Legal And Ethical Problems In Personal Data Protection Regulations

Rahma Hidayatu Tafiyana

Abstract: *In the modern digital era, personal data protection has become an increasingly pressing issue, giving rise to various legal and ethical challenges. This article investigates the problems that arise in connection with personal data protection regulations, outlining the legal and ethical dilemmas that arise amidst efforts to safeguard individual privacy in the digital era. An in-depth analysis of various legal and ethical perspectives was carried out to illustrate the complexity of the problems faced in dealing with personal data protection.*

Keywords: *Personal data protection, Regulation, Privacy, Digital era.*

INTRODUCTION

The rapid development in information and communication technology, especially in the digital era, has fundamentally altered the way personal data is collected, stored, and utilized (Graham et al., 2019). Along with this progress, concerns regarding the privacy and security of personal data have increasingly become a major focus in global society (Chang, 2021; Ismagilova et al., 2022; Madianou, 2019). In this context, regulations on personal data protection are essential to maintain a balance between technological innovation and individual rights. The significance of this topic is strongly reinforced by the fact that in the continually evolving digital ecosystem, personal data is a highly valuable asset (Birch et al., 2021; Subramaniam et al., 2019). Companies, governments, and other entities widely collect, process, and exchange users' personal data for various purposes, ranging from business analysis to product and service development. An overview of recent developments in personal data protection regulations reveals dynamic trends in various countries and regions. Some jurisdictions have introduced stricter laws to address challenges arising from the data revolution (Lehavi & Levine-Schnur, 2020; Saini et al., 2023). On the other hand, technologies such as artificial intelligence and big data analytics continue to evolve, posing new challenges in safeguarding the privacy and security of personal data. The importance of maintaining a balance between technological advancement and personal data protection becomes increasingly evident when considering its direct impact on public trust in innovation. Notable data security breaches frequently reported privacy violations, and the risk of data exploitation by irresponsible parties have heightened the need for an effective legal framework.

This research aims to analyze various regulations on personal data protection in the current digital era through findings from previous researchers via Google Scholar, ScienceDirect, and IEEE databases. The goal is to delve deeper into the ethical and legal challenges in determining the main outlines of research where scholarly work related to this

discipline is being developed. The research will analyze effective policies or practices in personal data protection regulations that can serve as models for other jurisdictions. Furthermore, the study will evaluate regulatory responses to ethical challenges, focusing on the effectiveness of existing personal data protection regulations, and assessing the extent to which these regulations have struck a balance between promoting technological innovation and protecting individual privacy rights. This involves evaluating their positive and negative impacts and identifying effective policy models or practices in personal data protection regulations that can be adopted or adapted by other jurisdictions as guidelines.

LITERATURE REVIEW

Regulation of Personal Data Protection in the Digital Era

In the rapidly evolving digital era, the substantial growth in the collection, storage, and processing of personal data raises concerns about individual privacy. Regulations on personal data protection have become a necessity to address these challenges, evolving significantly over time. Since the enforcement of the General Data Protection Regulation (GDPR) in the European Union in 2018, many other countries and regions have adopted similar approaches to safeguard individual privacy rights (Gstrein & Zwitter, 2021; Nicola & Pollicino, 2020; Niebel, 2021). According to (Deepa et al., 2022; Ienca & Vayena, 2020; Wachter & Mittelstadt, 2019), these measures reflect global awareness of the importance of personal data protection amid the digital era. Regulations on personal data protection have a significant impact on organizations and businesses. As stated by (Jia et al., 2021; Zaeem & Barber, 2021), the implementation of GDPR has driven changes in business practices and data security strategies. As a result, organizations must now pay attention to strict legal compliance and ensure that customer personal data is processed and stored appropriately (Li et al., 2019; Mazurek & Małagocka, 2019).

The Development of Technology and Current Ethical Challenges

The development of technology in the contemporary era has had a significant impact on various aspects of human life. As a result of continuous innovation, society has transformed various fields, ranging from health and education to industry and communication. While these changes bring benefits, the emerging ethical challenges are becoming increasingly complex. One of the most striking technological changes is the advancement of artificial intelligence (AI). Modern AI systems can perform complex tasks such as natural language processing, facial recognition, and even decision-making. However, the social and economic impact of AI

implementation raises ethical questions related to surveillance, data security, and the preservation of human jobs (Hagerty & Rubinov, 2019; Helbing, 2018).

Regulatory Response to Ethical Challenges

The rapid development of technology has brought about increasingly complex ethical challenges, necessitating careful regulatory responses to ensure responsible technology use. One primary response to ethical challenges is the development of regulations that can accommodate technological advancements without sacrificing ethical values. Numerous studies have highlighted the need for stricter regulations concerning data privacy (S. Park, 2019). Furthermore, the need to mitigate bias in artificial intelligence algorithms has led to calls for regulations governing the development, implementation, and use of algorithms (Hagerty & Rubinov, 2019; Helbing, 2018). Regulations also need to be responsive to the social and economic changes induced by technology. In the face of potential economic impacts that may create inequalities, regulations that can protect workers' rights and steer technological development towards social justice become increasingly important (Skaug Saetra et al., 2021; van Niekerk, 2020). Moreover, these regulations must be able to facilitate innovation without compromising fundamental ethical principles. In addition to formal regulations, collaboration between the government, industry, and civil society is also considered an effective response to ethical challenges. This participatory process can create more holistic regulations that are acceptable to all stakeholders (Rosas, 2019). By involving various parties, regulations can reflect diverse ethical values emerging from different perspectives. In the face of evolving ethical challenges alongside technology, wise and sustainable regulatory responses are key to achieving a balance between technological progress and fundamental ethical values.

Measuring the Balance Between Innovation and Privacy

In the context of rapid technological advancements, a significant challenge lies in efforts to achieve a balance between promoting innovation and safeguarding individual privacy. Effective regulations need to facilitate innovation without neglecting the increasingly crucial interests of privacy. Several studies have highlighted the need to measure and manage this balance so that technology can contribute maximally without compromising individual rights (Acquisti et al., 2020; Zhao et al., 2022). In measuring the balance between innovation and privacy, it is crucial to develop an adaptive regulatory framework. This allows regulations to adapt to technological changes and societal developments. Dynamic regulations can ensure that innovation continues to be encouraged while also addressing evolving privacy aspects over time (Rosas, 2019). Additionally, it is essential to involve stakeholders in the regulatory development process. Active engagement from industry, government, and civil society can

ensure that the resulting policies reflect diverse needs and values. This collaborative approach can help achieve a better balance between technological progress and privacy concerns (Roco, 2007; Ulnicane et al., 2021). The development of accurate measurement methods to assess the impact of innovation on privacy is also a primary focus. This may involve creating performance indicators and impact evaluations that cover critical aspects of privacy, such as user control over their data and the level of transparency in data usage (G. Park, 2019). In the effort to achieve a balance between innovation and privacy, collaboration among regulators, industry, and civil society is imperative. By incorporating diverse perspectives, it is possible to design regulations that support innovation without sacrificing individual privacy rights.

Comparison Study of Personal Data Protection Regulations

In addressing ethical challenges related to technology and privacy, comparing regulations on personal data protection in various regions becomes crucial to understanding different approaches to managing these issues. European data protection regulations, especially GDPR, have become a reference for many countries in establishing a data protection framework. GDPR emphasizes individuals' rights to control their data and imposes significant penalties for privacy violations (Acquisti et al., 2020; Zhao et al., 2022). This approach reflects a high focus on individual privacy rights. In the United States, laws like CCPA in California attempt to enhance personal data protection by granting consumers the right to know, delete, and block the use of their data (Chander et al., 2020; G. Park, 2019). However, this approach is still more fragmented compared to GDPR, with uncertainty in federal regulations. In Asia, countries such as Japan and South Korea have their respective laws on personal data protection, adopting some principles found in Europe and the United States. Nevertheless, there are significant differences in approach and implementation (Roco, 2007; Ulnicane et al., 2021). Japan, through the Personal Information Protection Act, establishes basic principles similar to GDPR, including individual rights over personal data. However, there are differences in technical approaches and supervision. In South Korea, regulations like the Personal Information Protection Act (PIPA) create stricter standards regarding the use of personal data, similar to the European approach. This comparison highlights the complexity of harmonizing regulations on personal data protection globally. Despite efforts to standardize, cultural, legal, and political differences remain significant factors in shaping data protection frameworks in various regions.

CONCEPTUAL FRAMEWORK AND METHODOLOGY

The conceptual framework of this study encompasses three main dimensions that form the foundation for analysis: the Dimension of Personal Data Protection Regulation, which investigates key elements in personal data protection regulations, including objectives, fundamental principles, and enforcement mechanisms. The research will analyze regulatory responses to technological developments and how these regulations ensure ethical compliance in managing personal data. Next is the Dimension of Ethical Challenges, where ethical challenges arising in the collection, processing, and use of personal data will be analyzed. Finally, the Dimension of Balance Between Innovation and Privacy aims to evaluate the balance produced by personal data protection regulations between promoting technological innovation and safeguarding individual privacy. This includes an assessment of the impact of regulations on technological development and the extent to which these regulations respond to market dynamics and societal needs. This study focuses on the development of personal data protection regulations and ethical challenges in the last two decades, with an emphasis on the current situation, while considering historical trends for a broader context. In terms of geographical scope, the research will compare regulations and responses to ethical challenges in several key jurisdictions that have had a significant impact on legal and technological developments.
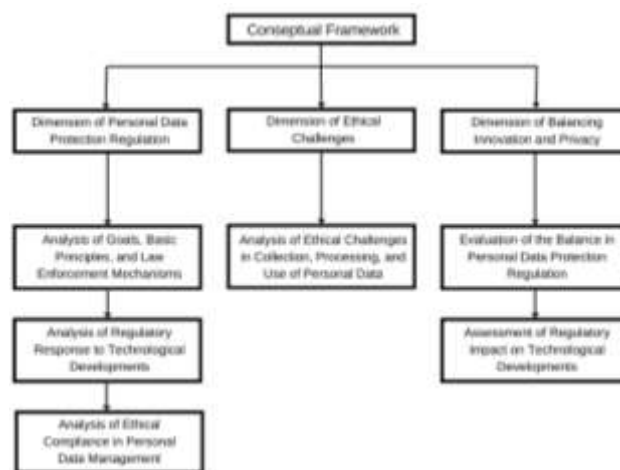
Figure 1. The three main dimensions shaping the conceptual framework of the study (Source: author's elaboration)

METHOD

The research methodology employs a systematic literature review method with a PRISMA (Page et al., 2021) diagram approach, without involving field research or direct interviews with stakeholders. There are also research limitations that do not cover the technical aspects of implementing personal data protection regulations, with a primary focus on legal

and ethical aspects. The study does not explore economic impacts or potential influences on business innovation.

RESULT AND ANALYSIS

Results of Database Search

From the search results using advanced search with predefined strings and keywords, initially, a total of 145 articles were found, but after further filtering and examination of keywords, titles, and abstracts, the number of results decreased to 67 journals. From this total, the articles were further observed and read more thoroughly, resulting in only 15 articles deemed relevant and suitable for inclusion in the research data. This reduction occurred because some articles were deemed invalid, not freely accessible, written in a language other than English, and the remaining due to duplication reasons from other scholarly journal provider databases. Similarly, using the same approach on Google Scholar, a total of 16 articles were found in the IEEE database. After applying filters, namely using only the English language and open access filter, 14 articles were found, but upon further reading, only 4 articles were deemed usable for the research. Not much different from the two previous scholarly journal databases, with the same advanced search features in data research, a total of 129 articles were found.
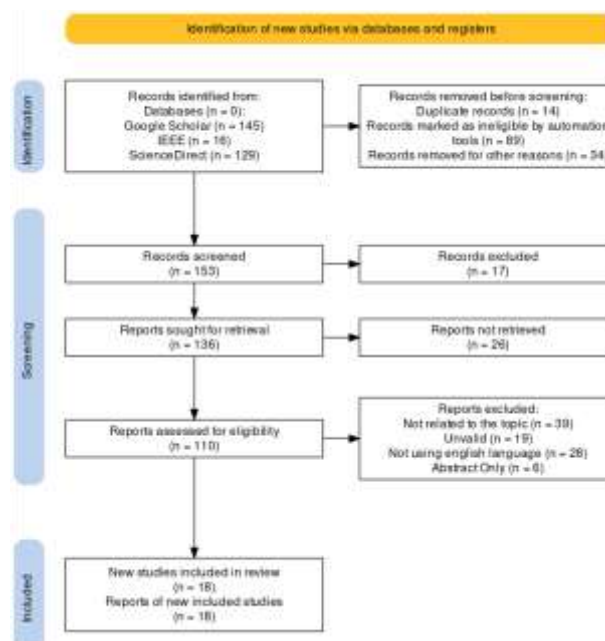

Figure 2. Flowchart PRISMA (Source: Adopted from (Page et al., 2021)

After additional filters were applied and further examination of the remaining article keywords, 8 articles were found to be included in this study. Information evaluation was conducted independently, and opinions were compared to form a consensus. This literature includes research articles published in the last 11 years (2010–2021) and covers all sectors

where personal data protection regulations are most active. Some sectors that emerged include gas, social, communication, economic, public, private, financial, and ethical regulations. From the search of scholarly journals from the three databases mentioned above, a total of 27 relevant articles were finally identified for this research. These 27 articles were read in their full-text versions, but nine of them were excluded because they did not provide in-depth discussions on the topic and did not mention existing challenges or opportunities, thus not meeting the predefined criteria. Figure 2 illustrates the flow diagram of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA).

The literature search identified 18 relevant articles in the field of law as the main focus of interest. These studies are organized into several general categories based on the type of legal specialization that overall discusses various challenges related to regulation, ethics, and personal data protection. Table 1 lists studies on ethical and legal challenges when dealing with regulations on the protection of personal data, with the studies sorted by year of publication.

Table 1. Study on the Challenges and Opportunities of Ethics and Law in the Practice of Personal Data Protection Regulation (Source: Author's elaboration)

Author	Praktik Regulasi Perlindungan Data Pribadi			Practice of Personal Data Protection Regulation
	Ethics and Regulation Implication/Needs	Ethics and Regulation Challenges	Ethics and Regulation Opportunities	
(Nawawi, 2022)	• Human Rights in Legal Protection • Forms of Human Rights Violations in Information Technology/Digital Environment	• Misuse of personal data is increasing due to the development of information technology.	• Benefits and legal certainty guarantees for the public regarding the protection of personal data, both electronically and non-electronically.	Indonesian
(Pijar et al., 2019)	• Ethical and regulatory implications of personal data protection in the context of SIM card registration. • The implementation of appropriate regulations to govern the use of personal data. • The need for comprehensive data protection regulations that cover all aspects of personal data protection.	• Risk of misuse of personal data through the involvement of third parties. • The effectiveness of dispute resolution procedures involving the Minister directly can be challenging for individuals who want to file complaints.	• The potential positive impact of adequate personal data protection on individuals, groups, and society as a whole.	Indonesian
(Tokarski, 2020)	• Legal regulations regarding the protection of personal data in the European Union within the context of EU Regulation 2016/679 concerning the processing of personal data, the free movement of data, and the repeal of Directive 95/46/EC.	• The increased widespread use of personal data by public and private entities, associations, and companies over time poses a threat to the security of personal data. • The global flow of data due to advancing technology. Freedom of expression information access. • Ensuring transparency and accountability in the processing of personal data, especially in data processed by automated systems or algorithms, is difficult to ascertain.	• Increased trust and confidence in digital services and the digital economy contribute to the increased adoption of digital services. • Trust is built between individuals and organizations processing data. • There is an increase in innovation in the field of data protection. • This encourages the development of new technologies and techniques for data protection, such as privacy-enhancing technologies and privacy and data protection by design and by default.	Poland

(Kuleshov et al., 2020)	• Protection of personal data within the regulations of digital technology in the context of ethics and regulations in the development and implementation of AI systems	• The procedures used in training current AI systems do not allow for the removal of data from the system's structure, which can make it difficult to comply with the withdrawal of consent requests. • The scale and scope of the use of AI systems and the need for effective governance and regulations to ensure the ethical protection and use of personal data.	• Mitigating the negative impacts of AI technology. • Development and implementation of a code of ethics and compliance rules to ensure that AI systems meet societal ethical criteria.	Moscow
(Deac, 2018)	• The ethical and regulatory implications of personal data protection compliance must be met by authorities or public bodies by basic principles and societal expectations.	• The rapid development of technology and globalization has led to an increase in the collection and exchange of personal data. • The creation of a trust climate enables the growth of the digital economy in the internal market. • Balancing privacy rights with the need for data processing for legitimate purposes, transparency, and accountability in data processing.	• Strict implementation of protection principles. • Supporting the development of the digital economy in the internal market. • Increasing trust and confidence in the digital economy, promoting innovation and growth.	Romania
(Fernandes et al., 2019)	• Proposed methodology for creating a GDPR catalog that can be used to build an information system that complies with GDPR.	• Interpretation and implementation of legal requirements related to data protection. • Technical and operational challenges.	• The development and implementation of regulatory systems can effectively protect personal data while preserving the free movement of such data.	Portugal
(Romaszewski & Trąbka, 2018)	• Regulation and ethical implications of personal data protection in the context of healthcare entities. • The importance of conducting a privacy impact assessment that considers the complete lifecycle management of personal data, from collection through processing to deletion.	• The specificity of medical data is often sensitive, requiring special attention and protection. • There is a need to assess the impact of personal data protection, taking into account the complete lifecycle management of personal data from collection to processing to deletion. • Security challenges arising from fast and non-standard access operations to medical data.	• The fundamental role of data controllers in ensuring the security of personal data. • Introduction of new regulations that will introduce several changes related to healthcare organization entities. • Improvement in service quality and enhancement of patient safety.	Poland
(Kalamata, 2019)	• Implications of the legal framework and assessment criteria used by the Supervisory Authority in penalty enforcement procedures in the context of Regulation (EU) 2016/679 on the protection of natural persons about the processing of personal data and the free movement of such data.	• The rapid development of technology and globalization in the collection, processing, exchange, and use of personal data. • Challenges for businesses and organizations involved in processing personal data.	• Greater control for individuals over their data and the reinforcement of their fundamental rights to privacy and data protection. • Opportunities for competitive advantages in the market for businesses and organizations.	Greece
(Belen Saglam et al., 2022)	• Reevaluation of information categorization and personal data. • Interface between data protection laws and technology developers to address outdated conceptualizations, resulting in an inadequate legal framework.	• The development of technology.	• The creation of global economic value that can drive innovation, productivity, and efficiency across multiple sectors.	United Kingdom
(Jakobi et al., 2022)	• The ethical and regulatory implications of personal data protection, as well as the need for responsible technology design under GDPR (Articles 12, 21, 25, and 35), concerning the rights of data subjects and the responsibilities of data controllers and processors.	• Identifying risks is challenging because privacy is quite subjective, requiring a user-centric design approach that incorporates the perspectives and needs of data subjects in the design process. • The importance of accountability in data-driven services and the need for a risk-based data protection approach in the digital realm.	• Increased trust and confidence of users in data-driven services. • Enhanced transparency of systems.	Germany
(Miller, 2022)	• Regulatory implications on big data analysis for individuals, organizations, and society in the realms of AI and Cloud.	• Ethical and regulatory challenges related to the protection of personal data in artificial intelligence (AI) projects.	• Increasing the adoption of AI systems. • Avoiding legal and reputational risks for organizations involved in AI projects.	Jerman

Reference	Focus / Ethical Implications	Challenges / Issues	Opportunities	Country
(Basarudin & Raji, 2022)	• The ethical and regulatory implications of personal data protection in the context of personalized advertising and algorithmic targeting.	• Consent and data minimization issues. • Legal limitations that are regional in nature make the enforcement of privacy laws and personal data protection beyond geographic boundaries a constraint and challenge.	• Increasing consumer trust and confidence in personalized advertising. • A strong relationship between companies and customers can be established. • The misuse of personal data can be prevented altogether.	Malaysia
(Stuurman & Kamara, 2016)	• A new approach related to the General Data Protection Regulation (GDPR) as a legal instrument to regulate the processing of personal data, supporting standardization in various ways.	• Data protection in the development and use of IoT applications.	• The creation of opportunities for developing standards to address various customer trust issues.	Netherlands
(Hadiyantina et al., 2021)	• Ethical implications in the concept of data protection are often considered as part of the protection of the right to privacy. • Regulatory implications on laws regarding personal data should include articles regulating the establishment of independent organizations specifically handling personal data protection and maintaining high integrity. • The urgency of personal data protection in policies related to massive collection of personal data from the population (e-commerce).	• Creation of new laws related to the protection of personal data. • Improvement of sanctions should be more explicit as they relate to the civil and personal rights of every citizen.	• Business opportunities for the establishment of a clear legal framework for the protection of personal data.	Indonesian
(Floridi, 2018)	• The new distinction between soft ethics, which comes into play after legal compliance with laws such as the General Data Protection Regulation (GDPR) in the European Union, and hard ethics, which precedes and contributes to shaping legislation.	• Digital governance. • Technological innovation.	• Enhancing the closeness of various organizations.	London
(Erdos, 2015)	• Enhancing the closeness of various organizations.	• Lack of harmonization in data protection laws across the European Economic Area (EEA) can lead to inconsistency in the protection of fundamental human rights, such as the right to privacy. • The processing of personal data by the media can jeopardize individual rights, such as non-discrimination and the right to reputation. • Costs and administrative burdens for businesses.	• Human rights justice and privacy security are preserved. • Opportunities for customer trust for businesses. • Business efficiency.	United Kingdom
(Spina, 2017)	• Ethical implications of the collection and use of data, especially in the context of "smart" metering for energy distribution.	• Ethical and regulatory challenges related to the protection of personal data in the digital economy. • Economic or social losses for individuals, erasure of rights and freedoms, and the creation of personal profiles. • Creating tension between the benefits of efficient energy distribution and the risks posed by the massive collection of personal data from electrical appliances. • The emergence of digital platforms, algorithms, and artificial intelligence raises questions about the role of risk regulation in data-driven digital economic governance.	• The creation of a stable digital economy. Strengthening individual rights against public and private entities. The emergence of data ethics can help ensure that ethical principles and values are well-maintained. Creating opportunities for innovation and economic growth.	United Kingdom

(Taupitz & Weigel, 2012)	• Regulation of personal data protection in biobanks and the ethical implications of data protection in medical research. Implications for emphasizing the importance of information-based consent and the purpose of consent in data processing.	• Challenges related to the storage, sharing, and secondary use of personal data in biobanks. • The need for additional regulations to ensure the protection of personal data in biobanks.	• Building public trust in medical research by ensuring that personal data is protected and used only for legitimate purposes. Potential for promotion/marketing.	Germany

Analysis of Ethical and Regulatory Implications in the Practice of Personal Data Protection Regulation.

The analysis results indicate the complexity and challenges of protecting personal data in the era of information and digital technology. The researched articles bring forth various implications related to the practice of self-data protection regulation in the current digital age across different countries. There is attention to the protection of human rights in the context of personal data processing, with a specific emphasis on the ethical aspects of using digital technology (Deac, 2018; Nawawi, 2022; Tokarski, 2020). These findings consistently highlight the importance of comprehensive regulations, covering issues such as data protection in the context of the continuously emerging AI systems, especially in Indonesia, and the need for careful impact assessments (Kuleshov et al., 2020; Miller, 2022). Furthermore, issues like data protection in media and SIM card registration (Pijar et al., 2019) also indicate the need for precise regulations and attention to ethical implications in specific contexts. Additionally, in business (Erdos, 2015; Hadiyantina et al., 2021; Kalamata, 2019; Spina, 2017), information technology, for example (Basarudin & Raji, 2022; Belen Saglam et al., 2022; Kuleshov et al., 2020; Miller, 2022; Nawawi, 2022; Stuurman & Kamara, 2016), and the health sector (Romaszewski & Trąbka, 2018; Taupitz & Weigel, 2012), there are various similarities reflecting key cross-contextual issues that need to be addressed to ensure effective protection of personal data.

Analysis of Challenges and Opportunities in the Practice of Personal Data Protection Regulation

Laws and regulations on personal data protection face several challenges and opportunities that need to be carefully considered. On one hand, the implementation of human rights principles in data protection poses ethical challenges. Emphasizing human rights principles in the context of regulating personal data, such as SIM card registration (Pijar et al., 2019), requires thoughtful consideration of privacy and access to personal information. These challenges require precise and appropriate regulations to maintain a balance between individual rights and security needs. Violations of human rights in digital technology (Erdos, 2015; Hadiyantina et al., 2021; Miller, 2022; Nawawi, 2022), such as misuse and sale of personal data, highlight the complexity of creating effective regulations. Regulations must be able to

identify and address harmful practices without hindering technological innovation. This is where the opportunity arises to design regulations that are adaptive and responsive to rapid technological developments. Regulations in the European Union, especially in the context of Regulation (EU) 2016/679, offer a model that can be adopted for personal data protection (Deac, 2018; Fernandes et al., 2019; Floridi, 2018; Kalamata, 2019; Spina, 2017; Tokarski, 2020). However, challenges remain in ensuring that regulations cover all aspects of personal data protection, while the opportunity lies in the formation of a catalog of requirements aligned with ethical and just principles.

Analysis of Data Protection and Confidentiality in the Practice of Personal Data Protection Regulation

Data protection and confidentiality always exist for any information accessible through digital documents. However, the General Data Protection Regulation (GDPR) has further classified and defined data points to facilitate understanding and management of personal data. For maximum data protection, many authors consider the need for uniform guidelines, similar to the GDPR applied in the European Union, for example (Dwivedi et al., 2022; Roberts et al., 2021; Shittu et al., 2021; Zaeem & Barber, 2021), supported by findings (Fernandes et al., 2019; Floridi, 2018; Jakobi et al., 2022; Kalamata, 2019; Spina, 2017; Stuurman & Kamara, 2016). Service providers in all articles have a significant responsibility for the use of devices, which should be secure and non-invasive so that individuals feel safe and unharmed. On the contrary, some entities, including governments or related institutions, for example, in research (Deac, 2018; Tokarski, 2020), must be very cautious when transmitting customer or resident data to others or third parties and in data storage. There are many hypotheses for ensuring maximum data protection when transmitting data and entire subject groups. Some articles discussing IoT and AI (Miller, 2022; Spina, 2017; Stuurman & Kamara, 2016) refer to data in electronic records. Strict legal aspects related to confidentiality and privacy violations can result in criminal, civil, and deontological offenses (Carlo & Corso, 2019; Shuman, 1985).

Analysis of Laws and Regulations in the Practice of Personal Data Protection Regulation

Considering the diverse approaches to various ethical and legal aspects in different areas, it is highly anticipated that there will be limited studies discussing laws and regulations. Most seem to provide insufficient constructive information and mainly express the need for unified legislation. The importance of personal data protection has laid the foundation for the formation of laws and regulations governing related practices within the scope of digital technology. Two crucial aspects that are the main focus of this analysis are Human Rights in

Legal Protection and Human Rights Violations in Digital Technology. Firstly, in the context of Human Rights (Erdos, 2015; Hadiyantina et al., 2021; Miller, 2022; Nawawi, 2022), ethical analysis highlights the fundamental principles of human rights in the protection of personal data. This includes the recognition that every individual has the right to engage in the regulation of their personal information. In the regulatory domain (Deac, 2018; Nawawi, 2022), legal protection is required to provide benefits and legal certainty to the public. Specifically, regulations should accommodate technological developments, ensuring the protection of personal data both electronically and non-electronically.

Secondly, in the analysis of human rights violations in digital technology (Floridi, 2018; Jakobi et al., 2022; Kuleshov et al., 2020; Spina, 2017; Tokarski, 2020), the ethical aspect highlights negative impacts such as misuse, theft, and sale of personal data. Effective regulations become crucial to protect individuals from these threats. By identifying forms of violations, regulations can be designed to address practices that harm human rights. Additionally, when considering SIM Card Registration (Pijar et al., 2019), ethical implications need to be investigated, particularly regarding privacy and access to personal information. Appropriate regulations to control the use of personal data in the context of SIM card registration are essential to ensure the protection of individual rights. In the overall framework, existing regulations in the European Union, such as Regulation EU 2016/679 (Tokarski, 2020), should also be examined. Ethical analysis in the implementation of EU regulations involves considering ethical values and fundamental principles, while the regulatory aspect emphasizes the need for comprehensive rules that cover all aspects of personal data protection. In the practice of personal data protection regulations, it is important to understand that the fundamental principles underlying regulations must align with Human Rights. These regulations, including GDPR, propose a methodology to create a catalog of requirements for personal data protection that aligns with ethical principles and justice.

Through an in-depth analysis of the general conditions for imposing administrative fines (Kalamata, 2019), we can understand how regulations ensure compliance and mitigate human rights violations. Furthermore, the protection of personal data in the context of healthcare entities highlights significant ethical and regulatory implications, where there needs to be a balance between medical innovation and the protection of personal data. Finally, focusing on digital governance as a new challenge emphasizes the need for a balanced approach between soft and hard ethics. Personal data protection regulations should include the establishment of independent organizations and clear sanctions to ensure compliance and the protection of civil and personal rights. Thus, the complexity and interconnection between

ethical and regulatory aspects in the practice of personal data protection regulations underscore the importance of maintaining a balance between technological innovation and human rights.

Discussion

Regarding the protection of personal data, it involves various aspects related to technological advancements, regulations, and ethical challenges. Concerns about the misuse of personal data have increased with the progress of technology and information. While these developments bring benefits such as increased efficiency and innovation, they also pose serious problems, including the risk of data misuse, personal data theft, and fraud. The risk of personal data misuse also arises from the involvement of third parties, adding complexity to data protection, as revealed by (Pijar et al., 2019). The resolution process involving the Minister directly can be a barrier for individuals who want to file complaints, raising questions about the effectiveness and fairness of handling such cases. The increased use of personal data by various entities, both public and private, as well as associations and companies, creates threats to the security of personal data (Tokarski, 2020). Technological constraints and the global flow of data add difficulties to enforcing data protection regulations, especially in the context of using automated systems and algorithms. The biggest challenge is balancing the protection of personal data with other fundamental rights, such as freedom of speech and access to information. These difficulties are exacerbated by the rapid pace of technological development and globalization, presenting ethical and regulatory challenges, especially in the context of activities involving sensitive medical data.

Although regulations such as GDPR have been introduced to address these challenges, their implementation requires collective efforts to ensure compliance and effectively protect personal data. The adoption of such regulations can help build trust between individuals and organizations processing data, encourage responsible innovation, and bring about greater economic benefits. In the context of personalized advertising, the protection of personal data becomes increasingly crucial, and regulations can play a key role in ensuring the security and privacy of consumers. The importance of digital ethics and regulations in digital governance and the digital economy cannot be ignored. Personal data protection involves not only legal issues but also ethical values that underlie the use and processing of data. By understanding and addressing these challenges, an environment can be built that supports sustainable, innovative, and ethical growth in the digital economy.

CONCLUSION AND RECOMMENDATIONS

From the three major scientific journal databases used in this research (Google Scholar, IEEE, and ScienceDirect), a total of 290 articles were found. However, after applying various filters and conducting further analysis, only 18 relevant scientific articles were identified for this research. Upon thorough review, the analysis of personal data protection indicates a fairly high complexity and challenges in the current era of digital technology. The research findings emphasize the need for comprehensive regulations, focusing on ethical aspects, human rights, and the urgency of emerging impact assessments. With an emphasis on the balance between data protection and medical innovation, challenges and opportunities are evident in adaptive regulations to technological advancements. Digital governance has become a new focus that requires regulations to understand its complexity. Data protection and confidentiality highlight the importance of data classification by GDPR and uniform guidelines. Regulations in the European Union serve as a model, with a focus on human rights and their violations, emphasizing the need for regulations in line with ethical principles. Therefore, the practice of personal data protection regulation requires a balanced approach between ethics, human rights, and technological progress to create a safe and ethical digital environment. Due to limitations in accessing scientific journal databases and language constraints, for future research, it would be beneficial to expand and add more articles, especially in the legal realm in the digital era, using databases like JSTOR, WoS, and HeinOnline (which have more scholarly publications in the field of law). Additionally, the legal framework can be further developed to be more effective in protecting personal data. Regarding the ethical and legal challenges in the use of personal data and research on recent regulatory trends, further research can be conducted using databases from various countries and regions on a broader scale.

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. https://doi.org/10.1002/JCPY.1191

Basarudin, N. A., & Raji, R. A. (2022). Implication of Personalized Advertising on Personal Data: A Legal Analysis of the EU General Data Protection Regulation. Environment-Behaviour Proceedings Journal, 7(22), 109–114. https://doi.org/10.21834/ebpj.v7i22.4160

Belen Saglam, R., Nurse, J. R. C., & Hodges, D. (2022). Personal information: Perceptions, types, and evolution. Journal of Information Security and Applications, 66. https://doi.org/10.1016/j.jisa.2022.103163

Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. Big Data and Society, 8(1). https://doi.org/10.1177/20539517211017308

Carlo, D., & Corso, D. (2019). Organizational Psychology and Technology: Ethical, Legal, and Practical Issues Related to Active Listening and Work-Related Stress Monitoring in Italy and Europe. International Journal of Developmental and Educational Psychology, 1(1). https://www.redalyc.org/articulo.oa?id=349859739019

Chander, A., Kaminski, M. E., & McGeveran, W. (2020). Catalyzing Privacy Law. Minnesota Law Review, 105. https://heinonline.org/HOL/Page?handle=hein.journals/mnlr105&id=1773&div=&collection=

Chang, V. (2021). An ethical framework for big data and smart cities. Technological Forecasting and Social Change, 165. https://doi.org/10.1016/j.techfore.2020.120559

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144, 17–39. https://doi.org/10.1016/J.COMNET.2018.07.017

Deac, A. (2018). Regulation (EU) 2016/679 of the European and of the Council Parliament and of the Council on the Protection of Indivduals with Regard to the Processing of Personal Data and the Free Movement of These Data. https://www.ceeol.com/search/article-detail?id=762413

Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., & Pathirana, P. N. (2022). A survey on blockchain for