Otar Chakhunashvili[*]

Salome Sigua[**]

Legal Aspects of Artificial Intelligence and Personal Data Protection Regulation: An Overview of National and International Practice[***]

The rapid development of information technologies and the integration of artificial intelligence (AI) into the public and private sectors have significantly expanded data processing activities. This process is accompanied by important legal and ethical challenges related to data protection.

The article aims to analyze the legal framework governing the processing of personal data by artificial intelligence systems in both international and national legislation. It examines the existing regulations, their effectiveness, and their compliance with the realities of modern technology.

Particular attention is given to the adequacy of current legal norms in addressing the unique capabilities and risks of AI, including issues of algorithmic bias, transparency, and the protection of users' rights.

Keywords: *Artificial Intelligence, personal data protection, algorithmic bias, protection of users' rights.*

1. Introduction

In the process of technological progress, numerous important issues arise, the fulfillment of which is considered essential in a democratic society. The protection of personal data is among those rights that have gained particular attention alongside the development of social relations and the means to regulate them. The right to

[*] Doctor of Law, Assistant Professor at the Faculty of Law of Ivane Javakhishvili Tbilisi State University. First Deputy Head of the Personal Data Protection Service.

[**] Invited Lecturer at the Faculty of Law of Ivane Javakhishvili Tbilisi State University.

[***] The article was prepared within the framework of the Young Scientists Grant Competition (YS-23-3460) funded by the Shota Rustaveli National Science Foundation of Georgia.

personal data protection is generally viewed as part of the broader right to privacy or the right to respect for private life. At first glance, these two rights may appear analogous and even interchangeable. However, within the European context, both are regarded as vital components of a sustainable democracy.

It is undeniable that artificial intelligence represents one of the latest scientific achievements in humanity's technological development, which will be applied — and indeed dominate — many fields in the near future. The Fourth Industrial Revolution can essentially be characterized by the development of new technologies such as artificial intelligence, robotics, nanotechnology, quantum computing, biotechnology, the Internet of Things (IoT), and blockchain, all of which will transform the way society lives and works.

There are many questions surrounding artificial intelligence; however, one of the most pressing issues today concerns the processing of personal data by AI systems. This technology is rapidly evolving, and the data it processes vary in both volume and content. Artificial intelligence learns from information obtained from multiple sources and processes vast amounts of data based on pre-defined algorithms. Consequently, it can be said that data have become the only "fuel" for artificial intelligence.

2. Analysis of National and International Legislative Acts Regulating Personal Data

Personal data refer to any information relating to an identified or identifiable natural person. Personal data may also consist of a combination of different pieces of information that, when processed together, allow the identification of an individual.[1] According to the legislation of the European Union and the Council of Europe, personal data are defined as information relating to an identified or identifiable natural person[2] whose identity is known or can be determined based on additional information. In determining whether a person is identifiable, the controller or any other entity engaged in data processing must take into account all reasonable means that could be used, either directly or indirectly, to identify the individual.[3]

The principle of the rule of law is one of the most important foundations of a democratic state.[4] In a state governed by the rule of law, the highest social values are

[1] European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].
[2] General Data Protection Regulation, Article 4(1); Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), Article 2(a).
[3] General Data Protection Regulation, Recital 26.
[4] Decision of the Constitutional Court of Georgia of 27 March 2017, No. 1/4/757, in the case "Citizen of Georgia Giorgi Kraveishvili v. Government of Georgia", Section II-4.

recognized as the individual, their dignity, rights, and freedoms. Accordingly, the state exists to serve its people, who themselves are the source of state authority.[5]

As most social and economic activities are now conducted online, greater importance has been attached to the protection of personal data and the right to privacy. According to recent data, out of 194 countries worldwide, 137 countries have adopted legislative acts regulating personal data protection, accounting for 71% of all states. It is noteworthy that 9% (approximately 17 countries) are in the process of developing such legislation, 15% (around 30 countries) have not yet adopted any, and for 5% (around 9 countries) no information is available.[6] It is significant that the majority of countries without personal data protection legislation are located on the African continent, while the countries for which information is unavailable are found both in Africa and Indonesia.

The adoption of international legal instruments related to personal data protection began in the 1970s,[7] when information technologies came into intensive use and several countries introduced legislation to regulate the processing of personal information by public authorities and large corporations. As a result, various data protection mechanisms[8] were established across Europe, and over time, data protection evolved into an independent value, no longer viewed merely as part of the right to privacy. Within the European Union's legal system, data protection is recognized as a fundamental right, distinct from the right to respect for private life.

The United Nations legal framework does not explicitly recognize personal data protection as a fundamental right, even though the right to privacy has long been acknowledged as such under international law. Specifically, Article 12 of the Universal Declaration of Human Rights (UDHR) concerns the right to respect for private and family life.[9] This declaration was the first international instrument to affirm that every person has the right to protect their private sphere from interference by others, particularly by the state. Although the UDHR does not have binding legal force, it holds significant status as the foundational instrument of international human rights law and has strongly influenced the development of human rights mechanisms in Europe. The Declaration distinguishes the inviolability of private life from unlawful interference not only by state authorities but also by private individuals (such as neighbors, employers, etc.).[10]

In addition to the Universal Declaration of Human Rights, various international instruments adopted by the United Nations have established global standards for the

[5] Scientific Journal "Young Lawyers", No. 5, joint publication of "Young Lawyers" and the "Educational Center of Lawyers", Tbilisi, 2016, 34.

[6] UN Trade&Development, Data Protection and Privacy Legislation, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> [17.01.2024].

[7] Handbook on European Data Protection Law, Publications Office of the European Union, 2018, 22.

[8] The European Union developed its first comprehensive data protection instrument in 1995: Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[9] Universal Declaration of Human Rights, Article 12.

[10] *Alfredsson G., Eide Asbjorn,* The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.

protection of privacy and private life. The first such instrument following the Declaration was the International Covenant on Civil and Political Rights (ICCPR), which entered into force in 1976. The ICCPR affirms that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[11] As an international treaty, it obliges signatory states to respect and protect civil rights, including the right to privacy. In 1989, the UN General Assembly adopted the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, which prohibits arbitrary or unlawful interference with the privacy, home, family, correspondence, or other rights of migrant workers and their family members. Subsequently, in 2006, the Convention on the Rights of Persons with Disabilities further defined the right to privacy and confidentiality for persons with disabilities, establishing binding obligations for its signatory states.

Soon after the adoption of the Universal Declaration of Human Rights, the right to respect for private life was also recognized in Europe. In 1950, the European Convention on Human Rights (ECHR) was adopted, establishing the fundamental right to respect for private life.[12] According to Article 8 of the ECHR, everyone has the right to respect for their private and family life, home, and correspondence. No public authority may interfere with the exercise of this right except as provided by law and when such interference is necessary in a democratic society for legitimate and significant public interests.

The adoption of international legal instruments concerning the protection of personal data mainly began between the 1960s and 1980s. With the emergence of information technologies in the 1960s, there arose an increasing need for detailed rules governing the protection of personal data. By the mid-1970s, the Committee of Ministers of the Council of Europe had adopted several resolutions on personal data protection, referring explicitly to Article 8 of the European Convention on Human Rights.[13] The first international instrument dedicated to the protection of personal data was the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14], also known as Convention No. 108. Adopted in 1981, it was ratified by the Parliament of Georgia in 2005.[15] This Convention was, and remains, the only international treaty with binding legal force in the field of data protection. It safeguards an individual's right to know what

[11] International Covenant on Civil and Political Rights (ICCPR), 1976, Article 17.

[12] European Convention on Human Rights, 1950, Article 8.

[13] Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20 September 1974.

[14] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

[15] EU Treaty Office, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> [20.01.2024].

information is held about them and, where necessary, to request its correction. Restrictions on the rights provided under the Convention are allowed only in cases involving overriding interests, such as national security or defence. Furthermore, the Convention provides for the free flow of personal data between the contracting parties while imposing certain restrictions on transfers to states whose legal frameworks do not ensure an adequate level of data protection.

In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on international data transfers to states that are not Parties to the Convention (so-called "third countries"), as well as a mandatory requirement for the establishment of a data protection supervisory authority at the national level. Most importantly, the Additional Protocol expanded the scope of the Convention.[16]

From 1995 until May 2018, the principal legal instrument for data protection within the European Union was Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (commonly referred to as the Data Protection Directive).[17] Adopted in 1995, the Directive aimed to harmonise the data protection laws of EU Member States, many of which already had national legislation in place, in order to ensure a high and consistent level of personal data protection and to facilitate the free flow of data between Member States. The free movement of goods, capital, services, and people within the internal market also required the unrestricted movement of data—something that could not be achieved without establishing an equally high standard of data protection across all Member States.

The General Data Protection Regulation (GDPR) was adopted by the European Union in 2016 to replace the previous directive adopted in 1995, at a time when the Internet was still in its infancy. The earlier directive proved insufficient to address the challenges posed by modern technologies and the digital environment, making it necessary to reform and replace it with a new, more comprehensive legal framework.[18] The GDPR has direct legal force across all EU Member States, although each state has updated its national data protection legislation to ensure full compliance with it.

The Constitution of Georgia guarantees individuals the right to respect for their private and family life, privacy of communication, and informational self-determination. It also stipulates that information contained in official records relating to a person's health, finances, or other personal matters shall not be accessible to others without that person's consent, except in cases provided by law where such

[16] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, CETS No. 181, 2001.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

[18] EDPS, The History of the General Data Protection Regulation, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].

access is necessary to ensure state or public security, protect public interests, public health, or the rights of others. This provision serves as the constitutional foundation for personal data protection in Georgia, the guarantees for which are implemented through various legislative acts, including the Law of Georgia "On Personal Data Protection."

The Law of Georgia "On Personal Data Protection" is the core legislative act governing the field of personal data protection. Its initial version entered into force on November 1, 2014, and was subsequently amended several times to bring it closer to international standards.

With the adoption of the new Law of Georgia "On Personal Data Protection," national legislation in this field has been substantially harmonized with European standards, thereby ensuring the introduction of internationally recognized principles and best practices in data protection. Following the adoption of the EU General Data Protection Regulation and the modernization of Convention 108, further alignment with European standards became necessary. Consequently, in 2023, the Parliament of Georgia adopted the new Law "On Personal Data Protection," which entered into force on March 1, 2024.[19]

Among the innovations introduced by the new law are the obligations imposed on controllers to manage risks arising from technological progress, particularly through the implementation of data protection impact assessments and the incorporation of the principles of "Privacy by Design" and "Privacy by Default." These provisions represent significant advancements in Georgian data protection law, aiming to proactively identify and mitigate potential risks to human rights in the context of rapid technological development.

Currently, the Law of Georgia "On Personal Data Protection" serves as the principal legislative framework regulating the fundamental principles of data processing and the legal aspects of automated data processing, including the use of AI systems. Under the law, data processing must pursue a legitimate purpose, adhere to the principle of protection against unlawful interference, and safeguard the rights of data subjects, including their rights to information, access, rectification, erasure, and objection.

3. Analysis of National and International Acts Regulating Artificial Intelligence

There is no doubt that artificial intelligence is one of the most important and most modern scientific achievements of technological progress, destined to significantly transform many fields in the near future and become firmly established within them. The fourth industrial revolution is closely linked to the development of innovative technologies — including artificial intelligence, robotics, nanotechnologies, quantum

[19] Law of Georgia on Personal Data Protection, 14/06/2023.

computing, biotechnology, the Internet of Things (IoT) and blockchain — technologies that will substantially reshape both our daily lives and patterns of work and activity.[20]

Artificial intelligence (AI) denotes the intelligence of computer machines that act as "intelligent agents." The term is used when a computer system seeks to imitate cognitive functions.[21]

The principal problems for personal data protection arise, on the one hand, from the volume and broad variety of personal data being processed, and on the other hand from the processing methods and their outcomes. The deployment of complex algorithms and software to transform large datasets into decision-making resources affects various groups of data subjects, in particular through profiling and discriminatory practices, and ultimately gives rise to serious data-protection concerns.[22]

Regulating artificial intelligence is a complex global challenge because it raises ethical, legal and technical issues. Given the rapid pace of AI development, legal regulation remains difficult for many states; as a result, regulation has largely taken the form of policy documents and national strategies. The mere adoption of action plans or framework documents is not a panacea, as demonstrated by the limited practicality of some country-level documents. The term "strategy" is widely used in contemporary political science and management, yet no single agreed definition exists; strategy is often understood primarily as a written strategic plan.

Canada adopted the first national AI strategy in 2017, soon followed by Japan and China; in the same year, Singapore and Finland also approved AI strategies. Since 2018, momentum has accelerated: the United States, Taiwan, Italy, the United Kingdom, Sweden, Mexico, Denmark, France, Australia, South Korea, Germany and India[23] adopted similar strategies, and the European Union approved its own AI development strategy in 2018.

On 13 March 2024, the European Parliament voted in plenary to support the European Commission's proposal for a regulation establishing harmonised rules on artificial intelligence (the "AI Act") (523 in favour; 46 against; 49 abstentions).[24] The AI Act is a binding instrument for EU Member States that aims to regulate the design, development and use of AI systems. It applies across the Union to both the public and private sectors, with specified exceptions — notably for AI systems intended for military, defence, national security, and certain research and development purposes. The Act imposes different obligations according to the potential risks and impacts of

[20] *Gabisonia, Z.,* Internet Law and Artificial Intelligence, "World of Lawyers," Tbilisi, 2022, 513.

[21] *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, 27, 32–58, 968–972; *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, 2.

[22] Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.

[23] *Dutton T.,* An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].

[24] OneTrust DataGuidence, <https://www.dataguidance.com/news/eueuropean-parliament-adopts-ai-act> [12.03.2024].

AI systems, classifying them into three main categories — "unacceptable risk," "high risk," and "limited risk" — with corresponding requirements for each category.

The Council of Europe Framework Convention on Artificial Intelligence, aimed at protecting human rights, democracy and the rule of law, is among the first international legal instruments to set standards for the development and use of AI that fully respect human dignity, personal freedoms and equality. The Convention emphasises that technological progress must not undermine human rights or democratic values. It prioritises transparency, accountability and security—essential conditions for creating systems that respect individual autonomy and safeguard data protection. Both the State and the private sector are required to take appropriate measures to prevent harm and to ensure effective protection of human rights, including through risk assessment, oversight and compensation mechanisms. The Convention's approach opposes discrimination and promotes fair and responsible use, thereby fostering not only technological development but also public trust and the preservation of the foundations of democratic governance.

The Organization for Economic Co-operation and Development (OECD) adopted its first Recommendation on Artificial Intelligence in 2019 to promote innovation while strengthening trust in AI systems and safeguarding fundamental human rights and freedoms. In 2023 the Recommendation was updated to provide a clearer definition of an artificial intelligence system in response to rapid technological developments. The OECD Recommendation sets out five high-level, value-based principles and five recommendations for national policy and international cooperation. However, these Recommendations are non-binding.[25]

In the United States, the White House Office of Science and Technology Policy published a non-binding plan on October 4, 2022, containing five principles designed to minimise harm from automated systems. On August 18, 2022, the National Institute of Standards and Technology (NIST) released the second draft of the AI Risk Management Framework, intended to help organisations that develop or deploy AI assess and manage associated risks. The Framework consists of voluntary guidelines and recommendations and is therefore non-binding.[26]

China[27] adopted its "Next-Generation Artificial Intelligence Development Plan" in 2017 and published Ethical Guidelines for the Governance of Artificial Intelligence in 2021. In January 2022, China introduced two laws addressing specific AI applications. The Algorithm Provisions for the Governance of Algorithmic Recommendations for Internet Information Services came into force in March 2023, while the Draft Deep

[25] OECD Recommendation of the Council on Artificial Intelligence, 2024

[26] *Kohn B., Pieper F. U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[27] *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.202].

Synthesis Provisions for the Governance of Internet Information Services remain at the draft stage.

Japan[28] has the second-largest IT sector among OECD countries and is heavily invested in research and development. It was also the second country to develop a national AI strategy. The "AI Technology Strategy," published in March 2017, includes an industrialization roadmap for AI services and structures AI development into three phases: Processing data for AI; 2. Public use of AI; and 3. Creation of AI ecosystems.

Japan's AI strategies and regulations are closely aligned with the country's broader "Society 5.0" initiative. The "Social Principles for Human-Centered Artificial Intelligence," developed by the Integrated Innovation Strategy Promotion Council and published by the Japanese government in March 2019, set out fundamental principles to guide the development of an AI-enabled society. The document outlines seven key social principles that society and the state should uphold in their approach to AI: (1) human-centeredness, (2) education and literacy, (3) data protection, (4) security, (5) fair competition, (6) fairness, accountability and transparency, and (7) innovation. These principles, however, are non-binding and serve primarily as policy guidance.

Brazil[29] is currently in the process of developing legislation to regulate AI. On December 1, 2022, the Brazilian Senate's Non-Permanent Jurisprudence Committee presented a report on AI regulation, which included a draft law. According to the committee's rapporteur, the proposed regulation is based on three central pillars: (1) safeguarding the rights of individuals affected by AI systems, (2) classifying levels of risk, and (3) establishing governance measures for companies that develop or operate AI systems.

The draft law also grants data subjects the right to request and obtain information from AI system providers regarding the scope and purpose of personal data processing.

Canada[30] was among the first countries to adopt a national AI strategy. In 2017, it introduced the five-year "Pan-Canadian AI Strategy," focused on fostering AI research and talent development. Unlike the strategies of many other countries, Canada's approach primarily emphasizes research, innovation, and the accumulation of knowledge in the field.

On June 16, 2022, the Canadian federal government introduced Bill C-27, known as the Digital Charter Implementation Act, which includes the Artificial Intelligence and Data Act (AIDA). AIDA regulates interprovincial and international trade in AI systems and seeks to mitigate risks and biased outcomes associated with high-impact AI

[28] *Habuka H.*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].

[29] *Kohn B., Pieper F. U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[30] *Gabisonia, Z.,* Internet Law and Artificial Intelligence, "World of Lawyers," Tbilisi, 2022, 526.

technologies. The law also empowers the government to restrict the use of AI systems that significantly infringe upon the legitimate rights and interests of individuals.[31]

Switzerland[32], in contrast to the European Union, does not consider it necessary to adopt a dedicated law regulating artificial intelligence. The Swiss government maintains that existing legal frameworks can be adapted to address AI-related challenges. For instance, the Data Protection Act contains provisions on AI transparency, while competition law, product liability law, and the Civil Code have been updated with relevant rules governing the use of artificial intelligence.

The UK[33] government began publishing sectoral reports on artificial intelligence in 2018 as part of its broader Industrial Strategy. Subsequently, on 29 March 2023, it released an AI White Paper outlining proposals for regulating the use of artificial intelligence (AI) in the UK. This document builds on the earlier AI Regulation Policy Paper, which articulated the government's vision for a "pro-innovation" and "context-specific" AI regulatory regime.

The UK approach diverges from the model adopted in the EU AI Act, as it does not introduce new, comprehensive legislation. Instead, it focuses on establishing principles and expectations for the development and deployment of AI, while empowering existing regulatory bodies—such as the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), and the Competition and Markets Authority (CMA)—to issue guidance and oversee AI applications within their respective mandates.

Denmark's[34] strategy, titled "Denmark's Digital Growth" (2018), aims to position the country as a global leader in the digital industrial revolution, thereby fostering national prosperity and economic growth.

Germany[35] also adopted a national Artificial Intelligence Strategy in 2018, jointly developed by the Federal Ministries of Economic Affairs, Research, and Labour. The German government seeks to safeguard its position as a leading research hub, enhance industrial competitiveness, and promote the application of AI across all sectors of society. To achieve these objectives, it committed an additional €500 million in 2019 to further AI policy initiatives.

---

[31] Government of Canada, The Artificial Intelligence and Data Act (AIDA)- Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].

[32] *Kohn B., Pieper F.U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[33] *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].

[34] Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].

[35] German Federal Government's AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].

India's[36] National Strategy for Artificial Intelligence (2018) emphasizes the use of AI not only as a driver of economic growth but also as a tool for social inclusion. Recognizing its position as one of the world's fastest-growing economies, India aims to leverage AI for transformative, inclusive, and sustainable development aligned with its broader socio-economic goals.

Italy[37] published an AI White Paper in 2018, which, unlike many other national strategies focused primarily on research or private sector adoption, concentrates on promoting the integration of AI technologies within public administration and improving government efficiency.

Malaysia[38] adopted its Artificial Intelligence Strategy 2021–2025 (AI-Rmap) in 2021, setting out a national roadmap for developing AI capabilities over a five-year period. The COVID-19 pandemic served as a catalyst for accelerating digital transformation, shaping Malaysia's strategic vision for AI. AI-Rmap was developed with three distinctive features: (1) alignment with global and national strategies on science, technology, and innovation; (2) a collaborative "Quadruple Helix" approach involving government, academia, industry, and society (GAIS); and (3) an entirely virtual development process, from inception to completion. The overarching goal is to establish a robust and sustainable AI innovation ecosystem, transforming Malaysia into a high-income, technologically advanced nation through the strategic application of artificial intelligence.

The Polish[39] government initiated discussions on the development of a national artificial intelligence strategy in May 2018 by convening the first roundtable dedicated to this topic. Subsequently, in December 2020, the Council of Ministers adopted the Polish National AI Strategy. The document encompasses a broad range of policy areas, including society, education, science, business, public administration, and international cooperation. It emphasizes the protection of human rights and dignity, the promotion of fair competition, and the establishment of an ethical framework for trustworthy AI. Furthermore, Poland aims to create conditions that foster the growth of an AI ecosystem across ethical, legal, technical-operational, and international dimensions.

Singapore[40] launched a five-year National AI Programme in 2017, supported by an investment of USD 150 million to enhance national capabilities in the field of artificial intelligence. Building on these efforts, in 2019 Singapore introduced its first National AI Strategy (NAIS), outlining measures to integrate AI into key sectors to drive

[36] India's National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].

[37] European Commission, National strategies on Artificial Intelligence, A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].

[38] Navigating the Future Malaysia's Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].

[39] Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].

[40] National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].

economic transformation. The government's updated NAIS 2.0 demonstrates Singapore's continued ambition to build a trusted, human-centric, and responsible AI ecosystem. The revised strategy focuses on fostering innovation, promoting public and private engagement, and ensuring that AI contributes to sustainable economic growth. Recognizing both the opportunities and challenges presented by AI, Singapore underscores the importance of responsible governance and risk mitigation to harness AI's potential while preventing adverse social and ethical consequences.

The Republic of Korea[41] adopted its National AI Strategy on 17 December 2019, under the vision "Towards a World Leader in AI Beyond IT." The strategy seeks to enhance Korea's digital competitiveness, generate significant economic value from AI technologies, and improve quality of life by 2030.

Sweden's[42] National AI Strategy, published in May 2018, outlines the government's overall policy direction for artificial intelligence. The strategy aims to establish a foundation for future initiatives to advance Sweden's prosperity and competitiveness through AI. It identifies four priority areas—education, research, innovation, and infrastructure—as key drivers of national development in this field.

The United Arab Emirates (UAE)[43] launched its Artificial Intelligence Strategy in 2017, positioning itself as a pioneer in the Middle East and becoming the first country globally to establish a dedicated Ministry[44] of Artificial Intelligence.[45] The central objective of the UAE's AI Strategy is to enhance government efficiency through the adoption of artificial intelligence technologies. Moreover, the UAE's long-term vision aims to position the country as a global leader in AI by 2031, reflecting its commitment to digital transformation and innovation-led governance.

In May 2018,[46] the ministries responsible for digital development in Denmark, Estonia, Finland, the Faroe Islands, Iceland, Latvia, Lithuania, Norway, Sweden, and the Faroe Islands published a Declaration on Artificial Intelligence in the Nordic–Baltic Region. The participating countries agreed to cooperate in order to *"develop and promote the use of artificial intelligence for the benefit of people."* The declaration identified seven key areas of cooperation: 1. improving opportunities for skills

[41] National Strategy for Artificial Intelligence of Korea, <https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9> [15.04.2024].

[42] European Commission, National Strategies on Artificial Intelligence. A European perspective in 2019, Country report Sweden, <https://knowledge4policy.ec.europa.eu/sites/default/files/sweden-ai-strategy-report.pdf> [15.04.2024].

[43] UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].

[44] Ministry of Artificial Intelligence of the United Arab Emirates, <https://ai.gov.ae/> [15.04.2024].

[45] UAE Strategy for Artificial Intelligence, <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence> [15.04.2024].

[46] Nordic Co-operation, AI in the Nordic-Baltic region, <https://www.norden.org/en/declaration/ai-nordic-baltic-region> [17.04.2024].

development; 2. increasing access to data; 3. developing ethical and transparent guidelines, standards, principles, and values; 4. establishing standards for hardware and software that ensure privacy, security, and trust; 5. ensuring that artificial intelligence plays a significant role in European discussions on the Digital Single Market; 6. avoiding unnecessary regulations; and 7. utilizing the Nordic policy framework of the Nordic Council of Ministers to facilitate regional collaboration.

As for Georgia, it is noteworthy that since 2024 the country has signed the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. As a post-Soviet state that is still in the process of developing its high-tech sector,[47] Georgia faces particular challenges in the creation and regulation of artificial intelligence systems. According to a 2024 statement by the Minister of Justice, technological progress necessitates the introduction of legal regulations that both promote innovation and safeguard human rights. To this end, an interdepartmental working group is being established within the Ministry of Justice to develop a legal framework for the regulation of AI compatible with EU law.

At present, there is no specific legislative act in Georgia that directly regulates the legal status, scope, or ethical standards applicable to artificial intelligence. While the use of technology is governed by general legal norms—such as the constitutional guarantee of privacy, the Law of Georgia on Personal Data Protection, and other sectoral acts—there are no explicit provisions addressing:

- Criteria for algorithmic transparency;
- The legal assessment of decision-making automation; or
- Ethical frameworks for the use of AI in the public and private sectors.

The Law of Georgia on Personal Data Protection does not contain explicit rules on AI but includes provisions relevant to automated data processing, which may encompass certain AI applications. Under the law, automated decision-making is permitted only if the accuracy, awareness, security, and rights of the data subject are ensured. Nevertheless, the law does not yet reflect the specific risks and regulatory challenges posed by AI technologies, highlighting the need for an additional legislative framework tailored to contemporary developments.

It is also important to note that in 2025, the Georgian government approved the Georgian Digital Governance Strategy 2025–2030, which proactively incorporates the development of an ethical and legal framework for the governance and regulation of artificial intelligence.[48]

The examples discussed above do not represent an exhaustive global picture. A growing number of countries are developing policy frameworks and action plans in this area. For instance, Argentina, Chile, Colombia, and Israel have adopted policy documents addressing artificial intelligence, while Australia, Bangladesh, Egypt, Indonesia, Mauritius, Peru, and Saudi Arabia have implemented national AI action plans. In Taiwan, the government is actively working on the adoption of a legislative

[47] Announcement available at: https://justice.gov.ge/?m=articles&id=OrginiwJBU

[48] Decree No. 100 of the Government of Georgia of April 3, 2025, On the Approval of the "Digital Governance Strategy of Georgia 2025–2030" and the "Action Plan for 2025–2026 of the Digital Governance Strategy of Georgia 2025–2030."

act on artificial intelligence; a draft law has already been prepared and is currently awaiting approval.

4. The Relationship Between Artificial Intelligence and Personal Data at the Legislative Level

Artificial intelligence has long ceased to be merely a technology of the future; in many respects, it has become a product of the present—one that, alongside simplifying everyday life, also poses numerous challenges for both developers and users. One of the most significant challenges concerns the boundary between the benefits of artificial intelligence and the protection of personal data. As the scope of artificial intelligence expands, so too do the risks associated with personal data. A clear example of this can be found in social networks, which are becoming increasingly enriched with automated, intelligent algorithms each year. Altogether, this enables AI-based systems to monitor our online activities, which in effect constitutes interference with our private lives.[49]

In the process of data processing carried out by artificial intelligence, the core principles of the General Data Protection Regulation (GDPR)—such as accountability, transparency, lawfulness, and data minimization—are often violated. AI systems frequently collect data in ways that do not clearly specify the purposes for which it will be used, thereby contradicting the principle of purpose limitation. Moreover, data is often processed without a valid legal basis, stored for indefinite periods, and used for purposes not previously agreed upon, thereby infringing the requirement of data minimization. Given the complexity and rapid development of technology, ensuring effective control and audit mechanisms proves difficult, which poses an additional challenge from the perspective of data protection.[50]

Artificial intelligence (AI) possesses the capability to recognize patterns that are imperceptible to the human eye, to learn, and to make predictions concerning individuals and groups. In this sense, AI can generate information that is otherwise difficult to obtain or may no longer exist. Consequently, data collected and processed through AI technologies can be used for longer periods and for broader purposes than those for which it was originally and consciously disclosed. The enhanced analytical and predictive capacities of AI are therefore likely to create an environment in which an individual can be identifiable based on information generated by, or associated with, them.[51]

[49] Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.

[50] *Chalubinska-Jentiewicz K., Nowikowska M.,* Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.

[51] OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].

AI systems enable the use of personal data of all categories for the purposes of analysis, prediction, and behavioral influence. Artificial intelligence transforms this data, and the results derived from it, into valuable products. In particular, AI makes possible the automation of decision-making processes in domains that traditionally require complex human judgments based on multiple and sometimes undefined criteria. In many instances, automated predictions and decisions can be not only more efficient but also more accurate and impartial than those made by humans, as AI systems are capable of avoiding typical cognitive biases and can be subjected to systematic oversight. However, algorithmic decisions are not immune to error or discrimination, and their misuse can result in violations of individual rights and freedoms.[52] It is noteworthy that under the Law of Georgia on Personal Data Protection, a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects concerning them.[53] As already noted, automated means may include artificial intelligence systems.

Since no specific legislative acts regulating artificial intelligence have yet been adopted, the relationship between artificial intelligence and personal data remains undefined at the legislative level. Nevertheless, it may be inferred that the personal data protection laws of most countries contain a general provision stating that data processing may be carried out by both automated and non-automated means—a formulation broad enough to be interpreted as encompassing the use of artificial intelligence systems.

At the international level, the European Union's Artificial Intelligence Act represents the first comprehensive legal framework establishing binding standards for the development, deployment, and use of AI systems, including obligations concerning the protection of personal data and privacy. Articles 7 and 8 of the Act explicitly guarantee the inviolability of private life and the respect for personal data, linking AI governance directly to fundamental rights protection.[54] Similarly, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law constitutes the first-ever legally binding international treaty in this domain, and it is of particular relevance for Georgia as a signatory state.

Pursuant to Article 28 of the EU AI Act, when artificial intelligence is used in the field of healthcare, the fundamental rights protected under the Charter of Fundamental Rights of the European Union—including the rights to private and family life and to personal data protection—must be fully respected. The Act also emphasizes that AI systems applied in the areas of migration, asylum, and border control affect individuals who are often in particularly vulnerable positions and dependent on the decisions of state authorities. Therefore, ensuring the accuracy, transparency, and

[52] European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020,
<https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].

[53] Law of Georgia on Personal Data Protection, Article 19.

[54] European Union Artificial Intelligence Act (EU AI Act), Paragraph 2.

non-discriminatory operation of AI systems in these contexts is essential for safeguarding the fundamental rights of the affected individuals.[55]

The Peruvian executive adopted a law promoting the use of artificial intelligence for economic and social development, introducing a risk-based regulatory approach similar to that of the European Union's AI Act. The law classifies potential risks, restricts certain high-risk systems, and explicitly incorporates data protection and privacy principles.[56] One of its core provisions refers to the principle of "privacy in artificial intelligence," according to which AI systems must not infringe upon individuals' privacy.[57] The right to privacy, understood broadly, encompasses the protection of private life, communications, and personal space from external interference. The right to personal data protection, while closely related, is a distinct aspect of this right, focusing specifically on ensuring that personal data are collected, processed, and stored lawfully, fairly, and transparently.

An interesting aspect of Saudi Arabia's strategy is that, since its establishment, the Saudi Data and Artificial Intelligence Authority (SDAIA) has been leading the national data and artificial intelligence agenda to advance the objectives of the Kingdom's Vision 2030. Most recently, SDAIA, in partnership with the Ministry of Communications and Information Technology (MCIT), has chaired the G20 Digital Economy Working Group and spearheaded the Kingdom's response to Covid-19 through the launch of applications such as Tawakkalna and Tabaud. In addition, the government has issued a series of policies – including the Kingdom's Data Classification Policy, Personal Data Protection Policy, Data Sharing Policy, Freedom of Information Policy, and Open Data Policy – thereby paving the way for a robust and business-friendly regulatory environment.

Below are several court decisions addressing the intersection between artificial intelligence and personal data.

On June 28, 2023, a U.S. federal court heard the case P.M. v. OpenAI LP, in which an anonymous group of plaintiffs filed a lawsuit against OpenAI LP (OpenAI) and Microsoft, Inc. (Microsoft). The plaintiffs alleged that OpenAI had misappropriated the personal and proprietary information of millions of individuals by collecting publicly available data from the Internet and social media platforms without users' knowledge or consent. They argued that OpenAI's practice of using such Internet-derived datasets to train its generative AI tools constituted theft, misappropriation, and violations of privacy and property rights. The allegedly collected information included names, addresses, phone numbers, email addresses, and financial data. According to the plaintiffs, OpenAI and Microsoft used this personal information to develop ChatGPT,

[55] Ibid, para 39.

[56] Access Alert: Peru's congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].

[57] Peru Law - LAW THAT PROMOTES THE USE OF ARTIFICIAL INTELLIGENCE IN FAVOR OF THE ECONOMIC AND SOCIAL DEVELOPMENT OF THE COUNTRY, Unique item, f, <https://busquedas.elperuano.pe/dispositivo/NL/2192926-1> [05.05.2024].

thereby violating the U.S. Electronic Communications Privacy Act, which prohibits the interception of electronic communications without prior court authorization.

This case is particularly significant as it underscores the obligation of AI companies to ensure transparency in their data collection practices and to establish appropriate legal bases—such as obtaining user consent—before processing personal data. It also serves as a reminder that consumers should remain aware of the privacy implications associated with the use of AI products and services, including their potential exposure to copyright infringement issues and other forms of harm linked to AI-related data practices.[58]

On July 11, 2023, in the case J.L. v. Alphabet Inc., a class action lawsuit was filed in a U.S. federal court against Google, alleging violations of privacy and copyright laws. The plaintiffs claimed that Google's generative AI products—including Bard (a text generator), Imagen and Gemini (two text-to-image diffusion models), MusicLM (a text-to-music tool), and Duet AI (a data visualization tool)—relied on data that the company had collected from the Internet without proper authorization.[59]

The lawsuit further alleged that Google used online information for AI training purposes without obtaining consent from the original data owners. Specifically, it was claimed that Google's AI products utilized copyrighted text, music, images, and other materials for training purposes without the necessary permissions.[60]

The issue of using publicly available online information for artificial intelligence training had also been addressed in the U.S. court case hiQ Labs, Inc. v. LinkedIn Corp. In that case, hiQ Labs, Inc. "scraped" data from publicly available profiles of LinkedIn users to provide employers with insights about job seekers and employment trends. The court ruled that the use of publicly available data does not, in itself, constitute a violation of privacy rights. However, it emphasized that privacy would be infringed if an AI system used data that was not publicly accessible and had been granted the legal status of "personal data."[61]

Italy became the first Western country to temporarily block the chatbot ChatGPT due to privacy concerns. The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) decided to suspend and investigate the chatbot—developed by OpenAI and supported by Microsoft—on the grounds that there was no legal basis to justify the collection and "mass storage" of personal data for the purpose of training the GPT AI modelThe Garante accused OpenAI of unlawfully collecting and retaining data of Italian data subjects, thereby violating the General Data Protection Regulation (GDPR). Additional concerns were raised about the lack of an effective age verification mechanism, which could expose minors to inappropriate content.

---

[58] Conexus law, OpenAI, and Microsoft sued in the US for §3 billion over alleged ChatGPT privacy violations, <https://www.conexuslaw.com/insight/openai-and-microsoft-sued-in-us-for-3-billion-over-alleged-chatgpt-privacy-violations/> [25.04.2024].

[59] J.L. et al. v. Alphabet Inc. et al. - 3:23-cv-03440

[60] *Christopher J. Valente, Stortz M.J., Wong A., Soskin P.E., Meredith M.W.,* US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].

[61] Ibid.

During the investigation, it was discovered that ChatGPT processed users' conversations, email addresses, and even the last four digits of their bank cards. According to the BBC, Italian authorities gave OpenAI 20 days to address these issues or face fines of up to 4% of its annual global revenue.[62] OpenAI denied the allegations. Ultimately, ChatGPT was temporarily blocked in Italy from March 31, 2023, to April 28, 2023, with the suspension lasting approximately four weeks (28 days).

Except for Italy, China has also taken restrictive measures against the use of ChatGPT. The Chinese government has banned the country's major technology companies from offering ChatGPT services to users. According to Nikkei Asia, the responses generated by the AI chatbot—developed by OpenAI and backed by Microsoft—would otherwise be subject to censorship by the Chinese Communist Party (CCP). Although ChatGPT is not officially available in China, some Internet users have managed to access it through virtual private networks (VPNs).[63]

The Hellenic Data Protection Authority (Hellenic DPA) imposed a €20 million fine on Clearview AI Inc. for violating the principles of lawfulness and transparency. The authority also prohibited the company from collecting or storing personal data within Greek territory without a valid legal basis. Clearview AI operates a facial recognition database in which personal data—specifically, photographs—are scraped from the Internet without the consent of the individuals concerned.[64]

Following Greece, the Austrian Data Protection Authority also issued a ruling against Clearview AI. The company reportedly maintains a database containing over 30 billion facial images sourced globally from publicly available materials such as media outlets, social networks, and online videos. It provides a sophisticated search service that enables artificial intelligence systems to generate profiles based on biometric data extracted from these images. These profiles can be further enriched with related information, including image tags, geolocation data, and source web pages, thereby heightening concerns about privacy, consent, and proportionality in the use of AI-driven facial recognition technologies.[65]

[62] ChatGPT was blocked in Italy, business formula <https://businessformula.ge/News/13437> [30.04.2024].

[63] *Papalashvili S., Nikkei Asia: China bans companies from using the ChatGPT service,* <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].

[64] Hellenic DPA fines Clearview AI 20 million euros, <https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> [25.04.2024].

[65] Decision by the Austrian SA against Clearview AI Infringements of Article 5,6,9,27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].

5. Conclusion

Although artificial intelligence and its regulation remain a relatively new reality for the global community, it is challenging to adopt definitive decisions regarding a system that continues to evolve and transform on a daily basis.

The processing of data by artificial intelligence may conflict with the fundamental requirements of the General Data Protection Regulation (GDPR)—particularly with respect to the principles of accountability, transparency, the existence of a lawful basis for data processing, and data minimization. Many AI applications involve the processing of personal data. On the one hand, such data may form part of the datasets used to train machine learning systems, particularly for the development of algorithmic models. On the other hand, these models can subsequently be employed to draw inferences about specific individuals based on personal data.

As this paper has demonstrated, legal instruments governing personal data protection exist at both the international and domestic levels. However, the key standards and principles for data protection and processing are primarily established by the General Data Protection Regulation, adopted by the Council of Europe, which sets a notably high standard for the protection of personal data. By contrast, the international legal framework governing artificial intelligence remains relatively new and largely untested in practice. The reviewed materials indicate that numerous countries have adopted recommendations, strategies, action plans, or policy documents addressing artificial intelligence at the national level. Nevertheless, it should be emphasized that these instruments are recommendatory in nature and lack binding legal force.

Bibliography:

1. European Convention on Human Rights, 1950, Articles 8 and 12.
2. European Union Artificial Intelligence Act (EU AI Act), para. 2.
3. European Union Artificial Intelligence Act (EU AI Act), para. 2.
4. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 1981.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, OJ 1995 L 281.
6. General Data Protection Regulation (GDPR), Article 4(1).
7. General Data Protection Regulation (GDPR), Recital 26.
8. Law of Georgia on Personal Data Protection, 14 June 2023.
9. International Covenant on Civil and Political Rights (ICCPR), 1976, Article 17.
10. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14.
11. Convention on the Rights of Persons with Disabilities, Article 22.
12. Access Alert: Peru's congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].
13. Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].
14. *Alfredsson G., Asbjorn E.*, The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.
15. *Chalubinska-Jentiewicz K., Nowikowska M.,* Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.
16. Constitutional Court of Georgia, Decision No. 1/4/757 of 27 March 2017, Citizen of Georgia Giorgi Kraveishvili v. Government of Georgia, II-4.
17. Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.
18. Decision by the Austrian SA against Clearview AI Infringements of Article 5, 6, 9, 27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].
19. *Dutton T.,* An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].

20. EDPS, The History of the General Data Protection Regulation, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].
21. European Commission, National strategies on Artificial Intelligence. A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].
22. European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].
23. European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].
24. *Gabisonia, Z.,* Internet Law and Artificial Intelligence. Jurists' World, Tbilisi, 2022, 513, 526.
25. German Federal Government's AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].
26. Government of Canada, The Artificial Intelligence and Data Act (AIDA)-Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].
27. *Habuka H.*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].
28. India's National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].
29. *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.2024].
30. *Kohn B.,* Pieper F.U., AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].
31. National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].

32. National Strategy for Artificial Intelligence of Korea, https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9 [15.04.2024].
33. Navigating the Future Malaysia's Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].
34. OECD Recommendation of the Council on Artificial Intelligence, 2024.
35. OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].
36. *Papalashvili, S. Nikkei Asia: China Prohibits Companies from Using ChatGPT Services. Retrieved from* <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].
37. Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].
38. *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].
39. *Russel S., Norvig P.*, Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, 27, 32–58, 968–972.
40. Scientific Journal "Young Lawyers", No. 5. Joint publication of "Young Lawyers" and the "Lawyers' Educational Center", Tbilisi, 2016, 34.
41. Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2009, 2.
42. UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].
43. *Valente Ch. J.*, Stortz M.J., Wong A., Soskin P.E., Meredith M.W., US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].