Mariami Giorgadze*

Legal Regulation of Artificial Intelligence Systems and Challenges related to Personal Data Protection

The objective of this article is to examine the current legal framework governing artificial intelligence, as well as the prevailing challenges concerning fundamental human rights, particularly the right to privacy and the protection of personal data in the context of AI operation and development. This study further explores the complexities and international best practices related to the processing of personal data by and through artificial intelligence.

***Keywords**: Artificial intelligence, fundamental human rights, personal data, legal regulation, data protection.*

1. Introduction

The advancement of technology has played a pivotal role throughout human history, profoundly transforming everyday life. A notable example is the series of industrial revolutions, which have driven significant social and economic changes since the late 18th century[1]. This evolution represents a continuous sequence of technological advancements, and today, in the era of the Fourth Industrial Revolution, artificial intelligence (AI), as one of its key manifestations, has the potential to bring about systemic transformations across various scientific fields and in daily human life[2].

The concept of artificial intelligence as a machine capable of human-like thinking emerged in the latter half of the 20th century. In 1950, the English

* Master of Law (LL.M.) at Ivane Javakhishvili Tbilisi State University, Faculty of Law; Specialist at the Office of the President, Personal Data Protection Service of Georgia.

[1] *Stearns P. N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013, 9-14.

[2] *Schwab K.,* The Fourth Industrial Revolution, Encyclopedia Britannica, 2023, <https://www.britannica.com> [10.01.2025].

scientist Alan Turing introduced the idea of creating a machine that could "think" at a human level through a learning algorithm, formulating the "Turing Test"[3]—a criterion for assessing whether a machine can replicate human thought processes[4]. Since then, AI has undergone multiple stages of development, including periods of waning interest, before reaching its current state of advanced capabilities[5]. An intriguing hypothesis presented in scientific literature suggests that the origins of modern artificial intelligence stem from a convergence of various distinct disciplines: philosophical inquiries into the relationship between human cognition and information processing, economic models for decision-making optimization, neuroscientific research into brain function and structure, and the mathematical and engineering advancements that have enabled the development of AI models as they exist today.[6]

Today, artificial intelligence and AI-driven technologies have become deeply integrated into various aspects of society and numerous scientific fields—what was once considered a "technology of the future" is now an integral part of reality. AI is widely utilized across social media, finance, education, and the medical sector[7]. Its global popularization has been significantly accelerated by the emergence of generative AI models, particularly ChatGPT[8].

The advancement of artificial intelligence systems holds great potential for enhancing and simplifying everyday life, as well as contributing to scientific progress. However, it is crucial to recognize that AI is not flawless, and in the context of automated decision-making, the risks to fundamental human rights intensify. AI models are developed and continuously refined through the processing of vast amounts of data, with decision-making and predictions often relying on information that includes personal data. Consequently, as artificial intelligence becomes the cornerstone of the world's technological future, it is imperative to remain vigilant in safeguarding individual rights—

[3] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., Pearson, 2021, 35-36.

[4] An examiner who communicates in writing with a machine and a real person must identify who is on the other side of the communication - a person or a machine that thinks like him. Additionally - Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].

[5] *Kingsley O. A.,* Artificial Intelligence Research: a Review on Dominant Themes, Methods, Frameworks and Future Research Directions, Telematics and Informatics Reports, Volume 14, 2024.

[6] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., 2021, 35-36.

[7] *Gleeson B.,* How AI Is Reshaping The Future Of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024]

[8] ChatGPT is a product of OpenAI, which has gained significant global attention for its artificial intelligence products since 2020-2022. It is a so-called "chatbot" capable of communicating and generating information in a manner similar to human interaction.

particularly the right to privacy and the protection of personal data—of those who are part of this evolving digital society.

The growing relevance of artificial intelligence, alongside digital technologies more broadly, presents significant challenges concerning fundamental human rights. In this context, the actions taken by supervisory authorities within their mandates play a particularly crucial role. Notably, one of the key priorities outlined in the 2025 Plan[9] for Scheduled Inspections of the Lawfulness of Personal Data Processing, established by the President of the Personal Data Protection Service, focuses specifically on modern technologies—encompassing both private and public institutions[10]. This initiative holds substantial importance in shaping national standards for personal data processing, advancing legal and practical frameworks, and safeguarding the right to privacy in the era of rapid technological development.

Furthermore, the European Data Protection Board (EDPB), at its 102nd plenary session on February 11, 2025, resolved to establish a Task Force on Artificial Intelligence[11], underscoring the increasing global attention on data processing by AI systems.

This paper examines the concept of artificial intelligence, the current state of legal regulations in this field, the existing and anticipated challenges posed by AI-driven technologies—particularly concerning personal data protection—and the critical considerations that must be addressed when processing data through artificial intelligence.

2. The Concept and Legal Regulation of Artificial Intelligence

2.1. The Concept of Artificial Intelligence: Systems and Models

The term “artificial intelligence” and its emergence as a distinct scientific field are linked to the 1956 Dartmouth Conference, where a group of researchers[12] sought to explore ways in which “machines could use language,

[9] Order No. B/1259 of the President of the Personal Data Protection Service of December 31, 2024 "On Approval of the Plan for Scheduled Inspections of the Lawfulness of Personal Data Processing for 2025".
[10] Ibid., Appendix №1 and №2.
[11] European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].
[12] John McCarthy (Assistant Professor of Mathematics, Dartmouth College), Marvin Minsky (Junior Fellow in Mathematics and Neuroscience, Harvard University), Nathaniel Rochester (Manager of Information Research, IBM Corporation), Claude Shannon (Mathematician, Bell Telephone Laboratories).Additionaly - History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence,

concepts, and abstractions to solve problems that were, at the time, considered uniquely human.[13]"

According to the modern definition, an artificial intelligence (AI) system is "a system based on machine technologies that, either explicitly or implicitly, analyzes how to generate outcomes—such as predictions, content, recommendations, or decisions—based on the information provided to it, which may influence the physical or virtual environment.[14]" Furthermore, AI systems exhibit varying degrees of autonomy[15] and adaptation during and after operation:

Autonomy – Refers to the extent to which an AI system can learn and operate independently, without human intervention, once granted autonomy and integrated into automated processes.

Adaptation – Denotes the system's ability to continue evolving beyond its initial development. This characteristic is particularly relevant to AI models based on machine learning, where the system refines its behavior through interaction with incoming data—such as a recognition system that adapts to an individual's voice over time.[16]

Machine learning is a model of artificial intelligence that replicates human learning through data and algorithms, enabling AI to make predictions and decisions based on new, similar data without requiring explicit programming for each specific task[17]. Various machine learning methods and algorithms are employed today, including linear regression, logistic regression, and decision trees, among others, each tailored to different types of data and problem-solving needs. Among these, one of the most widely used is the artificial neural network, which mimics the structure and functions of the human brain, allowing for the processing and analysis of complex data[18].

Deep learning, a subset of machine learning, utilizes multiple layers of neural networks (deep neural networks) and is capable of making decisions in

<https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].

[13] McCarth J., Minsky M.L., Rochester N., Shannon C. E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, 2, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Article 3(1).

[15] Organisation for Economic Co-operation and Development (OECD), Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.

[16] Ibid, 6.

[17] *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, 19, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf>.

[18] IBM, What is Artificial Intelligence (AI), <https://www.ibm.com/think/topics/artificial-intelligence?> [09.08.2024].

a manner akin to human cognition[19]. Leveraging specialized AI models—built upon foundational models such as Large Language Models (LLMs)—generative AI can perform various tasks, including the generation of text, images, and audio[20]. Prominent examples of such AI systems include ChatGPT, Gemini, Siri, and DALL·E 3, along with other widely recognized applications and platforms.

It is essential to emphasize that artificial intelligence models, while serving as fundamental components of AI systems, do not constitute AI systems in themselves. These models require additional elements—such as a user interface—to be integrated into a broader AI system[21]. The development of advanced and complex AI models is significantly influenced by the quantity, diversity, and quality of data used during the training process, which in turn affects the system's functionality and the challenges associated with it.

In addition to the numerous advantages of artificial intelligence highlighted thus far, AI also presents various risks. For instance, it may facilitate the spread of disinformation by generating synthetic content that humans perceive as real, or produce "hallucinations", where AI models convincingly convey false information. Bias and discrimination in AI-driven decisions and predictions, as well as data protection risks at different stages—including training, model operation, and human interaction—are also key concerns. Furthermore, AI presents challenges related to transparency and explainability, particularly in the case of so-called "black box" models, where decision-making processes remain opaque. The inability to appeal AI-generated outcomes and the risk of confidentiality breaches in cases of data protection incidents further highlight the need for a well-regulated and responsible approach to AI development and deployment.[22]

2.2. Legal Regulation of Artificial Intelligence

The challenges associated with the development and ethical use of artificial intelligence have led several modern nations to recognize the necessity of its legal regulation.

On August 1, 2024, the European Union's Artificial Intelligence Act entered into force. As the first legal regulatory framework for AI systems, it

[19] European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024, <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [09.08.2024].
[20] European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024, <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [09.08.2024].
[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 97.
[22] *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.

aims to safeguard security, fundamental rights, and ethical principles throughout the development and deployment of artificial intelligence[23]. The regulation addresses key issues such as high-risk and general-purpose AI, establishes rules for their governance, defines prohibited uses of AI, and mandates the creation of AI-related supervisory bodies at various levels. The act is set to be implemented in stages, with its full enforcement scheduled for 2030.[24]

On September 5, 2024, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy[25], and the Rule of Law was opened for signature, with Georgia as a contracting party[26]. This convention represents the first legally binding international instrument designed to balance AI usage with human rights protections. It outlines the fundamental principles that AI systems must adhere to throughout their lifecycle. Furthermore, on November 28, 2024, the Council of Europe Committee on Artificial Intelligence (CAI) approved HUDERIA, a tool designed to assist both public and private institutions in assessing AI-related risks to ensure the protection of human rights, democracy, and the rule of law.[27]

In addition to the aforementioned legal acts, opinions, studies, instruments, and various guidance recommendations developed by international organizations play a crucial role in the legal regulation of artificial intelligence. Notably, the Organization for Economic Cooperation and Development (OECD) has made significant contributions in this area, with its definition of an artificial intelligence system closely aligned with the concept outlined in the EU Artificial Intelligence Act. The OECD conducts extensive research and analysis to examine the transformative impact of artificial intelligence on society and the economy[28].

The United Nations Educational, Scientific and Cultural Organization (UNESCO) is also actively engaged in AI-related matters, focusing on areas such as the ethics of artificial intelligence, the use of AI systems in education, and

[23] EDPS, Artificial Intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [10.01.2025].
[24] <https://artificialintelligenceact.eu/implementation-timeline/> [01.06.2024].
[25] Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.
[26] Council of Europe (CoE), The Council of Europe Framework Convention on Artificial Intelligence, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> [10.01.2025].
[27] *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28.11.2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [09.08.2024].
[28] OECD, OECD Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [09.08.2024].

the intersection of artificial intelligence and gender equality, among other key issues.[29]

The United Nations (UN) continues to be actively involved in the development and regulation of artificial intelligence. An advisory body on artificial intelligence was established, and in March 2024, a resolution was adopted calling on states and other stakeholders to ethically develop, deploy, and operate AI systems, while ensuring the protection of human rights and freedoms[30].

In Georgia, the only existing legislation related to artificial intelligence is the 2020 Order of the President of the National Bank of Georgia, titled "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence, and Machine Learning Models". This order aims to establish a risk management framework for data-based statistical, AI, and machine learning models, promoting effective management of associated risks. It also outlines the process for building and using these models, particularly for entities under the supervision of the National Bank of Georgia[31].

Additionally, the Law on the State Budget of Georgia for 2025 includes plans related to artificial intelligence, including:

- Supporting the development of AI systems to benefit Georgian citizens and various sectors of the economy;
- Creating an international center of competence for AI, equipped with modern technologies and international expertise;
- Implementing AI systems to enhance the efficiency of the Ministry of Justice of Georgia's analytical and law-making activities, legal expertise of state contracts, and the conduct of proceedings in international courts and arbitrations, as well as providing simplified services to users of the Georgian Legislative Gazette;
- Studying and analyzing global AI trends, preparing conclusions and recommendations for adapting Georgian legislation to digital standards, and raising public awareness. Furthermore, the establishment of a Center for Legal Research on Artificial Intelligence is planned, based on the Training Center of the Ministry of Justice of Georgia.[32]

[29] *United Nations Educational, Scientific and Cultural Organization (UNESCO),* Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [09.08.2024].

[30] United Nations (UN), Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [09.08.2024].

[31] Order No. 151/04 of the President of the National Bank of Georgia of August 17, 2020 "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence and Machine Learning Models".

[32] Law of Georgia "On the State Budget of Georgia for 2025", 45-Ims-XImp, 10.12.2024, Article 15, §3 and §6.

Based on these developments, it is clear that artificial intelligence is not only one of the most trending fields of modern technology at the international level, but at the national level, the state is highly committed to promoting its integration across various sectors. This signals that the challenges posed by AI are not only a current concern, but its active integration into multiple fields will likely amplify its impact on fundamental human rights and freedoms.

3. Challenges related to the Processing of Personal Data by Artificial Intelligence

3.1. Data Processing by/through Artificial Intelligence and the Role of Data Supervisory Authorities in Regulating Systems

As previously noted, artificial intelligence (AI) systems require large amounts of data for their creation, development, and use, often involving the processing of personal data[33]. Under both international (e.g., the GDPR, Convention 108)[34] and national legislation (Georgian Law on Personal Data Protection), data processing includes any operation performed on data, such as collection, retrieval, interconnection, or grouping.[35]

AI systems may process personal data at various stages, including design, marketing, operation, and development. If personal data processing is required—such as for machine learning—it falls under data protection regulations. Additionally, an AI system may itself contain personal data, and its distribution may constitute processing if such data is disclosed to third parties.

AI can also be used for automated decision-making and profiling. For example, in resume filtering, where personal data is processed automatically, potentially leading to legal or other significant consequences[36].

[33] Personal data is “any information relating to an identified or identifiable natural person.” See Law of Georgia “On Personal Data Protection”, 3144-XIMs-XMP, 14.06.2023, Article 3, subparagraph “a”.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.

[35] Ibid Article 3, subparagraph "f".

[36] *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, 2023, <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [09.08.2024].

The use of artificial intelligence (AI) systems can be particularly significant in the medical field, enabling the rapid and accurate diagnosis of various conditions. In such cases, personal data may be collected through various devices, sensors, clinical equipment, or medical examinations. AI systems may process patient data during training, testing, and ongoing evaluation to enhance their functionality.

Typically, this involves processing special categories of data, which are more sensitive in relation to human rights and freedoms. As a result, such data is subject to specific regulations, necessitating depersonalization or pseudonymization to prevent the identification of individual patients [37].

Given the above, the involvement of data protection supervisory authorities in regulating artificial intelligence (AI) systems has become increasingly relevant. Today, a significant portion of the research and activities conducted by supervisory authorities and international data protection organizations focus specifically on AI. For instance, the UK's data protection supervisory authority, the Information Commissioner's Office (ICO), has designated AI as a priority area due to its high potential risks to individuals and their rights[38]. Similarly, the Spanish data protection supervisory authority, the Agencia Española de Protección de Datos (AEPD), has issued various recommendations on the use of AI in different contexts, such as biometric data processing[39]. Additionally, in some cases, supervisory authorities have evaluated instances of AI-driven data processing, which will be analyzed in the following chapters.

The 2023 Global Privacy Assembly (GPA) Resolution on Generative AI Systems emphasizes that data protection and processing principles form the fundamental basis for AI system development and operation. These principles include the lawfulness of processing, purpose specification and limitation of further use, data minimization, accuracy, transparency, security, accountability, the protection of data subjects' rights, and the prioritization of data protection by default before considering alternative approaches [40].

---

[37] *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the "Patient–Doctor" Relationship, 2024, 7-8.

[38] Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [09.08.2024].

[39] Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [09.08.2024].

[40] *Global Privacy Assembly(GPA),* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, 5-9, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf> [09.08.2024].

3.2. Key Issues related to Data Processing by Artificial Intelligence Systems

Both during the development of artificial intelligence (AI) systems and their subsequent use, the processing of data by these systems must be carefully considered. This includes information about various groups of individuals used in the training process—whether obtained from public sources or provided by users during system interaction. Additionally, when individuals or organizations process third-party personal data using AI technologies—such as in the banking sector for risk assessment, in employment services for evaluating candidates, in the medical field for timely disease diagnosis, or in law enforcement for identifying criminal activity—it is essential to uphold data processing principles. Furthermore, organizations must assess the legal basis for processing data in this manner to ensure compliance with relevant regulations.

3.2.1. Processing of Personal Data for the Development of Artificial Intelligence Models

The EU Artificial Intelligence Act establishes obligations and additional safeguards to ensure privacy and the protection of personal data throughout the entire lifecycle of an AI system. It emphasizes that personal data processing must adhere to the principle of data minimization and prioritize data protection as the default approach when developing new products or services before considering alternative methods. Furthermore, the Act requires providers to ensure compliance with these principles by implementing measures such as depersonalizing data, encrypting it, and utilizing technologies that allow AI systems to be trained without copying raw data or transferring it between parties.[41]

The processing of personal data by artificial intelligence (AI) presents various challenges. For instance, the growing demand for generative AI chatbots has highlighted the need to establish appropriate age restrictions.

[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 69.

Minors may be less aware of the risks associated with providing their personal data to such systems and may lack the ability to effectively safeguard their rights. According to UNESCO recommendations, the minimum age for using these systems should be set at 13 years[42]. Additionally, states must assess whether self-reported age verification is sufficient and ensure that providers of generative AI systems are held accountable in this regard. Furthermore, the responsibilities of parents and legal guardians in monitoring interactions between individuals under 13 years of age and AI systems should be clearly defined.

In one case involving data processing through an AI chatbot—designed to enhance users' emotional well-being, track character development, and assist in managing anxiety and stress—the data protection supervisory authority determined that processing minors' data could not be based on contractual performance. Given the absence of an effective age verification mechanism, the authority restricted the AI system's data processing for all users until the entity responsible for processing rectified the identified deficiencies.[43]

Artificial intelligence (AI) systems may process an unlimited amount of personal data, including both user-provided information and data collected during training. Therefore, it is essential to ensure data security by implementing all appropriate safeguards. For example, in 2023, a technical flaw in ChatGPT temporarily allowed users to interact with other users of the AI, leading to the exposure of personal data such as names, email addresses, and credit information. In this case, the supervisory authority held the controller accountable for failing to notify the incident and for not adequately assessing the legal basis for data processing during the training process, which was inconsistent with the obligation of accountability. Additionally, the privacy policy was only available in English and was not easily accessible to users, despite the AI system also processing the personal data of unregistered users. The company failed to disclose this in its policy document, thereby violating the principle of transparency[44]. These concerns are particularly significant in the context of AI-driven data processing, as a lack of awareness regarding the processing of personal data can limit fundamental rights, such as the right to appeal and the right to request information.

[42] UNESCO, Towards a human-centered approach to the use of generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [09.08.2024].

[43] *Garante per la Protezione dei Dati Personali (Garante)*, [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [09.08.2024].

[44] *Garante per la Protezione dei Dati Personali (Garante)*, [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [09.08.2024].

Data serves as the foundation for any artificial intelligence (AI) system, and its quality directly influences the outcomes produced by these systems. Incorrect or biased data representation can result in unfair or biased decisions and predictions. Historical data used in the training process may carry age-old social stigmas and reflect past discriminatory practices[45]. In addition to these historical biases, discriminatory approaches may arise from the improper representation of the characteristics of social groups or other relevant information during the training of AI systems. Overall, the processing of data from individuals by such AI systems may be degrading or otherwise negatively affect the rights of the data subject to whom the system is applied.

In the context of artificial intelligence (AI) models, issues concerning the "anonymity" of AI models (meaning that the AI does not process data related to an identified or identifiable person) and lawful data processing (based on legitimate interest) are of particular importance.

According to the European Data Protection Board (EDPB), the "anonymity" of an AI system should be assessed on a case-by-case basis. The EDPB asserts that AI systems whose training involved personal data cannot be considered anonymous under any circumstances. For an AI system to be regarded as depersonalized, it is necessary to obtain (or be able to obtain) the personal data of the individuals whose data was used during the development of the AI model. Additionally, the probability of retrieving these data through queries to the system—whether intentionally or unintentionally—must be minimal, considering the reasonable expectations of the controller or another responsible party.

The opinion further emphasizes that the assessment of the data protection supervisory authority should be based on the documentation provided to demonstrate the anonymity of the model.[46]

Regarding the processing of data based on legitimate interest for the development and operation of AI models, the European Data Protection Board (EDPB) emphasizes that there is no hierarchy between the grounds for processing data, and data controllers must identify the appropriate legal basis for their processing activities. Additionally, a three-step test must be applied when assessing legitimate interest. This includes: (1) identifying the existence of a legitimate interest, (2) determining the necessity of the processing to

[45] *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, 32,
<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [09.08.2024].

[46] *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43, <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> [09.08.2024].

achieve that interest, and (3) assessing the balance of interests between the legitimate interest and the rights and freedoms of the data subjects. [47]

It is important to note that legitimate interest must be (1) lawful, (2) clearly and specifically formulated, and (3) real (rather than abstract). In the case of artificial intelligence models, an example of a legitimate interest might be improving methods for identifying threats to an information system. The necessity of processing must be assessed in terms of (1) how useful the data processing is for achieving the legitimate interest and (2) whether there is a less restrictive way to achieve the same goal. When designing or developing AI methods, it is crucial to assess the proportionality of the data used—ensuring data minimization. When assessing the balance of interests, the categories of personal data, the context of the processing, and the potential impact on the rights of the data subjects should all be considered. Additionally, the reasonable expectations of the subjects regarding the use of their data must be taken into account.[48]

The EDPB opinion also highlights the need to implement appropriate measures to mitigate any negative impacts on the rights of the data subject. These measures differ from the mandatory provisions outlined in the General Data Protection Regulation and should be tailored to the specific characteristics of the AI model, its purpose, and the circumstances of the particular case.[49]

3.2.2. Processing of Personal Data through Artificial Intelligence

Depending on the purpose of artificial intelligence (AI), its conclusions or predictions may necessitate the processing of personal data of specific individuals. In cases where the use of modern technologies, based on the processing of personal data, may result in decisions that affect the individual, leading to legal or other consequences, there may be potential negative impacts on the fundamental rights and freedoms of the data subject. Consequently, individuals or entities using such technologies, as data controllers, have certain obligations, particularly with regard to personal data protection. In this context, it is essential to address issues such as

[47] *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, Version 1.0 (for public consultation), 2024, §12, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [09.08.2024].
[48] *EDPB*, Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024.
[49] Ibid.

transparency, accountability, lawfulness and fairness of the processing, data security, and conducting data protection impact assessments, among others.

The use of AI across various fields serves different purposes. For example, in the business sector, AI may be used to customize offers and services by analyzing user behavior; in the education sector, to facilitate processes and create personalized learning plans; in healthcare, to detect disease symptoms in a timely manner, diagnose conditions, and analyze diagnostics[50]; and in employment, to predict the likelihood of success in applying for a specific position based on personal information such as professional experience, education, and test results

In such cases, it is essential to first assess the legal basis that an organization may have for processing data through artificial intelligence (AI). For example, certain information about a user may be necessary to place an order or provide a service to them. However, a different legal basis may be required for further processing of this information through AI to analyze the subject's preferences. In most cases, this could be consent or legitimate interest. Additionally, if the basis for processing data through these technologies is the consent of the data subject, the subject should voluntarily give consent only after being provided with clear and understandable information. As for legitimate interest, this should be assessed individually in each specific case, with the criteria discussed in the previous chapter being considered. For example, in a decision by the Hungarian Data Protection Supervisory Authority, concerning a bank’s use of AI to analyze emotional elements of customer conversations to assess satisfaction, the subjects were informed about audio monitoring. However, they were not informed about the further processing of these recordings. The bank considered legitimate interest—quality control—as the basis for the data processing. The supervisory authority ruled that the processing of audio recordings of customers and employees using AI was unlawful. This decision was based on the fact that the legitimate interest assessment did not account for the proportionality of the processing. Furthermore, the users were not informed about the analysis of their voice, meaning they could not exercise their right to "opt out". Additionally, the impact assessment did not include mitigating measures to reduce the impact and risks to the rights of the data subjects. Based on these

[50] World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].

factors, the supervisory authority determined that the processing of personal data of users and employees through AI was inconsistent with the law. [51]

When processing data using artificial intelligence systems, it is also crucial to consider the principle of data minimization. According to the recommendation of the UK supervisory authority (ICO), employment agents should assess the information collected by artificial intelligence when using systems in the course of their activities. They must ensure that only the minimum necessary information is collected for the purposes of processing and that this data will not be used by AI providers for different purposes[52]. This approach should also be applied to other data processing processes involving artificial intelligence.

Transparency is one of the most important principles of data processing, and it requires that data subjects be provided with information about the processing of their personal data in a concise, easily understandable language, with the information being easily accessible[53]. Adhering to this principle can be particularly challenging when processing data through artificial intelligence, as many machine learning models are "black boxes" and do not explain their predictions in a way that is understandable to humans[54]. Consequently, interpreting and explaining decisions made by AI systems may be difficult even for those directly working with them, which creates specific challenges for the data controller in fulfilling their obligations.

The fair and dignified processing of data is also a fundamental principle that must be respected in all processing activities. As mentioned in the previous chapter, since the performance of artificial intelligence systems relies on the data used in their training process, there is a significant risk that these systems may not adequately reflect the characteristics of all societal groups or may be based on historical data that contains various stigmas. This can later lead the data controller to make biased, discriminatory decisions when using the system. Artificial intelligence systems are characterized by both historical, social, and algorithmic biases[55]. For instance, an artificial intelligence system used in the field of employment, whose training process was based on resumes

[51] *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [09.08.2024].
[52] *ICO,* AI tools in recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [09.08.2024].
[53] *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.
[54] *Cynthia Rudin,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, VOL 1, 2019, 206–215, <https://doi.org/10.1038/s42256-019-0048-x> [09.08.2024].
[55] *Dr. Kris SHRISHAK,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, *EDPB,* Support Pool of Experts Programme, 2024, 5-6, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [09.08.2024].

predominantly from male candidates, may, when deployed, filter out female candidates and preferentially select male candidates.[56]

In relation to the processing of data by means of artificial intelligence, it is also important to consider that the data subject has the right not to be subject to a decision made solely by automated means, which produces legal or other significant effects on them, except in cases where there is consent from the subject, it is necessary for the performance or conclusion of a contract, or it is provided for by law or subordinate acts[57]. Therefore, in these cases, decisions affecting the data subject should not be based solely on the predictions or conclusions of the system and must involve human supervision.

Due to the increased risk to the rights of the data subject and the high risk of their infringement, a data protection impact assessment may be necessary before processing data using artificial intelligence systems. This provides an additional safeguard for the protection of the subject's rights and helps the data controller demonstrate accountability and the lawfulness of processing[58]. An organization that decides to process data through artificial intelligence must ensure the security of these systems, including through technical or confidentiality documentation of the technology, and conduct periodic supervision within the scope of its competence.

4. Conclusion

Artificial intelligence is currently at the forefront of modern technologies and holds significant potential for the advancement of various fields. The application of these systems across sectors such as education, healthcare, law enforcement, business, and other areas vital for societal development can serve a range of purposes depending on the specific needs of each sector. AI can simplify tasks, analyze information, assess risks, make decisions, or predict/diagnose in a shorter timeframe. Given its expanding capabilities, there has been an increasing need for legal regulation of AI globally, leading to the development of frameworks such as the European Union Artificial Intelligence Act and the Council of Europe Framework Convention on Artificial Intelligence.

[56] *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [09.08.2024].
[57] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14.06.2023, Article 19 (1).
[58] *ICO,* How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [09.08.2024].

Moreover, the research and recommendations from various international organizations play a critical role in ensuring the ethical and human rights-compliant use of these systems. This lays the groundwork for creating and enhancing legal frameworks for these technologies and contributes to their effective implementation.

The creation of artificial intelligence systems requires a large volume of data, including personal data, with particularly high data demands in complex models. The processing of information about individuals by artificial intelligence is relevant not only during its training and development stages but may also encompass its entire "life cycle." Personal data processing can be carried out by organizations directly involved in artificial intelligence systems, as well as by data controllers who process data of individuals using artificial intelligence within the scope of their activities across various sectors. In many instances, this form of automated processing has the potential to pose threats to the fundamental rights of individuals.

When processing data using artificial intelligence, both individuals working with these technologies and organizations utilizing them must consider issues such as the legal basis for data processing, as well as the principles of minimization, transparency, fairness, purpose limitation, and security. Additionally, data protection regulations should be adhered to, particularly in cases involving decision-making through automated data processing. A data protection impact assessment should be conducted, especially when artificial intelligence is applied in sectors such as healthcare or in activities involving the processing of special categories of data. Furthermore, data subjects must be adequately informed, as failure to do so may result in the negligent restriction of their rights as data subjects.

Data protection supervisory authorities can play a crucial role in preventing and effectively addressing the negative impacts of data processing by artificial intelligence systems. It is important to emphasize the need for recommendation-type documents and policy guidelines related to these technologies. Furthermore, to mitigate the impacts of artificial intelligence systems and ensure their effective use—while safeguarding rights—it is essential to engage in various awareness-raising activities to inform the public. Such efforts will significantly contribute to reducing the negative consequences associated with these technologies.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
2. Law of Georgia "On the State Budget of Georgia for 2025", 10/12/2024.
3. Order No. B/1259 of the President of the Personal Data Protection Service of December 31, 2024 "On Approval of the Plan for Scheduled Inspections of the Lawfulness of Personal Data Processing for 2025".
4. Order No. 151/04 of the President of the National Bank of Georgia of August 17, 2020 "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence and Machine Learning Models".Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12/07/2024.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12/07/2024.
6. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04/05/2016.
8. Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [20.02.2025].
9. *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, [2023], <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [20.02.2025].
10. *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.
11. *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [20.02.2025].

12. *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the "Patient–Doctor" Relationship, September 2024.
13. *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28/11/2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [20.02.2025].
14. *EDPS*, Artificial intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [20.02.2025].
15. *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, 2024, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [20.02.2025].
16. *Gleeson B.,* How AI Is Reshaping the Future of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024].
17. Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].
18. History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence, <https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].
19. Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [20.02.2025].
20. *Information Commissioner's Office (ICO),* How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [20.02.2025].
21. *Information Commissioner's Office (ICO),* AI Tools in Recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [20.02.2025].
22. IBM, What is Artificial Intelligence (AI)?, <https://www.ibm.com/think/topics/artificial-intelligence> [09.08.2024].
23. *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf> [20.02.2025].

24. *Kingsley O. A.,* Artificial intelligence research: A review on dominant themes, methods, frameworks and future research directions, Telematics and Informatics Reports, Volume 14, 1.1, 2024, <https://doi.org/10.1016/j.teler.2024.100127> [20.02.2025].
25. *McCarth J., Minsky M. L., Rochester N., Shannon C. E.,* A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 31.08.1955, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> [20.02.2025].
26. OECD, Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [20.02.2025].
27. *Organisation for Economic Co-operation and Development* (*OECD),* Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.
28. *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.
29. *Russell S. J., Norvig P.,* Artificial Intelligence: A Modern Approach, 4th Global Edition, Pearson Education Limited, 2021.
30. *Rudin C.,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, Vol. 1, 2019, 206-215.
31. *Shrishak K.,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, EDPB, Support Pool of Experts Programme, 2024, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [20.02.2025].
32. *Schwab K.,* The Fourth Industrial Revolution, Encyclopedia Britannica, 31.05. 2023, <https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734> [10.01.2025].
33. *Stearns P. N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013.
34. The European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].
35. *The European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024,*

<https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [20.02.2025].

36. *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43.
37. *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [20.02.2025].
38. *The Global Privacy Assembly,* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf>
39. UNESCO, Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [20.02.2025].
40. *UNESCO,* Towards a Human-Centred Approach to the Use of Generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [20.02.2025].
41. *United Nations (UN),* Seizing The Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [20.02.2025].
42. World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].
43. *Garante per la Protezione dei Dati Personali (Garante),* [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [20.02.2025].
44. *Garante per la Protezione dei Dati Personali (Garante),* [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [20.02.2025].
45. *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [20.02.2025].
46. <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed> [20.02.2025].
47. <https://artificialintelligenceact.eu/implementation-timeline/> [20.02.2025].