Artificial Intelligence Act and GDPR: Implications for AI Solution Developers and Users in Romania

Associate professor **Camelia Daciana STOIAN**[1]
Professor **Dominic BUCERZAN**[2]
Lecturer **Radu Nicolae STOIAN**[3]
Assistant professor **Catalin Raul HALIC**[4]
Associate professor **Crina Anina BEJAN**[5]

Abstract

Artificial Intelligence (AI) poses a significant challenge for personal data protection legislation, substantially impacting the way Romanian companies develop and implement AI solutions, as well as affecting human rights. At the European level, the Artificial Intelligence Act (AIA)[6] introduces a regulatory framework for the responsible use of AI, which must be harmonized with the General Data Protection Regulation (GDPR). In this context, Romania faces challenges regarding the compatibility of its national legislation with these European regulations, particularly concerning automated data processing, algorithmic transparency, user rights, and the impact of AI use in judicial and administrative systems. The study examines the extent to which Romanian legislation is prepared to accommodate the new requirements imposed by the AIA, highlighting legal risks and additional obligations for companies developing AI-based solutions. It also evaluates the potential consequences for the Romanian technology market, including impacts on AI-focused startups and institutions utilizing artificial intelligence technologies in their operational processes. The study's conclusions emphasize the need for a proactive and integrated approach to ensure compliance with European standards while simultaneously protecting technological innovation and user rights.

Keywords: *artificial intelligence, data protection, Artificial Intelligence Act, GDPR, Romanian legislation, AI regulation.*

JEL Classification: K20, K23, K24

[1] Camelia Daciana Stoian - Faculty of Humanities and Social Sciences, "Aurel Vlaicu" University of Arad, Romania, ORCID: 0000-0003-2776-6244, av.stoiancameliadaciana@yahoo.com.

[2] Dominic Bucerzan - Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania, ORCID: 0000-0002-9260-9387, dominic@bbcomputer.ro.

[3] Radu Nicolae Stoian - Faculty of Law, "Vasile Goldiş" University of Arad, Romania, radustoian73@gmail.com.

[4] Catalin Raul Halic - Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania, ORCID: 0009-0002-0459-2464, haliccatalin@gmail.com.

[5] Crina Anina Bejan - Faculty of Exact Sciences, "Aurel Vlaicu" University of Arad, Romania, ORCID: 0000-0003-2868-2376, ratiu_anina@yahoo.com.

[6] Regulation of the European Parliament and of the Council of the European Union, No. 1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation).

DOI: https://doi.org/10.62768/ADJURIS/2025/3/09

Please cite this article as:
Stoian, Camelia Daciana, Dominic Bucerzan, Radu Nicolae Stoian, Catalin Raul Halic & Crina Anina Bejan, „Artificial Intelligence Act and GDPR: Implications for AI Solution Developers and Users in Romania", in Devetzis, Dimitrios, Dana Volosevici & Leonidas Sotiropoulos (eds.), *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 162-177.

1. Introduction

In recent years, artificial intelligence (AI) has rapidly evolved from a niche research field into a transformative force across multiple sectors, including healthcare, finance, education, and public administration[7]. Its capacity to process vast quantities of data, identify patterns, and make autonomous decisions introduces not only substantial opportunities but also serious legal and ethical concerns. Among the most pressing is the challenge of ensuring that AI systems respect fundamental rights, particularly the right to personal data protection, as enshrined in both national and European legal frameworks[8]. Although a growing body of academic work addresses the normative and theoretical implications of AI regulation, the current literature lacks comprehensive empirical studies that explore its impact across diverse organisational contexts[9] — particularly in smaller markets such as Romania. This gap underscores the importance of examining how emerging legal frameworks interact with real-world technological development.

At the European level, two major legal instruments shape the governance of artificial intelligence and data protection: the General Data Protection Regulation (GDPR)[10], which has been in force since 2018, and the newly adopted Artificial Intelligence Act (AIA)[11], the first comprehensive legal framework for AI

[7] Yiming Yuan, Yongming Sun and Hangyu Chen. 2024. "Does Artificial Intelligence Affect Firms' Inner Wage Gap?" *Applied Economics* 57 (19): 2365–71. doi: 10.1080/00036846.2024.2324090.

[8] Abdallah Q. Bataineh, Alaa S. Mushtaha, Ibrahim A. Abu-AlSondos, Saeed Hameed Aldulaimi, Marwan Abdeldayem. 2024. "Ethical & Legal Concerns of Artificial Intelligence in the Healthcare Sector," *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, pp. 491-495, doi: 10.1109/ICETSIS61505.2024.10459438.

[9] João Pedro Quintais 2025. "Generative AI, copyright and the AI Act." *Computer Law & Security Review*, vol. 56: 106107, https://doi.org/10.1016/j.clsr.2025.106107.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council 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).

[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

within the European Union. While the GDPR provides strong protections for personal data, including limitations on profiling and automated decision-making, the AIA introduces a risk-based approach to AI systems, imposing specific requirements on applications considered "high-risk". The interplay between these two regulations reflects the EU's broader commitment to promoting trustworthy AI that aligns with democratic values and fundamental rights. However, the simultaneous applicability of both instruments also creates legal complexity — particularly for organisations tasked with ensuring compliance in practice[12].

For Romania, the implementation of these regulatory frameworks presents unique challenges. As an EU member state with a rapidly developing tech ecosystem, Romania must align its national legislation and institutional practices with the obligations introduced by both the GDPR and the AIA. However, the current legal infrastructure lacks specific provisions addressing issues such as algorithmic transparency, automated decision-making, or discrimination resulting from AI systems. This regulatory gap raises concerns about both compliance and the protection of individual rights[13].

In addition to the legal dimension, the regulation of AI in Romania has direct implications for the country's economic ecosystem. Romania is home to both companies that develop AI solutions — such as automation, natural language processing, or behavioural authentication technologies—and organisations across sectors that rely on AI tools in their operations[14]. The integration of the GDPR and AIA into national practice is therefore not merely a matter of legal compliance, but one that will influence innovation, competitiveness, and the ability of local firms to scale within the EU digital market[15,16].

Romania, as both an emerging market and an EU member state, finds itself at a crossroads between significant technological potential and persistent legal and institutional challenges. In this context, the purpose of this article is to assess the readiness of Romanian legislation and institutional frameworks to accommodate the requirements of the Artificial Intelligence Act in conjunction with

[12] Lena Enqvist. 2024. "Rule-based versus AI-driven benefits allocation: GDPR and AIA legal implications and challenges for automation in public social security administration." Information & Communications Technology Law vol. 33, no. 2: 222-246, doi: 10.1080/13600834.2024.2349835.

[13] Anca Parmena Olimid, Catalina Maria Georgescu, and Daniel Alin Olimid. 2024. "Legal Analysis of EU Artificial Intelligence Act (2024): Insights from Personal Data Governance and Health Policy." *Access to Justice in Eastern Europe* 7(4): *120-42 <https://doi.org/10.33327/AJEE-18-7.4-a000103>.*

[14] Daniel Castro and Michael McLaughlin, "Who Is Winning the AI Race: China, the EU, or the United States?" Center for Data Innovation, January 2021, https://datainnovation.org/2021/01/who-is-winning-the-ai-race-china-the-eu-or-the-united-states-2021-update/.

[15] Chambers and Partners. (2024). Artificial Intelligence 2024 – Romania: Law & Practice Guide. Available at: https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/romania [Accessed 21 Mar. 2025].

[16] Nick Wallace and Daniel Castro (2018). *The Impact of the EU's New Data Protection Regulation on AI. Information Technology and Innovation Foundation (ITIF).* Available at: https://itif.org/publications/2018/03/26/impact-eu-new-data-protection-regulation-ai [Accessed 21 Mar. 2025].

the GDPR. The analysis also aims to explore the broader implications of this alignment for AI developers, users, and regulators, highlighting areas where proactive adaptation is essential.

2. The European Legal Framework: AIA and GDPR

The European Union has positioned itself as a global leader in regulating the digital environment, with the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AIA) as two cornerstone instruments. While the GDPR focuses on safeguarding personal data and ensuring individual control over data processing, the AIA introduces a framework for the ethical and safe development, deployment, and use of AI technologies. These instruments are designed to work in tandem, reinforcing the EU's commitment to human-centric, trustworthy AI.

The Artificial Intelligence Act introduces a tiered risk classification model, dividing AI systems into minimal, limited, high, and unacceptable risk categories. The classification is based on the intended use of the AI system, its potential to affect fundamental rights, and the degree of autonomy involved. High-risk systems are typically those used in sensitive contexts such as biometric identification, access to education or employment, healthcare, and legal decision-making. Once designated as high-risk, these systems are subject to a set of mandatory compliance obligations that go beyond general ethical recommendations, forming binding legal standards.

Real-life examples of such risks include AI algorithms used in hiring platforms, which may inadvertently exclude candidates based on biased training data, as alleged in *Mobley v. Workday Inc.*[17] and addressed in *EEOC v. iTutorGroup*[18]. In credit scoring, "black-box" models have drawn regulatory scrutiny from the U.S. Consumer Financial Protection Bureau (CFPB) for failing to provide explainable justifications for denied loans[19]. In the housing sector, *Louis v. SafeRent Solutions* revealed how tenant screening algorithms could systemically disadvantage applicants from minority backgrounds[20]. These examples highlight the necessity for strong oversight and legal accountability in high-risk AI domains.

[17] Mobley v. Workday Inc., Case No. 23-cv-770 (N.D. Cal. 2023). Reuters report: https://www.reuters.com/legal/litigation/workday-must-face-novel-bias-lawsuit-over-ai-screening-software-2024-07-15 [Accessed 16 Mar. 2025].

[18] EEOC v. iTutorGroup, U.S. Equal Employment Opportunity Commission settlement (2023). ABA summary: https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/navigating-ai-employment-bias-maze [Accessed 17 Mar. 2025].

[19] CFPB Guidance on Credit Algorithms (2022). Consumer Finance Protection Bureau: https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms [Accessed 18 Mar. 2025].

[20] *Louis v. SafeRent Solutions LLC*, Case No. 1:22-cv-10760 (D. Mass. 2023). AP coverage: https://apnews.com/article/ 1bc785c24a1b88bd425a8fa367ab2b23 [Accessed 18 Mar. 2025].

Effective data governance is a cornerstone of the Artificial Intelligence Act, particularly for high-risk AI systems. Developers are required to ensure that datasets used in training, validation, and testing are relevant, representative, and free from errors or distortions that could lead to biased outcomes. This is essential for preventing discriminatory or harmful outputs, especially in areas involving sensitive personal data. The AIA further mandates documentation of data provenance, justification for data collection methods, and traceability throughout the AI system's lifecycle.

The lack of proper data governance has already produced notable legal and regulatory consequences. In the case of *State v. Clearview AI*, multiple European data protection authorities fined and banned the facial recognition company for harvesting billions of images without consent — highlighting the importance of lawful and proportionate data collection practices[21],[22]. Similarly, the *Netherlands SyRI* case invalidated a government-run risk prediction system for violating privacy rights due to opaque data use and lack of transparency[23]. These examples reveal how flawed or unregulated data governance not only erodes public trust but also contravenes fundamental rights, placing both developers and users of AI systems at legal risk.

Transparency is a fundamental requirement for high-risk AI systems under the Artificial Intelligence Act. Developers must design systems that are not only technically robust but also capable of offering meaningful explanations of how decisions are made. This includes informing users that they are interacting with an AI system, clarifying the logic behind automated decisions, and enabling scrutiny by regulators and affected individuals. Explainability is particularly important when decisions significantly affect individuals' rights, such as access to credit, employment, or public services.

Legal disputes have demonstrated the dangers of opaque AI systems. In *Burdick v. Employment Development Department (EDD)*, California residents sued the state for relying on a flawed algorithm that wrongly denied unemployment benefits without meaningful explanation or recourse[24,25]. The court ruled that the system violated due process rights. Similarly, in the UK, the A-Level

[21] Clearview AI cases brought by data protection authorities across the EU (2021–2023). Example: France CNIL decision (2022): https://www.cnil.fr/en/clearview-ai-ordered-stop-reuse-facial-recognition-data-and-delete-data [Accessed 18 Mar. 2025].

[22] UK ICO enforcement: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-clearview-ai-inc-over-breach-of-uk-data-protection-laws [Accessed 18 Mar. 2025].

[23] Netherlands District Court of The Hague, ECLI:NL:RBDHA:2020:865 (SyRI case). Summary via Human Rights Watch: https://www.hrw.org/news/2020/02/06/dutch-court-halts-dystopian-surveillance-system [Accessed 18 Mar. 2025].

[24] Burdick v. EDD, U.S. District Court, Northern District of California, Case No. 3:21-cv-02808. News summary: https://www.reuters.com/legal/government/california-sued-over-flawed-algorithm-used-deny-jobless-benefits-2021-04-19 [Accessed 18 Mar. 2025].

[25] Case summary via EFF: https://www.eff.org/cases/burdick-v-california-edd [Accessed 18 Mar. 2025].

grading scandal of 2020 — where an algorithm downgraded thousands of students' grades based on opaque criteria — sparked widespread public backlash and led to the abandonment of the model[26,27]. These cases underscore the principle that algorithmic decision-making must be auditable, intelligible, and subject to human review when individual rights are at stake.

The Artificial Intelligence Act requires that high-risk AI systems include safeguards to ensure effective human oversight. This principle is based on the idea that human operators must remain meaningfully involved in decision-making processes, especially where the outcomes affect individuals' rights or safety. Oversight may involve the ability to interpret and contest AI outputs, intervene before harm occurs, or deactivate systems in real time. The AIA also mandates continuous risk management procedures, including the identification, assessment, and mitigation of foreseeable risks, as well as post-market monitoring and incident reporting.

Failure to implement such mechanisms has resulted in tangible harm. In Michigan Unemployment Insurance Agency (UIA), over 40,000 individuals were wrongly accused of fraud due to an automated system with no human oversight or appeal mechanism[28,29]. The state was later required to issue mass reimbursements and conduct human reviews of past decisions. Similarly, in Australia's infamous "Robodebt" case, a government-run AI system used flawed income-averaging algorithms to issue unlawful debt notices to welfare recipients without proper human verification[30,31]. A Royal Commission found systemic failures in governance, and the government ultimately repaid over AU$1.7 billion to affected citizens. These cases reinforce the necessity of embedding human judgement and accountability into the design and deployment of high-risk AI.

Although the Artificial Intelligence Act introduces AI-specific rules, the General Data Protection Regulation (GDPR) remains a cornerstone of data protection within the EU and is highly relevant to the development and deployment of AI systems. Key GDPR principles — such as lawfulness, fairness, transparency, and purpose limitation — directly affect how AI systems may collect and

[26] UK A-Level Algorithm Scandal (2020). Coverage by BBC News: https://www.bbc.com/news/education-53805 [Accessed 18 Mar. 2025].

[27] Analysis from The Guardian: https://www.theguardian.com/education/2020/aug/17/algorithm-that-downgraded-a-level-results-must-never-be-used-again 105 [Accessed 18 Mar. 2025].

[28] Michigan UIA scandal involving automated fraud detection (2013–2020). News summary: https://www.freep.com/story/news/local/michigan/2020/08/10/michigan-jobless-agency-fraudulent-claims/3335021001 [Accessed 16 Mar. 2025].

[29] Legal coverage: https://www.wnem.com/news/michigan-to-reimburse-residents-wrongly-flagged-by-ai-fraud-system/article_4e8e18fa-2c8a-11ed-84de-0b5be66b2f28.html [Accessed 16 Mar. 2025].

[30] Australia Robodebt Royal Commission (2023). ABC News coverage: https://www.abc.net.au/news/2023-07-07/robodebt-royal-commission-final-report-released/102567034 [Accessed 16 Mar. 2025].

[31] Royal Commission Report (official): https://robodebt.royalcommission.gov.au/publications/ final-report [Accessed 16 Mar. 2025].

process personal data. Particularly important are Article 22 GDPR, which grants individuals the right not to be subject to decisions based solely on automated processing, and Article 7, which governs conditions for valid consent. These provisions create clear legal boundaries for profiling, behavioural prediction, and algorithmic decision-making, requiring developers to incorporate safeguards such as human intervention, explanation, and contestability mechanisms.

Despite their shared goal of protecting fundamental rights, the AIA and GDPR differ in scope, structure, and enforcement mechanisms, occasionally leading to areas of overlap or regulatory tension. While the GDPR focuses on how personal data is processed, the AIA regulates the function and risk of the AI system as a whole, including those that do not necessarily involve personal data. However, in high-risk AI systems that due process personal data — such as biometric identification or credit scoring — the two instruments converge. One tension arises in relation to explainability: GDPR's transparency obligations require that individuals understand how decisions are made, while many AI systems operate as "black boxes" that defy easy interpretation. Additionally, ambiguity remains regarding how the two frameworks interact procedurally — for example, whether a system's AIA compliance can be interpreted as sufficient proof of GDPR compliance, or whether dual assessments are required. These uncertainties highlight the need for harmonised guidance and enforcement practices, particularly at the national level.

3. Romanian National Context: Legal Readiness and Gaps

Romania, as an EU member state, is directly subject to the provisions of both the GDPR and the forthcoming Artificial Intelligence Act. While the GDPR has been transposed and implemented through national legislation — particularly Law No. 190/2018, which provides national derogations and clarifications — the country currently lacks any dedicated legal framework for AI regulation. As of early 2025, there are no specific national laws governing algorithmic decision-making, transparency of AI systems, or the mitigation of algorithmic bias. In this context, the entry into force of the AIA presents both a legal and institutional challenge for Romania.

Despite Romania's alignment with the GDPR, the national legal framework remains silent on key aspects of AI governance, particularly in relation to algorithmic decision-making, transparency, and bias mitigation. Currently, there are no binding national provisions that define how automated decision systems should be audited, how their logic must be disclosed, or how discriminatory outcomes should be identified and prevented. The absence of such regulations creates a regulatory vacuum, especially in high-impact sectors like employment, credit, and public administration, where AI is already being deployed. Without legal clarity, Romanian companies and public institutions risk either under-regulating, thereby infringing fundamental rights, or over-complying, which may stifle innovation due to legal uncertainty.

Romanian companies engaged in the development of artificial intelligence technologies face substantial uncertainty due to the absence of a dedicated national legal framework governing algorithmic transparency, accountability, and bias mitigation. In the current context, these entities must rely primarily on the GDPR and anticipate the future applicability of the Artificial Intelligence Act, yet they lack specific national guidance tailored to AI-specific compliance. This creates ambiguity regarding lawful data processing, model auditing obligations, and explainability standards. Consequently, many AI developers may adopt a risk-averse posture, slowing innovation and investment. For instance, Romanian startups such as TypingDNA, which builds AI-based behavioural authentication, and Druid AI, which develops conversational AI systems, operate in a regulatory vacuum with limited domestic support for legal risk management[32]. These companies must navigate legal uncertainty on their own or through external EU guidance, which adds operational complexity and potential compliance costs.

Organisations that integrate AI systems into their operations — especially in sectors like finance, recruitment, and e-commerce — also encounter regulatory and reputational risks due to the lack of national standards. AI adoption in Romanian businesses is steadily increasing, yet the absence of rules on algorithmic decision-making or profiling opens the door to inconsistent practices. For example, financial institutions experimenting with AI-driven credit scoring or risk assessment tools often do so without clear guidance on transparency or user rights. A 2023 report noted growing consumer complaints related to automated loan refusals and opaque decision-making in digital banking services in Romania[33]. Without clear mechanisms for auditability and user recourse, such practices risk violating Articles 13–15 and 22 of the GDPR and may undermine public trust in AI-based services. In the absence of regulatory certainty, businesses are left to define their own compliance thresholds — an approach that may result in uneven protection of fundamental rights and reputational exposure.

Beyond individual companies, the regulatory vacuum has wider implications for Romania's economic positioning. In a highly competitive regional tech landscape, the lack of legal clarity in AI governance can act as a deterrent to both

[32] TypingDNA develops AI-based typing biometrics used for behavioural authentication in security systems. See: https://www.typingdna.com. Druid AI builds conversational AI and NLP solutions for enterprises and raised €14.2 million in Series A funding to support global expansion. See: EU Startups, "Druid raises €14.2M to scale AI-driven chatbots," (2022), available at: https://www.eu-startups.com/2022/05/bucharest-based-druid-snaps-up-e14-2-million-for-its-innovative-ai-driven-chatbots-and-is-set-to-soar [Accessed 16 Mar. 2025].

[33] Romanian Financial Supervisory Authority, Consumer Protection Division Reports (2023), summary data on digital finance complaints. See also public discussions in: HotNews.ro, "Credit digital refuzat automat? Lipsa de transparență la bănci poate atrage sancțiuni," (May 2023), available at: https://economie.hotnews.ro/stiri-finante_banci-26258435-credite-digitale-refuzate-automat-lipsa-transparentei-poate-atras-sanctiuni.htm [Accessed 16 Mar. 2025].

domestic innovation and foreign direct investment. Investors and multinational partners typically require predictable and stable legal environments — particularly in emerging technology sectors. In response, Romanian authorities adopted the National Strategy on Artificial Intelligence for 2024–2027, aiming to harmonise domestic policy with EU digital objectives, including the implementation of the AI Act[34]. The strategy highlights key focus areas such as digital public services, education, cybersecurity, and responsible AI development. However, as of early 2025, the strategy remains largely programmatic and lacks concrete legislative instruments or enforcement mechanisms. A proactive legal and institutional framework will be essential not only to attract investment but also to ensure ethical, lawful, and economically sustainable AI integration.

The institutional capacity to enforce data protection and future AI regulation in Romania remains limited. The National Authority for the Supervision of Personal Data Processing (ANSPDCP) is the primary body responsible for GDPR enforcement, but it has so far played a relatively modest role in the emerging debate around algorithmic accountability and AI oversight. Its enforcement actions have focused primarily on traditional data breaches, with limited public engagement or guidance regarding automated decision-making or profiling under Article 22 GDPR[35]. The judiciary has also faced challenges in addressing complex data-driven cases, due to limited technical expertise and the novelty of AI-related disputes. In the public sector, algorithmic tools are being introduced (e.g., in tax administration or digital public services), yet no unified framework or oversight mechanism exists to evaluate their legality or impact. This institutional lag poses risks not only for rights protection but also for effective implementation of the AI Act once it becomes fully applicable.

In addition to limited institutional readiness, Romania faces challenges stemming from regulatory fragmentation and legal ambiguity. While several digital strategies and policy frameworks exist — such as the National AI Strategy and various e-Governance initiatives — these remain largely aspirational and are not supported by enforceable legal instruments. Moreover, the interaction between horizontal legal norms (such as GDPR) and emerging sector-specific policies (e.g., in finance or health) has not been clearly articulated in legislation or practice. This lack of coherence creates uncertainty for private and public actors alike, as they struggle to interpret how existing rules apply to AI systems in the absence of case law, regulatory guidance, or coordinated enforcement. As Romania prepares to align with the Artificial Intelligence Act, addressing these legal and institutional inconsistencies will be essential to avoid fragmented implemen-

[34] U.S. Department of Commerce, “Romania – Digital Economy: Country Commercial Guide,” (2024), available at: https://www.trade.gov/country-commercial-guides/romania-digital-economy [Accessed 16 Mar. 2025].

[35] ANSPDCP – Annual Activity Reports (2019–2023). Available at: https://www.dataprotection.ro/?page=Raportare&lang=en.

tation and to ensure both innovation and fundamental rights are adequately protected.

4. AI Use in the Romanian Tech Ecosystem

In the last decade, Romania has emerged as a regional hub for technology and innovation, with a growing number of startups and scale-ups developing AI-driven solutions. Several Romanian-founded companies have gained international visibility through the integration of artificial intelligence into software products. Notably, UiPath, originally founded in Bucharest, became a global leader in robotic process automation (RPA), incorporating AI to enhance document understanding, task mining, and decision-making processes. Other firms, such as Druid AI, which develops conversational AI platforms for enterprise clients, and TypingDNA, known for behavioural biometrics and continuous authentication, exemplify the innovative applications of AI originating from the Romanian ecosystem[36]. These companies operate within or adjacent to the high-risk AI categories defined by the Artificial Intelligence Act, particularly in areas like workplace automation, identity verification, and customer interaction.

Romanian AI developers are active across a range of sectors, reflecting the country's growing integration into the European and global digital economy. In the enterprise automation space, UiPath remains the most prominent example, achieving "unicorn" status in 2018 and later listing on the New York Stock Exchange in 2021 — an achievement that brought international attention to the Romanian tech ecosystem. In the natural language processing and customer experience domains, Druid AI has expanded rapidly, securing €14.2 million in Series A funding in 2022 to support international expansion and product scaling[37]. In the field of cybersecurity and behavioural analytics, TypingDNA offers authentication tools based on AI-powered keystroke dynamics, with applications in fintech, education, and secure enterprise systems. Other emerging firms, such as MorphL (acquired by Algolia in 2021), applied AI to personalise user experiences in e-commerce environments[38].

Funding for AI startups in Romania comes from a mix of EU-backed programmes, venture capital, and local accelerators such as Techcelerator, which supports early-stage AI ventures with seed funding and regulatory mentoring. While access to funding has improved, Romanian AI developers still face structural constraints related to limited legal infrastructure, underdeveloped public-

[36] UiPath: https://www.uipath.com, Druid AI: https://www.druidai.com, TypingDNA: https://www.typingdna.com.

[37] "Druid raises €14.2M to scale AI-driven chatbots," EU Startups (2022). Available at: https://www.eu-startups.com/2022/05/bucharest-based-druid-snaps-up-e14-2-million-for-its-innovative-ai-driven-chatbots-and-is-set-to-soar.

[38] "Algolia acquires MorphL to personalize AI-powered search," TechCrunch (2021). Available at: https://techcrunch.com/2021/01/26/algolia-acquires-morphl/.

private partnerships, and a domestic market that remains risk-averse in adopting emerging technologies. These factors limit the scalability and long-term competitiveness of AI enterprises unless accompanied by targeted regulatory and institutional support.

The AI systems developed by Romanian companies are likely to fall under the “high-risk” category as defined by the Artificial Intelligence Act. These include applications used in areas such as biometric identification, access to financial services, employment, and customer profiling. For example, TypingDNA’s behavioural biometrics, used for continuous authentication in finance and education, involves sensitive personal data and could be classified as high-risk under the AIA due to its potential impact on access to essential services and data protection rights[39]. Similarly, Druid AI’s conversational platforms —when integrated into hiring platforms or health-related services — may be subject to stricter obligations depending on their deployment context. Even UiPath’s process automation tools, while general-purpose in nature, may fall under the AIA’s scope if used in judicial or public administrative settings where automated decision-making has legal consequences.

The AIA’s risk-based framework places considerable responsibility on developers to assess the intended use of their products and apply appropriate compliance mechanisms. This includes risk management systems, detailed documentation, human oversight protocols, and post-market monitoring —requirements that may place a disproportionate burden on small and medium-sized enterprises (SMEs), which make up the majority of Romania’s AI innovation landscape. Without national implementation guidelines or regulatory support structures, Romanian developers risk falling behind in both compliance and competitiveness, particularly when seeking to scale within the EU market.

AI adoption in Romania is no longer limited to developers — large companies and public institutions have also begun integrating AI technologies into their operational workflows. In the banking sector, institutions such as Banca Transilvania and BRD – Groupe Société Générale have implemented AI-driven tools for fraud detection, customer service chatbots, and credit scoring, aiming to improve efficiency and user experience[40]. Similarly, in the telecommunications industry, companies like Orange Romania and Vodafone have deployed AI for network optimisation, predictive maintenance, and customer engagement, including through virtual assistants and intelligent routing systems. These use cases illustrate Romania’s growing reliance on AI not just as a back-end optimisation

[39] For an overview of AIA’s “high-risk” categories, see: European Commission, “Proposal for a Regulation laying down harmonised rules on artificial intelligence,” (COM/2021/206 final). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[40] See Banca Transilvania AI chatbot “Raul,” launched for customer support services. Coverage: ZF Tech, “Banca Transilvania lansează Raul, asistent virtual bazat pe AI,” (2021), available at: https://www.zf.ro/business-hi-tech/banca-transilvania-lanseaza-raul-un-asistent-virtual-care-utilizeaza-19913929. See also: Orange Romania AI-driven customer services. Company new sroom: https://www.orange.ro/newsroom.

tool, but as a direct interface between service providers and consumers.

In the public sector, digitalisation strategies have included elements of AI integration, especially in areas such as tax administration (e.g., automated document processing at ANAF, the National Tax Administration Agency), health system logistics, and smart city initiatives.

However, the broader implementation of the GDPR and the forthcoming AIA introduces significant compliance obligations that can reshape business models and affect the cost-benefit calculus of adopting AI. Under these regulations, companies must assess whether their systems fall under high-risk classifications, ensure lawful data processing, and implement transparency, human oversight, and risk mitigation mechanisms. These requirements may increase operational costs, especially for smaller firms, while also raising concerns over legal liability and reputational risks. As a result, some companies may limit or delay AI deployment, particularly in sensitive areas such as finance or HR, where the stakes of non-compliance are higher. Balancing innovation with regulatory risk has thus become a key strategic consideration in Romania's evolving digital economy.

The integration of AI into the Romanian public sector presents both opportunities and substantial risks. Institutions such as the National Agency for Fiscal Administration (ANAF) and various municipal governments have begun exploring AI applications for document automation, service delivery optimisation, and predictive analytics. There are also discussions around AI-supported systems for case management in courts, digital legal research, and even resource allocation in public employment processes. However, in the absence of robust legal and ethical frameworks, the deployment of such systems risks violating principles of due process, non-discrimination, and administrative transparency.

Compliance with the Artificial Intelligence Act and GDPR will require public authorities to conduct fundamental rights impact assessments, ensure algorithmic transparency, and provide mechanisms for human oversight and contestability. These obligations may necessitate the creation of internal compliance units, staff retraining, and collaboration with external regulators—demands that many Romanian public institutions are currently ill-equipped to meet. Without proactive institutional adaptation, the use of AI in governance may exacerbate systemic inefficiencies or deepen existing social inequalities, rather than resolving them. As such, the adoption of AI in the public sector must be accompanied by a clear strategy for legal compliance, ethical alignment, and accountability.

5. Challenges and Strategic Directions for AI Governance in Romania

One of the most pressing challenges Romania faces in the context of AI governance is the lack of established mechanisms to ensure algorithmic transparency and explainability[41]. While the GDPR mandates user information rights and safeguards against fully automated decision-making (Article 22), these provisions are rarely enforced in practice. Moreover, the Artificial Intelligence Act introduces further requirements — such as risk classification, logging, and documentation — that public and private actors in Romania are largely unprepared to meet. Many existing AI systems, especially those procured or developed without a legal compliance framework, function as "black boxes," where decision logic is opaque even to their implementers. This undermines accountability, particularly in sectors like finance, employment, and public services where algorithmic decisions can significantly affect individual rights.

Another critical concern is the risk of algorithmic discrimination[42], particularly when AI systems are trained on biased or non-representative data. In Romania, this issue is amplified by the absence of formal auditing requirements or standardised evaluation procedures for bias detection. High-risk domains — such as credit scoring, recruitment, and welfare allocation — are especially vulnerable to unjustified disparities in outcomes. For instance, AI models used for pre-screening job applicants may inadvertently disadvantage certain demographic groups, while automated credit assessments could embed historical inequalities due to reliance on legacy datasets. Without dedicated national guidance, these risks remain difficult to identify and even harder to remedy, especially for smaller entities lacking internal legal or ethical oversight capacity.

Beyond technical and legal challenges, Romania's public institutions are limited in their capacity to implement, supervise, and enforce AI-related obligations[43]. Regulatory bodies such as ANSPDCP currently lack the specialised personnel and technical infrastructure to audit AI systems or issue sector-specific guidance. The judiciary, too, faces obstacles in adjudicating AI-related cases, which often require multidisciplinary expertise that is not yet integrated into judicial training. Similarly, most public institutions deploying AI do so without dedicated ethics committees, risk impact protocols, or transparent procurement rules. This institutional inertia could delay the effective enforcement of both GDPR and the AIA, undermining Romania's compliance with EU digital policy goals.

To address these challenges, Romania must adopt a proactive and coher-

[41] Polat Goktas. 2024. "Ethics, Transparency, and Explainability in Generative Ai Decision-Making Systems: A Comprehensive Bibliometric Study." *Journal of Decision Systems*, October, 1–29. doi: 10.1080/12460125.2024.2410042.

[42] Xukang Wang, Ying Cheng Wu, Xueliang Ji, Hongpeng Fu. 2024. "Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices." *Frontiers in Artificial Intelligence*, vol. 7: 1320277, https://doi.org/10.3389/frai.2024.1320277.

[43] Ahmed Oudah Mohammed Al-Dulaimi, Mohammed Abd-Al Wahab Mohammed. 2025 „Legal responsibility for errors caused by artificial intelligence (AI) in the public sector". *International Journal of Law and Management*, https://doi.org/10.1108/IJLMA-08-2024-0295.

ent strategy for AI governance. First, national legislation should explicitly integrate the obligations set forth in the AIA and clarify their relationship with existing data protection laws. Second, sector-specific regulatory guidelines should be developed — particularly in high-risk areas such as finance, education, and public administration — outlining best practices for transparency, data governance, and human oversight. Third, public investment should focus on institutional capacity-building, including the creation of expert units within regulators and the judiciary, as well as funding for algorithmic auditing infrastructure.

Finally, legal reform must be accompanied by economic and educational support mechanisms. This includes establishing regulatory sandboxes for AI innovation, where startups and SMEs can test high-risk systems under regulatory supervision; offering compliance toolkits for companies with limited in-house legal capacity; and integrating AI ethics and regulation into academic and professional training programs. These measures will help ensure that Romania's AI ecosystem remains competitive and responsible. Striking the right balance between innovation and rights protection is essential — not only for legal compliance with the AIA and GDPR, but for the long-term legitimacy and public acceptance of AI technologies in Romanian society.

6. Conclusions

Romania enters a new regulatory era defined by the interplay between the General Data Protection Regulation and the forthcoming Artificial Intelligence Act. In this environment it faces both significant challenges and valuable opportunities. While the country has demonstrated technological potential through its emerging AI startup ecosystem and growing digital infrastructure, its legal and institutional frameworks remain underdeveloped in key areas such as algorithmic transparency, bias mitigation, and risk accountability.

This paper has argued that the lack of national regulation specific to AI — and the limited institutional capacity to interpret and enforce EU-level standards — poses legal, economic, and societal risks. At the same time, compliance with the AIA and GDPR is not merely a regulatory burden; it is a strategic imperative for building public trust, enabling cross-border scalability, and fostering sustainable innovation.

To move forward, Romania must invest in legal harmonisation, institutional reform, and practical support mechanisms for both public and private actors. Only through a coordinated, forward-looking approach can the country effectively integrate AI into its legal and economic systems — while upholding fundamental rights and participating meaningfully in the European digital transformation.

Romania, as a Member State of the European Union, must align itself with the use of AI technologies and, following the adoption of the AI Act, must unquestionably adapt its entire legislative framework to reflect the aforementioned reference legal instruments. Clearly, at the institutional level, the real challenge lies in the effective mechanisms for responding to this complex set of requirements — responding proactively and comprehensively in areas where fundamental rights are affected by AI, in the context of the interplay between the AI Act and the GDPR, avoiding interpretative contradictions or overlapping regulations, and ensuring the availability of mechanisms both for contesting and for remedying decisions, as such situations will undoubtedly arise.

This "challenge" falls primarily on the Romanian legislator, who must be able to anticipate, at the national level, not only what has already emerged from the European framework, but also what is likely to arise from jurisprudence developed in parallel by the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR). The legislator must gain a deep, evolving understanding of the new legal relationships that will continuously emerge from the already ongoing interaction between citizens and the legal entities developing AI technologies.

Bibliography

1. Al-Dulaimi, Ahmed Oudah Mohammed & Mohammed Abd-Al Wahab Mohammed. 2025 „Legal responsibility for errors caused by artificial intelligence (AI) in the public sector". *International Journal of Law and Management*, https://doi.org/10.1108/IJLMA-08-2024-0295.
2. Bataineh, Abdallah Q., Alaa S. Mushtaha, Ibrahim A. Abu-AlSondos, Saeed Hameed Aldulaimi & Marwan Abdeldayem. 2024. "Ethical & Legal Concerns of Artificial Intelligence in the Healthcare Sector," *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, pp. 491-495, doi: 10.1109/ICETSIS61505.2024.10459438.
3. Castro, Daniel and Michael McLaughlin, "Who Is Winning the AI Race: China, the EU, or the United States?" Center for Data Innovation, January 2021, https://datainnovation.org/2021/01/who-is-winning-the-ai-race-china-the-eu-or-the-united-states-2021-update/.
4. Chambers and Partners. (2024). Artificial Intelligence 2024 – Romania: Law & Practice Guide. Available at: https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/romania [Accessed 21 Mar. 2025].
5. Enqvist, Lena 2024. "Rule-based versus AI-driven benefits allocation: GDPR and AIA legal implications and challenges for automation in public social security administration." *Information & Communications Technology Law* vol. 33, no. 2: 222-246, doi: 10.1080/13600834.2024.2349835.
6. Goktas, Polat. 2024. "Ethics, Transparency, and Explainability in Generative Ai Decision-Making Systems: A Comprehensive Bibliometric Study." *Journal of Decision Systems*, October, 1–29. doi: 10.1080/12460125.2024.2410042.
7. Olimid, Anca Parmena, Catalina Maria Georgescu and Daniel Alin Olimid. 2024. "Legal Analysis of EU Artificial Intelligence Act (2024): Insights from

Personal Data Governance and Health Policy." *Access to Justice in Eastern Europe* 7(4): *120-42 <https://doi.org/10.33327/AJEE-18-7.4-a000103>.*

8. Quintais, João Pedro. 2025. "Generative AI, copyright and the AI Act." *Computer Law & Security Review*, vol. 56: 106107, https://doi.org/10.1016/j.cl sr.2025.106107.
9. Regulation (EU) 2016/679 of the European Parliament and of the Council 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).
10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
11. Wallace, Nick and Daniel Castro (2018). *The Impact of the EU's New Data Protection Regulation on AI. Information Technology and Innovation Foundation (ITIF).* Available at: https://itif.org/pu blications/2018/03/26/impac t-eu-new-data-protection-regulation-ai [Accessed 21 Mar. 2025].
12. Wang, Xukang, Ying Cheng Wu, Xueliang Ji & Hongpeng Fu. 2024. "Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices." *Frontiers in Artificial Intelligence*, vol. 7: 1320277, https://doi.org/10.3389/frai.2024.1320277.
13. Yuan, Yiming, Yongming Sun and Hangyu Chen. 2024. "Does Artificial Intelligence Affect Firms' Inner Wage Gap?" *Applied Economics* 57 (19): 2365–71. doi: 10.1080/00036846.2024.23 24090.