

## Deepfake Dilemmas: Imagine Tomorrow's Surveillance Society through Three Scenarios

Fatma DOĞAN AKKAYA<sup>1</sup> 

<sup>1</sup>Asst. Prof. Dr., Kastamonu University, Faculty of Communication, Kastamonu, Türkiye

**Corresponding author :** Fatma DOĞAN AKKAYA  
**E-mail :** fatmanurdoganakkaya@gmail.com

### ABSTRACT

As deepfakes—hyperrealistic, manipulated media content becomes increasingly sophisticated, they raise critical questions about the future of social interaction and trust. Drawing on sociological insights enriched by the literature on virtual reality surveillance, this study explores the social landscapes that may emerge with the widespread adoption of deepfake avatars in the near future. Moving beyond technical considerations, the research employs social prediction methods to explore three potential future scenarios involving deepfake avatars: seamless integration that facilitates self-expression but complicates digital identity control; pervasive algorithmic surveillance that exacerbates social control and privacy issues; and the concept of ghost avatars, that is, digital representations that function as commodities or tools of resistance. This analysis highlights the ethical dilemmas surrounding deepfakes, particularly in relation to mass surveillance, digital self-control, and resistance movements. Contributing to scholarly discourse, the study underscores the need for proactive social and ethical frameworks to navigate the evolving deepfake landscape and highlights the importance of ongoing research for the responsible development and use of this powerful technology.

**Keywords:** Deepfake Technology, Artificial Intelligence (AI), Virtual Surveillance, Digital Society, Future Scenarios

**Submitted** : 31.03.2024  
**Revision Requested** : 26.05.2024  
**Last Revision Received** : 14.06.2024  
**Accepted** : 06.08.2024  
**Published Online** : 07.10.2024



This article is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

## 1. Introduction

Artificial intelligence (AI) has had a profound impact on media, blurring the distinction between reality and fabrication. Of particular concern are deepfakes, highly realistic AI-generated media content, which pose significant challenges due to their ease of production and rapid dissemination on social media platforms. There is a growing academic focus on the societal implications of deepfakes, highlighting their potential to undermine trust and spread misinformation. Urgent attention is needed to fully assess the impact and implications of these concepts in contemporary discourse.

Deepfake technology, which uses deep learning in AI, convincingly superimposes one person's face on another, much like a mask, by processing large datasets to understand different facial angles. Recently, it has gained popularity for entertainment by integrating famous characters into popular films or videos (Gissen, 2022). Mainstream media has also explored the potential of simulating news presentations using deepfake experiences (Hwang, 2023). It has also been used to resurrect historical figures in order to demonstrate its transformative power (Gibson, 2021). In addition, major brands have used deepfake technology to conduct awareness campaigns as part of their corporate social responsibility initiatives (Murray, 2021).

Conversely, academic research tends to present deepfake technologies in a negative manner. Systematic reviews highlight concerns about potential security breaches, whereas limited studies address broader societal impacts (Gamage et al., 2021). Research on the societal impacts of deepfakes highlights public discomfort with the unrestricted capabilities of the technology and the expected ethical, psychological, and physical impacts associated with manipulated audio-visual content (Westling, 2019; Hancock & Bailenson, 2021; Langa, 2021).

Deepfakes, which blur the line between physical and digital, aptly epitomize the transformative power of the digital revolution in societies (Negroponte, 1995). As technology advances rapidly, so does our interest in its social implications. Current research explores how companies (Bardzell, 2014; Mager and Katzenbach, 2021) shape perceptions, governments (Schmidt & Cohen, 2013; Manovich, 2014), and individuals (Dufva and Dufva, 2019; Suchman, 2012) adapt to this dizzying transformation. Despite conflicting predictions, such as fears that AI will dominate human intelligence (Bostrom, 2014; Barfield, 2015) or that AI will serve more sophisticated, futuristic societies (Brynjolfsson and McAfee, 2011; Schwab, 2016), technology is undeniably reshaping our world as a powerful mediator of societal development, as highlighted by influential thinkers such as Marx and Weber (Defleur, 1982).

This study explores the evolving concept of virtual identity within envisioned future communication systems consisting of interconnected virtual environments. Examining the impact of deepfakes aims to provide a deeper understanding of the social transformations wrought by digital technologies. Anticipating the rise of deepfakes in both public and private spheres, this research examines how technology will reshape society, ultimately focusing on how seamlessly integrated deepfakes will alter daily life. This paper critically interrogates ethical dilemmas such as autonomy, control, and resistance surrounding deepfakes and their manipulation of virtual self-perception. It argues that a comprehensive analysis of these issues is crucial for understanding the potential impact of various surveillance-based social control mechanisms on future societies. This study explores deepfakes not only as a form of manipulated media, but also as a novel form of technological surveillance, a crucial aspect often neglected in current research. This framework is based on a sociological perspective, an extensive theoretical foundation in surveillance studies, and is enriched by existing data. To achieve this goal, the study used the social prediction method, an indispensable element of sociology, as a framework for analyzing the social changes triggered by digital transformations. The proposed method is useful for analyzing future scenarios based on current trends and theoretical discussions.

This article begins with an insightful review of the technical aspects of deepfake technology, its origins, and its diverse manifestations. The analysis highlights how deepfakes differ from traditional manipulation and how technology blurs reality by drawing on research in security, media, psychology, law, and policy. Social impact reports, particularly from civil initiatives, further illuminate these concerns.

It then makes a critical link between deepfakes and surveillance, offering a nuanced summary of historical and contemporary surveillance studies. Driven by significant investment from technology giants, this future could see a rise in self-surveillance alongside the emergence of self-replicating avatars, malicious impersonation, and autonomous AI-powered digital identities.

Finally, the research concludes with three possible future scenarios shaped by deepfakes virtual selves: a world of balance between freedom and control in virtual spaces with avatars, a society trapped in constant algorithmic surveillance, and the endless commodification of fully digitalized beings through algorithmic surveillance, or the possibility of virtual escape where individuals resist control in digital afterlife.

## 2. Aim and Methodology

This study investigates how deepfakes, an AI technology that undermines media authenticity, could seamlessly integrate into future communication systems, reshaping human interaction and our understanding of reality within interconnected communities. The method integrates empirical evidence from academic papers, reports, and reliable sources, combining a sociological perspective with surveillance studies to deepen the existing research on digital technologies. This comprehensive approach aims to illuminate the ethical concerns, power dynamics, and broader societal implications of deepfakes.

Employing social forecasting—a cornerstone of sociology—the study seeks to comprehensively understand the multiple societal impacts of evolving digital technologies. While historically criticized for its association with positivist models of social engineering (Aldridge, 1999) and a long list of failures in terms of predictive accuracy (Henshel, 1982), contemporary sociology recognizes the value of this method in analyzing causal relationships and interpretable outcomes (Hofman et al., 2017). Watts (2014) advocated a renewed focus on sociological foresight, echoing Kaplan's (1940) emphasis on social prediction. This approach ensures that the discipline maintains scientific rigor and relevance through predictive analysis based on interpretable data.

In today's world of advanced algorithmic forecasting methods, a sociological lens is essential for examining the social implications of human-technology interactions. Compared to previous limitations in data and processing power (Martin et al., 2016), sociological prediction is now enabled by the availability of multi-source data, advances in computational processing, and the development of specialized algorithms (Chen et al., 2021). This allows for more accurate predictions and informed expectations from a social science perspective. This research, for instance, aims to forecast the societal impact of deepfakes by combining empirical AI research evidence with a sociological lens. This investigation provides an original perspective on the sociology of communication by analyzing the transformative potential of deepfakes.

## 3. Deepfake Technology and A Brief Review of Its Social Impacts

Deepfake technology uses state-of-the-art AI and machine learning techniques, such as deep neural networks (DNNs), Generative Adversarial Networks (GANs), and other complex algorithms to manipulate multimedia content (Kietzmann et al., 2020; Yu et al., 2021; Rana et al., 2022). For instance, using GANs, a well-known class of machine learning systems, these inputs are processed by a trained algorithm to generate high-fidelity synthetic media. (see Figure 1.). These synthetic creations can be meticulously crafted to replace a person's face in existing media, effectively fabricating entirely new audio, video, or images, or even attributing false statements to individuals.

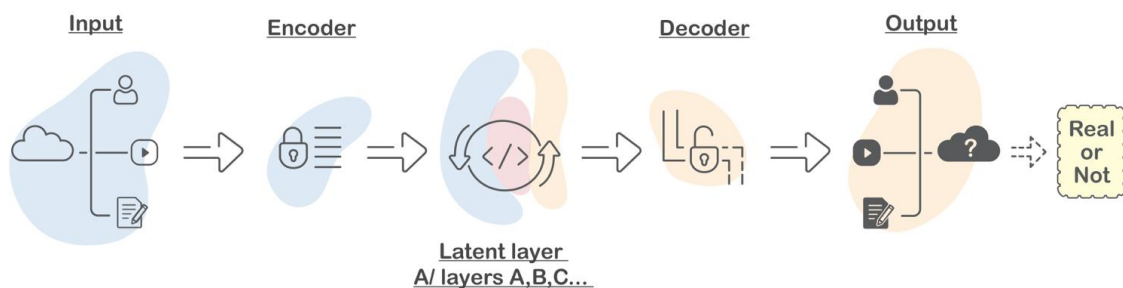


Figure 1. Basic algorithmic logic of deepfakes

Deepfake technology, a remarkable case of scientific progress, has recently come under significant scrutiny. A Reddit user first introduced the term "deepfakes" in 2017 to describe the use of face-swapping technology to create sexually explicit content featuring celebrities. This early instance exemplifies the ability to create deceptive content without ethical considerations. Subsequent cases involving impersonations of political figures and celebrities, along with fraudulent voice manipulation for financial gain, further highlighted the realistic and potentially harmful nature of deepfakes (Somers, 2020). Furthermore, Fagni et al. (2021) demonstrated how bot accounts simulating human behavior could generate fake text content on Twitter, further fueling the debate surrounding deepfakes. These developments have led to discussions on privacy violations, ethical boundaries, and intellectual property rights. Consequently, deepfakes have become a pressing security concern for governments, businesses, and the political sphere (Yu et al., 2021).

Although deepfakes and fake news share similarities in terms of the speed of dissemination, typology, and purpose, differentiation is necessary for a more nuanced understanding of contemporary communication dynamics. The negative

social and democratic impact of fake news has been well documented, while the response to fake news has been met with increased scrutiny and calls for caution. This is evidenced by pronouncements from technology centers (MIT Open Learning, 2020), academia (de Rancourt-Raymond & Smaili, 2023) and law enforcement (Busch et al., 2023) regarding the potential dangers of AI-generated media, particularly deepfakes. Public concern about deepfakes is growing due to their perceived security threat (iProov, 2022), with a notable gender gap in perception (Angell, 2020), while businesses show limited awareness and willingness to address the risks and benefits associated with the technology (Attestiv, 2021). These manipulations of visual, audio, and textual content pose an unprecedented threat to trust and authenticity in various digital media landscapes.

Deepfakes present two distinct challenges compared to other forms of manipulative content: *contextual persuasion and technological authorization*. Compared to traditional fictional narratives, deepfakes have an unprecedented power of persuasion. Köbis et al (2021) demonstrated that people's overconfidence in their ability to spot deepfakes blurs the line between reality and fiction, making them vulnerable to manipulation. Furthermore, Murphy and Flynn (2021) suggest that deepfakes use sophisticated persuasion techniques previously relegated to the realms of fantasy and science fiction, potentially implanting false memories. Technological authorization, however, refers to the ongoing struggle to maintain effective detection methods in the face of rapidly evolving deepfake production technology. As algorithm-based deepfake tools become increasingly sophisticated, detection methods may fall behind in the perpetual game of cat and mouse (Greengard, 2019; Kietzmann et al., 2020). The growing number of real-world incidents involving deepfakes underscores the urgency of addressing these concerns.

As Hancock et al. (2020) described, AI-mediated communication employs intelligent agents to modify, enhance, or generate messages that achieve specific communication goals. This area has seen a significant increase in deepfake content, with over 100 million deepfake videos circulating online by 2020 and over 5.4 billion views on YouTube between 2017 and 2020 (Sentinel, 2020). This rapid technological development has quickly attracted the attention of practitioners and academics. Owing to space limitations, this paper provides a concise overview of the main areas of academic focus, drawing on comprehensive literature reviews and prominent surveys.

A recent systematic review (Gamage et al., 2021) analyzing research from 2017 to 2021 highlights the emerging field of social science research on deepfakes, focusing on security concerns—particularly the ability of AI to mimic identities—as well as the psychological impact, legal regulation, and policy implications needed to address the societal threats posed by this technology. Hancock and Bailenson (2021) highlighted the urgency for innovative research, as even livestreaming, once a trusted medium, represents a critical breach of trust by manipulating real-time videoconferencing. Building on concerns about media credibility, Vaccari and Chadwick (2020) argued that deepfakes undermine trust in journalism and the media more broadly. This condition fosters an environment susceptible to misinformation, potentially worsening social divisions. The Council of Europe (Lacroix, 2020) expanded the discussion beyond explicit threats to include more implicit societal risks. Their report argued that all forms of AI bias have the potential to exacerbate social division, perpetuate stereotypes, and reinforce existing prejudices.

The rise of deepfakes has sparked widespread concern about their social impact. However, this concern often overlooks the critical aspect of deepfakes as a burgeoning form of technological surveillance. Surveillance theory provides a valuable framework for analyzing this under-researched facet of deepfakes. By examining how deepfakes interact with broader social surveillance practices, this theoretical lens illuminates the roles of different actors within the deepfake landscape and the ethical dilemmas surrounding their involvement.

#### **4. Sociological Reflections on Deepfakes through Surveillance**

A sociological lens can help unravel the complexities of deepfakes. Drawing on historical debates on surveillance, this perspective reveals a deep connection between manipulated media and broader societal control. By examining the roles of different actors, social norms, and the evolving surveillance landscape, this research explores the power dynamics, ethical complexities, and social implications embedded in the creation and dissemination of deepfakes. This approach aims to provide nuanced insights into the social transformations catalyzed by deepfakes, particularly how they reshape collective perceptions, the interplay between surveillance and trust and the evolving ethical landscape of the digital age.

Surveillance, which means 'to watch over' in French, refers to the systematic observation, monitoring and collection of information about individuals, groups or activities. This concept has been extensively studied and refined by scholars from various disciplines. Surveillance theory unfolds in three phases, with some overlap and continued influence. (Galič et al. (2017):

The first phase derives from Bentham's 18th-century model of the panopticon, an architectural concept that ensures constant visibility of the observed and fosters power dynamics through ever-present surveillance. Foucault (1977) theorized panopticism, a mode of power that relies on constant surveillance to cultivate self-regulation and conformity to social norms. As surveillance intensifies, the need for a central observer diminishes. Control becomes self-surveillance, with the individual internalizing the watchtower gaze.

In the second phase, the enduring significance of the panopticon extends beyond prisons to inform contemporary discussions on global surveillance. Deleuze and Guattari (1987) saw the panopticon as a broader symbol of social control in modern pervasive surveillance, echoing Haggerty and Ericson's (2000) notion of the surveillance assemblage, a network of components that form functional systems.

Finally, while traditional theories have focused on institutionalized control, the current distinguished by a technologically driven transition from unipolar to multipolar surveillance. Lyon's (2007) concept of "panopticommodity" and Whitaker's (1999) "participatory panopticon" highlight the normalization of surveillance, with commercial products and individuals actively engaging in mutual online data sharing, leading to a networked era of data surveillance. Consequently, the traditional panopticon with a central authority and the concept of a constantly monitored prisoner are becoming increasingly obsolete in this evolving multipolar surveillance and data collection landscape.

Deepfakes pose a novel challenge to surveillance theory, disrupting traditional paradigms by introducing sophisticated manipulated media. In addition to serving as tools for social control and information manipulation, deepfakes can potentially subvert established surveillance practices. This challenges the dominant panopticon model of discipline and punishment (Foucault, 1977) and requires a nuanced understanding of power dynamics in the digital age. Furthermore, deepfakes complicate the traditional view of collective and individual relations, offering avenues for entertainment, pleasure, and resistance to power structures (Haggerty, 2006; Mann, 2004). This necessitates a re-evaluation of surveillance theories to account for the dynamic interactions among governments, corporations, and individual users in the evolving landscape shaped by deepfake technology.

The proliferation of deepfakes highlights a significant imbalance in information and power dynamics. Organizations that can navigate AI-generated data wield considerable transformative influence, particularly in the realm of surveillance, where specialized tools enable the creation and dissemination of synthetic media. Clarke's concept of 'dataveillance' (1988) is highly relevant in this data-rich environment, describing the systematic monitoring of individuals through the collection and analysis of data from multiple sources. This extensive data collection not only influences consumer behavior, but also facilitates the manipulation of perceptions through deepfake interventions. AI-driven manipulation is increasingly used strategically in political conflicts (Giusti and Piras, 2020), branding disputes (Horowitz et al., 2022), and the production of synthetic media (Marcellino et al., 2023), reinforcing the prevailing power dynamics in these contexts.

Deepfakes, on the other hand, disrupt established power dynamics within surveillance and empower individuals to engage in counter-surveillance practices (Mann, Nolan, & Wellman, 2003). The burgeoning digital activism movement, led by social media and video activism, exemplifies this trend. Activists use online mobilization to circumvent traditional surveillance and document human rights violations, political injustices, and violence (Hermida & Hernández-Santaolalla, 2018; Gonzalez & Deckard, 2022). This can be defined as the "participatory surveillance" age, where users engage in self-monitoring and curating their online presence rather than being subjected to external observation (Albrechtslund, 2008).

However, deepfakes are a double-edged sword. Although they enable counter-surveillance, their ease of creation fuel concerns about misinformation and manipulation of public opinion. This participatory nature of deepfakes is consistent with Lyon's (2007) concept of the "panopticommodity," where individuals willingly share information that can be used to generate manipulated content.

Consequently, the rise of deepfakes requires a re-evaluation of surveillance theories. Recognizing both the risks of manipulation in the digital age and the empowering potential of counter-surveillance, surveillance theories must reassess the evolving technological landscape.

## 5. Deep Scenarios for Tomorrow's Society

Significant investments by technology giants, such as Meta's Oculus headsets and Microsoft's HoloLens, in augmented reality (AR)<sup>1</sup>, virtual reality (VR)<sup>2</sup>, and mixed reality (MR)<sup>3</sup> technologies point to a dramatic shift in the landscape of virtual experiences by 2020. Once limited to niche audiences, immersive reality (IR)<sup>4</sup> experiences are rapidly becoming mainstream due to evolving user expectations. These expectations go beyond futuristic novelty and include a desire for more realistic experiences, broader accessibility, and potentially transformative applications across multiple aspects of individual and societal life.

Industry leaders such as Meta, Alphabet, Apple, Microsoft, Epic Games, and Unity Technologies are leading this transformation. Their significant financial commitments, including billions in annual spending, large funding rounds, and strategic acquisitions (, 2022; Jungherr & Schlarb, 2022), extend beyond the consumer product market. Partnerships with government organizations, such as the US Army and the Pentagon, highlight the potential of AR/VR for multiple sectors (Nellis and Dave, 2021). This collective effort underscores a shared vision: shape the future of immersive digital environments and create a seamlessly integrated meta-universe.

In the midst of rapid technological progress, critical questions are raised about social implications, particularly selfhood in virtual realms. Moving beyond the era of self-surveillance on social media platforms (Albrechtslund, 2008), a new paradigm is emerging: *fake-your-self-surveillance*. This envisions a future in which individuals curate multiple digital identities within immersive reality environments, each embodying different roles and experiences. Advances in AI and machine learning can facilitate the creation of self-replicating avatars that can interact independently in virtual spaces.

However, this raises significant concerns about the potential for malicious impersonation and the erosion of trust in online interactions (Tariq et al., 2023). Furthermore, the prospect of fully autonomous AI-powered digital identities blurs the boundaries between real and virtual selves, raising profound questions about privacy, authenticity, and the nature of human connections in these augmented realities, necessitating the development of new ethical frameworks to govern social interactions in immersive environments.

Leveraging three future scenarios, the next part of this study explores the potential societal ramifications that may arise from the convergence of deepfakes and pervasive social surveillance applications in next-generation virtual environments. Using a surveillance studies lens, the research examines the roles of different actors and the ethical dilemmas they face in virtual environments. The analysis aims to illuminate potential outcomes regarding security, privacy and ethics within immersive realities, ultimately navigating the complexities of this evolving landscape to promote a safe and ethical digital future for all.

### 5.1. Scenario 1. Autonomy and Control of the Digital Self

The rapid development of personalized avatars for diverse digital interactions in work, education, healthcare, entertainment, and social settings presents an intriguing yet multifaceted prospect (Nowak & Fox, 2018). While entrusting routine tasks to digital counterparts promises greater organizational efficiency, more leisure time and more engaging social experiences (Blodgett and Tapia, 2011), concerns about vulnerability to manipulation, persuasion and control are simultaneously emerging across domains (Hadan et al., 2024). This dynamic calls for a thorough examination of the interplay between autonomy and vulnerability in technologically mediated environments.

The rise of deepfakes coincides with an increasing emphasis on global online interactions in virtual reality environments. These systems often employ lifelike avatars that can replicate individuals with incredible precision. This convergence raises profound concerns about manipulated social experiences, the erosion of online authenticity, and the nature of selfhood in digital spaces. As self-replicating avatars and highly detailed virtual environments proliferate, critical questions arise about the legitimacy of online interactions and the potential for exploitation in these virtual landscapes. The key question is whether these technological advances will ultimately empower individuals or expose them to new forms of manipulation and control.

To understand the blurring boundaries between humans and machines, we consider a hypothetical scenario: Adam, a professional whose career is closely linked to a network of multiple virtual personas (See Figure 2.). These semi-autonomous, artificially intelligent avatars represent a new approach to professional identity that transcends traditional boundaries. Designed to automate routine tasks such as attending training sessions, performing data analysis,

<sup>1</sup> Layers digital information onto the real world, enhancing user interaction via devices like smartphones or AR glasses.

<sup>2</sup> Overlays digital information to the real world, enhancing user perception and interaction via smartphones or AR glasses.

<sup>3</sup> Blend real and virtual elements to anchor digital content to the physical world and create a seamless blend of realities.

<sup>4</sup> Umbrella term combining AI, AR, VR, and MR technologies to engage users' senses, shaping captivating digital experiences.

conducting market research, or producing reports and reviews, these digital avatars improve the worker's efficiency and decision-making, thereby enhancing his or her value proposition in the labor market.

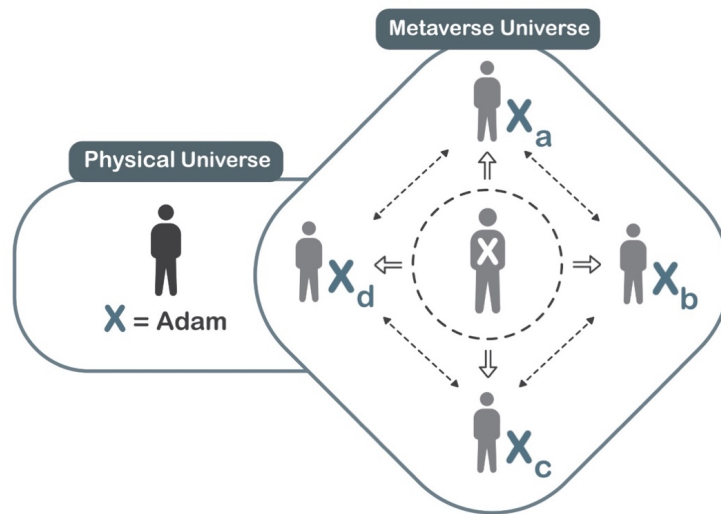


Figure 2. Adam's different avatars in the virtual world

The rapid integration of AI into digital environments poses a critical challenge to the very notion of self-hood. The creation of sophisticated digital avatars and the prospect of fully autonomous AI-driven identities in virtual environments require a re-evaluation of how we define and understand ourselves. The hypothetical scenario of Adam and his multiple AI personas illustrates this dilemma: will they fragment our sense of self or create a multifaceted identity that blends real and virtual experiences?

In today's digital landscape, the concept of a singular, static identity is increasingly being undermined. Surveillance practices now categorize individuals based on online profiles and digital footprints (Cheney-Lippold, 2011), transforming fragmented digital representations into marketable profiles (Fourcade and Healy, 2017). This shift reflects Deleuze's concept of the "dividual," in which individuals are seen as divided and segmented entities. This shift marks a shift from disciplinary societies to "societies of control," emphasizing the manipulation of digital representations over physical presence. Therefore, it is essential to re-evaluate social norms among these technological advances, particularly regarding the complex interplay of identity, representation, and control.

In 1992, Deleuze foresaw a world in which traditional institutions (family, school, etc.) would be transformed into coded entities governed by corporate structures. This shift, termed "modulation," positioned digital identities as commodities influenced by market forces, where their value is determined by utility and profit rather than intrinsic human value (Deleuze, 1992:6). Looking forward to the present, the integration of AI-driven replicas into everyday life has added a new layer to the fusion of technology and social structures. This convergence prompts a re-evaluation of the "surveillance assemblage" (Haggerty and Ericson, 2000). In this framework, human bodies are abstracted from their physical contexts and reconstructed as recognizable 'data doubles. These entities are subject to surveillance and intervention by sophisticated networks of modern technologies and practices, raising important questions about identity, autonomy, and social control (Haggerty and Ericson, 2000).

The *fake-your-self phenomenon*, a new conceptual tool for the surveillance of divided identities, can help us better understand the complex interactions between autonomy and surveillance in virtual environments. The rise of deepfakes and hyperrealistic manipulated content further blurs this line. Deepfakes allow the construction of meticulously crafted online personas, potentially empowering individuals to curate their online presence and transcend traditional limitations. However, this ability to manipulate online identities creates a paradox: the fine line between autonomy and a lack of self-determination. While individuals can exercise agency in crafting their online selves, the constant pressure to manage and perform these identities can blur the lines between genuine expression and constructed reality, potentially leading to loss of self-determination and a sense of inauthenticity.

In a fully virtual world, fragmented digital representations empowered by semi-autonomous AI replicas offer potential for self-control. Here, the end of life refers to the end of the task-performing digital identities rather than the tasks themselves. Individuals can transcend conventional boundaries and manage professional and social engagements through these proxies. However, as technological advances intertwine with personal agency, concerns arise about

whether individuals really retain control over their digitally curated identities or whether these replicas become tools of covert control.

This scenario highlights the need to move beyond the simplistic binary of real versus virtual to critically examine human-machine interactions in the digital age. The seamless integration of deepfake replicas requires careful exploration of redefined agency and responsibility within virtual communities. Potential consequences, such as reputational damage from exposed deepfakes, highlight critical ethical and legal issues. A comprehensive analysis that considers self-control, algorithmic bias, power dynamics, and transparency is essential. This research can inform future debates about the extent of individual control over their digital identities in the complex realm of AI-driven self-representation.

## **5.2. Scenario 2. Authentication and Disciplined Social Control**

Contemporary surveillance practices have transcended the centralized model of the panopticon era, characterized by a single observer and a multitude of observers. The dispersed network of technologies that characterise the current landscape significantly alters the paradigm of surveillance. The emerging surveillance mechanism is often framed positively, emphasizing transparency and public visibility (Galič et al. 2017). Proponents argue that doing so fosters a collaborative and empowering environment (Björklund, 2021).

However, a critical examination of societal engagement with AI-powered communication and information systems reveals their potential to mask more subtle forms of control. Algorithmic processes in the post-panoptic era raise concerns about bias and discrimination, particularly in criminal justice, credit scoring, and online recommendations (Crawford, 2021; Lyon, 2003). For instance, algorithmic bias can lead to facial recognition systems failing to recognize non-white people (Algorithmic Justice League, n.d.) or discriminating against female job applicants (Dastin, 2018). Social sorting also introduces bias, stigmatizing certain profiles as deviant (Lyon, 2003). In its most extreme form, government surveillance can be legitimized under the concept of BANopticon (Bigo, 2006). The term describes an exclusionary approach in which those perceived as security threats are deliberately excluded from the system (Bigo, 2006). This concept can be illustrated by the recent actions of the US government, which has pressured telecommunications service providers to hand over private information about individuals or entities deemed threat (& Laperruque, 2023).

The challenges posed by contemporary algorithmic surveillance necessitate theoretical reframing. Deleuze and Guattari (1987) posited a shift from the panoptic model of disciplinary self-surveillance toward a mode of social control centered on manipulating and homogenizing online representations. This shift fosters a novel form of self-surveillance that prompts individuals to curate their online presence in accordance with the perceived expectations of algorithms and online communities. Consequently, the primary targets of surveillance have transformed from individuals themselves to fragmented digital representations constructed in their algorithmic footprints (Deleuze, 1992). This phenomenon blurs the lines between self-presentation and self-surveillance, as individuals actively shape their online personas for both human audiences and algorithmic systems (Kang et al., 2010). Thus, a crucial question emerges: how will the rise of virtual identities, potentially near-perfect replicas, in future extended reality technologies reshape the concept of surveillance communities?

To illustrate the potential consequences of this reframing of surveillance, let us take the aforementioned example of Adam, who created deepfakes of himself and placed them in various virtual spaces. However, generating an unlimited number of these digital simulations and dispersing them across metaverses could lead to a phenomenon we can call identity inflation. This poses potential security and legal challenges for Adam. His virtual duplicates may be mistaken for real data, potentially subjecting him to exclusionary or punitive sanctions within the system. To mitigate this risk, consider a scenario in which Adam acquires certificates of authenticity for some of his replicas. This introduces a complex situation regarding Adam's ontological existence (his sense of self in a world overflowing with digital copies) and his potential submission to the control mechanisms embedded within these virtual environments.



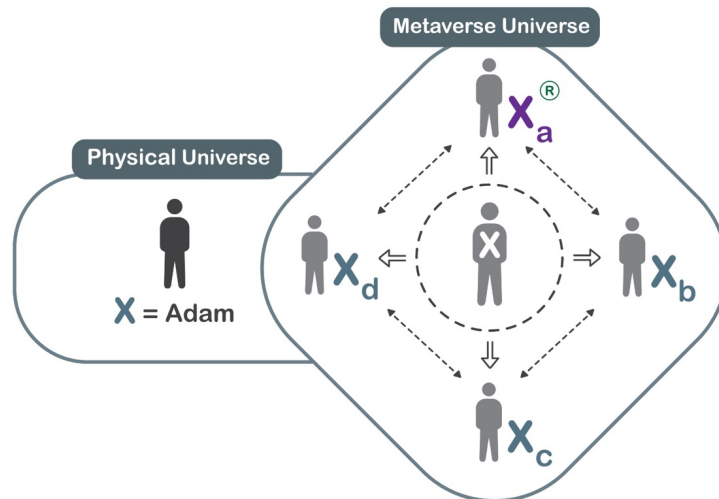


Figure 3. Registered version of digital avatars

The explosion of digital identities, exemplified by deepfakes, necessitates a radical shift in surveillance practices. Instead of directly monitoring individuals, the focus might move toward verifying the authenticity of online representations, potentially with user consent. Algorithmic systems that are adept at shaping online appearances are well-positioned for this role. However, this power comes at the risk of users. Actors may face pressure to conform to algorithmic standards of authenticity, leading to novel forms of online conformity dictated by algorithms. This scenario resembles a panoptic prison’s disciplinary self-assessment, where constant monitoring compels specific behaviors. The ghost of the panoptic tower, in a sense, might haunt us again in the digital realm.

This blurred line between self-presentation and self-surveillance aligns with the concept of ‘dataveillance’ (Clarke, 1988). Dataveillance involves systematically collecting and analyzing vast amounts of user data, including user behaviors and preferences. Unlike traditional surveillance, virtual environments actively involve users in creating their online identities and sharing personal information (Boyd, 2004). Social media platforms exemplify this trend. The constant curation of online personas foreshadows a future where self-presentation and self-surveillance merge voluntarily or unwittingly (Kang et al., 2010). This dynamic echoes Zuboff’s ‘surveillance capitalism’ (2015), in which platforms leverage user data to shape commercial practices and the very social structures within virtual spaces.

This burgeoning landscape of virtual identities presents a complex scenario that merges disciplinary self-assessment with the algorithmic social control inherent in data surveillance, forming what can be termed “*disciplined social control*.” Individuals engage in self-presentation by authorizing virtual replica identities and voluntarily sharing personal information. Akin to the panopticon effect, they strive to conform to the social norms of virtual spaces. Meanwhile, algorithmic systems wield immense power, fragmenting online identities into data points used to assess factors like creditworthiness and access. This fragmentation influences user choices, preferences, and perceptions.

Ethical questions emerge as individuals surrender control over their digital self-portraits to experience immersive VR experiences. The use of multiple virtual identities by a single individual further exacerbates these concerns. We urgently need to re-evaluate privacy considerations, user consent practices, and the commodification of personal data. Further research is crucial for understanding the long-term consequences of this novel form of self-surveillance and its potential impact on individual autonomy and social structures within virtual environments.

### 5.3. Scenario 3. Compliance Versus Resistance in Digital Afterlife

Michel Foucault’s (1977) seminal work on the panopticon served as a powerful critique of top-down surveillance, highlighting its capacity to disempower individuals. However, the contemporary landscape reveals a more complex interplay between surveillance structures and individual agency. While technological advances have undeniably increased the reach and sophistication of surveillance practices, they have also inadvertently fostered resistance movements that have actively challenged these power dynamics.

This is particularly relevant when considering the concept of “digital afterlife,” a hypothetical scenario in which digital avatars transcend physical boundaries and potentially exist in perpetuity. In this context, the following question arises: Will these digital avatars passively submit to the ever-questioning gaze of algorithmic systems or will alternative

forms of resistance emerge? In a mind-boggling future, imagine Adam again—not as a physical being but as an ever-evolving digital essence residing in a virtual world (Figure 4). Here, the lines between life and death are blurred, with virtual identities potentially outliving physical counterparts. These *ghost avatars*, constantly evolving thanks to AI, mean that people are creating an immortal fake version of themselves: the digital afterlife is no longer a distant fantasy (Mason-Robbie and Savin-Baden, 2020). These concepts are rapidly moving from science fiction to reality. A growing body of research has focused on digital resurrection projects of historical figures, celebrities, and people's deceased loved ones to understand their potential for education, entertainment, and even to help people cope with grief (Sherlock, 2013; Basset, 2018; Rodríguez Reséndiz and Rodríguez Reséndiz, 2024).

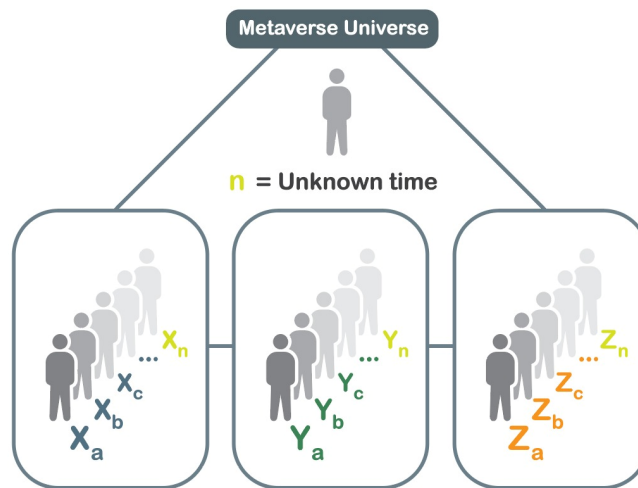


Figure 4. Ghost avatars in digital afterlife

Digital resurrection, while alluring, poses significant ethical and privacy challenges. Ghost avatars containing the personal data of deceased persons raise crucial issues of custodianship and exploitation. Even more worrying is the potential subsumption of a person's digitized essence—body, mind, memories, social connections, and even virtual possessions—by the ever-expanding apparatus of surveillance capitalism. Trapped in a super-panopticon' (Poster, 1995), individuals surrender their entire existence to a vast, ever-scrutinizing database. This is consistent with Zuboff's (2015) notion that the digitized self is the ultimate source of behavioral surplus. This data fuels algorithms that predict and potentially manipulate behaviors, eroding privacy and autonomy under constant algorithmic surveillance. Moreover, the commodification of the self reaches new extremes. Memories, relationships, and virtual properties become potential commodities within this all-encompassing system. The super-panopticon is transformed into a marketplace of human experience, raising profound ethical questions about the ownership and control of our digital selves in a world dominated by surveillance capitalism.

Algorithmic exploitation of data is a valid concern. However, this scenario avoids a purely dystopian view. Contemporary surveillance scholarship explores an appealing shift in power relations. Concepts such as "coveillance" (Mann et al., 2003) and "participatory surveillance" (Albrechtslund, 2008) exemplify this shift. These concepts move away from the panoptic model by emphasizing reciprocal surveillance, where users actively engage in online spaces and shape online narratives. The concept of "sousveillance," which implies that user-generated surveillance might subvert social control or resist powerful forces, adds further depth to the conversation. (Mann et al., 2003). Online platforms for citizen journalism and whistleblowing illustrate the potential of counter-surveillance tactics in the digital age. However, the potential misuse of these tactics warrants further investigation.

This user-driven approach indicates a more balanced power dynamic in which individuals are not simply passive subjects but also empowered participants. Further evidence for this user-driven approach comes from various studies on content moderation on platforms such as Twitter and YouTube (Mearns, 2015) and user engagement in review and rating services (Adams, 2012) and video streaming communities (Talvitie-Lamberg, 2018). These studies illustrate how users are actively involved in monitoring and challenging content, potentially disrupting established narratives in online communities.

In this context, ghost avatars unfettered by the limitations of physical existence present a unique opportunity. Free from the traditional sanctions and social pressures governing physical life, they could play a significant role in

social progress and intellectual advancement. Imagine historically significant figures such as human rights defenders, pioneering scientists, or inspirational role models transformed into autonomous digital identities powered by AI. These avatars can serve as invaluable resources, disseminate knowledge, advocate for positive change, and inspire future generations. Their persistence in the digital realm allows them to transcend the limitations of time and space, potentially amplifying their impact on a global scale.

This strategy goes beyond merely questioning private rules, as Koskela's (2004) exhibitionism term signifies. Instead, it uses the visibility of these avatars to promote positive social change. By actively engaging with the digital landscape, they can contribute to important discussions, educate the public on pressing issues, and mobilize support for critical causes. Ultimately, they can undermine the power imbalance inherent in top-down surveillance, empower individuals with knowledge, and foster a sense of collective responsibility.

Furthermore, while deepfakes disrupt trust and social interaction, they present a fascinating paradox. Their ability to create manipulated avatars represents a potential weapon against algorithmic surveillance. These "smoke screens" can confuse data collection efforts, hindering the ability of algorithms to track and profile online behaviors. This disrupts the very systems that deepfakes were 'born' to exploit—the ever-expanding apparatus of surveillance capitalism. However, the effectiveness of this resistance tactic is likely to be temporary. As deepfake detection methods evolve, the arms race between users and surveillance systems intensifies. Ultimately, more sustainable solutions lie in advocating robust privacy regulations and raising public awareness about the pervasiveness of such technologies.

Recognizing that ethical and privacy uncertainties surrounding digital resurrection are paramount is important. However, alongside these concerns lies the potential to propose ghost avatars for positive social and intellectual purposes. Further research is necessary to explore this potential and navigate the complex landscape of emerging digital afterlife. This research highlights the importance of developing strong ethical frameworks to ensure that avatars contribute positively to humanity without suffering exploitation.

## 6. Conclusion

This study explored the multifaceted societal implications of deepfakes, a rapidly developing AI technology with the potential to disrupt traditional social interaction norms and reshape surveillance practices in increasingly networked virtual environments. Using a sociological perspective enriched by social prediction methods and insights from surveillance studies, this research went beyond the technical aspects of deepfakes to examine their potential impact on human behavior, social control mechanisms, and the nature of selfhood in the digital age.

The three future scenarios presented—a world of balanced control through avatars, a society trapped in algorithmic surveillance, and a virtual escape through purely digital existence—highlighted the range of possibilities that may emerge as deepfakes become more sophisticated and integrated into everyday life. These scenarios underscore the urgency of proactive reflection on the ethical dilemmas surrounding deepfakes, particularly in relation to autonomy, control, and resistance within virtual spaces.

Further research is necessary to navigate the complexities of this evolving landscape. This includes in-depth analyses of the potential psychological and social impacts of deepfakes on individuals and communities. Furthermore, the development of robust legal frameworks that address the ownership and control of deepfakes, as well as the ethical implications of digital life, is paramount.

By promoting a comprehensive understanding of the multifaceted societal implications of deepfakes, this research aims to contribute to a future where technological innovation fosters social progress and safeguards individual autonomy in the digital realm. As deepfakes continue to evolve, ongoing critical dialog and collaboration between policymakers, technologists, social scientists, and the public will be essential in shaping a future where this technology serves rather than undermines humanity.

---

**Peer-review:** Externally peer-reviewed.

**Conflict of Interest:** The author has no conflict of interest to declare.

**Grant Support:** The author declared that this study has received no financial support.

---

### ORCID :

Fatma DOĞAN AKKAYA 0000-0002-6296-5591

## REFERENCES

- Adams, S. (2013). Post-panoptic surveillance through healthcare rating sites: Who's watching whom?. *Information, Communication & Society*, 16(2), 215–235.
- Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, 13(3). <https://doi.org/10.5210/fm.v13i3.2142>
- Aldridge, A. (1999). Prediction in sociology: Prospects for a devalued activity. *Sociological Research Online*, 4(3), 57–62.
- Algorithmic Justice League (n.d). <https://www.ajl.org/>
- Angell, M. (2020, Feb 9). How real is the deepfake threat? *American Banker*. Retrieved from <https://www.americanbanker.com/creditunions/news/how-real-is-the-deepfake-threat>
- Attestiv (2021, May) Deepfakes: The Business threat: Inagural deepfakes in business survey results. Retrieved from [https://f.hubspotusercontent30.net/hubfs/7603739/deepfake\\_report2021.pdf?\\_\\_hstc=143725418.1879e4f87f3af9d371de4bc1807298ac.1724673569402.1724673569402.1724673569402.1&\\_\\_hssc=143725418.1.1724673569402&\\_\\_hsfp=1308513962&hsCtaTracking=2eea443f-cbd5-4229-a7c2-5237a703046d%7Cdab0da4f-7ddd-4586-b257-5fce836345bd](https://f.hubspotusercontent30.net/hubfs/7603739/deepfake_report2021.pdf?__hstc=143725418.1879e4f87f3af9d371de4bc1807298ac.1724673569402.1724673569402.1724673569402.1&__hssc=143725418.1.1724673569402&__hsfp=1308513962&hsCtaTracking=2eea443f-cbd5-4229-a7c2-5237a703046d%7Cdab0da4f-7ddd-4586-b257-5fce836345bd)
- Bardzell, J. (2014). Social media and the making of global imaginaries. *Information, Communication & Society*, 17(3), 329–347.
- Barfield, W. (2015). *Cyber-Humans: Our Future with Machines*. Copernicus Cham Springer.
- Bassett, D. J. (2018). Digital afterlives: From social media platforms to thanabots and beyond. In C. Tandy (Ed.), *Death and anti-death, Volume 16: Two hundred years after Frankenstein*. (pp. 27–38). Ria University Press.
- Bentham, J., (1995). *The Panopticon Writings*. Bozovic, Miran (Ed.), London, UK: Verso.
- Benzinga (2022, May 14). Apple Vs. Google: Which one is winning the augmented reality race? *Business Insider*. Retrieved from <https://markets.businessinsider.com/news/stocks/apple-vs-google-which-one-is-winning-the-augmented-reality-race-1031460242>
- Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 46–68). Portland: Willan Publishing.
- Björklund, F. (2021). Trust and surveillance: An odd couple or a perfect pair?. (Eds)cViola, L. A., & Laidler, P. (2022). In *Trust and Transparency in an Age of Surveillance* (pp. 183-200). Routledge.
- Blodgett, B., & Tapia, A. (2011). Do avatars dream of electronic picket lines?: The blurring of work and play in virtual environments, *Information Technology & People*, 24 (1), 26–45.
- Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.
- Boyd, D., (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- Brynjolfsson, E., & McAfee, A. (2011). *Race against the machine: How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy*. Lexington, VA: Beard Books.
- Busch, E., Ware, J., & Brief, I. P. (2023, December). The weaponisation of deepfakes. *International center for counter-terrorism*. Retrieved from <https://www.icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf>
- Chen, Y., Wu, X., Hu, A. He, G., & Ju, G. (2021). Social prediction: a new research paradigm based on machine learning. *Journal of Chinese Sociology*. 8 (15).
- Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture and Society*, 28(6), pp. 164–181.
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512.
- Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
- Dastin, J. (2018, Oct 11). Amazon scraps a secret AI recruiting tool that showed bias against women. Retrieved from <https://www.reuters.com/article/us-amazon-comjobs-automation-insight-idUSKCN1MK08G/>
- De Rancourt-Raymond, A. and Smaili, N. (2023). The unethical use of deepfakes. *Journal of Financial Crime*, 30(4), 1066–1077.
- Defleur, L. B. (1982). Technology, social change, and the future of sociology. *The Pacific Sociological Review*, 25 (4), 403–417.
- Deleuze, G., and Guattari, F. (1987). *A thousand plateaus: capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.
- Deleuze, G. (1992). Postscript on the societies of control. *October* 59, 3–7. <http://www.jstor.org/stable/778828>
- Dufva, T., & Dufva, M. (2019). Grasping the future of the digital society. *Futures*, 107, 17–28.
- Fagni, T., Falchi, F., Gambini, M., Martella, A., & Tesconi, M. (2021). TweepFake: About detecting deepfake tweets. *Plos One*, 16(5). Retrieved from <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0251415>
- Fourcade, M., & Healy, K. (2017). Seeing like a market. *Socio-economic Review*, 15(1), 9–29.
- Foucault, M., (1977). *Discipline and punish: The birth of the prison*. Vintage, New York.
- Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and Beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30(1), 9–37.
- Gamage, D., Chen, J., & Sasahara, K. (2021, Oct 7). The emergence of deepfakes and their societal implications: A systematic review. Paper presented at Truth and Trust International Conference. Retrieved from [https://truthandtrustonline.com/wp-content/uploads/2021/10/TTO2021\\_paper\\_20.pdf](https://truthandtrustonline.com/wp-content/uploads/2021/10/TTO2021_paper_20.pdf)
- Gibson, A. (2021, May 17). Keeping It Real: Historians in the Deepfake Era. *Perspectives on History*. Retrieved from <https://www.historians.org/perspectives-article/keeping-it-real-historians-in-the-deepfake-era-may-2021/>
- Gissen, L. (2022, Nov 21). Talented impressionist morphs into twenty different celebrities using jaw-dropping deepfake technology... So, can you work out who they all are of them? *Mail Online*. Retrieved from

- <https://www.dailymail.co.uk/femail/article-11445427/Impressionist-transforms-celebrities-using-wild-deepfake-technology.html>
- Greengard, S. (2019). Will deepfakes do deep damage?. *Communications of the ACM*, 63(1), 17–19.
- Giusti, S., & Piras, E. (Eds.). (2020). *Democracy and fake news: information manipulation and post-truth politics*. Routledge.
- Gonzalez, S. M., & Deckard, F. M. (2022). We Got Witnesses: Black women's counter-surveillance for navigating police violence and legal estrangement. *Social Problems*, 71 (3), 894–911.
- Hadan, H., Choong, L., Zhang-Kennedy, L., & Nacke, L. E. (2024). Deceived by immersion: A systematic analysis of deceptive design in extended reality. *ACM Computing Surveys*, 56(10), 1–25.
- Haggerty, K. D., & Ericson, R. V. (1999). Governing the young. In R. Smandych (ed.) *Governable Places: Readings on Governmentality and Crime Control*, Dartmouth, UK: Ashgate.
- Haggerty, K.D. & Ericson, R.V. (2000) The surveillant assemblage. *British Journal of Sociology*. 51(4), 605–622.
- Haggerty, K. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 23–45). Portland: Willan Publishing.
- Hancock, J. T, Naaman, M., & Levy, K. (2020) AI-mediated communication: Definition, research agenda, and ethical considerations. *Journal of Computer-Mediated Communication*. 25(1). 89–10. <https://doi.org/10.1093/jcmc/zmz022>
- Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. *Cyberpsychology, Behavior, and Social Networking*. 24(3).149–152. <http://doi.org/10.1089/cyber.2021.29208.jth>
- Henshel, R. L. (1982). Sociology and social forecasting. *Annual Review of Sociology*, 8(1), 57–79.
- Hermida, A., & Hernández-Santaolalla, V. (2018). Twitter and video activism as tools for counter-surveillance: The case of social protests in Spain. *Information, Communication & Society*, 21(3), 416–433
- Hofman, J.M., A. Sharma, &D.J. Watts. (2017). Prediction and explanation in social systems. *Science*. 355(6324). 486–488.
- Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2022, Jul 25). Strategic competition in the era of artificial intelligence. *Center for a New American Security*. Retrieved from <https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence>
- Hwang, S. (2023, Sep 26). In South Korea, AI-driven virtual humans are becoming mainstream. *The Japan Times*. Retrieved from <https://www.japantimes.co.jp/business/2023/09/26/tech/ai-humans-south-korea/>
- iProov.com. (2022, Aug 26). Protecting against deepfakes: statistics and solutions. Retrieved from <http://www.iproov.com/blog/deepfakes-statistics-solutions-biometric-protection>
- Jungherr, A., and Schlarb, D. B. (2022). The extended reach of game engine companies: Epic Games and Unity Technologies provide platforms for extended reality and metaverse applications. *Social Media + Society*, 8(2), doi:10.1177/20563051221107641
- Kang, J., Shilton, K., Estrin, D., & Burke, J. (2011). Self-Surveillance and privacy. *Iowa Law Review*, 97, 809.
- Kaplan, O. (1940). Prediction in the social sciences. *Philosophy of Science*. 7(4): 492–498.
- Kelly, J. (2022, Jan 21). The metaverse set off a battle between Google, Apple, Microsoft, and Meta to build virtual and augmented reality (VR) headsets. *Forbes*. Retrieved from <https://www.forbes.com/sites/jackkelly/2022/01/21/the-metaverse-set-off-a-battle-between-tech-giants-google-apple-microsoft-and-meta-to-build-virtual-and-augmented-reality-headsets/?sh=6b4516c239c6>.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, 63(2), 135-146.
- Koskela, H. (2004). Webcams, TV shows, and mobile phones: empowering exhibitionism. *Surveillance and Society*, 2(2/3), 199–215.
- Köbis, N. C., Doležalová, B., & Soraperra, I. (2021). Fooled twice: People cannot detect deepfakes but think they can. *Iscience*, 24(11). <https://doi.org/10.1016/j.isci.2021.103364>.
- Lacroix, C. (2020, Sep). Preventing discrimination caused by the use of artificial intelligence [Report 1]. *Committee on Equality and Non-Discrimination. Council of Europe*. Retrieved from <https://assembly.coe.int/LifeRay/EGA/Pdf/TextesProvisoires/2020/20200915-PreventingDiscriminationAI-EN.pdf>
- Langa, J. (2021). Deepfakes, real consequences: Crafting legislation to combat threats posed by deepfakes. *Boston University Law Review*, 101, 761-801.
- Lyon, D. (Ed.). (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. London: Routledge.
- Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 3–20). Portland: Willan Publishing.
- Lyon, D., (2007). *Surveillance studies: An overview*. Polity Press, UK: Cambridge.
- Lyon, D., (2003). *Surveillance after September 11*. Polity Press, UK: Cambridge.
- Mager, A., & Katzenbach, C. (2021). Future imaginaries in the making and governing of digital technology: Multiple, contested, commodified. *New Media and Society*, 23(2), 223–236.
- Mann, S., Nolan, J., & Wellman, B. (2003) Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, 1(3), 331–355.
- Mann, S. (2004). "Sousveillance": inverse surveillance in multimedia imaging. In Proceedings of the 12th annual ACM international conference on Multimedia. *Association for Computing Machinery*. New York, USA, 620–627. <https://doi.org/10.1145/1027527.1027673>
- Manovich, L. (2014). *The language of new media*. MIT Press.
- Marcellino, W., Beauchamp-Mustafaga, N., Kerrigan, A., Navarre Chao, L., & Smith, J. (2023, Sep 7). The rise of generative AI and the coming era of social media manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI. *RAND Commentary*. Retrieved from <https://www.rand.org/pubs/perspectives/PEA2679-1.html>

- Martin, T., Hofman, J. M., Sharma, A., Anderson, A., & Watts, D. J. (2016, April). Exploring limits to prediction in complex social systems. In Proceedings of the 25th international conference on world wide web (pp. 683–694). Retrieved from <https://www.cs.toronto.edu/ashton/pubs/limpred.pdf>
- Marx, G. (2003) 'A tack in the shoe: neutralizing and resisting the new surveillance'. *Journal of Social Issues*, 59(2), 369–390.
- Mearns, G. W., Richardson, R. and Robson, L. (2015). Enact the internet and social media on the public sector's frontline. *New Technology, Work and Employment*, 30(3), 190–208.
- Murphy, G. & Flynn, E. (2021). Deepfake false memories. *Memory*, 30(4), 480–492.
- Murray, J. (2021). Deepfakes and digital avatars: the new celebrity brand ambassadors. Retrieved from <https://www.campaignlive.co.uk/article/deepfakes-digital-avatars-new-celebrity-brand-ambassadors/1713070>.
- MIT Open Learning (2020, Jul 20): Tackling the misinformation epidemic with “In Event of Moon Disaster”. Retrieved from <https://news.mit.edu/2020/mit-tackles-misinformation-in-event-of-moon-disaster-0720>.
- Murphy, G.; Ching, D.; Twomey, J., & Linehan C. (2023) Face/Off: Changing the face of movies with deepfakes. *Plos One*. 18(7). <https://doi.org/10.1371/journal.pone.0287503>
- Negroponte, N. (1995). *Being digital*. Alfred A. Knopf.
- Nellis, S. & Dave, P. (2021, Apr 1). Microsoft wins \$21.9 billion contract with U.S. Army to supply augmented reality headsets. *Reuters*. Retrieved from <https://www.reuters.com/article/us-microsoft-army/microsoft-wins-21-9-billion-contract-with-u-s-army-to-supply-augmented-reality-headsets-idUSKBN2BN36B/>
- Nojeim, G. ,& Laperruque, J. (2023, Dec 8). Government surveillance: A trojan horse in a house Intel committee bill massively expands FISA 702 surveillance. *Center for Democracy & Technology*. Retrieved from <https://cdt.org/insights/a-trojan-horse-in-a-house-intel-committee-bill-massively-expands-fisa-702-surveillance/>
- Nowak, K. L., & Fox, J. (2018). Avatars and computer-mediated communication: a review of the definitions, uses, and effects of digital representations. *Review of Communication Research*. 6. 30–53.
- Poster, M. (1995). *The second machine age*. Polity.
- M. S. Rana, M. N. Nobi, and B. Murali & Sung H. (2022) .Deepfake detection: A systematic literature review. *IEEE Access* 10, 25494–25513. doi: 10.1109/ACCESS.2022.3154404.
- Rodríguez Reséndiz, H., & Rodríguez Reséndiz, J. (2024). Digital resurrection: Challenging the boundary between life and death with artificial intelligence. *Philosophies*, 9(3), 71.
- Savin-Baden, M., & Mason-Robbie, V. (Eds.). (2020). *Digital afterlife: Death matters in a digital age*. CRC Press.
- Sherlock, A. (2013). Larger than life: Digital resurrection and the re-enchantment of society. *The Information Society*, 29(3), pp. 164–176.
- Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. John Murray.
- Schwab, K. (2016). *The fourth industrial revolution*. Crown publishing.
- Sentinel (2020, Oct). Deepfaked 2020: The tipping point: The current threat landscape, its impact on the U.S. 2020 elections, and the coming of AI-generated events at scale. [Report]. Retrieved from <https://thesentinel.ai/media/Deepfakes%202020:%20Tipping%20Point,%20Sentinel.pdf>
- Somers, M. (2020, Jul 21) Deepfakes, explained. *MIT Management Sloan School*. Retrieved from <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>
- Suchman, L. (2012, online publication), (2006, print publication). *Human-machine reconfigurations: Plans and situated actions*. Cambridge University Press.
- Talvitie-Lamberg, K. (2018). Video streaming and internalized surveillance. *Surveillance and Society*, 16(2).
- Tariq, S., Abuadbba, A. and Moore, K. (2023, July). Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices. *Proceedings of the 2nd Workshop on Security Implications of Deepfakes and Cheapfakes* (pp. 16–19). Retrieved from <https://doi.org/10.1145/3595353.3595880>
- Yu, P., Xia, Z., Fei, J. & Lu, Y. (2021). A survey on deepfake video detection. *IET Biometrics: The Institute of Engineering and Technology*. 10(6). 607–624.
- Watts, D. J. (2014). Common Sense and Sociological Explanations. *American Journal of Sociology*. 120(2): 313–351.
- Westling, J. (2019). Are Deep Fakes a Shallow Concern? A critical analysis of the likely societal reaction to deep fakes. *TPRC47: The 47th Research Conference on Communication, Information, and Internet Policy; 2019*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3426174](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3426174).
- Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York: The New Press.
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social media+ society*, 6(1), 2056305120903408.
- Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*. 30. 75–89.

### How cite this article

Doğan Akkaya, F. (2024). Deepfake dilemmas: imagine tomorrow's surveillance society through three scenarios. *Journal of Economy Culture and Society*, 70, 121-134. [10.26650/JECS2024-1462119](https://doi.org/10.26650/JECS2024-1462119)