https://doi.org/10.55843/SG243271b

LEGAL EVALUATION OF DATA PRIVACY AND SURVEILLANCE ISSUES

Dr. Janet Butukova

ABSTRACT

This article, titled The Legal Evaluation of Data Privacy and Surveillance Issues, examines the impact of data privacy and surveillance technologies on individuals' fundamental rights and freedoms in an era where digitalization is rapidly accelerating. The study begins by defining the concepts of data privacy and surveillance, emphasizing their relationship to the right to privacy.

The first section of the article discusses the threats posed to the right to privacy by digital-age technologies such as big data, artificial intelligence, and facial recognition systems. It highlights how these technologies are utilized both in democratic regimes to ensure public safety and in authoritarian regimes to restrict individuals' rights and freedoms. Existing international legal regulations governing the use of surveillance technologies are analyzed, with particular focus on frameworks established by the United Nations, the European Union, and the European Court of Human Rights (ECtHR). The adequacy of these regulations is critically examined.

Special emphasis is placed on the General Data Protection Regulation (GDPR) of the European Union and its provisions aimed at strengthening individuals' control over their personal data. The national data protection policies implemented under the GDPR in countries like Germany and France are detailed as examples of best practices in this field. However, the article underscores the inadequacy of these regulations in keeping pace with rapidly advancing technologies and emphasizes the necessity of enhancing them through global cooperation.

Another key focus of the article is the potential impact of surveillance technologies on human rights. In addition to the right to privacy, the study explores how surveillance technologies pose threats to fundamental rights such as freedom of expression and freedom of assembly. The discussion examines how living under the constant fear of being monitored weakens democratic participation and individual freedoms.

Finally, the article provides recommendations for strengthening the legal framework and ensuring that surveillance practices align with the principles of transparency and accountability. Proposals include establishing ethical and legal boundaries for artificial intelligence-based surveillance systems, creating independent oversight mechanisms, and raising public awareness. Additionally, the article emphasizes the critical importance of developing international data protection treaties and global standards to create a legal framework that aligns with the dynamics of the digital age.

This study offers a comprehensive examination of the existing legal and ethical challenges in balancing data privacy and surveillance technologies and proposes solutions within the framework of human rights protection.**Key words:** Sustainability, Occupational Safety, Personal Protective Equipment (PPE), Awareness, Safety Culture, Construction Sector.

Keywords: Data Privacy, Evaluation, Legal, Surveillance.

Dr. Janet BUTUKOVA
Vilnius University,
Faculty of Law

e-mail:
j.butukova@gmail.com

UDK: 342.738:004
342.738:681.51

Declaration of interest: The authors reported no conflict of interest related to this article.

Introduction

In the digitalized world, the concepts of data privacy and surveillance have become two critical issues directly affecting individuals' fundamental rights and freedoms. Data privacy refers to the protection of individuals' personal information from unauthorized access, misuse, or sharing. This concept is closely linked to the right to privacy and holds significant importance in the context of human rights protection (Westin, 1967). Surveillance, on the other hand, is a broader concept that involves monitoring and recording individuals' activities, behaviors, or communications. This practice has become increasingly prevalent, particularly through surveillance technologies employed by states and private sectors (Lyon, 2007). While surveillance practices are often legitimized on grounds of public security and national interests, they pose serious threats to individuals' freedoms and private lives (Solove, 2004).

The prominence of data privacy and surveillance is largely attributed to the rapid advancement of digital technologies and the onset of the big data era. Today, individuals share personal data with every action they take on digital platforms. These data are collected and processed through various sources, including social media usage, mobile applications, e-commerce platforms, and internet browsers (Zuboff, 2019). When this process occurs without individuals' consent or when the collected data are used unlawfully, violations of data privacy and the right to privacy ensue (Nuredin,2023a).

The acceleration of technological advancements and the increased capacity for data collection and processing have elevated surveillance practices to a new dimension. Technologies such as artificial intelligence, big data analytics, facial recognition systems, and the Internet of Things now enable a deeper analysis of individuals' private lives than ever before (Taylor, Floridi, & Van der Sloot, 2017). These developments have laid the groundwork for monitoring not only individuals' online activities but also their offline behaviors. For instance, facial recognition technologies can instantly track a person's physical location, while analyses of content shared on social media platforms can reveal detailed insights into a person's thoughts and social relationships (Privacy International, 2018).

These technological advancements have produced both positive and negative effects on human rights. On the one hand, technology provides

tools to more effectively protect human rights; on the other hand, it facilitates the proliferation of practices that threaten individuals' right to privacy. Under authoritarian regimes, technological surveillance tools are often employed to undermine individuals' freedom of expression, right to assembly, and private lives (Nuredin, 2023b). For example, censorship of social media platforms increases pressure on individuals' freedom of thought and expression, while mass surveillance practices enable continuous control over citizens' behaviors (Solove, 2004).

In democratic regimes, it is widely debated that the use of surveillance technologies should be restricted to legitimate purposes such as ensuring public safety and combating terrorism. However, even in such contexts, legal and ethical challenges frequently arise (Zuboff, 2019). When technology is not adequately regulated within a legal framework, it becomes impossible to safeguard individuals' fundamental rights, leaving them to live under constant surveillance anxiety. This reality resembles the dystopian vision of a perpetual surveillance society depicted in George Orwell's novel 1984.

This article aims to examine the issues of data privacy and surveillance from a legal perspective. It will evaluate existing national and international legal frameworks, particularly concerning the protection of individuals' right to privacy, and question their adequacy. Furthermore, the article will discuss legal and ethical approaches that can be applied to strike a balance between data privacy and surveillance (United Nations, 1948; European Union, 2016).

1. Data Privacy and the Right to Privacy: Legal Foundations and Principles

1.1. The Place of the Right to Privacy in Human Rights Law

The right to privacy is considered one of the cornerstones of human rights law. It ensures the protection of individuals from interference in their private lives and is explicitly defined and guaranteed in numerous international treaties. Notably, Article 8 of the European Convention on Human Rights (ECHR) explicitly addresses the right to privacy, ensuring respect for individuals' private and family life, home, and correspondence (Nuredin, 2022). This provision not only safeguards personal data but also restricts potential intrusions by states or third parties into individuals' private lives.

Article 8 of the ECHR encompasses both negative and positive obligations concerning the protection of privacy. Negative obligations require states to refrain from arbitrary interference in individuals' private lives, while positive obligations mandate states to implement effective legal measures to protect private life from interference by third parties (Westin, 1967). In this context, the protection of the right to privacy serves as a safeguard not only against state actions but also against practices carried out by the private sector.

Moreover, the right to privacy is clearly articulated in international instruments such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). These texts guarantee the privacy of individuals' private lives, family relations, homes, and communications, protecting them from arbitrary interference (United Nations, 1948). However, these provisions often fall short in addressing the new challenges posed by the digital age, necessitating continuous updates and reforms in this field (Nuredin,2023a).

1.2. Data Protection Regulations (GDPR and Examples from Germany and France)

One of the most pressing issues of the digital era is the violation of rights during the collection, processing, and storage of personal data. To address this, data protection regulations aim to ensure that personal information is handled lawfully while preventing potential violations of individual rights during these processes (European Union, 2016).

The European Union's General Data Protection Regulation (GDPR) is one of the most comprehensive frameworks for personal data protection on an international scale. GDPR establishes the fundamental principles for the collection, processing, and storage of personal data and imposes various obligations on data controllers to ensure that individuals have greater control over their data. For instance, under GDPR, individuals have the right to know what data has been collected about them, request corrections to inaccurate information, and, when necessary, demand its deletion (Zuboff, 2019). Additionally, the regulation mandates that data controllers maintain high levels of transparency and accountability regarding the protection of personal data.

Countries like Germany and France have implemented robust data protection policies under the GDPR framework, serving as exemplary models of best practices in this domain. Germany's Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) and France's Informatique et Libertés Act have both strengthened their national data protection frameworks to align with GDPR. These laws illustrate the effectiveness of harmonized legal approaches in enhancing data privacy protections. However, the rapid pace of technological advancements often outstrips existing legal frameworks, highlighting the need for continuous international collaboration and adaptive reforms.

1.3. The Importance of Data Privacy in the Digital Age

The digital age has introduced unprecedented challenges to the right to privacy. Today, individuals share personal data with every interaction on online platforms, and these data are processed through technologies such as big data analytics, artificial intelligence, and surveillance systems (Solove, 2004). This phenomenon has given rise to a privacy crisis that impacts not only individuals' online identities but also their offline lives.

Data privacy plays a crucial role in safeguarding individuals' private lives. Unauthorized collection, processing, or sharing of personal data not only infringes on the right to privacy but also threatens other fundamental rights, including security, freedom, and equality (Nuredin, 2023b). These violations underline the critical importance of effective data protection regulations and their role in mitigating risks to privacy in an increasingly digitalized world.

2. Mass Surveillance Systems: Applications and Risks

The advancement of surveillance technologies, particularly in the digital age, has profoundly transformed individuals' daily lives. Mass surveillance systems, integrating tools such as big data analytics, artificial intelligence algorithms, and high-resolution cameras, have found widespread application in monitoring both online and offline activities of individuals (Lyon, 2007; Zuboff, 2019).

One of the primary applications of mass surveillance systems is to ensure national security and public order. Governments frequently employ these systems under the pretext of combating terrorism, reducing crime rates, and enhancing public safety. For instance, urban security management

systems, including extensive CCTV networks, have become prevalent worldwide, enabling real-time monitoring of public spaces (Solove, 2004). Additionally, surveillance technologies are extensively utilized in border security, crowd control during public demonstrations, and election monitoring (Privacy International, 2018).

2.1. Surveillance Practices of Governments and the Private Sector

As surveillance technologies become more pervasive, the boundaries between governmental and private sector usage of these tools have increasingly blurred. Governments primarily employ mass surveillance under the guise of ensuring national security and maintaining public order, whereas private entities focus on collecting individuals' data for commercial purposes (Nuredin,2023a).

2.2. Government Surveillance Practices

Governments often justify the use of surveillance technologies for legitimate objectives such as crime prevention, counterterrorism, and the enhancement of public safety. However, the unregulated use of these technologies can lead to significant human rights violations. In authoritarian regimes, for example, surveillance tools are frequently used as instruments of repression, targeting dissenting voices, restricting freedom of expression, and increasing societal control (Nuredin, 2022).

Mass surveillance activities conducted by intelligence agencies in many countries have been criticized for infringing on the privacy of individuals' communications. A prominent example is the National Security Agency's (NSA) surveillance program revealed by Edward Snowden, which highlighted the mass monitoring of phone and internet communications involving millions of individuals in the United States and allied nations (Greenwald, 2014).

2.3. Private Sector Surveillance Practices

The private sector employs surveillance technologies primarily to analyze individuals' behaviors and leverage such data for commercial purposes. Social media platforms, e-commerce websites, and mobile applications, for instance, track online activities and transform this data into actionable insights through big data analytics (Zuboff, 2019). These practices raise

significant concerns regarding individuals' privacy and the ethical use of personal data.

2.4. Evaluating Surveillance Technologies in the Context of Human Rights Violations

The impact of surveillance technologies on human rights must be critically assessed, particularly concerning fundamental rights such as the right to privacy, freedom of expression, and the right to assembly (Nuredin, 2023b). While the use of these technologies is often legitimized under the premise of protecting individual rights, their practical implementation frequently results in severe violations.

Surveillance practices can undermine the privacy and autonomy of individuals, as well as suppress democratic participation and civil liberties. For instance, the pervasive feeling of being constantly monitored can discourage free expression, stifle dissent, and erode the foundational principles of democratic societies. Addressing these issues requires robust legal frameworks, oversight mechanisms, and ethical considerations to balance the benefits and risks associated with surveillance technologies.

3. The Adequacy of International and National Legal Frameworks

3.1. Analysis of Existing International Legal Frameworks (UN, EU, ECtHR)

The proliferation of surveillance technologies and the increasing need for data protection in the digital age have underscored the necessity for international legal frameworks to adapt to these new realities. International law has introduced various mechanisms to protect individuals' right to privacy and to limit the scope of mass surveillance practices (United Nations, 1948; United Nations, 1966). However, the adequacy of these frameworks is frequently questioned, particularly in terms of keeping pace with technological advancements and establishing effective oversight mechanisms (Bygrave, 2014; Kuner, 2020).

The United Nations (UN) provides a global framework aimed at safeguarding individuals' right to privacy. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) guarantee protection against arbitrary interference with individuals' private lives, families, homes, and correspondence (United Nations, 1948; United Nations,

1966). Additionally, the UN Human Rights Council has issued resolutions addressing the right to privacy in the digital era and has investigated the impact of surveillance technologies on individual rights through special rapporteurs (Bošnjak, 2020). However, UN resolutions often lack binding authority, and their enforceability at the national level remains limited.

The European Union (EU) has established more comprehensive and binding regulations to safeguard data protection and the right to privacy. The General Data Protection Regulation (GDPR) is widely recognized as one of the most robust frameworks for data protection worldwide (European Union, 2016). The GDPR imposes strict obligations on data processors to ensure the protection of personal data and grants individuals greater control over their data (Bygrave, 2014; Zuboff, 2019). For instance, under the GDPR, individuals have the right to access information about the collection, processing, and storage of their personal data. Additionally, the regulation provides effective mechanisms for redress in cases of data breaches (Kuner, 2020).

The European Court of Human Rights (ECtHR) plays a critical role in upholding the right to privacy under Article 8 of the European Convention on Human Rights (ECHR). The court has issued binding decisions aimed at limiting state surveillance practices and ensuring that they comply with the principles of necessity and proportionality. For example, in the case of Big Brother Watch v. United Kingdom (2018), the court found that the UK government's mass data collection practices violated individuals' right to privacy (ECtHR, 2018).

Despite the presence of these mechanisms, the effectiveness of international frameworks in safeguarding privacy rights often falls short, particularly in adapting to rapidly evolving surveillance technologies. The lack of adequate enforcement and oversight mechanisms further exacerbates this issue (Zuboff, 2019).

3.2. Examination of Data Protection and Surveillance Regulations in Germany and France

Germany and France, as EU member states bound by the GDPR, have implemented strong national regulations to address data protection and surveillance practices (European Union, 2016). Both countries have

integrated the GDPR into their national legal systems and adopted additional measures to enhance individuals' privacy rights (Kuner, 2020).

Germany is considered a leader in GDPR implementation and has introduced supplementary regulations to strengthen its data protection regime. The Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) has been updated to align with the GDPR and to address data processing activities, particularly in the public sector (Bäcker, 2020). The BDSG outlines detailed rules to ensure that data controllers process personal data lawfully and transparently (Bygrave, 2014). Moreover, German data protection authorities, such as the Federal Data Protection Commissioner, actively oversee surveillance practices and safeguard individuals' rights (European Data Protection Board, 2020).

Germany has also imposed strict limitations on the use of surveillance technologies, such as facial recognition systems in public spaces, which are only permitted under specific circumstances. These technologies are subject to rigorous oversight mechanisms to prevent violations of individual rights (Bäcker, 2020). The Federal Constitutional Court of Germany has delivered landmark rulings emphasizing the protection of privacy in the digital age and limiting the state's mass surveillance activities (Federal Constitutional Court of Germany, 2020).

France has also established a robust framework for data protection under the GDPR. The Informatique et Libertés Act has been updated to reinforce privacy rights in line with the GDPR (CNIL, 2020). The French data protection authority, CNIL (Commission Nationale de l'Informatique et des Libertés), is responsible for ensuring compliance with data protection laws and monitoring the use of surveillance technologies to prevent violations of individual rights (Gellert, 2020). CNIL has the authority to impose sanctions on data controllers and provide guidance to enhance transparency and accountability.

While France has emphasized the use of surveillance technologies for public safety, it has also introduced legal safeguards to prevent misuse. For instance, the use of facial recognition technologies in France is limited to specific scenarios, such as counterterrorism efforts (CNIL, 2020). Additionally, the French Constitutional Council has underscored the necessity of aligning surveillance practices with human rights standards (Gellert, 2020).

The experiences of Germany and France demonstrate the importance of strong national mechanisms in regulating data protection and surveillance technologies. However, both countries face challenges in addressing new technological developments and must continuously update their regulations to remain effective (Zuboff, 2019).

3.3. Legal Gaps and the Need for Reform

The rapid advancement of surveillance technologies has exposed significant gaps in existing legal frameworks. Both national and international regulations struggle to keep pace with technological developments, resulting in inadequate protection of individual rights (Zuboff, 2019).

Key Legal Gaps:

- Artificial Intelligence and Big Data: The use of AI technologies to process large datasets poses a significant threat to privacy rights. Current regulations fail to clearly define the ethical and legal boundaries of these technologies (Bygrave, 2014). For example, the reliance on biased datasets in AI training increases the risk of discriminatory practices (Gasser & Almeida, 2017).

- Lack of International Cooperation: Given the global impact of surveillance technologies, stronger international cooperation mechanisms are required. However, differing approaches among states hinder the development of effective global regulations (Kuner, 2020).

- Transparency and Accountability Deficits: Both governments and private entities often lack transparency in their use of surveillance technologies, leading to rights violations. The absence of robust oversight mechanisms limits individuals' access to information about surveillance practices (Gellert, 2020; Cate, 2010).

Reform Proposals:

- AI Regulations: New legal frameworks should be developed to govern the role of AI in data processing. For instance, the EU's proposed "Artificial Intelligence Act" seeks to establish ethical guidelines for the use of AI technologies (European Commission, 2021).

- Independent Oversight Mechanisms: Surveillance practices should be subject to transparent and independent oversight. Models such as Germany's Federal Data Protection Commissioner offer valuable insights into effective monitoring systems (Bäcker, 2020).

- International Collaboration: States should cooperate to develop common standards for the ethical and legal use of surveillance technologies. The UN Human Rights Council's resolutions on privacy in the digital age underscore the importance of global collaboration (UN Human Rights Council, 2019).

While international and national legal frameworks play a critical role in addressing the challenges posed by surveillance technologies, continuous updates, enhanced transparency, and greater international collaboration are essential to ensure their effectiveness in the digital age (Zuboff, 2019). The examples of Germany and France illustrate the potential for strong regulations, yet they also highlight the urgent need for global and inclusive solutions to meet the dynamic challenges of modern technology (Kuner, 2020).

CONCLUSION AND RECOMMENDATIONS

The Need to Balance Data Privacy and Surveillance

In the digital age, achieving a delicate balance between data privacy and surveillance practices represents one of the most significant challenges for modern legal systems. On the one hand, governments and private entities utilize surveillance technologies to enhance security, personalize services, and improve efficiency. On the other hand, the excessive use of these technologies poses substantial threats to individuals' right to privacy, particularly in democratic societies where safeguarding fundamental rights and freedoms becomes increasingly challenging.

Balancing data privacy with surveillance requires a compromise between public security and individual rights. For instance, while surveillance technologies employed for legitimate purposes such as counterterrorism may serve public safety, they also risk infringing on fundamental rights like freedom of expression, the right to privacy, and freedom of assembly. Similarly, the private sector's use of surveillance practices to monitor consumer behavior and analyze data for commercial gains raises ethical

and legal concerns when individuals' data is collected, processed, and shared without consent.

To maintain this balance, surveillance practices must adhere to the principles of proportionality, necessity, and transparency. The principle of proportionality ensures that surveillance practices remain limited and measured in their scope, while necessity restricts such practices to genuinely required situations. Transparency, in turn, guarantees that individuals are informed about surveillance activities and that these activities are subject to oversight. However, the practical application of these principles depends on the presence of effective national and international regulatory frameworks and monitoring mechanisms.

Recommendations to Prevent Human Rights Violations

With the growing prevalence of surveillance technologies, it is essential to adopt various measures to protect individuals' fundamental rights and freedoms. The following recommendations are particularly significant:

- Strengthening Legal Frameworks

More detailed regulations should be developed to define the ethical and legal boundaries of surveillance technologies. These regulations should ensure that surveillance practices are proportional while safeguarding individuals' right to privacy. For example, special provisions for artificial intelligence (AI)-based surveillance systems can help mitigate the risks these (Nuredin, A., & Inan, T. C., 2024) systems pose to human rights.

- Establishing Independent Oversight Mechanisms

Governments and private entities should be subjected to independent and robust oversight mechanisms to monitor surveillance practices. These mechanisms should promote regular reporting, transparency, and accountability to prevent rights violations.

- Education and Awareness Campaigns

Raising public awareness about privacy rights and data security is crucial. Public authorities and civil society organizations should organize awareness campaigns to help individuals understand and protect their rights.

 Enhancing International Cooperation

Given the global impact of surveillance technologies, international cooperation and the development of universal standards are imperative. States must agree on a common framework to secure cross-border data flows and protect human rights. International initiatives led by organizations like the United Nations and the European Union can play a pivotal role in ensuring the effective implementation of such regulations.

 Promoting Technological Solutions and Ethical Standards

Technological advancements can also serve as tools to protect individual rights. For instance, the widespread adoption of privacy-preserving encryption technologies can secure individuals' digital rights. Furthermore, technology companies should adhere to ethical principles and incorporate (Nuredin, A., & Nuredin, M.2023) accountability mechanisms into their practices.

Strategic Approaches for Future Legal Frameworks

Considering the dynamic nature of the digital age, existing legal frameworks must adapt to technological advancements and anticipate future challenges. Strategic approaches for future regulations may include the following:

- Flexible and Adaptive Legal Frameworks: To keep pace with rapid technological developments, legal frameworks must be flexible and adaptable. Rather than rigid and static rules, evolving frameworks that respond to technological changes, particularly in AI and big data analytics, are crucial.

- Strengthening Data Rights: Future regulations should aim to empower individuals to exercise greater control over their data. For instance, reinforcing rights such as "data portability" would allow individuals to control their data and transfer it to other platforms if necessary.

- Ethical Guidelines and Industry Standards: Encouraging adherence to ethical guidelines through non-binding but influential international standards can limit surveillance practices while aligning with the principles of human rights protection.

- International Data Protection Agreements: The increasing cross-border flow of data necessitates a global framework for data protection. Binding international agreements among states are essential. The European Union's GDPR model could serve as a global benchmark and guide other regions in formulating their regulations.

- Specific Regulations for AI-Based Surveillance Technologies: Given the potential risks AI-based surveillance technologies pose to human rights, dedicated regulations are required. These regulations should enhance algorithmic transparency, prevent discrimination, and ensure compliance with ethical norms.

- Human Rights-Centered Approach: Future regulations should prioritize human rights. Surveillance practices must be designed and implemented with strict oversight mechanisms to ensure that fundamental rights such as the right to privacy, freedom of expression, and freedom of assembly are not violated.

Balancing data privacy with surveillance technologies is crucial for protecting human rights in the digital age. Achieving this balance requires not only robust national regulations but also a global legal framework founded on international cooperation. Continuous updates and oversight of existing regulations are necessary to safeguard individuals' rights and freedoms.

Additionally, the rapid advancement of technology demands solutions that address current issues while preparing for future challenges. Flexible and ethically grounded regulations can ensure the sustainable protection of human rights in the digital era. Governments, private entities, and the international community must collectively develop a shared understanding and work in coordination to secure individuals' rights and freedoms.

BIBLIOGRAPHY

Bäcker, M. (2020). The implementation of the GDPR in Germany: Challenges and solutions. European Data Protection Law Review, 6(1), 34–45.

Bošnjak, M. (2020). The challenges of personal data protection in the digital age. Pravni zapisi, 11(2), 53–67.

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press.

Cate, F. H. (2010). The failure of fair information practice principles. In C. J. Bennett & R. M. Bayley (Eds.), Privacy rights in the global digital economy (pp. 61–77). MIT Press.

CNIL (Commission Nationale de l'Informatique et des Libertés). (2020). Annual report: Data protection challenges in France. Retrieved from https://www.cnil.fr

European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Retrieved from https://eur-lex.europa.eu

European Court of Human Rights (ECtHR). (2018). Big Brother Watch and Others v. The United Kingdom (App No. 58170/13). Retrieved from https://hudoc.echr.coe.int

European Data Protection Board. (2020). Guidelines on data processing and security in public institutions. Retrieved from https://edpb.europa.eu

European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L119. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Union. (2021). Artificial Intelligence in Europe: Legal and ethical implications. Official Journal of the European Union, L119.

Federal Constitutional Court of Germany. (2020). Decision on surveillance and data protection. Retrieved from https://www.bundesverfassungsgericht.de

Gasser, U., & Almeida, V. (2017). A layered model for AI governance. IEEE Internet Computing, 21(6), 58–62.

Gellert, R. (2020). The role of data protection authorities in enforcing GDPR in France. International Review of Law, Computers & Technology, 34(4), 289–306.

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

Kuner, C. (2020). The GDPR and the internet: The global impact of the general data protection regulation. International Data Privacy Law, 10(1), 5–16.

Lyon, D. (2007). Surveillance studies: An overview. Polity Press.

Nuredin, A. (2022). Uluslararası İnsan Hakları Hukuku. International Vision University.

Nuredin, A. (2023a). LEGAL STATUS OF ARTIFICIAL INTELLIGENCE AND THE VIOLATION OF HUMAN RIGHTS. Sui Generis, 2(1), 7-28.

Nuredin, A. (2023b). Fourth-Generation Human Rights and the Violation of the Concept of Privacy. International Scientific Journal Vision, 8(1), 9-23.

Nuredin, A., & Nuredin, M. (2023). Farklı alanlarda etik. International Vision University.

Nuredin, A., & Inan, T. C. (2024). THE IMPACT OF AI-BASED DECISION-MAKING SYSTEMS ON JUSTICE AND EQUALITY. International Scientific Journal Vision, 9-33.

Privacy International. (2018). Eyes wide open: What's behind the rise of facial recognition technology? Retrieved from https://privacyinternational.org

Solove, D. J. (2004). The digital person: Technology and privacy in the information age. NYU Press.

Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). (2017). Group privacy: New challenges of data technologies. Springer.

United Nations. (1948). Universal Declaration of Human Rights (UDHR). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (1966). International Covenant on Civil and Political Rights. Retrieved from https://www.ohchr.org

UN Human Rights Council. (2019). Report of the Special Rapporteur on the right to privacy in the digital age. Retrieved from https://www.ohchr.org

Westin, A. F. (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.