Politics and Governance
2024 • Volume 12 • Article 8572
https://doi.org/10.17645/pag.8572

cogitatio

ARTICLE

Open Access Journal

Navigating Digital Privacy and Surveillance: Post-Covid Regulatory and Theoretical Insights

Karolina Małagocka

Department of Marketing, Kozminski University, Poland

Correspondence: Karolina Małagocka (kmalagocka@kozminski.edu.pl)

Submitted: 30 April 2024 **Accepted:** 19 August 2024 **Published:** 2 December 2024

Issue: This article is part of the issue "The Decline of Economic and Political Freedom After Covid-19: A New Authoritarian Dawn?" edited by Christopher A. Hartwell (ZHAW School of Management and Law / Kozminski University), fully open access at https://doi.org/10.17645/pag.i359

Abstract

The Covid-19 pandemic has highlighted and accelerated existing trends in digital privacy, intensifying the balance between public health needs and privacy rights. This article examines the concept of digital unfreedom and its growing relevance post-Covid-19, focusing on the balance between public health needs and privacy rights. It explores the evolution of digital freedom pre- and post-pandemic through four key concepts: control over personal information; freedom from surveillance; respectful data protection; and the right to bodily autonomy. Emphasizing the critical importance of privacy in public health strategies, this article calls for vigilant regulatory reforms to protect individual rights and ensure equitable data practices.

Keywords

data protection; digital unfreedom; personal information; privacy; privacy regulation

1. Introduction

The Covid-19 pandemic has significantly influenced the privacy landscape, necessitating a reevaluation of foundational privacy concepts amidst accelerating digitalization. This article focuses on the balance between digital privacy and surveillance in the post-Covid-19 era, emphasizing regulatory challenges and opportunities. Technologies such as contact-tracing apps have raised significant concerns regarding privacy and data misuse (Ahmad & Chauhan, 2020; AlFaadhel & Latif, 2022). The increased surveillance by governments and corporations has intensified these debates (Newell, 2021), highlighting the urgent need for balanced and adaptive privacy regulations. Before the Covid-19 pandemic, digital privacy was primarily concerned with the protection of personal data from unauthorized access and misuse, as articulated by scholars like Solove (2022) and Nissenbaum (2020). Privacy frameworks such as the General Data Protection

Regulation (GDPR) in the EU and the California Consumer Privacy Act in the US emphasize data minimization, consent, and individual rights to access and delete personal data. The pandemic has significantly influenced digital privacy, highlighting the importance of addressing both business and government access to personal data as governed by frameworks like the GDPR. The widespread use of digital surveillance tools during the pandemic has highlighted the need for adaptive privacy regulations that address both public health and personal freedom.

The Covid-19 pandemic has intensified the conflict between public health imperatives and individual privacy rights, leading to more sophisticated surveillance mechanisms (Mello & Parmet, 2021). Such practices, including the rapid deployment of surveillance technologies and expanded data collection during the pandemic, underscore the urgent need for balanced and adaptive privacy regulations to prevent misuse and protect individual rights. Digital infrastructures enable extensive monitoring, leading to new forms of resistance and illustrating the dual-edged nature of digitalization in surveillance. The pandemic accelerated the integration of AI and medical research technologies, exposing vulnerabilities in existing privacy frameworks and intensifying the reliance on digital technologies in daily life. It is imperative that these regulations delicately balance civil liberties with the pressing needs of public health security in the digital era (Li et al., 2023; Newlands et al., 2020; Schmit et al., 2022).

The pandemic has revealed significant gaps in existing privacy regulations. The convenience and efficiency of digital monitoring may tempt authorities to extend their use beyond immediate health emergencies, potentially establishing a new norm in surveillance practices (Donelle et al., 2023; A. Ferretti & Vayena, 2022), highlighting the urgency for comprehensive privacy reforms to address new challenges. Literature reveals the significant regulatory and societal changes due to Covid-19, emphasizing the necessity for stringent privacy laws. These shifts highlight the increased relevance of digital unfreedom and the need for robust regulatory frameworks to protect digital rights in the post-pandemic world.

This article aims to delve into the significant shifts in the understanding of privacy and digital unfreedom resulting from the Covid-19 pandemic. By examining the increased integration of digital technologies in daily life and the corresponding expansion of governmental and private surveillance, the article aims to determine whether the concept of digital unfreedom has grown in relevance and necessity after the pandemic. To accomplish this, the article is organized to explore several key themes, beginning with the contextualization of privacy and digital unfreedom. Discussions will focus on the changes in privacy perception and the implications of enhanced digital surveillance. This sets the stage for a comprehensive examination of four pivotal privacy concepts: control over personal information; freedom from surveillance; respectful data protection; and the right to bodily autonomy. Each section will dissect existing regulatory frameworks, critique their effectiveness in the new normal, and suggest possible reforms. The culmination of this analysis will lead to a synthesis of the findings, where the balance between individual rights and collective health needs will be debated, and legislative and policy recommendations to safeguard privacy in a post-pandemic world will be proposed. This structured exploration aims to provide a nuanced perspective on privacy, emphasizing the need for updated, resilient privacy legislation addressing the complexities introduced by digital technologies and global health emergencies.

2. Contextualization of Privacy and Digital Unfreedom

The Covid-19 pandemic has drastically altered the digital landscape by accelerating the use of surveillance tools such as contact-tracing apps and digital health passports, raising significant privacy concerns (Bennett, 2023; Meireles, 2024). Digital unfreedom reflects the expanded surveillance capabilities that undermine privacy. The pandemic has particularly highlighted how enhanced monitoring capabilities can infringe on individual privacy and freedom (Eck & Hatz, 2020; Taylor et al., 2020). Digital unfreedom is characterized by pervasive data collection, erosion of privacy, and potential misuse of surveillance technologies (Rusinova, 2022). Surveillance tools, including mobile tracking apps, digital health monitoring systems, and biometric data collection technologies, pose significant privacy risks and can lead to data abuse. Concurrently, there is a recognized need for robust privacy protections to balance these developments and protect individual freedoms (Panneer et al., 2021). The literature suggests that while digital technologies offer numerous benefits, they also pose significant risks to privacy and autonomy, necessitating a careful and balanced approach to regulation and oversight (Meireles, 2024).

The varied approaches to digital surveillance and data privacy during the pandemic underscore the importance of robust regulatory frameworks. China's case demonstrates the dual nature of digital surveillance technologies, enhancing state control and public health monitoring while posing risks to individual freedoms (Hillman, 2021). Conversely, the European experience with GDPR illustrates the advantages of a unified approach to data protection, emphasizing transparency, accountability, and individual control over personal data (Georgiadis & Poels, 2022). Future policies must balance public health needs with privacy protections, ensuring transparency and robust security measures (Renda, 2022). The pandemic has highlighted the critical need for updated and resilient privacy regulations by global entities such as the EU and national governments including China. By learning from different regulatory approaches and their impacts on digital freedom and privacy, policymakers can better navigate the challenges of the digital age. In non-democratic regimes, such as China, where the rule of law differs significantly from the EU and other democracies, digital privacy is often subordinated to state control and surveillance, whereas in democratic societies, privacy rights are emphasized, though the pandemic has tested these frameworks (Hillman, 2021). The Personal Information Protection Law (PIPL) in China, while progressive in some respects, still allows significant government access to personal data (Calzada, 2022). Conversely, democratic societies tend to emphasize individual privacy rights and transparency. The GDPR in Europe sets a high standard for data protection, emphasizing user consent and control over personal data (Georgiadis & Poels, 2022). However, even in democracies, the pandemic has tested these frameworks, as seen with the rapid implementation of contact-tracing apps and other surveillance measures (Sideri & Prainsack, 2023).

3. Concepts for Understanding Privacy

3.1. Control Over Personal Information

Control over personal information refers to individuals' ability to manage and regulate the disclosure and use of their personal data. In the EU, this control is a cornerstone of data protection, particularly emphasized through regulations like the GDPR, which focus on safeguarding digital information. In contrast, the US approach to privacy is broader, encompassing both digital and non-digital information, with a mix of federal and state

laws that address different aspects of privacy (Cloarec et al., 2022; Lazaro & Metayer, 2015; C. Prince, 2018; Shulman & Meyer, 2022).

Autonomy allows individuals to control their data usage and sharing, protecting privacy and personal dignity, and setting boundaries on access (Andorno, 2022; Lundgren, 2020; Miraut Martín, 2021). However, effectively managing personal data is challenging due to opaque and complex privacy policies. This challenge is exacerbated by the varying definitions and expectations of "privacy" and "data protection" across different regions like the US and EU. The digital environment further complicates control, making effective management difficult and necessitating clear, region-specific guidelines (Fleming et al., 2023).

The Covid-19 pandemic highlighted the urgency of robust privacy controls, as public health measures like contact tracing required extensive data collection. This situation underlined the necessity for privacy frameworks that can adapt to the unique demands of unprecedented circumstances (Bradford et al., 2020; Martinez-Martin et al., 2020; Sharon, 2021). The pandemic also drastically increased reliance on digital technologies for remote work, education, and health monitoring, leading to a significant increase in data sharing and collection. These developments further emphasized the need for updated privacy frameworks that can address these new realities.

Contact-tracing apps and health monitoring tools have raised significant privacy concerns, underscoring the importance of robust controls and transparent data management practices. While the GDPR provides comprehensive protection for commercial data practices, it does not typically cover government access to personal data, which remains a significant concern. This access is governed separately by national laws within EU member states, highlighting the need for a more integrated regulatory approach. Government surveillance issues are often regulated at the national level in EU member states, as seen in France's state of emergency post-2015 Paris attacks. Furthermore, GDPR primarily regulates commercial data practices and does not apply to law enforcement uses of data, which are governed by national laws within EU member states.

The importance of robust regulatory frameworks has become increasingly apparent. The GDPR in the EU sets a high standard for data protection, emphasizing transparency, accountability, and individual control. GDPR has reshaped data handling in Europe, requiring clear consent and granting individuals extensive rights over their data (Mazurek & Małagocka, 2019; McLennan et al., 2020; Schäfer et al., 2023). In contrast, the US employs a sector-based approach to data protection, focusing primarily on businesses through various federal and state-level regulations, while government surveillance is regulated through separate legal frameworks (e.g., the USA PATRIOT Act). This approach reflects the varied and fragmented nature of privacy regulation in the US, highlighting the distinction between commercial data protection and government surveillance.

China's PIPL is often compared to GDPR but reflects China's unique socio-political context of state surveillance (Calzada, 2022; Determann et al., 2021). Enforcement and practical application remain concerns, particularly regarding state access to data. Other regions, such as parts of Asia and Latin America, have also been influenced by GDPR. For instance, Japan and South Korea have strengthened their data protection laws to align with GDPR standards, partly to facilitate trade with Europe (Rana et al., 2021). Brazil's General Data Protection Law mirrors GDPR principles, providing comprehensive rights and imposing strict obligations (J. T. Prince & Wallsten, 2022; Pool et al., 2024).

In democratic countries, adopting GDPR-like frameworks involves transparent legislative processes and engagement with civil society. These countries typically have robust legal systems ensuring the enforcement of data protection laws and respect for privacy rights. Japan and South Korea's regulations, for example, align with GDPR standards, reflecting commitments to human rights and international norms. Non-democratic countries face challenges in adopting similar measures due to weaker rule of law protections and state interests in surveillance. While China's PIPL includes GDPR-like provisions, its implementation is complicated by the government's surveillance priorities (Calzada, 2022). Nonetheless, international pressure and trade considerations can drive incremental improvements in data protection in these contexts.

Enhancing global data management requires improving encryption, secure data processing, and strengthening regulatory frameworks. Harmonizing privacy laws globally would provide a consistent environment for businesses and consumers, ensuring robust privacy protection (Andrew & Baker, 2021; Brough & Martin, 2021; Solove, 2022). Ongoing dialogue between policymakers, businesses, and civil society is essential to align regulations with technological advancements and societal expectations.

In conclusion, as the digital landscape evolves, data privacy frameworks must adapt. Drawing from successful models like GDPR while addressing unique regional challenges can help develop a cohesive global approach. Ensuring robust data protection supports autonomy, fosters trust, and promotes a fair digital future. Establishing predictable regulatory schemes for businesses is an additional benefit, enhancing global trade and economic stability while safeguarding individual privacy rights.

3.2. Freedom From Surveillance

Surveillance traditionally involves the monitoring, tracking, and recording of individuals' behaviors and activities by governmental organizations to ensure public safety, enforce laws, or collect data for administrative purposes. Before the Covid-19 pandemic, surveillance was often perceived through the lens of security versus privacy, with debates centered on the extent to which governments should monitor individuals to prevent crime and terrorism without infringing on personal privacy (Friedewald et al., 2017; Marwick, 2022; Nissenbaum, 2020). The pandemic has introduced new tracking technologies for public health, raising long-term privacy and freedom concerns. This necessitates a nuanced approach to balancing public health and individual privacy rights (Andrew & Baker, 2021; Marwick, 2022).

In the EU, the legal framework regarding surveillance is tightly regulated under the GDPR, which provides stringent guidelines on data minimization, purpose limitation, and individual consent. GDPR emphasizes that surveillance must be necessary, proportionate, and transparent (Aho & Duffield, 2020; Georgiadis & Poels, 2022). In contrast, the US has a patchwork of federal and state laws providing varying degrees of protection against surveillance. US federal and state laws grant varying degrees of protection against surveillance, with recent efforts focusing primarily on strengthening consumer privacy rights rather than addressing government surveillance comprehensively.

China presents a contrasting scenario where surveillance is extensively integrated into public safety and governance. The Chinese government employs a vast network of CCTV cameras equipped with facial recognition technology, alongside a robust legal framework that includes the Cybersecurity Law and the PIPL. While these laws regulate data handling and aim to protect personal information, they also allow for

significant government access to data, raising concerns about abuses of power and infringements on individual privacy (Aho & Duffield, 2020; Pernot-Leplay, 2020).

Technological advancements have significantly increased surveillance capabilities, challenging privacy. Facial recognition technology, for instance, analyzes facial features from video feeds in real-time to match them against a database of known faces. Its use has become common in areas like shopping centers, transport hubs, and city streets, tracking everything from criminals to pedestrian traffic patterns. The erosion of anonymity through facial recognition is profound; individuals can no longer assume anonymity in public spaces (Hassandoust et al., 2021; Kostka et al., 2021; Smith & Miller, 2022). This has significant implications for personal privacy and the collective freedom to assemble without being monitored. Furthermore, these technologies often operate without clear signage or explicit consent from those being observed, leading to covert surveillance (Waelen, 2023).

CCTV systems equipped with advanced analytical capabilities take surveillance a step further. Modern CCTV systems are not just passive recording devices but are equipped with software that can analyze video footage for specific behaviors, emotions, and even group interactions. These systems can trigger alerts for unusual activities, enabling a proactive approach to surveillance. However, continuous monitoring and analysis of public behaviors can create a society where every action is recorded and scrutinized, leading to a chilling effect on free expression and behavior in public areas (Murray, 2023; Stoycheff et al., 2019). These systems are often integrated with other data sources, such as social media, public records, and commercial databases, creating comprehensive profiles of individuals that detail their habits, routines, and personal preferences. This integration can lead to significant privacy loss, as aspects of an individual's life that they may not choose to disclose are nonetheless observed and recorded (Connor & Doan, 2021; Marwick, 2022).

The use of mobile location data for contact tracing during the Covid-19 pandemic illustrated another dimension of surveillance. Mobile devices, carried by virtually every adult and many children, became tools for public health monitoring. Apps designed for contact tracing could track the spreading of the virus by monitoring the movements of individuals and their interactions with others (Juneau et al., 2023; Li et al., 2023). While these measures were essential for managing the pandemic, they also demonstrated how quickly and extensively personal devices could be used to monitor individuals. The deployment of such technology has raised concerns about its potential misuse. Originally intended for contact tracing, the technology could be used for more invasive forms of surveillance, such as tracking political affiliations, attendance at events, or adherence to government mandates. Repurposing health data for surveillance purposes without stringent safeguards could lead to significant intrusions into personal privacy (Miao et al., 2024; Searight, 2024).

As these technologies become more embedded in everyday life, the potential for overreach presents a clear and present threat to personal freedoms. To navigate this landscape effectively, robust frameworks are needed to regulate the use of such technologies. These should ensure transparency in how data is collected, stored, and used, and provide individuals with the right to opt-out of non-essential tracking. Moreover, public awareness and understanding of these technologies and their potential impacts are crucial for fostering informed consent and ensuring that surveillance tools are used responsibly and ethically.

3.3. Respectful Data Protection: Ensuring Dignity and Equity in Data Practices

Respectful data protection goes beyond traditional privacy boundaries to incorporate broader considerations of dignity, fairness, and transparency in handling personal data. It emphasizes ethical standards and respect for individual autonomy in data practices, advocating for a holistic approach where data protection is not solely about securing data from unauthorized access but also about ensuring that data usage aligns with the expectations and well-being of the data subjects (Bennett Moses & Weatherall, 2023).

The Covid-19 pandemic has underscored the critical importance of transparency in data practices. Before the pandemic, transparency primarily focused on informing users about the collection and use of their data, often in commercial contexts. However, the pandemic broadened the scope of transparency to include how personal data is utilized in public health initiatives (Yang et al., 2020). Regulatory changes pushed for greater transparency in handling personal data by governments and health organizations, including detailed disclosures about the purposes of data collection, entities involved, and measures to protect data privacy. This shift aims to build public trust and encourage participation in health monitoring programs critical for managing public health responses. Transparency empowers individuals with knowledge about how their data is handled, enabling informed decisions regarding their personal information. Transparent practices ensure awareness and understanding of data use implications, essential for maintaining public trust and compliance with data protection laws (Olorunfemi et al., 2024; Redmiles, 2022).

The GDPR in the EU is a cornerstone example of respectful data protection influencing global data privacy practices. GDPR emphasizes consent, transparency, and the right to privacy, setting a robust standard for data practices worldwide. It requires clear information about data processing activities and explicit consent from data subjects, ensuring understanding and agreement on data use. GDPR sets a transparency standard in data protection, specifying the legal basis for data processing, storage duration, and rights available to individuals, ensuring respect for individual dignity and preferences (Lancieri, 2022; Tzanou, 2023).

The pandemic challenged the resilience and adaptability of data protection regulations like GDPR. Implementing contact-tracing apps and health data analytics necessitated a reevaluation of privacy norms to balance public health objectives with transparency and ethical data usage (Goetzen et al., 2021; Sideri & Prainsack, 2023). Respectful data protection emerged as a critical concept in privacy discussions, reflecting a recognition that protecting privacy involves ensuring fair, transparent data use aligned with individual expectations and rights. Respectful data protection empowers individuals with control over their personal information, ensuring data use respects privacy and broader human rights (Akinsanmi & Salami, 2021).

The pandemic highlighted the importance of flexible yet robust data protection regulations to accommodate emergency public health measures while upholding strong privacy standards. It stressed maintaining a balance between public health security and individual privacy rights through transparent and respectful data handling practices (Campbell-Verduyn & Gstrein, 2024; Liu et al., 2023). During the pandemic, public compliance with health monitoring efforts heavily depended on trust, contingent upon transparency concerning data use, access, and protective measures (Houser & Bagby, 2023; Stalla-Bourdillon et al., 2020). The crisis catalyzed more stringent and clear regulations around data usage during emergencies, enhancing legal frameworks to ensure respectful and ethical handling of data collected for public health purposes. These adjustments set new precedents for personal data use in crises, emphasizing the need for regulations

that dynamically balance public health needs with privacy protections. They demonstrated that respectful data protection fosters a societal framework supporting ethical data usage in critical situations.

3.4. Right to Bodily Autonomy

Bodily autonomy is the right of individuals to make decisions over their own bodies without external interference. Traditionally rooted in healthcare and human rights, this concept has evolved significantly with digital technologies capable of monitoring biological parameters (Ferdowsian, 2020; Trauner, 2024). Bodily autonomy emphasizes control of personal health data, which is increasingly challenged by modern technologies. The proliferation of wearable technology, such as fitness trackers and smartwatches, impacts bodily autonomy by monitoring health metrics like heart rate and sleep patterns. While beneficial for personal health management, these devices pose privacy risks as they collect sensitive data that could be accessed by unauthorized parties. Similarly, advancements in medical technology, such as remote monitoring devices, improve patient care but raise concerns about data security and misuse.

The Covid-19 pandemic catalyzed the expanded use of technologies that monitor bodily functions for public health surveillance. Governments and health organizations employed contact-tracing apps and thermal scanners to track virus spread. While essential for public health, these technologies raised privacy concerns. Digital contact-tracing apps highlighted the tension between collective health benefits and individual privacy rights, collecting data on movements and interactions and posing risks of misuse (L. Ferretti et al., 2024; Gerke et al., 2020).

The ethical implications of technologies affecting bodily autonomy necessitate robust privacy protections and transparent data handling practices (Blasimme & Vayena, 2020; L. Ferretti et al., 2024). Concerns about "function creep," where health data collected during a pandemic is later used for intrusive surveillance or commercial exploitation without consent, have grown (Colizza et al., 2021; Sweeney, 2020). The pandemic highlighted the need for stringent privacy protections and regulations tailored to health-related data. The collection or processing of health data during emergencies must be transparent, respect user consent, and adhere to principles of minimality and necessity (Blasimme & Vayena, 2020; L. Ferretti et al., 2024).

To respect and protect bodily autonomy in the digital age, comprehensive privacy frameworks must balance the benefits and risks of health monitoring technologies. These frameworks should ensure transparency in data collection, usage, and sharing, enabling informed decisions (Renda, 2022; Trauner, 2024). Consent mechanisms must be clear, informed, and easily revocable, allowing individuals to opt out without forfeiting essential services. Robust security measures are essential to protect data from unauthorized access and breaches, while stringent regulatory oversight is required to adapt laws to rapid technological advancements (Kwan, 2023; Montanari Vergallo et al., 2021).

In democratic countries, adopting GDPR-like frameworks involves transparent legislative processes and engagement with civil society. These countries typically have robust legal systems ensuring enforcement of data protection laws and respect for privacy rights. For instance, Japan's and South Korea's regulations align with GDPR standards, reflecting commitments to human rights and international norms. Non-democratic countries face challenges in adopting similar measures due to weaker rule of law protections and state interests in surveillance. While China's PIPL includes GDPR-like provisions, its implementation is complicated

by the government's surveillance priorities (Calzada, 2022). Nonetheless, international pressure and trade considerations can drive incremental improvements in data protection in these contexts. Furthermore, international collaboration through organizations like the OECD and the UN, which have a special rapporteur for privacy, can help develop global standards for data protection and privacy ethics. These efforts should focus on aligning ethical standards across nations while respecting local contexts (Robinson et al., 2021).

The interconnection between bodily autonomy and other privacy concepts, such as control over personal information and freedom from surveillance, is evident. Control over health data is fundamental to personal autonomy and privacy. This requires robust regulatory frameworks similar to those for personal information and surveillance. The transparency and ethical considerations essential for respectful data protection are equally critical for bodily autonomy. Handling health data with dignity and fairness aligns with the principles of respectful data protection, creating a cohesive framework that upholds human rights in the digital age. The Covid-19 pandemic highlighted the need for enhanced data protection and underscored the interconnected nature of privacy rights. As technology advances, balancing public health advancements with safeguarding individual rights becomes paramount. A holistic approach integrating principles from control over personal information, freedom from surveillance, and respectful data protection is essential to uphold bodily autonomy.

4. Discussion: Integrating Privacy Concepts in the Context of Digital Transformation

The reviewed literature underscores the profound impact of Covid-19 on digital freedom, revealing significant regulatory, societal, and technological changes. These shifts highlight the increased relevance of digital unfreedom and the urgent need for robust regulatory frameworks to protect digital rights in the post-pandemic world. It is crucial for future policies to balance public health needs with privacy protections, ensuring a transparent, accountable, and secure approach to data management. In developed societies, advanced digital infrastructures have facilitated sophisticated surveillance and data collection mechanisms. These societies, exemplified by the EU and the US, have established comprehensive privacy regulations like the GDPR and the California Consumer Privacy Act (Chander et al., 2020; Naqvi & Batool, 2023). However, the pandemic revealed gaps in these frameworks, prompting calls for more resilient and adaptive privacy protection (McLennan et al., 2020). Less digitally developed societies face unique challenges in balancing digital privacy with technological advancement. These regions often lack robust legal frameworks for data protection, making them more vulnerable to privacy breaches and surveillance abuses (Ehimuan et al., 2024). The pandemic highlighted the need for international cooperation and support to develop effective privacy regulations that can protect citizens' rights in these contexts (Rana et al., 2021).

Balancing security and privacy is critical, especially as the pandemic underscored the need for public health measures that can infringe on personal privacy (Acquisti et al., 2020; Filip, 2022). The goal is to create an adaptable equilibrium that responds to evolving threats and technological advancements. Digital tools like contact-tracing apps have shown public health benefits but also raised concerns about surveillance and data collection. The challenge lies in creating a dynamic equilibrium that can adapt to the evolving landscape of threats and technological advancements. Continuous assessment and adaptation of privacy laws and regulations are required to ensure privacy is protected without stifling innovation or compromising public health and safety. To navigate these challenges, a comprehensive approach to privacy and data protection is essential, integrating the principles of control over personal information, freedom from surveillance,

respectful data protection, and the right to bodily autonomy. Each of these principles addresses a critical aspect of digital freedom and privacy, and together they form a cohesive framework for future policymaking.

Control over personal information emphasizes the individual's right to manage and regulate their personal data, ensuring autonomy in the digital age. Robust privacy controls and transparent data management practices are essential to empower individuals and protect their dignity (Cloarec et al., 2022; Shulman & Meyer, 2022). Meanwhile, *freedom from surveillance* highlights the need to protect individuals from intrusive monitoring by state and non-state actors, advocating for stringent regulations to ensure that surveillance practices are necessary, proportionate, and transparent, thus safeguarding civil liberties (Marwick, 2022; Nissenbaum, 2020). *Respectful data protection*, focusing on ethical standards and fairness in data practices, calls for transparency in data handling to ensure individuals are informed about how their data is used and that their rights are respected, building trust and encouraging participation in digital health initiatives (Bennett Moses & Weatherall, 2023). Lastly, the *right to bodily autonomy* underscores the critical importance of individuals making decisions about their bodies and health data without external interference. The pandemic has underscored the need for clear consent mechanisms and robust security measures to protect sensitive health information, ensuring that health data collection and usage adhere to principles of minimality and necessity (Ferdowsian, 2020; Trauner, 2024). Integrating these principles forms a comprehensive framework that addresses the multifaceted challenges of digital privacy, promoting a balanced approach that upholds human dignity and autonomy in the digital age. Future policies must consider technology's broader implications on society, ensuring digital advancements are matched with progressive privacy protections. Policymakers, technology developers, and civil society must collaborate to craft policies that address the nuanced implications of digital technologies. Education and awareness programs are equally important to empower users to understand and exercise their privacy rights effectively.

The integration of these four principles—control over personal information, freedom from surveillance, respectful data protection, and the right to bodily autonomy—into a unified framework will help ensure that digital technologies serve the public good without compromising fundamental human rights. As we move further into the digital age, these principles will guide the development of a society that values both technological advancements and fundamental human rights. The ongoing discourse on privacy, intensified by the pandemic, will likely continue to evolve, reflecting the complex relationship between technology, privacy, and society. By adopting a balanced approach that safeguards privacy while addressing public health needs, future regulatory frameworks can protect individual rights and promote trust in digital systems, ultimately fostering a fair and equitable digital future.

5. Conclusions

The Covid-19 pandemic has catalyzed substantial changes in the perception and regulation of digital freedom. This article has highlighted key literature illustrating these shifts, emphasizing the need for ongoing vigilance and adaptation of regulatory frameworks to protect digital rights in an increasingly digital world. Contact tracing, essential for containing the virus, has highlighted significant privacy risks, necessitating rigorous policy frameworks to ensure transparency and protection of sensitive information. Pandemic responses have increased data collection, compromising privacy and shifting towards digital surveillance and broad data-sharing, weakening safeguards for sensitive information. These observations underscore the urgent need to reform privacy laws to address pandemic-related challenges.

Understanding the intersection of privacy and public health during the pandemic is crucial for future policies. This involves developing privacy-preserving strategies that effectively balance public health responses without compromising privacy protections. Further research is needed to explore privacy-preserving techniques in pandemic response and to ensure that future digital health strategies are built on robust, transparent, and accountable frameworks. Integrating the principles of control over personal information, freedom from surveillance, respectful data protection, and the right to bodily autonomy is essential.

Control over personal information ensures individuals' right to manage and regulate their personal data, providing autonomy in the digital age. *Freedom from surveillance* protects individuals from intrusive monitoring, advocating for necessary, proportionate, and transparent surveillance practices. *Respectful data protection* emphasizes ethical standards and fairness, ensuring individuals are informed about their data use, building trust, and encouraging participation in digital health initiatives. Lastly, the *right to bodily autonomy* underscores the importance of individuals making decisions about their bodies and health data without external interference.

By adopting a balanced approach that regulates business access to personal data, as exemplified by the GDPR, while also addressing the complexities of government access, future regulatory frameworks can protect individual rights and promote trust in digital systems. These principles together form a cohesive framework that promotes human dignity and autonomy in the digital age, ensuring digital technologies serve the public good without compromising fundamental human rights. The ongoing discourse on privacy, intensified by the pandemic, will likely continue to evolve, reflecting the complex relationship between technology, privacy, and society.

Conflict of Interests

The author declares no conflict of interests.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, *30*(4), 736–758.

Ahmad, N., & Chauhan, P. (2020). State of data privacy during Covid-19. *Computer*, *53*(10), 119–122.

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187–212.

Akinsanmi, T., & Salami, A. (2021). Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic. *Data & Policy*, *3*, Article e27.

AlFaadhel, A., & Latif, R. (2022). Privacy concerned on contact-tracing application during Covid-19. In *2022 Fifth international conference of women in data science at Prince Sultan University (WiDS PSU)* (pp. 143–145). IEEE.

Andorno, R. (2022). Human dignity, life sciences technologies and the renewed imperative to preserve human freedom. In M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, & R. Andorno (Eds.), *The Cambridge handbook of information technology, life sciences and human rights* (pp. 273–285). Cambridge University Press.

Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*, 565–578.

Bennett, W. L. (2023). Killing the golden goose? A framework for regulating disruptive technologies. *Information, Communication & Society*, *26*(1), 16–36.

Bennett Moses, L., & Weatherall, K. G. (2023). *Data problems and legal solutions*: *Some thoughts beyond privacy* (UNSW Law Research Paper No. 23-21). Data and the Digital Self: What the 21st Century Needs (Australian Computer Society, 2023).

Blasimme, A., & Vayena, E. (2020). What's next for Covid-19 apps? Governance and oversight. *Science*, *370*(6518), 760–762.

Bradford, L., Aboy, M., & Liddell, K. (2020). COVID-19 contact tracing apps: A stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, *7*(1), 1–34.

Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the Covid-19 pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108–110.

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150.

Campbell-Verduyn, M., & Gstrein, O. J. (2024). Limits and lessons of Covid-19 apps. In C. Egger, R. Magni-Berton, & E. de Saint-Phalle (Eds.), *Covid-19 containment policies in Europe* (pp. 115–132). Springer Nature.

Chander, A., Kaminski, M. E., & McGeveran, W. (2020). Catalyzing privacy law. *Minnesota Law Review*, *105*, 1733–1802.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, *39*(3), 647–661.

Colizza, V., Grill, E., Mikolajczyk, R., Cattuto, C., Kucharski, A., Riley, S., Kendall, M., Lythgoe, K., Bonsall, D., Wymant, C., Abeler-Dörner, L., Ferretti, L., & Fraser, C. (2021). Time to evaluate Covid-19 contact-tracing apps. *Nature Medicine*, *27*(3), 361–362.

Connor, B. T., & Doan, L. (2021). Government and corporate surveillance: Moral discourse on privacy in the civil sphere. *Information, Communication & Society*, *24*(1), 52–68.

Determann, L., Ruan, Z. J., Gao, T., & Tam, J. (2021). China's draft personal information protection law. *Journal of Data Protection & Privacy*, *4*(3), 235–259.

Donelle, L., Comer, L., Hiebert, B., Hall, J., Shelley, J. J., Smith, M. J., Kothari, A., Burkell, J., Stranges, S., Cooke, T., Shelley, J. M., Gilliland, J., Ngole, M., & Facca, D. (2023). Use of digital technologies for public health surveillance during the Covid-19 pandemic: A scoping review. *Digital Health*, *9*. https://doi.org/10.1177/20552076231173220

Eck, K., & Hatz, S. (2020). State surveillance and the Covid-19 crisis. *Journal of Human Rights*, *19*(5), 603–612.

Ehimuan, B., Chimezie, O., Akagha, O. V., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070.

Ferdowsian, H. (2020). The right to bodily sovereignty and its importance to mental and physical well-being. In L. S. M. Johnson, A. Fenton, & A. Shriver (Eds.), *Neuroethics and nonhuman animals* (pp. 255–270). Springer.

Ferretti, A., & Vayena, E. (2022). In the shadow of privacy: overlooked ethical concerns in Covid-19 digital epidemiology. *Epidemics*, *41*, Article 100652.

Ferretti, L., Wymant, C., Petrie, J., Tsallis, D., Kendall, M., Ledda, A., Di Lauro, F., Fowler, A., Di Francia, A., Panovska-Griffiths, J., Abeler-Dörner, L., Charalambides, M., Briers, M., & Fraser, C. (2024). Digital measurement of SARS-CoV-2 transmission risk from 7 million contacts. *Nature*, *626*(7997), 145–150.

Filip, K., & Albrecht, K. (2022). Regulating harm: Tensions between data privacy and data transparency. *Journal of Regulatory Compliance*, *8*, 115–131.

Fleming, P., Edwards, S. G., Bayliss, A. P., & Seger, C. R. (2023). Tell me more, tell me more: Repeated personal data requests increase disclosure. *Journal of Cybersecurity*, *9*(1), Article tyad005.

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R., & Peissl, W. (Eds.). (2017). *Surveillance, privacy and security*. Taylor & Francis.

Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, *44*, Article 105640.

Gerke, S., Shachar, C., Chai, P. R., & Cohen, I. G. (2020). Regulatory safety and privacy concerns of home monitoring technologies during Covid-19. *Nature Medicine*, *26*(8), 1176–1182.

Goetzen, A., Dooley, S., & Redmiles, E. M. (2021). *Ctrl-Shift: How privacy sentiment changed from 2019 to 2021* (arXiv:2110.09437v2). arXiv.

Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2021). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, *28*(3), 463-471.

Hillman, J. E. (2021). *The digital silk road: China's quest to wire the world and win the future*. Profile Books.

Houser, K. A., & Bagby, J. W. (2023). The data trust solution to data sharing problems. *Vanderbilt Journal of Entertainment and Technology Law*, *25*(1), 113–180.

Juneau, C. E., Briand, A. S., Collazzo, P., Siebert, U., & Pueyo, T. (2023). Effective contact tracing for Covid-19: A systematic review. *Global Epidemiology*, *5*, Article 100103.

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, *30*(6), 671–690.

Kwan, T. H. (2023). comparative analysis of Digital Contact-Tracing Technologies for Informing Public Health Policies. *Engineering Proceedings*, *55*(1), Article 5.

Lancieri, F. (2022). Narrowing data protection's enforcement gap. *Maine Law Review*, *74*(1), 15–72.

Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale? *SCRIPTed*, *12*(1), 3–34.

Li, C., Li, H., & Fu, S. (2023). Coping with Covid-19 using contact tracing mobile apps. *Industrial Management & Data Systems*, *123*(5), 1440–1464.

Liu, E., Rao, S., Havron, S., Ho, G., Savage, S., Voelker, G. M., & McCoy, D. (2023). No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*, *2023*(1), 207–224.

Lundgren, B. (2020). A dilemma for privacy as control. *The Journal of Ethics*, *24*(2), 165–175.

Martinez-Martin, N., Wieten, S., Magnus, D., & Cho, M. K. (2020). Digital contact tracing, privacy, and public health. *Hastings Center Report*, *50*(3), 43–46.

Marwick, A. (2022). Privacy without power: What privacy research can learn from surveillance studies. *Surveillance & Society*, *20*(4), 397–405.

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344–364.

McLennan, S., Celi, L. A., & Buyx, A. (2020). Covid-19: Putting the General Data Protection Regulation to the test. *JMIR Public Health and Surveillance*, *6*(2), Article e19279.

Meireles, A. V. (2024). Digital rights in perspective: The evolution of the debate in the Internet Governance Forum. *Politics & Policy*, *52*(1), 12–32.

Mello, M. M., & Parmet, W. E. (2021). Public health law after Covid-19. *New England Journal of Medicine*, *385*(13), 1153–1155.

Miao, J., Wang, Z., Wu, Z., Ning, X., & Tiwari, P. (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Systems with Applications*, *237*, Article 121329.

Miraut Martín, L. (2021). New realities, new rights: Some reflections on the need to safeguard personal data. In L. Miraut Martín & Zalucki, M. (Eds.), *Artificial Intelligence and Human Rights* (pp. 24–47). Dykinson.

Montanari Vergallo, G., Zaami, S., & Marinelli, E. (2021). The COVID-19 pandemic and contact tracing technologies, between upholding the right to health and personal data protection. *European Review for Medical and Pharmacological Sciences*, *25*(5), 2449–2456.

Murray, D. (2023). Adapting a human rights-based framework to inform militaries' artificial intelligence decision-making processes. *Louis ULJ*, *68*, 293–327.

Naqvi, S. K. H., & Batool, K. (2023). A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *4*(1), 326–332.

Newell, B. C. (2021). *Police visibility: Privacy, surveillance, and the false promise of body-worn cameras*. University of California Press.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), Article 2053951720976680.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In K. W. Miller & M. Taddeo (Eds.), *The ethics of information technologies* (pp. 141–178). Routledge.

Olorunfemi, O., Oyegoke, E. O., Abiodun, O. O., Kunle-Abioye, F. B., & Ayeni, B. A. (2024). Achieving a balance between ethical and legal obligations with regard to confidentiality and patient privacy. *Amrita Journal of Medicine*, *20*(3), 90–93.

Panneer, S., Kantamaneni, K., Pushparaj, R. R. B., Shekhar, S., Bhat, L., & Rice, L. (2021). Multistakeholder participation in disaster management—The case of the Covid-19 pandemic. *Healthcare*, *9*(2), Article 203.

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the US and the EU? *Penn State Journal of Law & International Affairs*, *8*, Article 49.

Pool, J., Akhlaghpour, S., & Burton-Jones, A. (2024). Unpacking the complexities of health record misuse: Insights from Australian health services. *Information Technology & People*. Advance online publication. https://doi.org/10.1108/ITP-12-2022-0931

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human–Computer Studies*, *110*, 21–32.

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms? *Journal of Economics & Management Strategy*, *31*(4), 841–861.

Rana, O., Llanos, J., & Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. *Academia Letters*, *2021*(April), 1–6.

Redmiles, E. M. (2022). The need for respectful technologies: Going beyond privacy. In H. Werthner, E. Prem, E. A. Lee, & C. Ghezzi (Eds.), *Perspectives on digital humanism* (pp. 309–313). Springer.

Renda, A. (2022). Covid-19 and privacy: A European dilemma. *Digital Policy, Regulation and Governance*, *24*(2), 109–117.

Robinson, L., Kizawa, K., & Ronchi, E. (2021). *Interoperability of privacy and data protection frameworks* (OECD Going Digital Toolkit Notes No. 21). OECD Publishing.

Rusinova, V. (2022). Privacy and the legalisation of mass surveillance: In search of a second wind for international human rights law. *The International Journal of Human Rights*, *26*(4), 740–756.

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, *66*(4), 493–504.

Schmit, C., Larson, B. N., & Kum, H. C. (2022). Data privacy in the time of plague. *Yale Journal of Health Policy, Law, and Ethics*, *21*(1), 152–227.

Searight, H. R. (2024). Ethical dilemmas and future implications of Covid-19. *Cambridge Scholars Publishing*.

Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, *23*(Suppl 1), 45–57.

Shulman, Y., & Meyer, J. (2022). Degrees of perceived control over personal information: Effects of information relevance and levels of processing. *IEEE Access*, *10*, 40596–40608.

Sideri, K., & Prainsack, B. (2023). Covid-19 contact tracing apps and the governance of collective action: Social nudges deliberation and solidarity in Europe and beyond. *Policy Studies*, *44*(1), 132–153.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, *37*, 167–175.

Solove, D. J. (2022). The limitations of privacy rights. *Notre Dame Law Review*, *98*(3), 975–1036.

Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*, *2*, Article e4.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), 602–619.

Sweeney, Y. (2020). Tracking the debate on Covid-19 surveillance tools. *Nature Machine Intelligence*, *2*(6), 301–304.

Taylor, L., Sharma, G., Martin, A., & Jameson, S. (Eds.). (2020). *Data justice and Covid-19: Global perspectives*. Meatspace Press.

Trauner, M. (2024). My body whose choice? A case for a fundamental right to bodily autonomy. *Brooklyn Law Review*, *89*(2), 643–679.

Tzanou, M. (2023). *Health data privacy under the GDPR: Big data challenges and regulatory responses*. Taylor & Francis.

Waelen, R. A. (2023). The struggle for recognition in the age of facial recognition technology. *AI and Ethics*, *3*(1), 215–222.

Yang, T., Shen, K., He, S., Li, E., Sun, P., Chen, P., Zuo, L., Hu, J., Mo, Y., Zhang, W., Zhang, H., Chen, H., & Guo, Y. (2020). *CovidNet: To bring data transparency in the era of Covid-19*. arXiv. https://doi.org/10.48550/arXiv.2005.10948

About the Author

Karolina Małagocka (PhD) is an assistant professor at Kozminski University, specializing in human behavior in cyberspace, particularly in the context of privacy. Her research explores the psychological and social aspects of digital privacy, consumer trust, and data security. With extensive experience in both academia and industry, Dr. Małagocka contributes valuable insights into how individuals interact with digital environments, emphasizing the importance of privacy in the evolving digital landscape. She holds a PhD in management and is a recognized expert in privacy and consumer behavior.