded in seven influential scholarly topic on AI and surveillance

instance, while public health surveillance and disease surveillance share a number of contentious ethical issues, their primary focuses are diverse. As an illustration, the central emphasis of disease surveillance is on state and citizen surveillance, whereas the primary focus of public health surveillance is on privacy concerns.

4 Topic modeling and content analysis

4.1 Topic 1: public health surveillance & privacy during pandemics

Human rights violations are facilitated by cutting-edge technologies, which empowers governments to collect biometric and other personal data and legalize AI-based tracking systems in the premise of public health protection [19]. During pandemics, notably COVID-19, tracking systems have been employed to conduct epidemiological surveillance of individuals at risk [65]. However, there is rising concern that AI surveillance for reasons such as detecting new COVID-19 cases or collecting data from healthy and severely ill individuals is being employed for purposes other than public health management, thereby breaching individuals' privacy [53], decreasing citizens' trust and voluntary adoption of these technologies [65]. In some studies, AI-based surveillance is described as a form of biopolitics and as a tool for enhancing government surveillance and control [60]. Scholars have proposed technical solutions to mitigate the ethical ramifications of AI-based surveillance systems, such as de-identification and anonymization of data and differential privacy [21, 48], 2021c). Conversely, other scholars believe that a balance should be struck between data privacy and public health [34], and that broader privacy laws, such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, should be adopted [26, 53]. More precisely, research indicates that AI surveillance of vulnerable and marginalized populations should be implemented cautiously. Additionally, they advocate for collaborative and multidisciplinary efforts [22]. Due to the fact that governments are developing AI surveillance systems in collaboration with technology companies, prior research has emphasized the importance of developing governance frameworks, exercising control over various actors, and increasing technology companies' social and political accountability [7].

AI surveillance has been fraught with privacy concerns beyond pandemics. With the emergence of surveillance societies [50], a slew of worries about privacy and the blurring of lines between human–machine interaction have surfaced [22], as have new forms of government control and warfare [32]. Researchers have voiced worry that the automated collecting of personal data has exacerbated the power imbalance between citizens and governments and technology companies [41], as well as the secrecy and lack of transparency of corporations [13]. These concerns have led to the development of technical solutions such as privacy by design, privacy by default [26] and differential privacy [8], and new governance frameworks [7].

Biometric facial recognition has been identified as a significant concern, because it creates privacy concerns when employed for citizen surveillance, crime control, activity monitoring, and facial expression evaluation [8], posing a threat by automating unauthorized access to personal data such as facial images [57]. A second significant area of worry with AI technology is the use of health wearables and applications. In these instances, the gathering and processing of personal data must be authorized, transparent, and duration and scope limited [26].

4.2 Topic 2: video surveillance systems & facial recognition in transportation

The second issue with AI surveillance is the implementation of video surveillance systems (VSM) and facial recognition in public transportation. The majority of research have focused on applications of AI to transportation surveillance; very few have addressed the ethical and legal consequences of such applications. Studies identify that employing AI surveillance in transportation is primarily intended to reduce trespassing frequency and deaths [71], monitor terrorist activity and suspicious behavior [42], improve public safety and crime-fighting capabilities [14], and develop intelligent traffic surveillance systems [30]. Despite its efficacy, AI surveillance in transportation has sparked ethical concerns, particularly when the police and the government collaborate to execute AI-based surveillance systems in public transportation zones [14]. Studies illustrate the intricate interrelationships between human and computer authority [56], human rights breaches [1], and threats to civil liberties and freedoms [14]. Other studies assert that there is no universally applicable human rights framework or regulatory standards for facial recognition and video surveillance technologies [1]. In light of smart policing initiatives in public spaces, such as the transit system, human rights breaches are highly exacerbated when minorities, African-Americans, and children are engaged [68]. In some cases, these efforts could lead to the remedy of unconstitutional practices and racial discrimination [40]. There have been some studies, suggesting that the ethical concerns surrounding facial recognition technology should extend beyond privacy and transparency to include issues of equality, diversity, and inclusion [1].

4.3 Topic 3: military surveillance

The third most significant category of studies focuses on physical AI, robotics, and AI-based devices in the military, as well as military surveillance, as these technologies have progressed beyond science fiction movies [15]. These technologies may offer tremendous benefits, including increased precision and accuracy, as well as automation of military measures and counterterrorism programs; however, some researchers have highlighted concerns that autonomous AI-based drones and technologies in the military will ramp up discriminatory practices and unaccountable military activity on a political and legal level [58]. Furthermore, research have demonstrated that applications of Unmanned Aerial Vehicles (UAVs) and drones constitute complex technologies augmented by a variety of technologies [69], necessitating the development of specialized legal frameworks to address civil liberties and privacy concerns [18]. Noncombatant civilians are being killed by military drones, igniting much controversy [6]. Previous research has raised concerns regarding armed and autonomous robots' ability to accurately discern between combatants and non-combatants, or to distinguish between dangerous and nonthreatening conduct [28]. There are a variety of ethical concerns surrounding autonomous AI-based military technology, including ambiguity about who is responsible and if these technologies are capable of unethical or illegal behavior [55].

4.4 Topic 4: disease surveillance

The fourth key theme in AI surveillance has been the surveillance of diseases in the context of capitalism and the emergence of surveillance capitalism. Concerns have primarily developed as a result of COVID-19 and government collaborations with large technological corporations [48]. Shoshana Zuboff first proposed the concept of surveillance capitalism in 2007, contending that Facebook and Google, two technological companies, earn financial success and help governments with political advertising by selling algorithmic-driven, micro-targeted profiles of individuals [26, 66]. COVID-19 provided opportunities for technology companies to pass legislation that boosted their commercial benefit while limiting citizens' freedom of movement and access to their personal information [11]. Numerous ethical questions have been voiced about artificial intelligence's application in healthcare. Scholars dispute whether artificial intelligence and its applications, such as tracing systems, are desirable for citizen spying or disease surveillance in both democratic and dictatorial nations [16]. Depersonalization and dehumanization, as well as discrimination and disciplinary care, are among these ethical concerns [43]. Further ethical risks of AI-based disease surveillance include politicization of care, anti-democracy and social dissimilatory practices, and violations of human rights [48].

4.5 Topic 5: urban surveillance and smart cities

The fifth most discussed topic of AI surveillance is smart cities and the collection of personal data for urban planning. Studies point out anxieties regarding the leakage of personal information [54], full automation and absence of humans[10], and control of city facilities and influence on citizens lives [70]. As studies have shown, among the most sensitive and ethically problematic forms of personal data in a smart city are customer profiles, time-spatial travel, and automated fair collection [9]. Smart city surveillance compromises human privacy on a variety of levels, including identity privacy, query privacy, location privacy, footprint privacy, and owner privacy [31]. Citizens' privacy concerns are primarily triggered by their perceptions of city data and the rationale for its use [63], as well as unlawful access to confidential data and cyberattacks that disrupt the delivery of city services physically. [61]. According to study undertaken by [72], other ethical issues confronting smart cities include control and data ownership, friction between the public and private sectors, social inclusion and citizen involvement, and subsequent disparities and prejudice.

4.6 Topic 6: computational surveillance

The sixth topic explores computational surveillance, soft computing, and security challenges faced at the time of the development of computational intelligence. According to [12], computational intelligence can be defined as the design, application, and development of biologically and linguistically motivated computational paradigms, including natural language processing, natural language understanding, and natural language generation models. As computational intelligence advances, attention is being directed to computational ethics, so that it can be distinguished from machine ethics and robot ethics [51]. Scholars frequently use soft computing techniques, such as natural language processing (NLP), to promote civility and monitor hate speech, cyberbullying, toxic comments, and abusive language [49]. Furthermore, computational intelligence has been employed to detect propaganda, fake, and manipulated news [36]. During the COVID-19 outbreak, computational intelligence was extensively used for disease surveillance [39]. In the wake of cyberattacks on computational intelligence applications[23], security-enabled design techniques and algorithms, as well as the construction of secured software and the strengthening of threat modeling during software development, were put into practice [2, 38].

Furthermore, computational intelligence has also been incorporated into the political sphere for the purpose of

fabricating propaganda, fake news, and hate speech. In light of this trend, concerns have been raised regarding the vulnerability of individuals, political parties, institutions, and communities, as well as the possibility of manipulating them for destructive reasons [27]. At the dawn of the deepfake era [20], deep learning algorithms and generative adversarial networks (GANs) aggravated the situation by altering the appearance of human subjects on existing photographs and videos to make them appear like someone else [59].

4.7 Topic 7: security and data surveillance

The seventh topic pertains to security and data surveillance. In recent studies, concerns regarding the automated decision-making capabilities of AI systems have generated concerns regarding security and data surveillance among citizens, which has hampered their adoption of these technologies [37]. A rising tide of datafication and data-driven surveillance has contributed to a life fraught with uncertainty, with civil society concerned about countering threats posed by surveillance, data exploitation, and vulnerable systems susceptible to cyberattacks [24]. The increasing availability and usage of big data has invaded everyday life, threatening citizens' privacy and security in intelligent surroundings packed with technology that extract personal information [3]. Due to the infiltration of big data into every facet of human life and the abundance of citizens' digital footprints, covert monitoring of citizens' behaviors, intentions, and preferences is now conceivable. According to Forbes magazine, the US government secretly ordered Google to provide information about customers who type in specific search phrases [5]; highlighting governments' unlawful access to consumers' digital data.

5 Historical evolution of surveillance concepts

This section of the article examines the evolution of surveillance concepts across time. As illustrated in Fig. 4, prior to 2012, topics, such as vehicle tracking, computer vision, predictive models, border surveillance, and military applications, were among the most linked concepts in scientific study. This means that the experts emphasized the importance of AI for military and border surveillance. From 2012 to 2014, the development of statistical models and machine learning techniques gained prominence. Between 2014 and 2016, attention was mostly focused on the societal ramifications of artificial intelligence surveillance, particularly in e-commerce, crime, healthcare, and the environment. Between 2016 and 2018, security concepts, such as security systems, network security, and national security, gained popularity, as did the employment of video surveillance, drones, and unmanned aerial vehicles (UAVs) for object detection. Between 2018 and 2020, attention was concentrated on the rise of big data, the Internet of Things, drones, data privacy, legislation and regulation, and citizen acceptance of technology. After 2020, pandemics, COVID-19, contact tracing, human rights, capitalism, and surveillance in transportation became popular topics (Fig. 5).

6 Discussion and literature gaps

We conducted a co-occurrence analysis and a content analysis of 279 scientific papers on AI and surveillance authored by social science and humanities experts. Our investigation found seven significant scholarly topics that receive significant attention from the scientific community. These topics demonstrate the ambiguous boundaries between dichotomous forms of surveillance: public health surveillance versus state surveillance; transportation surveillance versus national security surveillance; peace surveillance versus military surveillance; disease surveillance versus surveillance capitalism; urban surveillance versus citizen ubiquitous surveillance; computational surveillance versus fakeness surveillance; and data surveillance versus invasive surveillance.

The most distressing topic in AI surveillance is public health surveillance and the deployment of COVID tracing applications, which blur the boundaries between citizen and public health surveillance. As the COVID pandemic expanded across the globe in 2019, various countries developed mobile-based contact tracing applications to track and halt the virus's transmission. Concerns about privacy and surveillance emerges as a result of these applications' capacity to autonomously access their users' location and contacts [45, 47], 2021c), fueling public suspicion that these applications were instruments of citizen surveillance. Ethical considerations are heightened in countries where citizens are required to adopt the applications. Due to compulsory installation, a lack of proper rules, and collaboration with technology corporations, individuals lacked trust and harbored conspiracy theories that these applications were employed for citizen surveillance and capitalism's empowerment, rather than public health surveillance. The significant drawback of these studies on artificial intelligence for public health surveillance is the absence of studies examining the indirect effects of contextual factors on the adoption of AI-based public health surveillance systems. Multiple sociological, economic, and political considerations, as well as their indirect and complicated interconnections, should be explored to develop more viable solutions, policies, and strategies for mitigating surveillance vulnerabilities. Furthermore, additional studies on the design and user experience of mobile applications may be beneficial to provide users with a greater

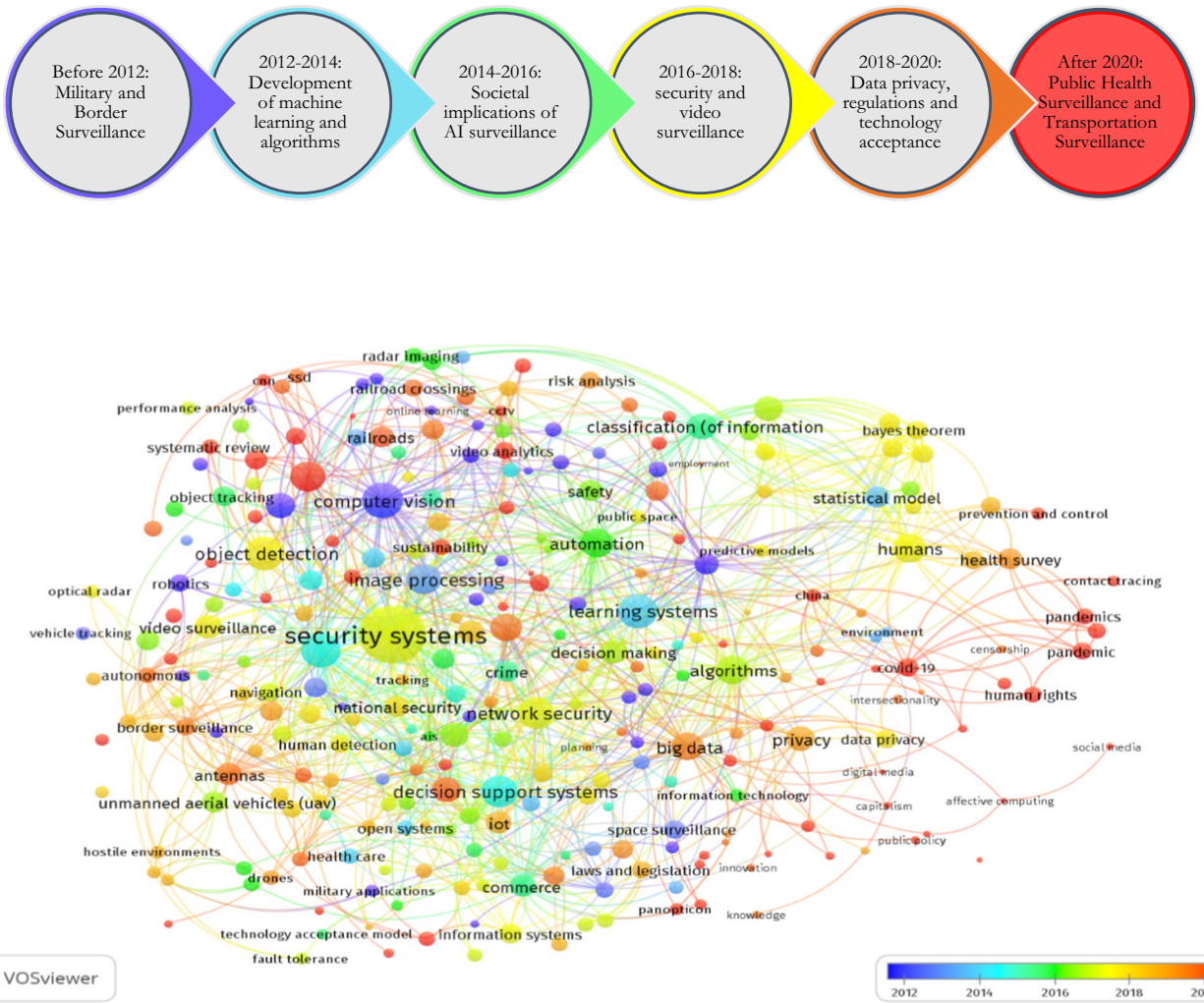

Fig. 4 Historical evolution of concepts on AI surveillance

level of power and control over their privacy preferences. To replace text-based, lengthy, and complex user agreements, interactive and simplified privacy agreements are required. Additionally, appropriate governance frameworks, ethical norms, and rules for AI-based surveillance should be devised to mitigate bias and socioeconomic inequity. Despite the fact that the majority of governments adhere to their collaborations with private technology corporations, additional strategies should be developed to foster civil society participation, so they can better distinguish between state surveillance of citizens and public health surveillance initiatives.

A second significant worry voiced by social scientists and humanities academics concerns the prominence of facial recognition and video surveillance technologies in the transportation sector, as well as the blurred line between this technology and national security. This issue is becoming increasingly significant as a result of the transportation industry's collaboration with police and national security agencies to detect suspicious and terrorist activity. One of the literature's flaws is the dearth of studies on citizens' perspectives on the ethics of facial recognition and video surveillance systems in transportation, law enforcement, and national security. To address racial bias and inaccuracies in face recognition algorithms, more precise ethical regulations are expected, as these algorithms may result in prejudiced and discriminatory judgements, as well as severe effects on minorities and people of color. Additionally, there is the matter of informed consent to consider. Several governments have deployed video surveillance cameras in public locations and on streets. As these cameras currently capture individuals' facial data autonomously, additional means for obtaining citizens' explicit and informed consent for the collection and use of their biometric data must be devised.

Military surveillance is the third topic that social scientists and humanities scholars have addressed extensively. The autonomy of military weapons, their accuracy and precision in avoiding targeting non-combatants, and their legal and political accountability are highly addressed by

Fig. 5 Varied perspectives regarding AI surveillance in healthcare, public transportation, military, pandemic management, urban planning, communications, and big data

scholars. However, very few studies have examined international regulations and diplomatic tensions caused by military drones. In addition, in contrast to existing studies that focus on the transparency of algorithms programming AI-based machines, more research needs to be conducted on the "reasonability" of algorithms to better understand the reasons behind how a drone decides who is a non-combatant civilian. The features and reasons for the engineering of military weapons should be studied further. It should be clarified who decides and approves the algorithmic features and reasons that result in autonomous drone actions. Does an engineer design features that are characteristic of a non-combatant civilian and apply them to a drone? Do military stakeholders develop these features and deliver them to engineering teams for use in developing algorithms and drones? In what manner do stakeholders determine the characteristics of a civilian? In the event of an error, who is responsible? Was it the result of human error? Did it occur due to a malfunctioning machine? It would be beneficial to conduct further research to understand the governance of "feature and reason engineering" of military drones, as well as the processes and procedures used during this process. While more AI studies focus on the development of features, more studies should emphasize the development of reasons to better answer questions such as why certain features were selected as features of a non-combatant civilian. In addition, more studies should be conducted regarding the partnership of military agencies with technology companies that produce advanced materials and fabrication technologies, as well as next-generation antennas, which increase the autonomy of drones, reduce the need for human operators, and allow for collaborative autonomous information sharing among drones. It is important to distinguish between the use of drones for peaceful civilian purposes and the use of drones for military and wartime purposes.

One of the most prominent topics covered is the surveillance of disease, the partnership of governments with technology companies, and the emergence of "surveillance capitalism," whereby companies monetize the data collected by tracking citizens' movements and behaviors. As a result of the development of mobile health apps embedded with artificial intelligence and other digital technologies, this topic expressed concerns about reducing the autonomy and control of citizens over their movements and personal data. The studies focused primarily on the normative and societal ramifications of these applications on users' lives. Research should be conducted to understand the strategies and alliances that technology companies utilize to convert

private user experiences into data-driven and predictive markets based on uncertain human futures. How should public health startups, or companies such as Theranos and fake patents be considered in this context? Following the government's increase in funding for pandemic crises, a mushroom of startups and patents appeared, claiming their innovations and patents would provide efficient remedies. It is imperative that more studies be performed on the functionalities of AI-based medical patents and innovations to determine the reliability and validity of innovations and distinguish them from fakes and fraudulent ones to reduce the monetary benefits of fraud and threats to human safety.

The fifth highly regarded topic is about smart cities and the blurred boundaries between urban surveillance and citizen ubiquitous surveillance in autonomous urban environments. In urban contexts integrated with artificial intelligence, the Internet of Things, and ubiquitous computing systems, there is a high level of contention related to the autonomous collection of citizen data. In totalitarian regimes as well as democratic regimes, the vertical transmission of disparate and mass sources of urban data from citizens into one entity raises concerns about panopticism and persistent surveillance of citizens. To better understand the ethical implications of embedded ubiquitous computing into an environment and context-aware services without citizens' awareness and control, more research is required on informed consent, autonomy, and privacy. Most citizens are unaware of what pieces of their personal information are being captured, when they are captured, as well as with whom and for what purposes the captured information is stored and shared. Moreover, human–computer interaction (HCI) scholars should conduct more design-centered research, so that the interface of context-aware services provides citizens with a greater sense of autonomy and control when interacting with autonomous environments.

The sixth highly debated topic pertains to computation surveillance and soft computing as a subset of artificial intelligence, fabrications, and fakeries that can be generated through soft computing strategies. Computational intelligence has been extensively used to monitor civility in online communications. However, it has also been utilized to promote fakeness, such as deepfakes. Recent surpluses of deepfakes necessitate more studies regarding the ethical challenges of deepfakes and the need for regulatory frameworks that limit algorithm-based fabrications and manipulations. Data surveillance and intrusive surveillance are the last highly discussed topics. This topic addresses the issue of invasion of privacy and security in the age of big data. In spite of this, very few studies have examined the topic of surveillance and invasion in the age of big data. Furthermore, it is important to conduct more research to analyze aspects of intrusive and covert surveillance of citizens empowered by data sources surrounding the everyday lives of citizens.

7 Conclusion

This study identified a series of the most often debated arguments around the surveillance effects of artificial intelligence. However, AI is not exclusively vulnerable to negative monitoring mechanisms. Consequently, future research might compare the detrimental and beneficial consequences of AI surveillance. Moreover, in our study, we only considered the most frequently discussed controversial aspects of AI surveillance. Future research may conduct systematic literate reviews or text mining to identify alternative scholarly discourses on AI surveillance. In this study, we concentrated on scholarly discussions of AI's disputed surveillance implications. Future research can investigate the perspectives of other stakeholders in the AI ecosystem, such as policymakers and citizens, to comprehend their opinions on AI surveillance, for instance by conducting policy analysis, Twitter analysis, or survey analysis.

Funding There is no funding for this research.

References

1. Almeida, D., Shmarko, K., 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. AI Ethics **2021**, 1–11 (2021). https://doi.org/10.1007/S43681-021-00077-W
2. Althar, R.R., Samanta, D.: The realist approach for evaluation of computational intelligence in software engineering. Innov. Syst. Softw. Eng. (2021). https://doi.org/10.1007/S11334-020-00383-2
3. Ball, K., Di Domenico, M.L., Nunan, D.: Big Data Surveillance and the Body-subject. Body Soc **22**, 58–81 (2016). https://doi.org/10.1177/1357034X15624973
4. Bragazzi, N.L., Dai, H., Damiani, G., Behzadifar, M., Martini, M., Wu, J.: How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic. Int. J. Environ. Res. Public Heal. **17**, 3176 (2020). https://doi.org/10.3390/IJERPH17093176
5. Brewster T, 2021. Government Secretly Orders Google To Identify Anyone Who Searched A Sexual Assault Victim's Name, Address Or Telephone Number [WWW Document]. Forbes. URL https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/?sh=4d6273c07c97 (accessed 3.27.22).
6. Byrne, E.F.: Making drones to kill civilians: is it ethical? J. Bus. Ethics. (2015). https://doi.org/10.1007/S10551-015-2950-4
7. Caparini, M., Gogolewska, A.: Governance challenges of transformative technologies. Connections **20**, 91–100 (2021). https://doi.org/10.11610/CONNECTIONS.20.1.06
8. Chamikara, M.A.P., Bertok, P., Khalil, I., Liu, D., Camtepe, S.: Privacy preserving face recognition utilizing differential privacy. Comput. Secur. **97**, 101951 (2020). https://doi.org/10.1016/J.COSE.2020.101951
9. Chang, V.: An ethical framework for big data and smart cities. Technol. Forecast. Soc. Change **165**, 120559 (2021). https://doi.org/10.1016/J.TECHFORE.2020.120559

10. Cooke, P.: Image and reality: 'digital twins' in smart factory automotive process innovation—critical issues. Reg. Stud. (2021). https://doi.org/10.1080/00343404.2021.1959544
11. Cosgrove, L., Karter, J.M., Morrill, Z., McGinley, M.: Psychology and Surveillance Capitalism: The Risk of Pushing Mental Health Apps During the COVID-19 Pandemic. J Human Psychol **60**, 611–625 (2020). https://doi.org/10.1177/0022167820937498
12. Deshpande, A., Razmjooy, N., Estrela, V.V.: Introduction to computational intelligence and super-resolution intell. Methods super-resolution image process. Appl Comput (2021). https://doi.org/10.1007/978-3-030-67921-7_1
13. Dewandre, N.: Big data: from modern fears to enlightened and vigilant embrace of new beginnings. Big Data Soc (2020). https://doi.org/10.1177/2053951720936708
14. Dworzecki, J., Nowicka, I.: Artificial intelligence (AI) and ICT-enhanced solutions in the activities of police formations in Poland. Adv. Sci. Technol. Secur. Appl. (2021). https://doi.org/10.1007/978-3-030-88972-2_11
15. Lage Dyndal, G., Arne Berntsen, T., Redse-Johansen, S.: Autonomous military drones—no longer science fiction. Romanian Military Thinking 2 (2017)
16. Eck, K., Hatz, S.: State surveillance and the COVID-19 crisis. J Human Rights (2020). https://doi.org/10.1080/14754835.2020.1816163
17. Feldstein, S., 2022. The Global Expansion of AI Surveillance [WWW Document]. Carnegie Endow. Int. Peace. URL https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (accessed 3.10.22).
18. Finn, R.L., Wright, D.: Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput. Law Secur. Rev. **28**, 184–194 (2012). https://doi.org/10.1016/J.CLSR.2012.01.005
19. Gnatik, E.N., Николаевна, ГЕ.: 'New normality' of the covid-19 era: Opportunities, limitations, risks. Rudn J. Sociol. **21**, 769–782 (2021). https://doi.org/10.22363/2313-2272-2021-21-4-769-782
20. Guera, D., Delp, E.J., 2019. Deepfake Video Detection Using Recurrent Neural Networks. Proc. AVSS 2018 - 2018 15th IEEE Int. Conf. Adv. Video Signal-Based Surveill. https://doi.org/10.1109/AVSS.2018.8639163
21. Idrees, S.M., Nowostawski, M., Jameel, R.: Blockchain-based digital contact tracing apps for COVID-19 pandemic management: issues, challenges, solutions, and future directions. JMIR Med Inf (2021). https://doi.org/10.2196/25245
22. Johnson, K.N., Reyes, C.L.: Exploring the implications of artificial intelligence. J. Int. Comp. L. **8**, 315 (2021)
23. Kalinin M.O., Krundyshev V.M.: Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions Proc 2021 5th World Conf. Secur. Sustain Smart Trends Syst (2021). https://doi.org/10.1109/WORLDS451998.2021.9514004
24. Kazansky, B.: 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. Big Data Soc (2021). https://doi.org/10.1177/2053951720985557
25. Kiliç, M., 2021. Ethico-Juridical Dimension of Artificial Intelligence Application in the Combat to Covid-19 Pandemics 299–317. https://doi.org/10.1007/978-981-33-6811-8_16
26. Lawlor, B.: An overview of the 2021 NISO plus conference: global connections and global conversations. Inf. Serv. Use **41**, 1–37 (2021). https://doi.org/10.3233/ISU-210120
27. Lazer, D.M.J., Baum, M.A., Benkler, Y., Berinsky, A.J., Greenhill, K.M., Menczer, F., Metzger, M.J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S.A., Sunstein, C.R., Thorson, E.A., Watts, D.J., Zittrain, J.L.: The science of fake news: addressing fake news requires a multidisciplinary effort. Science (2018). https://doi.org/10.1126/SCIENCE.AAO2998/SUPPL_FILE/AAO2998_LAZER_SM.PDF
28. Lin, P., Abney, K., Bekey, G.: Robot ethics: mapping the issues for a mechanized world. Artif. Intell. **175**, 942–949 (2011). https://doi.org/10.1016/J.ARTINT.2010.11.026
29. Lou, W., Qiu, J.: Semantic information retrieval research based on co-occurrence analysis. Online Inf. Rev. **38**, 4–23 (2014). https://doi.org/10.1108/OIR-11-2012-0203/FULL/XML
30. Mandal, V., Mussah, A.R., Jin, P., Adu-Gyamfi, Y.: Artificial intelligence-enabled traffic monitoring system. Sustain **12**, 9177 (2020). https://doi.org/10.3390/SU12219177
31. Martinez-Balleste, A., Perez-Martinez, P., Solanas, A.: The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Commun. Mag. **51**, 136–141 (2013). https://doi.org/10.1109/MCOM.2013.6525606
32. Maus, G.: Decoding, hacking, and optimizing societies: exploring potential applications of human data analytics in sociological engineering, both internally and as offensive weapons. Proc. 2015 Sci Inf. Conf. SAI **2015**, 538–547 (2015). https://doi.org/10.1109/SAI.2015.7237195
33. Miller, T.: Explanation in artificial intelligence: insights from the social sciences. Artif. Intell. **267**, 1–38 (2019). https://doi.org/10.1016/J.ARTINT.2018.07.007
34. Naudé, W.: Artificial intelligence vs COVID-19: limitations, constraints and pitfalls. AI Soc (2020). https://doi.org/10.1007/S00146-020-00978-0
35. Nguyen, M.T., Truong, L.H., Tran, T.T., Chien, C.F.: Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5. Comput. Ind. Eng. (2020). https://doi.org/10.1016/J.CIE.2020.106671
36. Oshikawa, R., Qian, J., Wang, W.Y.: A survey on natural language processing for fake news detection. Lr. 2020—12th Int. Conf. Lang. Resour. Eval. Conf. Proc. (2018). https://doi.org/10.48550/arxiv.1811.00770
37. Park, Y.J., Jones-Jang, S.M.: Surveillance, security, and AI as technological acceptance. AI Soc. **2021**, 1–12 (2022). https://doi.org/10.1007/S00146-021-01331-9
38. Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A.: Vulnerability analysis at industrial internet of things platform on dark web network using computational intelligence. Stud. Comput. Intell. **950**, 39–51 (2021). https://doi.org/10.1007/978-981-16-0407-2_4
39. Raza, K., Maryam, Q., S.,: An introduction to computational intelligence in COVID-19: surveillance, prevention, prediction, and diagnosis. Stud. Comput. Intell. **923**, 3–18 (2021). https://doi.org/10.1007/978-981-15-8534-0_1
40. Ringrose, K., 2019. Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. Virginia Law Rev. Online 105.
41. Rinik, C.: Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem. Int. Rev. Law Comput. Technol. **34**(3), 342–363 (2020). https://doi.org/10.1080/13600869.2019.1594621
42. Roussi, A.: Resisting the rise of facial recognition. Nature **587**, 350–353 (2020). https://doi.org/10.1038/D41586-020-03188-2
43. Rubeis, G.: The disruptive power of artificial intelligence ethical aspects of gerontechnology in elderly care. Arch. Gerontol. Geriatr. (2020). https://doi.org/10.1016/j.archger.2020.104186
44. Saheb, T., Amini, B., Kiaei Alamdari, F.: Quantitative analysis of the development of digital marketing field: Bibliometric analysis and network mapping. Int. J. Inf. Manag. Data Insights (2021). https://doi.org/10.1016/j.jjimei.2021.100018
45. Saheb, T., Cabanillas, F.J.L., Higueras, E.: The risks and benefits of Internet of Things (IoT) and their influence on smartwatch use. Spanish J. Mark. ESIC (2022). https://doi.org/10.1108/SJME-07-2021-0129/FULL/PDF

46. Saheb, T., Saheb, M.: Analyzing and visualizing knowledge structures of health informatics from 1974 to 2018: A bibliometric and social network analysis. Healthc. Inform. Res. (2019). https://doi.org/10.4258/hir.2019.25.2.61
47. Saheb, T., Sabour, E., Qanbary, F., Saheb, T.: Delineating privacy aspects of COVID tracing applications embedded with proximity measurement technologies & digital technologies. Technol. Soc. **69**, 101968 (2022). https://doi.org/10.1016/J.TECHSOC.2022.101968
48. Saheb, T., Saheb, T., Carpenter, D.O.: Mapping research strands of ethics of artificial intelligence in healthcare: a bibliometric and content analysis. Comput. Biol. Med. **135**, 104660 (2021). https://doi.org/10.1016/J.COMPBIOMED.2021.104660
49. Schmidt, A., Wiegand, M., 2017. A Survey on Hate Speech Detection using Natural Language Processing. Soc. 2017 - 5th Int. Work. Nat. Lang. Process. Soc. Media, Proc. Work. AFNLP SIG Soc. 1–10. https://doi.org/10.18653/V1/W17-1101
50. Schoenherr, J.R., 2020. Understanding Surveillance Societies: Social Cognition and the Adoption of Surveillance Technologies. Int. Symp. Technol. Soc. Proc. 2020-November, 346–357. https://doi.org/10.1109/ISTAS50296.2020.9462205
51. Segun, S.T.: From machine ethics to computational ethics. AI Soc. **36**, 263–276 (2021). https://doi.org/10.1007/s00146-020-01010-1
52. Sekalala, S., Dagron, S., Forman, L., Mason Meier, B.: Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 Crisis. Heal. Hum. Rights J. **22**, 7–20 (2020)
53. Shachar, C., Gerke, S., Adashi, E.Y.: AI surveillance during pandemics: ethical implementation imperatives. Hastings Cent. Rep. **50**, 18–21 (2020). https://doi.org/10.1002/hast.1125
54. Shimizu, Y., Osaki, S., Hashimoto, T., Karasawa, K.: How do people view various kinds of smart city services? Focus on the acquisition of personal information. Sustain. **13**, 11062 (2021). https://doi.org/10.3390/SU131911062
55. Shook, J.R., Solymosi, T., Giordano, J.: Ethical constraints and contexts of artificial intelligent systems in national security, intelligence, and defense/military operations. Artif. Intell. Glob. Secur. (2020). https://doi.org/10.1108/978-1-78973-811-720201008
56. Smith, B.W., 2020. Ethics of Artificial Intelligence in Transport, in: Dubber, M., Pasquale, F.,, Das, S. (Eds.), The Oxford Handbook of Ethics of Artificial Intelligence.
57. Smith, M., Miller, S.: The ethical application of biometric facial recognition technology. AI Soc (2021). https://doi.org/10.1007/S00146-021-01199-9
58. Suchman, L.: Algorithmic warfare and the reinvention of accuracy. Crit. Stud. Secur. **8**(2), 175–187 (2020). https://doi.org/10.1080/21624887.2020.1760587
59. Suratkar, S., Bhiungade, S., Pitale, J., Soni, K., Badgujar, T., Kazi, F.: Deep-fake video detection approaches using convolutional – recurrent neural networks. J. Control Decis. (2022). https://doi.org/10.1080/23307706.2022.2033644
60. Sylvia, J.J.: The biopolitics of social distancing. Media Soc Soc (2020). https://doi.org/10.1177/2056305120947661
61. Thilakarathne, N.N., Madhuka Priyashan, W.D.: An overview of security and privacy in smart cities. EAI/Springer Innov. Commun. Comput. (2022). https://doi.org/10.1007/978-3-030-82715-1_2
62. van Eck, N.J., Waltman, L.: Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics **84**, 523–538 (2010). https://doi.org/10.1007/s11192-009-0146-3
63. van Zoonen, L.: Privacy concerns in smart cities. Gov. Inf. Q. **33**, 472–480 (2016). https://doi.org/10.1016/J.GIQ.2016.06.004
64. Veloutsou, C., Mafe, C.R.: Brands as relationship builders in the virtual world: a bibliometric analysis. Electron. Commer. Res. Appl. (2019). https://doi.org/10.1016/j.elerap.2019.100901
65. Wai-Loon Ho, C., Caals, K., Zhang, H., Ho, L., Caals, K., Zhang, H.: Heralding the digitalization of life in post-pandemic East Asian Societies. J. Bioethical Inq. **174**(17), 657–661 (2020). https://doi.org/10.1007/S11673-020-10050-7
66. White, C.L., Boatwright, B.: Social media ethics in the data economy: issues of social responsibility for using Facebook for public relations. Public Relat. Rev. (2020). https://doi.org/10.1016/J.PUBREV.2020.101980
67. Wright, N., 2018. How Artificial Intelligence Will Reshape the Global Order. Foreign Aff. 10.
68. Yuan, M., Nikouei, S.Y., Fitwi, A., Chen, Y., Dong, Y., 2020. Minor Privacy Protection through Real-time Video Processing at the Edge. Proc. - Int. Conf. Comput. Commun. Networks, ICCCN 2020-August. https://doi.org/10.1109/ICCCN49398.2020.9209632
69. Završnik, A.: Introduction: Situating Drones in Surveillance Societies. Drones Unmanned Aer. Syst. Leg. Soc. Implic. Secur. Surveill (2016). https://doi.org/10.1007/978-3-319-23760-2_1
70. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.S.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**, 122–129 (2017). https://doi.org/10.1109/MCOM.2017.1600267CM
71. Zhang, Z., Zaman, A., Xu, J., Liu, X.: Artificial intelligence-aided railroad trespassing detection and data analytics: methodology and a case study. Accid. Anal. Prev. (2022). https://doi.org/10.1016/J.AAP.2022.106594
72. Ziosi, M., Hewitt, B., Juneja, P., Taddeo, M., Floridi, L.: Smart cities: mapping their ethical implications. SSRN Electron J (2022). https://doi.org/10.2139/SSRN.4001761