SCIENTIFIC CULTURE

www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 7359-7368*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo.12426746**

# DIGITAL RIGHTS AND DATA PRIVACY IN THE ERA OF ARTIFICIAL INTELLIGENCE: LEGAL CHALLENGES, ETHICAL CONSIDERATIONS, AND GLOBAL REGULATORY FRAMEWORKS

**Sachin B Jadhav[1*], Shalini Hanok[2], Tigulla Rajitha[3], DR.R.Balakrishnan[4], Mr. Venkoba Kutagamari[5], Dr. Rajendra Kumar Ganiya[6]**

*[1*]Assistant Professor, Department of Integrated BTech (AI), Sanjivani University Email ID: seesachinjadhav@gmail.com ORCID ID: https://orcid.org/0009-0007-2635-3356*

*[2]Associate Professor, Department of Electronics and Communication Engineering, ATME College of Engineering, Mysuru, Karnataka Specialization: Cyber Security Email I'd: shalini.prabhakar@gmail.com Orcid I'd:0000-0001-5639-8415*

*[3]Assistant Professor, School of Information Science, Presidency University, Bangalore. Specialisation: Computer Applications ORCID ID : 0009-0007-6405-8905 Email ID : rajithat26@gmail.com*

*[4]Associate Professor, School of Information Science, Presidency University Specialization: Data base Management system ORCID ID : 0009-0000-9630-8509 Email ID : rbalabala72@gmail.com*

*[5]Assistant Professor, Grade 1 School of Information Science, Presidency University, Bengaluru Specialization: Cyber Security and ML ORCID ID: 0009-0001-0841-510X Email I'd: venkobaskutagamari25@gmail.com*

*[6]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., 522302, India. ORCID ID: 0000-0002-9959-5985, Email ID: rajendragk@kluniversity.in*

**Received: 24/11/2025**
**Accepted: 19/03/2026**

*Corresponding Author: Sachin B Jadhav (seesachinjadhav@gmail.com)*

## ABSTRACT

***The rapid growth of artificial intelligence (AI) has increased the scale of personal data processing, which has raised serious concerns about personal data rights and privacy. The existing regulations, such as the General Data Protection Regulation (GDPR), are intended to address these issues, but their applicability to AI-based technologies remains a question. To analyze the relevance and effectiveness of GDPR provisions in the context of AI, identify associated legal and ethical challenges, and examine regulatory gaps in governing AI-based data processing. A qualitative doctrinal research approach was adopted using a structured GDPR question–answer dataset. The dataset was analyzed through thematic categorization, statistical evaluation, and interpretive legal analysis to assess key regulatory domains and their implications for AI systems. The analysis revealed that GDPR provisions are primarily focused on governance mechanisms, including accountability, data subject rights, and enforcement structures. Statistical findings demonstrated significant variability in textual complexity and thematic distribution across regulatory domains. Key challenges identified include limitations in transparency, difficulties in implementing the right to explanation, and gaps in addressing algorithmic bias and automated decision-making. While GDPR provides a comprehensive foundation for data protection, it***

***lacks explicit provisions for AI-specific challenges. Effective AI governance requires integration of legal, technical, and ethical frameworks, along with adaptive regulatory approaches to ensure the protection of digital rights in evolving technological environments.***

**KEYWORDS:** Artificial Intelligence, Data Privacy, GDPR, Digital Rights, AI Governance.

**Introduction**

The widely spread development of artificial intelligence (AI) has radically changed the data generation and processing environment and their way of usage and the issue of digital rights and data privacy become the matter of serious concern. The increasing penetration of AI in a multitude of industries, including the healthcare sector, the administrative sector and the business mechanisms, has increased the amount and level of the handling of personal data, consequently intensifying the need to possess powerful legal and ethical regulations. The historical and traditional right to privacy is currently undergoing the process of definition, in the context of algorithmic systems that work with big amounts of personal and sensitive information [1].

The use of AI powered systems heavily depend on processes that are data intensive usually requiring the collection, storage and analysis of individual information in ways previously not been experienced. This growth has resulted in the appearance of new data misuse, unauthorized access and bias in the algorithms, which have to be addressed by even stronger regulatory mechanisms to protect the privacy of individuals [2]. Simultaneously, the growing importance of data in business and advertising has also further underpinned the importance of ensuring the privacy of the users since the companies are increasingly relying on the information of the users to make certain decisions and provide personalized services [3]. The AI and data privacy intertwining is especially clear in the health care industry, where giant databases and sophisticated analytical software are used to improve clinical performance, but also, threaten the security of data and the ethics regulation [4]. The field of healthcare is one of the most urgent cases of the dual influence of AI on both the risks of innovation and privacy. The use of AI in clinical systems has made the functionalities better in terms of taking decision, predicting and carrying out operations; however, it has also led to severe problems of data confidentiality, consent, compliance with regulations [5]. The implementation of digital decision support systems and tools based on artificial intelligence requires a special attention to the legal framework, in order to avoid the problem of the undermining of patient rights or the level of protection of their data [6]. In addition, increasing the demand of transparency into the transactions of data points out the significance of the balancing between the innovation and accountability especially in the context of sensitive health data [7].

The association of AI to data privacy is also not made easy by ethical factors. In such sensitive fields as reproductive health and clinical decision-making, the use of AI may cause a problem of fairness, bias, and equal access to the technology [8]. Apprehension about data privacy in healthcare has also been greatly reported and danger posed by big data associations and its potential abuse in AI-based data systems [9]. Moreover, the introduction of robotics and AI in the health care sector raises wider concerns of ethics such as autonomy, accountability, and ethical issues relating to the automated decision-making processes [10].

As part of these challenges, the regulatory frameworks of the concept like the General Data Protection Regulation (GDPR) have increased as broad legal provisions to ensure the safety of personal data and liability in the processing of data. Among the principles that are defined in the GDPR, such as lawfulness, transparency, limited purpose, and data minimization, there are supposed to be applied to control the collection and utilization of personal data in the digital sphere [11]. They are especially applicable in the context of AI, where such concepts as consent and transparency are often put to the test because of the amount and sophistication of the data processing occurring. Among the most important issues of GDPR that are closely connected with the problem of AI is attitude to an automated decision making and an idea of a right to an explanation. The purpose of this provision is to make sure that the citizens do not undergo decision-making performed by automated mechanisms but with no meaningful control by humans [12]. Such rights however have not been implemented practically, especially when considering obfuscated machine learning models where their working can hardly be understood. Ethical theories have thus been put forward to add to the law regulations, which highlight the importance of fairness, accountability, and transparency in AI systems [13]. The diversity of AI governance practices across the world also demonstrates the variety of the approaches various jurisdictions have to current issues of data privacy. Different standards of ethics and policy frames have been put in place to regulate the proper use of AI and the need to cooperate internationally and to harmonize the norms has been underlined [14]. AI governance models are increasingly targeting a stratified approach, where a combination of legal, technical and organizational controls work together to ensure a multi-faceted regulation of AI systems [15].

Even with these developments there are very large loopholes in the regulation of the AI driven data processing. Current legislations will find it hard to keep up with the fast-paced technology and thus have uncertainties and constraints in implementing them to newly developed AI applications. Lack of direct AI-related provisions in most rules also requires interpretation-based strategies which would apply the old data protection principles to the new technological environment. Therefore, interdisciplinary studies based on legal, ethical and technological approaches to these issues are increasingly demanded, which will help to deal with the emerging problems of digital rights and data privacy in the era of artificial intelligence.

The proposed research is focused on analysing the overlapping of the provisions of the GDPR, the AI technologies and the data privacy issues with a structural set of GDPR articles. The systematic analysis will help the research to find out major principles of law, their application to AI systems and clarify the regulatory gaps that still need more consideration.

## Methodology

### Study Design

In order to study the rights on digital information and the data privacy in the context of artificial intelligence, the qualitative approach of doctrinal research was applied. The analysis combines both the data-based analysis structured and interpretive legal logic to overcome the relevance and constraint of the General Data Protection Regulation (GDPR) in regulating the processing of data via AI. The design focuses on the systematic extraction, categorization and interpretation of the provisions of law as opposed to empirical or experimental research.

### Data Source

As the main source of data, a structured GDPR question-answer dataset was used [16]. Likewise, in each of the entries, there was a GDPR article content along with the related question-answer units and related metadata that comprised of article identification, chapter classification, and text-length attributes. The dataset included a wide set of GDPR provisions in different chapters, including important areas of the regulation, namely, data processing principles, data rights of subjects, controller and processor liabilities, cross-border data transfers, and enforcement rules.

### Preparation and Organization of the Data

Each and every entry was carefully revised and categorized based on the article numbers and relevance based on their topics. Divided articles were rearranged rationally in the analysis process to allow doctrinal integrity to be maintained e.g. those articles marked as continued sections. Questionanswer format was used as the major tool of interpretation making it possible to extract the legal meanings, regulatory will and implications of operation in a structured manner. There was no pre-treatment of the dataset to cover the missing values or inconsistency since it was complete and was internally consistent.

### Analytical Framework

The paper employed thematic legal analysis method. First of all, content of datasets was divided into the main GDPR categories like lawfulness and transparency, purpose limitation and data minimization, data subject rights, controller and processor obligations, automated decisions and profiling and cross-border data transfers and enforcement. After that, each thematic group was analyzed in terms of artificial intelligence systems. In this case, the special focus was put on the following issues: the processing of large-scale data for learning and decision-making in automated ways in accordance with the provisions of Article 22, transparency and explainability, as well as the role of consent and lawfulness in the AI world.

The interpretation of law analysis was conducted in terms of the extent, benefits, and drawbacks of the provisions of the GDPR in terms of addressing the AI issues. In this case, it was necessary to find the regulatory gray zones, possible gaps, and conflicts between the established principles of data protection and the customs of the AI world. To put GDPR within the context of a shifting world environment of regulations, a comparative approach was also added. The selected foreign models and policy strategies in regards to AI regulations were discussed in order to find the difference or similarity in the regulatory design. This parallel helped to evaluate the conformity or nonconformity of the GDPR to the future standards of the regulation of digital rights and AI.

### Inclusion and Exclusion criteria

The analysis included GDPR provisions which are directly or indirectly linked with the processing of data on personal data, automated decision-making and profiling, and rights and obligations, which are linked with data governance. Articles that were of little to no importance to AI or processing digital data were filtered out to remain focused on the analysis. The parts that were not added with

interpretive value after a reduction were also removed during the process of the consolidation.

**Results**

Empirical research conducted on the dataset of questions and answers of the GDPR revealed that the dataset had a clear structural, thematic and linguistic characteristics which represented the regulatory framework of the data protection law and its importance in relation to the data processing by artificial intelligence.

**Organization and Dispersion of Data**

The data set was a set of 995 records, which were associated with 99 different GDPR articles which are spread in various regulatory chapters. Participation of various provisions in the unbalanced distribution of entries for the chapters were as follows, whereas Controller and Processor provisions had the highest number of entries, followed by Cooperation and Consistency and Rights of the Data Subject. Other chapters such as Delegated Acts and Implementing Acts and General Provisions were not that well represented. This distribution reveals that there are high levels of operational governance, mechanisms of compliance and structures of enforcement in the dataset.

The prevalence of the controller-processor-related content can be taken as a sign of the regulatory focus on accountability and organizational responsibility as the primary focus of both GDPR compliance and AI system governance. Table 1 presents the descriptive characteristics of the dataset variables.

**Table 1:** Descriptive Statistics of Dataset Variables

| Variable | Mean | SD | Min | Median | Max |
|---|---|---|---|---|---|
| Article Word Count | 302.43 | 245.93 | 31 | 230 | 958 |
| Question Word Count | 15.52 | 6.42 | 3 | 14 | 45 |
| Answer Word Count | 38.69 | 29.98 | 1 | 31 | 317 |

**Textual Characteristics**

Textual features analysed quantitatively indicated that average length of the article content was about 302 words with a significant variation between the entries. The average length of the questions accounted for about 15 words and the mean length of answers was about 39 words, which means that there was a concise formulation of the legal questions, and the explanatory answers were relatively detailed.

The scope of answer sizes was greatly increased and some answers were over 300 words long which suggest that there was variability in the depth of interpretation at least based on the complexity of the legal provision. This variability allows the data set to be used in short form retrieval tasks as well as the more specific legal interpretation. Table 2 is the relations between textual variables.

**Table 2: Correlation Analysis**

| Variables | Article WC | Question WC | Answer WC |
|---|---|---|---|
| Article Word Count | 1.000 | 0.140 | 0.375 |
| Question Word Count | 0.140 | 1.000 | 0.188 |
| Answer Word Count | 0.375 | 0.188 | 1.000 |

**Thematic Concentration of Legal Provisions**

The data content of the datasets was thematized and several major regulatory areas identified. The biggest cluster was provisions regarding controller and processor obligations which focused on accountability, documentation of compliance and implementation of technical and organizational measures. Another significant area was the rights of data subjects because of the major presence of the rights of the person to data protection in the context of the GDPR.

The representatives of the chapters about co-operation, consistency and supervisory authorities also showed marked representation which implies the significance of institutional enforcement and regulatory co-ordination. Conversely, underlying principles and general provisions although they are represented were not as dense represented in the data set structure. The distribution of regulatory domains as it is represented in Table 3 is thematic.

**Table 3:** Thematic Weight Distribution Based on Chapter Grouping

| Regulatory Domain Category | Chapters Included | Total Entries | Percentage (%) |
|---|---|---|---|
| Governance and Accountability | Controller & processor, cooperation, supervisory auth. | 456 | 45.83 |
| Data Subject Rights | Rights of the data subject | 120 | 12.06 |
| Enforcement and Legal Remedies | Remedies, penalties | 80 | 8.04 |
| Core Principles | Principles, general provisions | 120 | 12.06 |
| Data Transfer and Special Cases | Transfers, specific processing situations | 139 | 13.97 |
| Residual Regulatory Provisions | Final, delegated acts | 80 | 8.04 |

**Patterns in Question–Answer Mapping**

The dataset had a pattern constancy, with each article or segment of article in GDPR being linked to specific targeted questions on particular legal interpretations. The questions that were asked were mostly of definitional or scope nature, as they concerned the purpose, applicability and requirements of individual provisions.

Direct, article based explanations of answers are usually summaries of most important legal obligations or rights. This format allowed easy facility between the text of the law and the interpretation product to give chambered extraction of regulation sense. The fact that several entries may exist on some articles including continuations, shows segmentation of complex provisions into granules which are easier to compose. Figure 1 shows the correlation between the length of the questions and length of answers.

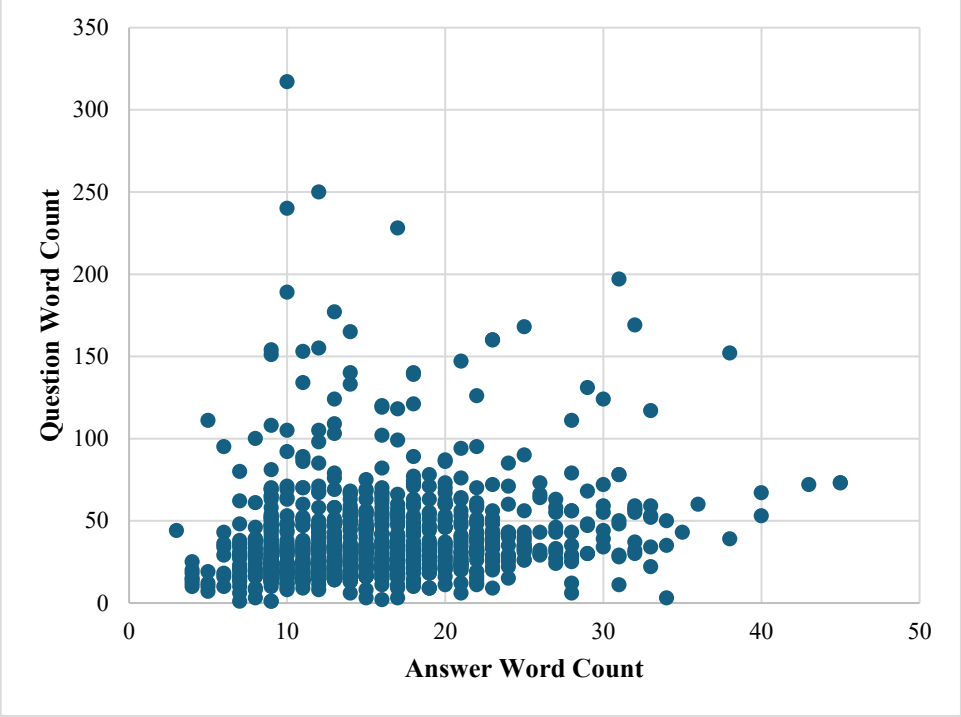


**Figure 1:** Relationship between question length and answer length in the GDPR question–answer dataset, illustrating variability in interpretive depth across legal provisions

**Relevance to Artificial Intelligence Contexts**

The thematic analysis showed that there is a high level of applicability of some of the provisions of the GDPR to data processing using AI. The areas of high frequency such as controller obligations, data subject rights and data transfers between countries relate directly to problems in AI governance such as accountability, user control and global data flows.

Other provisions in regards to automated decision-making and profiling were not prevailing in numbers, but still present and directly applied to the AI systems. The provisions underscope regulatory protections including human control and legal right

to appeal automated decision-making that is essential in algorithmic settings. Distribution of regulatory areas related to AI situations is shown in figure 2.

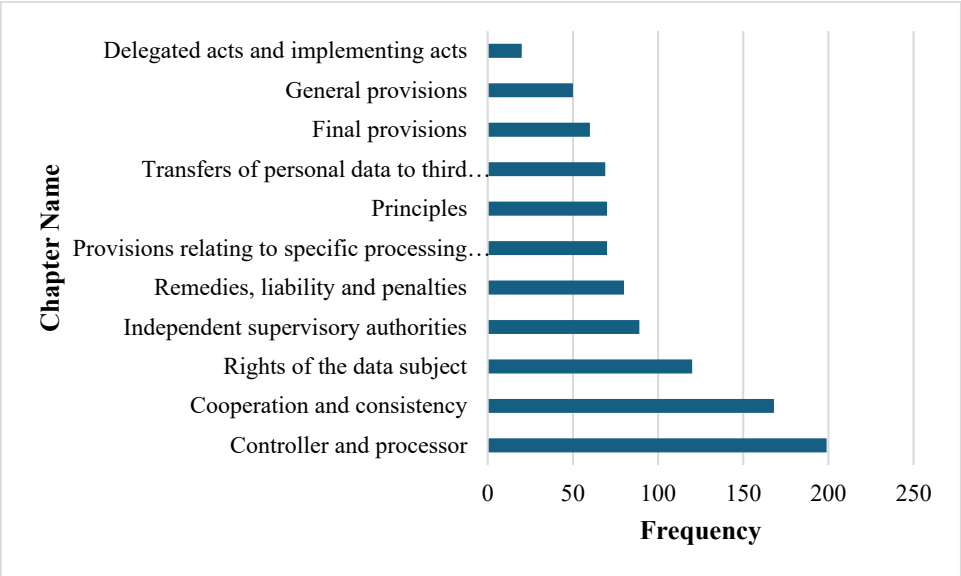


**Figure 2:** Distribution of GDPR regulatory domains relevant to artificial intelligence contexts, highlighting the prominence of governance, accountability, and data subject rights

**Structural Implications for AI Governance**

The data frame format shows that the GDPR regulation is extremely geared towards the regulation mechanisms as opposed to technological specificity. The high value of accountability, enforcement and institutional coordination implies that organizational obligations are used to exercise regulatory control instead of regulating system directly.

This structural orientation is congruent with the requirement of an AI governance where the responsibility tends to be shared among several actors, such as data controllers, data processors and system developers. Nevertheless, the fact that there are not any AI-specific terms or provisions included in the data set, means that the application of GDPR to AI is not based on the planned regulatory implementation but on the interpretive expansion of it.

**Gaps and Deficiency in AI Situation**

The analysis of the collected data suggests that though, GDPR is extensive in its coverage of data protection principles and its governing mechanisms, it does not explicitly cover such important features of AI systems as continuous learning, model opacities, and aggregation of large-scale data. The lack of unambiguous references to algorithmic procedures implies the interpretive mapping of the available provisions on an AI environment.

Moreover, as helpful as the categorization of articles into isolated entries with the goal of granular analysis, can break up the interpretation of complicated provisions when seen in isolation. This is one structural feature that must be carefully consolidated on the legal analysis process in order to ensure the doctrinal coherence.

The results reveal that a comprehensive image of GDPR provisions exists based on the emphasis on accountability, data subjects' rights, and enforcement. The use of GDPR can be facilitated in research on legal analysis and data governance in AI based on its thematic distribution and textual features. However, there are no specific provisions on AI based on the need to apply GDPR through an interpretive approach.

**Discussion**

The fruits of such research show the complexity of the digital rights and the data privacy in the context of the artificial intelligence systems, especially when viewed in the context of the existing regulatory environment. The fact that the AI is becoming an issue in the context of the data privacy systems has led to an increased number of concerns with regard to the accountability and the transparency of the systems. It is a matter of importance to consider the legal provisions and the applicability thereof with a critical eye [17].

The data privacy has evolved from the perspective of the data privacy of an individual to an economic and

institutional concept, showing the importance of the data privacy in the context of the contemporary world [18]. This is especially true with regard to the AI systems, as the information of the individual becomes one of the key resources that is being utilized for the decision-making process. The increased dependence on the data sets also increases the risks that may not be possible to address with the help of the existing legal provisions [19].

Among the key issues observed at this paper, one of them is the association with the interpretation and application of the concept of right to explanation in the GDPR. Although this provision is considered as one of the basis of the accountability of algorithms, it has been argued that such a right is not explicitly protected by the regulation which brings an ambiguity to the practical use of it [18]. The technical acuity of numerous machine learning models is a further disadvantage which is greater because such models are black boxes, meaning they are hard to interpret [24]. Meaningful AI system transparency is therefore an important regulatory and technical challenge.

The issue of accountability becomes another important issue in AI system governance. The ability to outsource the decision on algorithms is a key move towards achieving both the legal and the moral norms. Nonetheless, the decentralized nature of the AI creation, which implies the involvement of multiple players, such as providers of big data, system developers, and end-users, complicates the allocation of responsibility [20]. This level of complexity, therefore, requires the establishment of effective systems of accountability that go beyond being a creation of the law to include technical auditing and monitoring systems [21].

New studies have shown that it is crucial to establish end-to-end accountability systems, which consider the entire lifecycle of AI systems, including the data collection and training of AI models, as well as the deployment and review of AI systems, to ensure that there is a connection between the high-level principles and the implementation to ensure that AI systems operate in a manner that is consistent with regulatory norms and known expectations within a given society [22]. The success of these systems, however, depends on the availability of standardized auditing methodologies and evaluation tools.

The question of equity in AI systems is also problematic, especially when it comes to sociotechnical systems in which there are processes that are both algorithmic and multifaceted social processes [23]. It is a relative concept, and when an effort to formalize it in technical systems is made, there are tendencies to simplify the assumptions, which might not be in line with the real world. This abstraction might have some undesirable effects, such as "reinforcing pre-existing layers of inequality or even creating bias of a different kind."

As a solution to these problems, there are ethical guidelines that have been proposed, and the most important one is transparency, accountability, and fairness. The application of abstract principles, however, has also been criticized as having "no practical implications in terms of enforcement and as being unable to resolve conflicts between values." To illustrate, transparency as an objective may conflict with the need to keep proprietary data confidential or to keep systems secure to the extent that the need for context-specific approach to AI governance is essential [24].

The fact that the AI systems are designed to make high-stakes decisions also raises the need to consider the issues of fairness and accountability in creating the system. Research has suggested that the stakeholders need to have a set of design interventions to ensure that the algorithmic systems are in accordance with the values and the laws of the public sector [25]. This research supports the fact that there is a demand of interdisciplinary efforts between legal professionals, technologists and policymakers to create successful AI governance models.

Generally speaking, as it has been discussed, the current data protection schemes are not able to cover all the problems that are raised by AI technologies. While the regulations, such as the GDPR, are good starting points in terms of the privacy and protection of the data, there is a need to extend the application of such regulations to artificial intelligence systems in terms of their interpretation and evolution. The lack of provisions regarding artificial intelligence is evidence of the need to evolve regulations, with the support of empirical studies and interaction.

**Conclusion**

The research indicates that digital rights and data privacy are being threatened in the wake of the spread of AI and data-driven technologies, which have been advancing at an intense rate. Based on the analysis of structures using the GDPR, it indicates that even though there are regulation frameworks that have been established to provide a solid foundation in the protection of personal data, it does not have all the requirements to deal with the intricacy provided by AI. The principles that have been core in transparency, accountability, and

fairness are still in the forefront but have been limited by the problem of algorithmic opaqueness, volume data processing, and the problem of distributed responsibility. Therefore, the results have indicated that the GDPR has been more focused on the mechanisms of governance rather than being technology-specific. This has led to gaps in the interpretation of the regulations in the context of their application in AI. Dilemmas in the context of AI, such as in the context of decision-making, explainability, and bias, are to be regulated in a more unified way. The ethical systems are solidary to the legal regulations, and in order to be effective, they are to be enforced and applied in context. Adaptive and interdisciplinary approaches are to be made in the context of legal, technical, and ethical insights in order to provide responsible AI governance. The regulation in the context of the future is to be made in a way to resolve the gap between the theoretical frameworks and reality, in a way that the innovation in the sphere of AI would not affect the basic right to privacy.

**References**


1. Gilani SR, Al-Matrooshi AM, Khan MH. Right of privacy and the growing scope of artificial intelligence. *Current Trends in Law and Society*. 2023;3(1):1–1. DOI: 10.52131/ctls.2023.0301.0011
2. Kotov D. Data security and privacy in the age of artificial intelligence. *Universum Technical Science Journal*. 2024;6(123). DOI: 10.32743/UniTech.2024.123.6.17820
3. Martin KD, Murphy PE. The role of data privacy in marketing. *J Acad Mark Sci*. 2017;45:135–155. DOI: 10.1007/s11747-016-0495-4
4. Hsieh C, Shao S, Sung S, Hsieh MH, Tsai DH, Lin S, Lai E. Taiwan's National Health Insurance Research Database (NHIRD): in the era of artificial intelligence, causal inference, and data security. *Clinical Epidemiology*. 2025;17:967–981. DOI: 10.2147/clep.s553894
5. El-Bassal NAM, El-Sayed AAI, Elgamal HG. Empowering nurses in the AI era: investigating the interplay between professionalism, AI readiness, and self-efficacy. *BMC Nursing*. 2025;24(1):1287. DOI: 10.1186/s12912-025-03896-y
6. Mitchell C, Ploem C. Legal challenges for the implementation of advanced clinical digital decision support systems in Europe. J Clin Transl Res. 2018;3(Suppl 3):424–430. DOI: 10.18053/jctres.03.2017S3.007
7. Crowson MG, Tan JZH, Dunn J, et al. The need to develop health data transaction disclosure requirements to balance transparency, privacy, and progressive use. *Lancet Digital Health*. 2026;8(2):100947. DOI: 10.1016/j.landig.2025.100947
8. Friend J, Brindis CD, Upadhyay UD. Abortion AI: Toward an equity-centered research agenda for AI and abortion. *Contraception*. 2025. DOI: 10.1016/j.contraception.2025.111241
9. Yadav N, Pandey S, Gupta A, Dudani P, Gupta S, Rangarajan K. Data privacy in healthcare: In the era of artificial intelligence. *Indian Dermatol Online J*. 2023;14(6):788–792. DOI: 10.4103/idoj.idoj_543_23
10. Elendu C, Amaechi DC, Elendu TC, et al. Ethical implications of AI and robotics in healthcare: A review. *Medicine*. 2023;102(50):e36671. DOI: 10.1097/md.0000000000036671
11. Voigt P, von dem Bussche A. *The EU General Data Protection Regulation (GDPR)*. Springer; 2017. DOI: 10.1007/978-3-319-57959-7
12. Goodman B, Flaxman S. European Union regulations on algorithmic decision making and a "right to explanation." *AI Magazine*. 2017;38(3):50–57. DOI: 10.1609/aimag.v38i3.2741
13. Floridi L, Cowls J, Beltrametti M, et al. AI4People—An ethical framework for a good AI society. *Minds Mach*. 2018;28(4):689–707. DOI: 10.1007/s11023-018-9482-5
14. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nat Mach Intell*. 2019;1(9):389–399. DOI: 10.1038/s42256-019-0088-2
15. Gasser U, Almeida VAF. A layered model for AI governance. *IEEE Internet Comput*. 2017;21(6):58–62. DOI: 10.1109/MIC.2017.4180835
16. Bunescu I. GDPR Articles Dataset. Kaggle; 2023. Available: https://www.kaggle.com/datasets/iuliabunescu23/gdpr-articles-dataset
17. Kuner C, Cate FH, Millard C, Svantesson DJB. The business of privacy. *Int Data Priv Law*. 2013;3(2):65–66. DOI: 10.1093/idpl/ipt003
18. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the GDPR. *Int Data Priv Law*. 2017;7(2):76–99. DOI: 10.1093/idpl/ipx005
19. Rhoen M, Feng QY. Why the 'computer says no': illustrating big data's discrimination risk. *Int Data Priv Law*. 2018;8(2):140–159. DOI: 10.1093/idpl/ipy005

20. Diakopoulos N. Accountability in algorithmic decision making. *Commun ACM*. 2016;59(2):56–62. DOI: 10.1145/2844110
21. Selbst AD, Boyd D, Friedler SA, et al. Fairness and abstraction in sociotechnical systems. 2019. DOI: 10.1145/3287560.3287598
22. Raji ID, Smart A, White RN, et al. Closing the AI accountability gap. 2020. DOI: 10.1145/3351095.3372873
23. Whittlestone J, Nyrup R, Alexandrova A, Cave S. The role and limits of principles in AI ethics. 2019. DOI: 10.1145/3306618.3314289
24. Burrell J. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data Soc*. 2016;3(1). DOI: 10.1177/2053951715622512
25. Veale M, Van Kleek M, Binns R. Fairness and accountability design needs. 2018. DOI: 10.1145/3173574.3174014