Proceeding of the International Conference on Law and Human Rights
Volume. 1, Number. 2, Year 2024
Page 94-99
Available online at: https://prosiding.appihi.or.id/index.php/ICLEHR

Digital Privacy and Human Rights : The Legal Challenges of Mass Surveillance

Miguel Torres[1*], Sofia Beatriz Mendoza[2]
[1,2] University of Batangas College of Law, Phillipines

Abstract: *The rise of mass surveillance technologies has raised significant concerns regarding digital privacy and human rights. This paper explores the legal implications of government surveillance programs and their impact on fundamental rights, such as freedom of expression and the right to privacy. Through a comparative analysis of data protection laws in different jurisdictions, this study assesses the balance between national security and individual rights in the digital age.*

Keywords: *digital privacy, mass surveillance, human rights law, data protection, freedom of expression*

1. INTRODUCTION

The rapid advancement of information technology has transformed various aspects of human life, providing convenience and efficiency in communication, commerce, and governance. However, these advancements also introduce serious concerns regarding digital privacy and the protection of human rights. One of the most pressing issues in this domain is mass surveillance conducted by governments and technology corporations under the pretext of national security and public order (Zuboff, 2019). This phenomenon has sparked debates on the extent to which surveillance practices should be regulated to safeguard individual freedoms while addressing security concerns.

Numerous studies have examined the implications of mass surveillance on human rights. Scholars argue that excessive surveillance measures often infringe on fundamental rights such as privacy, freedom of expression, and freedom of association (Deibert, 2019). While governments justify surveillance initiatives as necessary countermeasures against cyber threats and terrorism, human rights organizations emphasize that such practices may lead to unjustified intrusions and misuse of personal data (Richards, 2013). The European Court of Human Rights (ECHR) and the United Nations (UN) have expressed concerns over mass surveillance, urging the implementation of stronger legal frameworks to uphold privacy rights (UN General Assembly, 2013).

The existing legal frameworks governing digital surveillance vary across jurisdictions, reflecting different approaches to balancing security and privacy. For instance, the General Data Protection Regulation (GDPR) in the European Union (EU) establishes strict guidelines on data collection and processing, ensuring individuals' rights to privacy and transparency (European Commission, 2016). In contrast, laws such as the USA PATRIOT Act grant broad surveillance powers to law enforcement agencies, raising concerns about potential human rights violations (Solove, 2011). This disparity highlights

Received: October30, 2024; Revised: November 30, 2024; Accepted: December 18, 2024; Published: December 30, 2024

the necessity of a comprehensive legal approach to regulate digital surveillance in a manner that respects fundamental rights while addressing security needs.

Despite the growing body of literature on mass surveillance, a significant gap remains in understanding how international and domestic legal frameworks can be harmonized to create an effective balance between security and individual rights. Current research tends to focus on either the technical aspects of surveillance mechanisms or the ethical implications, but there is a lack of integrated studies that analyze both dimensions alongside legal considerations (Bauman et al., 2014). Addressing this gap is crucial to ensuring that technological advancements do not undermine democratic principles and human rights protections.

Therefore, this study aims to analyze the intersection of digital surveillance, security policies, and human rights by examining existing international and national legal frameworks. By identifying the strengths and weaknesses of current regulations, this research seeks to propose recommendations for developing a more balanced and ethical approach to digital surveillance. The findings will contribute to the broader discourse on cybersecurity, privacy laws, and human rights, offering valuable insights for policymakers, legal scholars, and technology stakeholders.

2. LITERATURE REVIEW

Several previous studies have discussed the impact of mass surveillance on human rights, including:

- UN Human Rights Convention – Establishes the right to privacy as part of human rights that must be protected by states.
- European Union General Data Protection Regulation (GDPR) – Regulation that provides protection for the use of personal data by government and private entities.
- USA Patriot Act – Expands the US government's authority to access individual data under the pretext of national security.
- Edward Snowden (2013) – Revealing the mass surveillance scandal by the NSA, which sparked a global debate about personal data protection.
- Zuboff, S. (2019), The Age of Surveillance Capitalism – Revealing how technology companies exploit user data for commercial and political interests.

From this various literature, it appears that mass surveillance has become a global issue that demands more attention from the legal and public policy side. These studies provide essential insights into how legal frameworks and ethical considerations intersect in

the realm of digital surveillance. They form the theoretical foundation for understanding the balance between security and individual rights, highlighting the urgency of addressing this issue in a comprehensive manner.

3. METHODOLOGY

This research employs a qualitative approach with a comparative analysis method to evaluate data protection policies across multiple jurisdictions. The study design includes document analysis, case studies, and secondary interview analysis.

- Document Analysis: Reviewing relevant laws and regulations concerning data protection and digital surveillance in various countries. Key legal instruments analyzed include the General Data Protection Regulation (GDPR) of the European Union, the USA PATRIOT Act, and China's Cybersecurity Law (European Commission, 2016; Solove, 2011).
- Case Studies: Examining significant cases of privacy rights violations due to mass surveillance, such as the Snowden revelations and mass data collection by intelligence agencies (Zuboff, 2019; UN General Assembly, 2013). Countries such as the United States, the European Union, and China serve as focal points for comparative analysis.
- Secondary Interviews: Utilizing reports from the United Nations, Amnesty International, and other human rights organizations to assess the broader implications of mass surveillance on privacy rights (Deibert, 2019; Richards, 2013).

Data analysis follows a thematic approach, categorizing findings into key themes such as legal protection measures, ethical considerations, and enforcement challenges. The study aims to provide a comprehensive understanding of how different jurisdictions regulate digital surveillance while balancing security concerns and individual rights.

4. RESULTS

From the research results, several main points were found regarding mass surveillance and its impact on human rights:

Violation of Privacy Rights

Many countries use surveillance technology without sufficient transparency (Greenwald, 2014). Large-scale data collection is often carried out without individual consent (Solove, 2021). Such practices raise concerns about the extent of state and corporate power over personal data (Zuboff, 2019).

Threats to Freedom of Expression

Close supervision can create a psychological effect that makes individuals afraid to express their opinions freely (Penney, 2017). Journalists and activists are often targets of surveillance under the pretext of national security (Privacy International, 2018).

Differences in Legal Approaches in Various Countries

- European Union: Implements strict policies towards data protection through GDPR (European Parliament, 2016).
- United States: Has regulations such as the Patriot Act that expand the government's surveillance powers (Lyon, 2015).
- China: Has a strict monitoring system integrated with the social credit system (Creemers, 2018).

The Role of Technology Companies

Companies like Google, Facebook, and Amazon collect and monetize user data on a massive scale (Zuboff, 2019). Unclear privacy policies often allow companies to share data with governments (Pasquale, 2015).

5. DISCUSSION

The research results show that although digital surveillance is often claimed to be aimed at enhancing national security, this practice often violates human rights principles (Deibert, 2020). In many countries, regulations governing digital surveillance are still not strong enough to protect individuals from abuse of power by the state or corporations (UNHRC, 2019).

One of the main challenges is how to balance national security interests with individual rights (Solove, 2021). The European Union with GDPR has provided an example of how strict policies can be implemented to protect personal data. However, other countries are still lagging behind in adopting similar regulations (Bennett & Raab, 2020).

Apart from that, transparency and accountability in digital supervision are still problems. Many countries do not have independent oversight mechanisms that can ensure that data collection is carried out in accordance with applicable laws (Privacy International, 2018). The findings also align with previous research by Lyon (2015) and Greenwald (2014), who emphasized that mass surveillance is often conducted without sufficient legal safeguards.

Implications

The results of this study contribute to both theoretical and applied perspectives. Theoretically, it strengthens the argument that privacy is a fundamental human right that requires robust legal protection (Warren & Brandeis, 1890). From an applied perspective, policymakers must consider stricter regulations and independent oversight mechanisms to prevent surveillance abuse (UNHRC, 2019).

6. CONCLUSION AND RECOMMENDATIONS

Mass surveillance in the digital era presents significant challenges in safeguarding human rights. Despite existing regulations designed to protect digital privacy, numerous legal loopholes still allow for the misuse of individual data. The findings of this study highlight that while digital surveillance is often justified under the premise of national security, it frequently leads to violations of privacy and freedom of expression. The discrepancies in legal frameworks across different jurisdictions further exacerbate these challenges, as seen in the European Union's strict GDPR policies compared to more invasive surveillance measures in countries like the United States and China.

To address these issues, several concrete steps must be taken to enhance digital privacy protection. Strengthening data protection regulations on a global scale is essential to ensure uniform safeguards against mass surveillance. Governments and technology companies must also prioritize transparency in their surveillance practices to maintain public trust and accountability. Additionally, establishing robust oversight mechanisms is crucial to prevent potential abuses of power and to uphold fundamental human rights.

While this study provides an in-depth analysis of the intersection between surveillance and human rights, its scope is limited by the availability of publicly accessible data and regional variations in legal enforcement. Future research should explore the effectiveness of international legal frameworks in mitigating surveillance-related human rights violations and investigate emerging technologies that could further impact digital privacy. By implementing stronger regulatory measures and promoting ethical surveillance practices, a balance between national security and individual freedoms can be achieved without compromising the core principles of human rights.

REFERENCE

Amnesty International. (2020). *Report on digital surveillance and human rights*.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121-144. https://doi.org/XXXXX

Deibert, R. J. (2019). *Reset: Reclaiming the internet for civil society*. House of Anansi.

European Commission. (2016). *General Data Protection Regulation (GDPR)*. Retrieved from https://eur-lex.europa.eu

European Parliament. (2016). *General Data Protection Regulation (GDPR)*.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Human Rights Watch. (2021). *State of surveillance report*.

Lyon, D. (2015). *Surveillance after Snowden*. Polity.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934-1965.

Snowden, E. (2019). *Permanent record*. Macmillan.

Solove, D. J. (2006). *Understanding privacy*. Harvard University Press.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

U.S. Congress. (2001). *USA Patriot Act*.

United Nations General Assembly. (2013). *The right to privacy in the digital age*. Retrieved from https://www.ohchr.org/en/issues/digitalprivacy

United Nations. (1948). *Universal Declaration of Human Rights*.

Westin, A. (1967). *Privacy and freedom*. Atheneum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.