Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

RESEARCH ARTICLE

Research Article

THE EU ARTIFICIAL INTELLIGENCE ACT AND DATA PROTECTION CHALLENGES FOR NON-EU CITIZENS: COMPARATIVE INSIGHTS FROM THE WESTERN BALKANS

Fjorida Ballauri

DOI:
https://doi.org/10.33327/AJEE-18-9.3-a0001992

Date of submission: 04 Feb 2026
Date of acceptance: 27 Apr 2026
Online First Publication: 12 June 2026

Disclaimer:
The author declares that her opinions and views expressed in this manuscript are free from any impact of any organisations.

ABSTRACT

Background: *In the era of artificial intelligence, data protection and privacy rights have become critical components of the European Union's legal order. This study examines the interaction between the EU Artificial Intelligence Act of 2024 and the General Data Protection Regulation, focusing on their implications for non-EU countries, particularly Albania. The adoption of the EU Artificial Intelligence Act has reshaped the legal framework governing artificial intelligence and personal data protection in Europe. However, the practical implications of these instruments for non-EU citizens, particularly in Western Balkan countries as EU candidate countries, remain underexplored.*

Methods: *The study adopts a combined comparative legal and empirical methodology. It integrates a comparative legal analysis to evaluate the extent of alignment between domestic legislation and EU standards, a questionnaire-based survey of 178 respondents to assess public awareness and* perceptions *of*

privacy rights, and an analysis of attitudes towards the risks associated with artificial intelligence and personal data processing. It provides quantitative evidence that complements the legal analysis by illustrating how regulatory frameworks are perceived and experienced in practice. Based on the questionnaire data identifying Meta Platforms as the most widely used social media platform in Albania, the study includes a case study designed as an experimental rights-exercise test involving a data-access request submitted to the company, aimed at examining the cross-border enforceability of data-subject rights.

Results and Conclusions: *The findings reveal a significant gap between formal legislative harmonisation with EU data-protection and AI standards and their effective implementation in Western Balkan candidate countries. Survey evidence from 178 Albanian respondents indicates limited awareness of personal data rights, low trust in institutional protection, and widespread uncertainty about AI-driven profiling and data use. The case study further demonstrates challenges in enforcing rights against foreign entities. Strengthening supervisory mechanisms and adopting the EU's risk-based approach to AI regulation are recommended to ensure effective protection of personal data in candidate countries. Effective data protection measures for non-EU citizens require strengthening supervisory cooperation, enhancing enforcement capacity, and adopting the EU AI Act's risk-based governance model in domestic law.*

1 INTRODUCTION

The protection of personal data is a fundamental right guaranteed by Article 8(1) of the Charter of Fundamental Rights of the European Union[1] and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).[2] The rapid evolution of technology has increased the risks to privacy and data integrity, requiring every state to strengthen guarantees for these rights, especially in the era of artificial intelligence (AI).

The development of technology is progressing rapidly, and everyday data management problems pose a risk to fundamental human rights in private life and across social and economic spheres. The protection of personal data is an obligation that every state must undertake in light of developments in the field of artificial intelligence. The EU has recently taken concrete measures to regulate the use of artificial intelligence in various applications, bringing guarantees for the fundamental rights of EU citizens. While the General Data Protection Regulation (GDPR)[3] provides extensive protection for EU citizens, non-EU citizens remain vulnerable to profiling and cross-border data transfers. Few studies address how AI regulation affects these populations.

1 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
2 Treaty on the Functioning of the European Union (Consolidated versions) [2016] OJ C 202/47.
3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

European countries such as Albania, Kosovo, Montenegro, North Macedonia, Serbia, and Bosnia and Herzegovina are currently candidates for EU membership and, as such, have moved forward with the approximation of their legislation to EU standards. However, without becoming a member state, they cannot enjoy the protection that EU legislation and its law enforcement instruments provide. The article aims to address the research question: To what extent do national data protection frameworks in Western Balkan countries, especially in Albania, provide protection comparable to that under the GDPR and the AI Act?

The paper explores whether citizens in candidate countries enjoy effective protection comparable to that guaranteed by the GDPR and the AI Act.[4] The EU's regulation on AI is expected to serve as a guide for other European countries that are not part of the EU. Under these conditions, other countries should implement regulatory and legal measures so that the privacy policies of companies that will use AI are assessed and monitored by responsible institutions before they are implemented for citizens.

2 METHODOLOGY AND SCOPE OF RESEARCH

The methodology of this study combines comparative legal analysis with empirical research, integrating doctrinal analysis, a questionnaire-based survey, and a case study. The comparative legal analysis evaluates the extent to which domestic legislation aligns with EU standards through textual, systematic, and teleological interpretation. The empirical component is based on a structured questionnaire administered to 178 respondents, in line with established survey research methodologies.[5] The case study follows an experimental approach to assessing the enforceability of data-subject rights in practice, consistent with case study research design principles.[6] This mixed-methods approach enables a comprehensive assessment of both legal norms and their practical implementation.[7] Together, these methods enable a comprehensive examination of the gap between legislative harmonisation and its effective application in practice.

4 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) [2024] OJ L 2024/1689 <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 25 January 2026.

5 Alan Bryman, *Social Research Methods* (5th edn, OUP 2016); Don A Dillman, Jolene D Smyth and Leah Melani Christian, *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method* (4th edn, Wiley 2014).

6 Robert K Yin, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE 2018).

7 Peter Cane and Herbert M Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (OUP 2010); John W Creswell and J David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th edn, SAGE 2018).

The realisation of this study was inspired by an article titled "Meta trains artificial intelligence on the data of Balkan citizens without warning". In this article, it was stated that: "*Everything happened without notice or explanation and millions of users in the Western Balkans were not even informed about Meta's new "Privacy Policy", which was published on June 26, 2024. Users from the Western Balkans were not informed about the innovation, while citizens of the European Union, when entering the platforms, received a warning that the policy was changing and then had the option to withdraw data from the planned artificial intelligence training.*"[8]

In particular, this paper analyses EU legislation governing the protection of personal data in the context of the development and use of artificial intelligence in EU Member States. The analysis is conducted from a comparative perspective, focusing on Western Balkan countries and, more specifically, on Albania, for which a more detailed comparative assessment is provided. Although EU candidate countries, such as Albania and other Western Balkan countries, are harmonising their domestic legislation with EU law and regulations, the level of legal protection available to citizens of these non-EU countries, particularly in the practical implementation of the law and the exercise of supervisory powers by domestic authorities, remains questionable.

A comparative legal analysis was conducted between the EU framework and national legislation in Albania. Empirical data were collected through an online questionnaire[9] of 178 respondents to assess awareness of personal data rights. The study applies a doctrinal and empirical approach and limits its scope to the interaction between GDPR principles[10] and the Albanian Law No. 124/2024.[11] The questionnaire was designed, using the Google Forms platform, in which 178 Albanian citizens of different ages participated, with the aim of collecting their perceptions about the security of their personal data when using applications such as Facebook, Instagram, etc., as well as on their knowledge of rights, the guarantees offered by legislation, their assessment of the use of their personal data, and whether they had encountered the use of their personal data without their knowledge or consent. The survey was voluntary and anonymous. Participants were informed of the study's purpose and their right to withdraw at any time, ensuring compliance with ethical standards for social research and the principles of informed consent. All participants

8 Natallija Jovanoviq, 'Meta trajnon pa paralajmërim inteligjencën artificiale mbi të dhënat e qytetarëve të Ballkanit' (*Radio Evropa e Lirë,* 5 August 2024) <https://www.evropaelire.org/a/meta-trajnon-paparalajmerim-inteligjencen-artificiale-mbi-te-dhenat-e-qytetareve-ballkanit-/33066127.html> accessed 25 January 2026.

9 Fjorida Ballauri, 'The Questionnaire on the Awareness and Experience of Albanian Citizens Regarding the Protection of Personal Data and Privacy in the Digital Age' (*Google Forms*, 2025) <https://docs.google.com/forms/d/1rXEv9an-fZNGD79VSr5K52HUu2KDDLX0AF05DLFwVOQ/edit#responses> accessed 25 January 2026.

10 Regulation (EU) 2016/679 (n 3).

11 Law of the Republic of Albania No 124/2024 'On Personal Data Protection' (adopted 19 December 2024) [2025] Official Gazette 9.

provided informed consent prior to participation. The survey was conducted anonymously. The data were analysed in aggregate form to ensure confidentiality and compliance with ethical research standards. No personal identifiers were collected, and the results were analysed in aggregate form. Among the 178 respondents, 60.7% were women, 37.6% men, and 1.7% preferred not to disclose. The largest age group was aged 26–40 years (46%), followed by 41–60 years (30.3%), 18–25 years (11.2%), and under 18 years (5.6%).

The questionnaire included sections on basic information, awareness of the new legal framework (Law No. 124/2024), and understanding of key concepts such as personal data and individual rights. The respondents are asked about their own experiences with potential data misuse, combining predefined answers with open-ended questions to capture real-life situations. Further sections focused on awareness of complaint mechanisms, patterns of social media use, and perceptions of how personal data are used online, particularly in relation to profiling and targeted advertising. Finally, participants were asked how protected they felt and whether more public awareness is needed. Taken together, the questionnaire was designed to provide a clearer picture of how the legal framework operates in practice, highlighting the gap between formal rules and people's actual knowledge and experiences.

According to the data collected, more women (60.7% of the respondents) responded than men (37.6% of the respondents). Meanwhile, 1.7% (of the respondents preferred not to answer this question). The aim was to collect data on the information of different citizens regarding the protection of their personal data when using Facebook, Instagram, etc., as well as on their knowledge of rights, the guarantees offered by legislation, their assessment of the use of their personal data, and whether they had encountered the use of their personal data without their knowledge or consent. The collected data were analysed using descriptive statistical methods. The empirical findings are integrated with the doctrinal analysis of the Albanian legal framework and relevant EU standards. This combined approach allows for the identification of structural gaps between normative regulation and practical enforcement. In addition to the doctrinal and empirical components, this study incorporated an experimental element designed to test the practical enforceability of data subject rights under the newly adopted Albanian Law No. 124/2024 on personal data protection. The objective was to verify whether a non-EU citizen can effectively exercise rights analogous to those guaranteed under the GDPR, specifically the rights of access, information, and erasure when interacting with a major global platform.

On 12 July 2025, a formal request was submitted to the designated Meta Platforms data protection contact address (mydataprivacyrights@fb.com). The request sought:

1. A comprehensive summary of personal data collected prior to 2024 remains stored by the company.
2. The purposes for which this data continues to be processed.
3. The identity of any third party with whom the data has been shared before or after 2024.

4. Confirmation of whether the data had been included in automated processes, such as profiling or targeted advertising; and
5. The planned retention period for such data.

The request explicitly cited the 30-day response period established under Article 14 of Law No. 124/2024, mirroring Article 12(3) of the GDPR. Despite the formal submission and the expiration of the legal deadline, Meta Platforms has not responded.

This result illustrates a practical enforcement gap between the formal rights recognised by national law and their practical realisation, particularly where data controllers are established outside the supervisory authority's jurisdiction. The experiment thus provides empirical evidence for the paper's broader finding that legal harmonisation with EU standards does not automatically ensure effective protection for non-EU citizens in cross-border digital contexts.

Combining desk-based research, comparative assessment of EU legislation and the study of the results of the specific questionnaire designed by the author,[12] this study aims to provide a comprehensive and comparative analysis of the legal framework of the non-EU countries in the protection of personal data and the challenges when AI technology is used.

The study does not provide a full sociological analysis of attitudes but focuses on the legal and institutional dimensions of data protection.

3 LIMITATIONS OF THE STUDY

This study presents several limitations that should be acknowledged. The empirical component is based on a questionnaire conducted with 178 respondents, which, while sufficient to identify general trends, does not provide a fully representative sample of the Albanian population. The findings should, therefore, be interpreted as indicative rather than exhaustive.

The questionnaire primarily captures self-reported perceptions and levels of awareness, which may be influenced by subjective understanding or recall bias. Nevertheless, its inclusion provides valuable insight into the practical dimension of data protection, highlighting the gap between formal legal guarantees and citizens' real-world experiences. The case study is limited to a single platform, Meta Platforms, and to one experimental rights-exercise request. While this approach allows for a concrete assessment of cross-border enforceability, it does not fully capture the diversity of practices across different digital service providers.

12 Ballauri (n 9).

Despite these limitations, the combined use of doctrinal analysis, empirical data, and the case study provides a more practical view of the overall research design. The questionnaire contributes to the research field by providing rare empirical evidence on public awareness and perceptions in a non-EU context, an area underexplored in the existing literature.

4 LITERATURE REVIEW

Legal and practical discussions on the regulation of artificial intelligence (AI) and data protection have advanced rapidly since the adoption of the GDPR.[13] However, important debates remain regarding governance, enforcement, and extraterritorial effects. The GDPR and the recently adopted EU Artificial Intelligence Act[14] together form the normative framework against which national harmonisation efforts should be assessed. The GDPR establishes substantive rights and procedural safeguards concerning profiling and international data transfers (Arts. 20–50), while the EU AI Act introduces a risk-based regulatory model that distinguishes between unacceptable, high-risk, and low-risk AI systems. These instruments provide the legal benchmark commonly used in comparative literature to evaluate the level of protection in non-EU jurisdictions.

A growing body of legal scholarship examines the limits of existing anti-discrimination and data protection frameworks when applied to algorithmic decision-making. Philipp Hacker foregrounds the legal and practical challenges in teaching fairness to AI,[15] arguing that normative prescriptions must be paired with procedural safeguards such as audits and impact assessments. Complementing this. Michael Veale and Frederik Zuiderveen Borgesius further demystify the AI Act by clarifying its interplay with existing EU data protection law and its likely enforcement challenges,[16] concluding that national authorities will face significant burdens in ensuring consistent interpretation and accountability across Member States.

Empirical and technical perspectives also contribute to this debate. Studies on algorithmic harm spanning employment, advertising, and biometric systems, illustrate how biased training data and opaque models can produce discriminatory outcomes not easily redressed by classical anti-discrimination law[17]. At the same time, recent policy guidance has

13 Regulation (EU) 2016/679 (n 3).

14 Regulation (EU) 2024/1689 (n 4).

15 Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55(4) Common Market Law Review 1143, doi:10.54648/cola2018095.

16 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law & Security Review 97, doi:10.9785/cri-2021-220402.

17 Frederik Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24(10) The International Journal of Human Rights 1572, doi:10.1080/13642987.2020.1743976.

expanded the operational understanding of AI-related data protection. The European Data Protection Board issued its Guidelines on AI and Data Protection, which interpret how the principles of lawfulness, fairness, and transparency apply to AI systems under the GDPR and AI Act.[18] The guidelines stress the importance of "data minimisation by design" and the use of impact assessments for all high-risk AI applications.

International and institutional reports bridge academic critique and regulatory practice. The European Parliament's 2021 study on biometric recognition[19] clarifies the ethical and human-rights rationale for restrictive measures on facial recognition and mass surveillance. The NIST AI Risk Management Framework[20] provides operational tools for assessing and mitigating AI risks, relevant even outside the United States. In parallel, the European Data Protection Board Annual Report for 2024 on Cross-Border AI Compliance identifies enforcement inconsistencies among Member States and highlights the limited oversight capacity in associated countries,[21] including EU candidates, to monitor AI-related data transfers. Council of Europe instruments, most notably Convention 108+ [22] continue to provide a multilateral avenue for achieving interoperable standards that complement EU rules and reduce legal fragmentation. A distinct strand of literature addresses the extraterritorial implications of EU rules and the realpolitik of enforcement. Oscar J. Gstrein and Andrej Zwitter note that while the GDPR projects normative standards beyond EU borders, practical protection for non-EU citizens depends on the presence of supervisory cooperation and technical capacity.[23] Case studies from candidate states show that formal legislative transposition often coexists with weak enforcement and limited public awareness.[24]

18 European Data Protection Supervisor, *Generative AI and the EUDPR: Orientations for ensuring data protection compliance when using Generative AI systems* (version 2, EDPS 2025) <https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-10-28-guidance-generative-ai-strengthening-data-protection-rapidly-changing-digital-era_en> accessed 25 January 2026.

19 Gloria González Fuster and Michalina Nadolna Peeters, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (European Parliament EPRS 2021) doi:10.2861/384495.

20 National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, US Department of Commerce 2023) <https://www.nist.gov/itl/ai-risk-management-framework> accessed 25 January 2026.

21 European Data Protection Board, *Annual Report 2024: Protecting Personal Data in a Changing Landscape* (EDPB 2024) <https://www.edpb.europa.eu/news/news/2025/edpb-annual-report-2024-protecting-personal-data-changing-landscape_en> accessed 25 January 2026.

22 Council of Europe, *Convention 108 +: Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (CoE 2018) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 25 January 2026.

23 Oskar J Gstrein and Andrej Zwitter, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10(3) Internet Policy Review, doi:10.14763/2021.3.1576.

24 See, European Commission, *Albania 2024 Report* (SWD(2024) 690 final, 30 October 2024) <https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52024SC0690> accessed 25 January 2026; Information and Data Protection Commissioner, *Annual Report 2024* (IDPC 2025) <https://idp.al/en/annual-reports/> accessed 25 January 2026.

5 TRANSFER OF PERSONAL DATA AND ALIGNMENT OF ALBANIAN LEGISLATION WITH EU STANDARDS

Public security concerns and crime prevention policies, particularly in counter-terrorism, have led to the adoption of surveillance and monitoring measures at both the EU and national levels. These measures frequently involve the processing of personal data by law enforcement authorities, raising important questions regarding the balance between public security and the protection of fundamental rights.

The General Data Protection Regulation[25] and the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data"[26] are the main EU documents to guarantee the protection of personal data, as a fundamental right. The protection and free movement of data processed by law enforcement authorities for the purposes of prevention, investigation, detection, prosecution of criminal offences, or the execution of criminal penalties are regulated by this directive, allowing member states a certain level of flexibility to incorporate it into their domestic law.

The Directive on data protection in the police and justice sectors aims to balance the objectives of personal data protection with the objectives of security policies and public interest. This directive provides that any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and may be processed only for specific purposes laid down by law. This, in itself, does not prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. Natural persons should be made aware of the risks, rules, safeguards, and rights in relation to the processing of their personal data, and how to exercise their rights in this regard. In particular, the specific purposes for which the personal data are processed should be explicit, legitimate, and determined at the time of the collection. The personal data should be adequate and relevant for the purposes for which it is processed. It should be ensured that the personal data collected is not excessive and not kept longer than is necessary for the purpose for

25 Regulation (EU) 2016/679 (n 3).

26 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection, or Prosecution of Criminal Offences and on the Free Movement of Such Data (2016) OJ L 119/89.

which it is processed. Personal data should be processed only if the purpose of the processing cannot reasonably be fulfilled by other means.[27]

Albania, North Macedonia, Serbia, Montenegro, Bosnia and Herzegovina, and Kosovo have made efforts to align with the GDPR by amending their personal data protection laws. In the framework of harmonisation, the legislation with the EU's Acquis Communautaire,[28] Albania has adopted a new law in 2024, no. 124 "On personal data protection",[29] aiming to be fully aligned with the GDPR, but with some shortcomings in practical implementation, which are addressed below.

This law aimed to be fully aligned with the acquis of the European Union and specifically the transposition of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data". The Personal Data Protection Authority in Albania, the Commissioner for Personal Data Protection, has been granted additional powers, but not on a level with EU authorities. Albanian law provides a greater scope for data processing without consent when carried out by state authorities, unlike the GDPR's narrow approach. On the other hand, there are no legal measures for data protection in the context of automatic profiling and artificial intelligence, which are important pillars of the GDPR and the subject of this paper's analysis. Comparing the provisions on international data transfer, it is found that the GDPR imposes very strict criteria for data transfers outside the EU, while Law 124/2024 treats them more generally and, in some cases, even allows data transfers if the data subject has given consent.

Serbia[30] and North Macedonia[31] have incorporated many elements of the GDPR into their laws, but the supervisory authorities do not have the full capacity of the EU to monitor and provide citizens with the guarantees they need to protect their personal data. Kosovo[32] has an improved law that attempts to align with the GDPR (2019), but implementation remains difficult due to the same problems in the supervisory mechanisms of the responsible authorities.

27 ibid, para 26.

28 See, European Commission, 'Chapters of the acquis' (*Enlargement and Eastern Neighbourhood*, 2012) <https://enlargement.ec.europa.eu/enlargement-policy/conditions-membership/chapters-acquis_en> accessed 25 January 2026.

29 Law of the Republic of Albania No 124/2024 (n 11).

30 Law of the Republic of Serbia 'On Personal Data Protection' [2018] Official Gazette 87.

31 Law of the Republic of North Macedonia 'On Personal Data Protection' [2019] Official Gazette 42/20 and 294/21.

32 Law of the Republic of Kosovo No 06/L-082 'On Protection of Personal Data' [2019] Official Gazette 6.

The Albanian Law 124/2024 on personal data protection is in line with and guarantees the implementation of the obligations in relation to public security and the provisions of Directive 2016/680 regarding the processing of data for the purposes of prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties. In Chapter IV, this law contains provisions on the international transfer of data. The conditions for the legality of international transfer remain almost the same, however, an innovation brought by the law is the inclusion of cases for allowing the transfer of personal data without the authorization of the Commissioner, to countries with an insufficient level of data protection, also introducing, in this context, new instruments, aimed at guaranteeing appropriate safeguards for the rights and freedoms of data subjects, such as: "Standard data protection clauses" and "Binding rules of the group of commercial companies".

However, practice has demonstrated that the use of Standard Contractual Clauses alone does not provide sufficient safeguards to ensure the adequate protection of data subjects. The case of Ireland[33] and the issue of data transfers under standard contractual clauses (SCCs) by Meta (Facebook, Instagram) show that this is a sensitive issue for EU countries as well. Meanwhile, for other countries outside the EU, this situation appears even more uncertain, despite the fact that the law may be complete, most companies that process data, such as Meta, etc., do not yet have a designated representative to comply with and provide the guarantees that the legislation in the field of data protection requires. The transfer of data in the absence of an adequacy decision constitutes an object of analysis of this paper, because it is directly related to the possibility of obtaining personal data from applications that use AI.

Albanian Law no. 124/2024 provides, among other things, in its Article 41, point 3, the possibility of transferring data, when there is no adequacy decision or appropriate safeguards. In such a case, the transfer of personal data to a third country or an international organisation will only take place if one of the following conditions applies:

- the data subject has given his or her informed and explicit consent to the proposed international data transfer, having been clearly informed of the risks of the transfer.
- the transfer is necessary for the performance of a contract between the data subject and the data controller, for the implementation of pre-contractual measures taken at the request of the data subject or the transfer is necessary for the conclusion, or performance, of a contract between the data controller and a third party in the interests of the data subject.

33 See, '1.2 billion Euro fine for Facebook as a Result of EDPB Binding Decision' (*European Data Protection Board*, 22 May 2023) <https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en> accessed 25 January 2026. This fine, which is the largest GDPR fine ever, was imposed for Meta's transfers of personal data to the U.S. on the basis of standard contractual clauses (SCCs) since 16 July 2020. Furthermore, Meta has been ordered to bring its data transfers into compliance with the GDPR.

- the processing is necessary to protect the vital interests of the data subject or of another
- natural person where the data subject is physically unable to give consent, or where the right to act has been withdrawn or restricted.
- the transfer is necessary for reasons of important public interest.
- processing is necessary for the establishment, exercise or defence of a right, obligation, or legitimate interest before a court or public authority.
- the transfer is made from a register which by law is open to consultation and provides
- information to the public, provided that the transfer only includes certain information
- and not entire sections of the register.

Albanian Law no. 124/2024 is almost fully aligned with the GDPR. Whereas Article 41 of this law, unlike the provisions of the GDPR, does not provide the same guarantees and conditions in the case of data transfers in the absence of an adequacy decision. Article 41, point 3 letter a) provides that "In the absence of an adequacy decision or of appropriate safeguards in accordance with point 1 of this article, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall only take place if one of the following conditions applies:

> *a) the data subject has given informed and explicit consent to the proposed international data transfer, having been clearly informed of the risks of the transfer.*

The key issue concerns the adequacy of citizen protection when using online platforms and social media networks. The permission that this provision has given to the transfer of data in the absence of an adequacy decision, in the case of point a), i.e. when the data subject himself has given informed and explicit consent to the proposed international transfer of data, does not comply with the protection offered by the GDPR (see Article 46 of the GDPR). The information is clearly presumed to have been provided after being notified of the risks of the transfer, in this case, by the recipient or processor of the data. In online applications, this information is included in the terms of reference, which generally no one reads.[34]

34 A 2017 study by Jonathan Obar and Anne Oeldorf-Hirsch found that only 1% of users read the terms of service in detail. See: See, David Berreby, 'Click to Agree with What? No One Reads Terms of Service, Studies Confirm' *The Guardian* (London, 3 March 2017) <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print?utm_source=chatgpt.com> accessed 25 January 2026.

Unlike this approach in Albanian legislation, the GDPR provides stronger criteria for data transfers in the absence of an adequacy decision. The problem becomes even more evident when, today, this clause, which leaves it to the subject to give consent, may increase the risk and reduce the protection of the personal data of Albanian citizens, given that users of social media networks do not read the terms of service. Users routinely provide consent without informed evaluation or assessment of the level of data that will be used, because they are in a hurry to use the requested application. A significant number of users are unaware of their rights regarding personal data, and some do not know that there is legislation for this purpose.

Similar dynamics are observed in other Western Balkan countries. Kosovo's 2019 legislation[35] on data protection reflects GDPR principles but lacks clear mechanisms for cross-border enforcement. North Macedonia's Data Protection Law[36] introduced GDPR-style rights, yet implementation has been hampered by low public awareness and insufficient technical capacity among data controllers. Serbia's Law on Personal Data Protection,[37] also modelled on the GDPR, has achieved high formal alignment but remains constrained by the limited resources of the Commissioner for Information of the public importance and personal data protection.[38] These patterns confirm that while legal texts in the region mirror EU instruments, functional equivalence in enforcement and citizen protection is still missing.

6 AUTOMATED PROFILING UNDER AI SYSTEMS: LEGAL RISKS AND INDIVIDUAL PROTECTION

The GDPR provides protection even when users knowingly disclose personal data on social media networks (e.g., photos, locations, private events). The companies that manage these networks (such as Meta/Facebook, TikTok, X/Twitter, Instagram, etc.) are not exempt from their legal obligations for data protection. When a user voluntarily publishes personal information, it remains personal data under the GDPR. The right to privacy and control over data is not lost, except in very limited cases. Even on a social media platform, data processing must be limited to what is necessary for the expressed purpose.[39]

The conscious publication of user data on social media networks does not relieve platforms of their obligation to protect it. Companies that manage social media networks

35 Law of the Republic of Kosovo No 06/L-082 (n 32).

36 Law of the Republic of North Macedonia 'On Personal Data Protection' (n 31).

37 Law of the Republic of Serbia 'On Personal Data Protection' (n 30).

38 SIGMA and OECD, *Public Administration in the Western Balkans 2024: Regional Overview of Assessments against the Principles of Public Administration* (OECD Publishing 2022) doi:10.1787/9c2f22f8-en.

39 See, Regulation (EU) 2016/679 (n 3) art 5.

have a full legal obligation to respect the rights of individuals, process data carefully, provide transparency, and guarantee the security of information, even when this information is "self-posted" by users.

How protected are the personal data of social media network users, and how vulnerable are they to phenomena such as profiling in the future?

If we refer to the definition given in Albanian Law on Data Protection, "Profiling"[40] is any form of automated processing of personal data, which consists of using data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning his or her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The risk that profiling poses in the daily use of computer systems is directly related to the violation of fundamental rights of citizens, such as equality, non-discrimination on grounds of gender, ethnicity, religion, education, economic status, social status, etc. Albanian law offers reasonable protection against profiling and the protection of sensitive personal data. Article 53 of Law no. 124/2024 provides for an absolute prohibition on profiling through automated decision-making when it results in discrimination against citizens based on sensitive data. However, despite the legal provisions adopted in accordance with the GDPR, the mechanisms, control instruments and capacities of the supervisory authority towards entities that use AI in their applications are limited in practice.[41]

Law no.124/2024 applies to the processing of personal data and to the data controller[42] which is not located in the Republic of Albania, but the processing is related to:

i. The provision of goods or services, irrespective of whether compensation of the data subject is required, to such data subjects in the Republic of Albania.

ii. The monitoring of the data subjects 'behaviour as far as it takes place within the Republic of Albania.

The legal changes, approved by Albanian Law no. 124/2024, have brought greater guarantees for the protection of personal data; however, in practice, concrete steps and mechanisms to implement them are lacking. The law came into force in February 2025, and Albania and other Western Balkan countries still do not have Meta (Facebook/Instagram, etc.) representatives appointed. In the absence of effective international cooperation mechanisms or binding agreements, the enforcement of data protection law against foreign companies remains structurally limited. Although data

40 See, Law of the Republic of Albania No 124/2024 (n 11) art 5, para 19.

41 See for more information: Information and Data Protection Commissioner, *Annual Report 2022* (IDPC 2023) <https://idp.al/en/annual-reports/> accessed 25 January 2026; Information and Data Protection Commissioner, *Annual Report 2023* (IDPC 2024) <https://idp.al/en/annual-reports/> accessed 25 January 2026; Information and Data Protection Commissioner, *Annual Report 2024* (n 24).

42 Law of the Republic of Albania No 124/2024 (n 11) art 4, para 1, b).

protection regimes such as the GDPR claim extraterritorial applicability, there is a persistent gap between legal norms and their practical enforcement, particularly where foreign entities do not recognise the authority of national supervisory bodies. In such cases, the supervisory role risks remain more formal rather than effective.[43]

7 THE EU ARTIFICIAL INTELLIGENCE ACT AND ITS INTERACTION WITH DATA PROTECTION STANDARDS

In the era of digitalisation and the development of artificial intelligence, protecting personal data and the right to privacy will be the greatest challenge for individuals and states. The increasing use of AI across sectors such as social, cultural, and economic life, with effects and consequences for the protection of fundamental human rights, has highlighted the need for a regulatory framework. This framework should first prioritise human well-being. For this reason, the EU has approved Regulation (EU) 2024/1689 of the European Parliament and of the Council, adopted on June 13, 2024, the Artificial Intelligence Act, which entered into force in August 2025.[44]

As a prerequisite, this act emphasises that AI should be a human-centric technology. It should serve as a tool for people, with the aim of increasing human well-being.[45] The focus of the regulation is to balance the development of AI with the protection of people from potential risks, ensuring the free cross-border movement of AI-enabled goods and services while preventing Member States from imposing unnecessary restrictions. The European Union has made regulations on artificial intelligence systems using a risk-based approach that establishes different obligations for providers and users of artificial intelligence systems depending on the level of risk.[46]

The term "risk" is defined in Article 3 of the EU AI Act as: "the combination of the probability of an occurrence of harm and the severity of that harm." If an AI system presents an "unacceptable" risk level, such as those used for social scoring or cognitive manipulation of vulnerable individuals, it will be prohibited. For example, real-time biometric identification systems, such as facial recognition, are prohibited. AI systems that pose a "high-risk", for instance, to health, education, law enforcement, security, or fundamental

43 Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235, doi:10.1093/idpl/ipv019; Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017); Michal Czerniawski and Dan Svantesson, 'Challenges to the Extraterritorial Enforcement of Data Privacy Law – EU Case Study' in *Dataskyddet 50 år – historia, aktuella problem och framtid* (Stiftelsen Juridisk Fakultetslitteratur 2024) 127, doi:10.53292/bd1fa11c.f5b3afbe.

44 Regulation (EU) 2024/1689 (n 4).

45 ibid, para (6).

46 Jeroen van der Heijden, 'Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda' (2021) 11(3) SAGE Open 21582440211, doi:10.1177/21582440211032202.

rights will require evaluation before being made available on the market and, afterwards, through post-market monitoring. For these cases, there will be stricter safety, traceability, and transparency obligations during their lifespan, as is the case for low-risk AI systems, *i.e.* those that interact with natural people (*e.g.*, chatbots), and that create or manipulate sounds, images, and videos (*e.g.*, deepfakes). Low-risk AI systems, on the other hand, place responsibility for personal risk assessment on the user, who can choose to use the tool at their own discretion. In this case, the user must have enough information about the risk and possibilities when using the tool.[47]

The EU AI Act explicitly prohibits real-time biometric identification systems, such as facial recognition (Article 5(h). Biometrics and AI potentially allow for the broad surveillance of individuals, the potential impact of which is not limited to one or more specific fundamental rights, but can affect democracy itself.[48] AI algorithms can be influenced by biased or poor-quality training data, leading to discriminatory or unfair outcomes.[49] This is because existing categories of EU anti-discrimination law are not easily applicable to algorithmic decision-making.[50]

A study requested by the JURI and PETI committees of the European Parliament Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces,[51] as an important document before the adoption of the EU AI Act, where among other things, it was suggested to add total surveillance as an additional prohibited AI practice. The EU AI Act prohibits the use of biometric identification systems in publicly accessible spaces even for law enforcement, unless and insofar as such use is strictly necessary for one of the following objectives:[52]

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing people.

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack.

47 See, Regulation (EU) 2024/1689 (n 4) art 3.

48 Fuster and Peeters (n 19) 33.

49 The use of facial and voice recognition systems has raised concerns about gender and race biases. Google, for example, was found to display job advertisements with high salaries predominantly to male users, while female users were shown fewer ads for high-paying jobs. This highlights the gender-biased discrimination in these systems.

50 Hacker (n 15).

51 Christiane Wendehorst and Yannic Duller, *Biometric Recognition and Behavioral Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioral Detection Techniques with a Focus on Their Current and Future Use in Public Spaces* (European Union 2021).

52 See, Regulation (EU) 2024/1689 (n 4) art 5 (h).

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

In line with the presumption of innocence, natural persons in the Union should always be judged on their actual behaviour. Natural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of debt or type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof.[53]

On the other hand, the EU AI Act foresaw that, the placing on the market, the putting into service for that specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage, should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy[54]. Some chat message apps, like WhatsApp, etc., use a "high level of security" for their communications, including facial recognition.

Users grant permission for the use of facial recognition technologies through the privacy and security settings of digital devices and applications in exchange for enhanced security.

What about tomorrow? The question that arises here is how protected is the personal data that individuals share on social media networks today with their consent, for higher "security" in communications? For example, special initiatives like that of Denmark, which aims to legalise the individual's right to patent their image and voice, essentially show concern and measures to prevent high-risk situations for the individual, such as identity theft and personal data misuse of technology and artificial intelligence.[55] The Danish government is to clamp down on the creation and dissemination of AI-generated deepfakes by changing copyright law to ensure that everybody has the right to their own body, facial features and voice. The Danish government said it would strengthen protection against digital imitations of people's identities with what it believes to be the first law of its kind in Europe.[56]

53 ibid, para 42.

54 ibid, para 43.

55 See for more information, Miranda Bryant, 'Denmark to tackle deepfakes by giving people copyright to their own features' *The Guardian* (London, 27 June 2025) <https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence> accessed 25 January 2026.

56 ibid

There is a fear that AI could become a technology capable of "enslaving" human beings.[57] Open-AI CEO Sam Altman, who was among the signatories of the statement *"Mitigating the risk of extinction by AI should be a global priority along with other risks on a societal scale such as pandemics and nuclear wars,"*[58] expressed his concerns about the impact of AI applications on areas related to rights and social inequality assumptions.[59] In response to a question about the legal framework for AI, Altman says a legal or policy framework for AI is needed. He compares ChatGPT conversations with those made with doctors, lawyers, and therapists and opines that AI chatbots should be granted the same legal privileges.[60] Although Altman had pointed out that many people tell AI very personal details about their lives, which could have serious consequences in legal cases.

Individuals, day after day, are sharing personal data, due to the short time available, in return for a modest payment (today) for the performance of daily tasks by an intelligent computer, which in most cases is used as a ubiquitous personal agenda, and in many others as a place where they can search and find answers to questions for any possible interest, creating dependence on its use in everyday life and giving up without realizing it from the development of critical thinking and reason before making a decision. The latter is most worrying for today's society. This concern has been recently raised by the CEO of OPEN IA, one of the artificial intelligence platforms. People rely on ChatGPT too much. There are young people who say, *"I can't make any decision in my life without telling ChatGPT everything that's going on. It knows me, it knows my friends. "I'm going to do whatever it says"*[61] Altman expressed concern about over-reliance on ChatGPT for personal decision-making. It is worrying that young people consider AI to be the "final voice" on every issue in life. He expressed serious concern that many younger users are placing too much emotional trust in ChatGPT, treating it not just as a tool, but as a kind of life coach or operating system. Such trust may lead to passive decision-making and diminished personal judgment. Emphasising the benefits of artificial intelligence (AI) tools like ChatGPT, Altman said

57 'Statement on AI Risk Press Coverage' (*Center for AI Safety*, 2025) <https://aistatement.com/> accessed 25 January 2026.

58 'Statement on AI Risk: AI Experts and Public Figures Express their Concern about AI Risk' (*Center for AI Safety*, 29 July 2025) <https://aistatement.com/> accessed 25 January 2026.

59 ibid. The statement "Mitigating the risk of extinction by AI should be a global priority along with other societal-scale risks such as pandemics and nuclear war".

60 Jibin Joseph, 'Altman Warns that your ChatGPT Conversations Can (and Will) Be Used Against You in Court' (*PC Mag*, 4 August 2025) <https://www.pcmag.com/news/altman-anything-you-say-to-chatgpt-can-and-will-be-used-against-you-in> accessed 25 January 2026.

61 During a speech at a Federal Reserve banking conference in late July 2025, he expressed serious concern that many younger users are placing too much emotional trust in ChatGPT—treating it not just as a tool, but as a kind of life coach or operating system. See, Henry Chandonnet, 'Sam Altman is Worried Some Young People Have an Emotional Over Reliance on ChatGPT when Making Decisions' (*Business Insider*, 23 July 2025) <https://www.aol.com/sam-altman-worried-young-people-181115911.html> accessed 25 January 2026.

society needs new guardrails to address these risks.[62] The CEO of OPENAI, asked these questions: are we not late with the generation of young people who are living and being formed in this technological development that is progressing at a galloping pace? Should we see the consequences and damage before taking measures?

Every state must intervene by first undertaking awareness campaigns for young people and citizens, and secondly by reviewing domestic legislation on the protection of individual rights, as well as continuously monitoring the processing of citizens' data.

Also, given the risks[63] that accompany uncontrolled use of AI, especially in malicious use, such as bioterrorism, unleashing AI agents, persuasive AIs,[64] concentration of power, etc. It is more than urgent to have regulatory and controlling legislation for all countries. The EU AI Act, adopted by the European Parliament, constitutes an important step in protecting the personal data of EU citizens by defining areas of risk and imposing restrictions on the activities of various entities using AI systems. Today, the problem remains evident for the Western Balkan countries, which are not subject to the EU AI Act. These countries must take concrete measures, including amendments or improvements to domestic legislation, to provide the necessary protection for citizens and public safety against the misuse of AI. The Western Balkan countries and Albania already have an important roadmap, the EU AI Act, which is a good start on the path to the controlled use of AI. As emphasised in the preamble of this EU document, *"AI should be a human-centric technology"*, to serve the individual and be used for the benefit of public safety. The EU AI Act's risk-based approach introduces an important regulatory model that candidate countries could adopt. The distinction between unacceptable, high, and low-risk AI systems provides a structured method for balancing innovation with rights protection. However, without corresponding national instruments, such as risk assessment procedures or AI supervisory boards, Western Balkan states will continue to depend on EU-level norms without possessing equivalent internal mechanisms.

62 'Sam Altman Concerned by Young People's Over-Reliance on ChatGPT' *The Economic Times* (Mumbai, 26 July 2025) <https://economictimes.indiatimes.com/tech/technology/sam-altman-concerned-by-young-peoples-over-reliance-on-chatgpt/articleshow/122920673.cms?from=mdr> accessed 25 January 2026.

63 See for more information, 'An Overview of Catastrophic AI Risks' (*Center for AI Safety*, 2025) <https://safe.ai/ai-risk> accessed 25 January 2026.

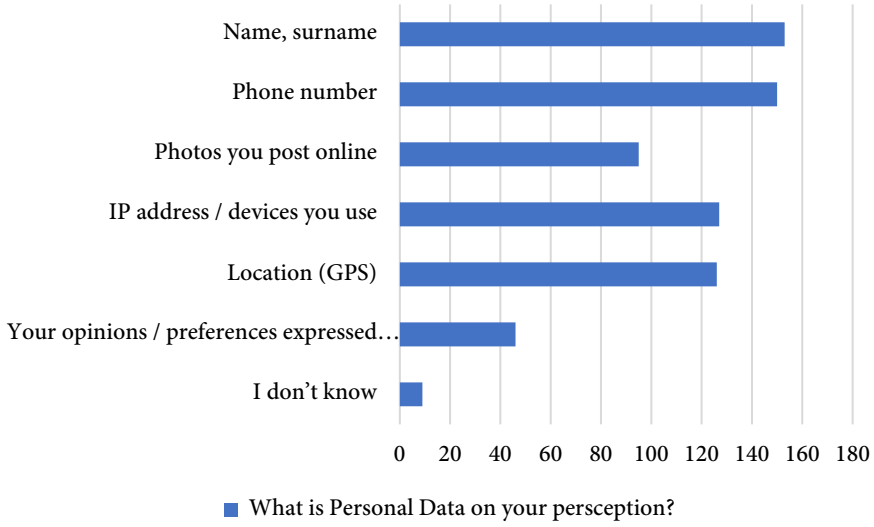
64 The concept of "Persuasive Ais" - AI could facilitate large-scale disinformation campaigns by tailoring arguments to individual users, potentially shaping public beliefs and destabilizing society. As people are already forming relationships with chatbots, powerful actors could leverage these AIs considered as "friends" for influence" -explained in the 'An Overview of Catastrophic AI Risks' (n 63).

8 EMPIRICAL INSIGHTS FROM THE SURVEY

The empirical findings[65] reveal a significant gap between the formal legal framework on personal data protection and the level of public awareness and practical enforcement in Albania. Although most respondents indicated some level of awareness of the existence of Law No. 124/2024, only a limited proportion demonstrated substantive knowledge of its content, while a considerable percentage reported no awareness at all. From the answers given, most respondents (52.8%) were aware that the new Albania law on the protection of personal data is in force, but they do not know its content well. 25.8% were unaware of the content of this law, and 21.3% were aware of it.

Half of the respondents reported no cases of unauthorised data use, while 20.8% confirmed such cases and 29.2% were unsure. Concerning complaints, 75.3% had never considered filing one, 12.4% had, and 12.4% were unaware of the competent authority.

Respondents were also asked about their opinion of what personal data is, allowing them to choose several options. Below are the results of their perception of what personal data is in their opinion.[66]

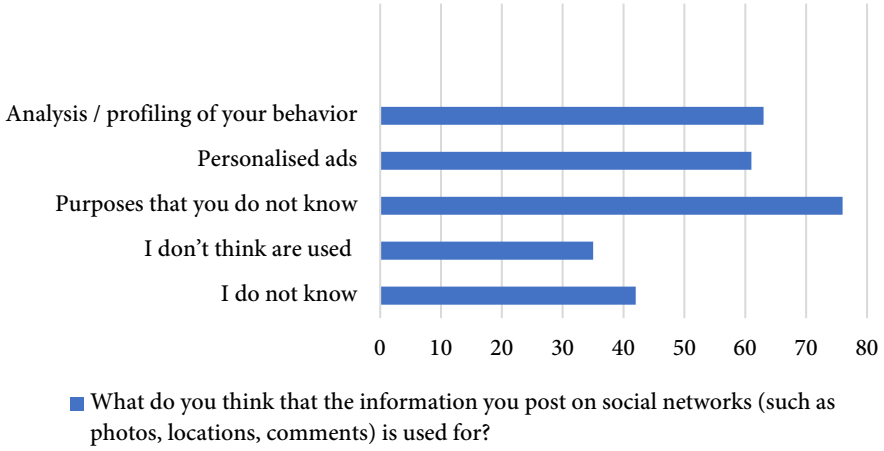


Graph 1. Perception of personal data categories

65 Ballauri (n 9).

66 The graphs were created by the author.

Meanwhile, regarding whether they had ever considered filing a complaint with the authorities for personal data breaches, 75.3% responded negatively, 12.4% responded positively, and 12.4% did not know that such an authority existed. When analysing the data from the next question, regarding the use of information they publish on social media networks, the results are presented in Graph 2. Most of the respondents (42.7 %) said that they didn't know the purpose of the processing of their data; 34.3 % believed they were used for personalised ads, and 35.4 % for analysis or profiling of their behaviour. Only 19.7% believed their data was not used, and 23.6% answered that they didn't know.



Graph 2. Acknowledgement about data processing

Regarding the data used by social media networks, 42.7% of respondents said they did not know the purpose, 34.3% believed data were used for targeted ads, 35.4% for profiling, and 19.7% thought their data were not used. When asked whether online behaviour could be analysed for digital profiling, 63.5% agreed, 12.4% disagreed, and 24.2% acknowledged hearing about it but did not fully understand.

The results indicate that Meta Platforms-owned platforms, particularly Instagram (78.1%) and Facebook (52.2%), are among the most frequently used social media networks among respondents. This widespread use highlights the central role of these platforms in users' daily digital activities in Albania. The findings provide empirical justification for selecting Meta Platforms as the focus of the case study, as these platforms represent the primary environment in which personal data are generated, processed, and potentially subject to AI-driven profiling. Consequently, any limitations in the enforcement of data protection rights on these platforms may significantly affect a large proportion of users.

Perceived protection of personal data in Albania is very low, with only 2% feeling protected. Nevertheless, 92.7% emphasized the need for more awareness campaigns on data protection and digital security.

The survey results underline a clear implementation gap between legal transposition and citizens' practical experience. Citizens' awareness of their rights remains limited, and most users do not know how their personal data is processed or how to file a complaint. This low level of awareness further weakens the practical enforceability of the law, since data protection regimes rely on active participation by informed data subjects. While Albania has aligned its legislation with EU standards, awareness and enforcement remain limited. This gap sets the stage for the following discussion, which examines the structural and institutional factors that explain why formal compliance has not yet translated into effective protection.

The questionnaire results provide a detailed picture of how personal data protection is perceived and experienced in practice. Although 52.8% of respondents stated they are aware of the new law, only 21.3% reported familiarity with its content, while 25.8% acknowledged only limited knowledge, indicating that awareness remains largely superficial. Regarding understanding personal data, most participants correctly identified basic elements such as names (86%) and phone numbers (84.3%), yet fewer recognised more complex categories, such as online preferences (25.8%), revealing gaps in conceptual understanding. Awareness of data protection rights also appears limited, with only 28.1% confirming knowledge of correction or deletion, while 54.5% remained uncertain.

A significant proportion of respondents reported exposure to potential data misuse: 20.8% indicated that their personal data had been used without consent, and an additional 50% were unsure, suggesting widespread uncertainty about data practices. However, despite these experiences, only 12.4% had considered filing a complaint, while 75.3% had not, often due to a lack of awareness of competent authorities. At the same time, perceptions of digital tracking are widespread: 63.5% reported frequently seeing advertisements linked to their searches or conversations, and an equal 63.5% acknowledged that online behaviour can be used to build digital profiles, even if understanding remains partial. Finally, perceptions of protection remain low, with 42.7% feeling only slightly protected and 35.4% sufficiently protected, while very few (14%) feel strongly protected.

Overall, these findings suggest that while individuals are increasingly aware of data-driven practices and their potential risks, there remains a substantial gap between legal protections and effective public understanding, trust, and engagement with available enforcement mechanisms.

The empirical findings reinforce the conclusions drawn from the legal analysis. The Albanian legal framework demonstrates a high level of formal alignment with EU standards, but the questionnaire results reveal limited public awareness and low

engagement with enforcement mechanisms. This disconnect suggests that legal harmonisation alone is insufficient to ensure effective protection of personal data. From a theoretical perspective, the findings support existing scholarship emphasising the importance of enforcement capacity and institutional effectiveness in data protection regimes. In practice, they highlight the need for stronger supervisory mechanisms, increased public awareness, and improved cross-border cooperation to ensure that legal rights are not merely formal but effectively exercisable.

9 CONCLUSIONS

The development of technology is progressing rapidly, and the use of IA in online applications could pose severe risks to users, especially when they are unaware of how their personal data is processed. The protection of personal data and privacy rights is an obligation that every state must undertake in light of developments in the field of artificial intelligence.

GDPR provides legal protection even when users knowingly disclose personal data on social media networks. The companies that manage these networks (such as Meta/Facebook, TikTok, X/Twitter, Instagram, etc.) are not exempt from their legal obligations for data protection. Even when a user voluntarily publishes personal information, it remains personal data under the GDPR.

The risk that profiling poses in the daily use of computer systems is directly related to the violation of fundamental rights of citizens, such as equality, non-discrimination on grounds of gender, ethnicity, religion, education, economic status, social status, etc. The new Albanian law on the protection of personal data offers reasonable protection from profiling and the protection of sensitive data. This law provides, among other things, the possibility of transferring data when there is no adequacy decision and when the data subject has given informed and explicit consent to the proposed international data transfer, having been clearly informed of the risks of the transfer. This legal permission to transfer data in the absence of an adequacy decision does not comply with the protection offered by Article 46 of the GDPR. This provision could create a practical gap and a serious risk for Albanian citizens' personal data when using social media networks and online applications.

The European Union has recently taken concrete measures to regulate the use of artificial intelligence in various applications, bringing guarantees for the fundamental rights of EU citizens. The AI Act, adopted recently by the European Parliament, is an important regulatory framework for artificial intelligence across various applications, providing guarantees for the fundamental rights of EU citizens. Uncontrolled use of AI carries serious risks, especially in malicious applications such as bioterrorism, the unleashing of AI agents, and the concentration of power.

The study concludes that Western Balkan countries, despite formal alignment with the GDPR, face structural challenges in implementing AI-related data protection safeguards. Albania's new Law No. 124/2024 still permits data transfers based solely on consent, a provision inconsistent with Article 46 of the GDPR. To ensure equivalence with EU protection standards, candidate states should strengthen their supervisory authorities and ensure their independence. Also, it is needed to establish binding adequacy mechanisms and adopt national strategies for AI risk management. The AI Act should serve as a guiding instrument for these reforms.

REFERENCES

1. Ballauri F, 'The Questionnaire on the Awareness and Experience of Albanian Citizens Regarding the Protection of Personal Data and Privacy in the Digital Age' (*Google Forms*, 2025) <https://docs.google.com/forms/d/1rXEv9an-fZNGD79VSr5K52HUu2KDDLX0AF05DLFwVOQ/edit#responses> accessed 25 January 2026
2. Berreby D, 'Click to Agree with What? No One Reads Terms of Service, Studies Confirm' *The Guardian* (London, 3 March 2017) <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print?utm_source=chatgpt.com> accessed 25 January 2026
3. Bryant M, 'Denmark to tackle deepfakes by giving people copyright to their own features' *The Guardian* (London, 27 June 2025) <https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence> accessed 25 January 2026.
4. Bryman A, *Social Research Methods* (5th edn, OUP 2016)
5. Cane P and Kritzer HM (eds), *The Oxford Handbook of Empirical Legal Research* (OUP 2010)
6. Chandonnet H, 'Sam Altman is Worried Some Young People Have an Emotional Over Reliance on ChatGPT when Making Decisions' (*Business Insider*, 23 July 2025) <https://www.aol.com/sam-altman-worried-young-people-181115911.html> accessed 25 January 2026
7. Creswell JW and Creswell JD, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th edn, SAGE 2018)
8. Czerniawski M and Svantesson D, 'Challenges to the Extraterritorial Enforcement of Data Privacy Law – EU Case Study' in *Dataskyddet 50 år – historia, aktuella problem och framtid* (Stiftelsen Juridisk Fakultetslitteratur 2024) 127, doi:10.53292/bd1fa11c.f5b3afbe
9. Dillman DA, Smyth JD and Christian LM, *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method* (4th edn, Wiley 2014)

10. González Fuster G and Nadolna Peeters M, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (European Parliament EPRS 2021) doi:10.2861/384495

11. Gstrein OJ and Zwitter A, 'Extraterritorial Application of the GDPR: Promoting European Values or Power?' (2021) 10(3) Internet Policy Review, doi:10.14763/2021.3.1576

12. Hacker P, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55(4) Common Market Law Review 1143, doi:10.54648/cola2018095

13. Heijden J, 'Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda' (2021) 11(3) SAGE Open 21582440211, doi:10.1177/21582440211032202

14. Joseph J, 'Altman Warns that your ChatGPT Conversations Can (and Will) Be Used Against You in Court' (*PC Mag*, 4 August 2025) <https://www.pcmag.com/news/altman-anything-you-say-to-chatgpt-can-and-will-be-used-against-you-in> accessed 25 January 2026.

15. Jovanoviq N, 'Meta trajnon pa paralajmërim inteligjencën artificiale mbi të dhënat e qytetarëve të Ballkanit' (*Radio Evropa e Lirë,* 5 August 2024) <https://www.evropaelire.org/a/meta-trajnon-paparalajmerim-inteligjencen-artificiale-mbi-te-dhenat-e-qytetareve-ballkanit-/33066127.html> accessed 25 January 2026

16. Kuner C, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5(4) International Data Privacy Law 235, doi:10.1093/idpl/ipv019

17. Svantesson DJB, *Solving the Internet Jurisdiction Puzzle* (OUP 2017)

18. Veale M and Zuiderveen Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law & Security Review 97, doi:10.9785/cri-2021-220402

19. Wendehorst C and Duller Y, *Biometric Recognition and Behavioral Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioral Detection Techniques with a Focus on Their Current and Future Use in Public Spaces* (European Union 2021)

20. Yin RK, *Case Study Research and Applications: Design and Methods* (6th edn, SAGE 2018)

21. Zuiderveen Borgesius F, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24(10) The International Journal of Human Rights 1572, doi:10.1080/13642987.2020.1743976

Appendix A:
Questionnaire on Data Protection Awareness in Albania

A.1 Structure of the Questionnaire

The questionnaire was designed to assess citizens' awareness, perceptions, and practical experience regarding personal data protection in the digital environment, with particular attention to artificial intelligence-related risks. It was administered online via Google Forms and structured into four main sections:

1. **Demographic Data**

   Collection of basic respondent characteristics (age, gender).

2. **Awareness of Legal Framework**

   Evaluation of knowledge regarding Law No. 124/2024 on personal data protection.

3. **Understanding of Personal Data and Rights**

   Assessment of respondents' conceptual understanding of personal data and related rights.

4. **Experience and Perceptions of Data Use**

   Examination of real-life experiences, perceptions of data processing practices, and awareness of profiling and digital risks.

A.2 Questionnaire Items (Reconstructed from Survey Instrument)

Section 1: Demographic Data

1. What is your age group?
   - Under 18
   - 18–25
   - 26–40
   - 41–60
   - Over 60
2. What is your gender?
   - Female
   - Male
   - Prefer not to say

Section 2: Awareness of Legal Framework

3. Are you aware that Law No. 124/2024 on personal data protection of has entered into force in Albania?
    - o Yes, and I am familiar with its content
    - o Yes, but I do not know its content well
    - o No

Section 3: Understanding of Personal Data

4. In your opinion, which of the following constitute personal data? *(multiple answers possible)*
    - o Name and surname
    - o Phone number
    - o Photos posted online
    - o IP address / devices used
    - o Location (GPS)
    - o Online opinions / preferences
    - o I do not know

Section 4: Awareness of Rights

5. Are you aware of your rights regarding personal data (e.g., access, correction, deletion)?
    - o Yes
    - o No
    - o Not sure

Section 5: Experience with Data Use

6. Have you ever experienced or suspected that your personal data was used without your consent?
    - o Yes
    - o No
    - o Not sure

7. If yes how did this happen?
8. Have you ever considered filing a complaint with the competent authority for personal data protection?
    - Yes
    - No
    - I did not know such a possibility existed
9. Which social media network do you use the most?
    - Facebook
    - Instagram
    - TikTok
    - YouTube
    - LinkedIn
    - Others

Section 6: Perception of Data Processing

10. Have you ever felt that your privacy has been violated using social media networks
    - Yes
    - No
    - Not sure
11. Do you think that the information you post on social media networks (such as photos, locations, comments) is used for? *(multiple answers possible)*
    - Personalized ads
    - Analysis / profiling of your behaviour
    - Purposes you don't know
    - I don't think they are used
    - I don't know

12. Do you believe that your online behaviour can be analysed to create a digital profile?
    - o Yes
    - o No
    - o I have heard about it but do not fully understand

Section 7: Perceived Level of Protection

13. How protected do you feel regarding your personal data when using online platforms?
    - o Very protected
    - o Moderately protected
    - o Slightly protected
    - o Not protected

Section 8: Need for Awareness

14. Do you believe there is a need for increased public awareness on data protection and digital security?
    - o Yes
    - o No
    - o Maybe

AUTHOR'S INFORMATION

Fjorida Ballauri
PhD, Faculty of Security and Investigation, Security Academy of Albania, Albania
Fjorida.Ballauri@asp.gov.al
fjori.k@gmail.com
https://orcid.org/0009-0002-7121-6266
Corresponding author, solely responsible for preparing the manuscript.

Competing interests: No competing interests were disclosed.

Disclaimer: The author declares that her opinions and views expressed in this manuscript are free from any impact of any organisations.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Ballauri F, 'The EU Artificial Intelligence Act and Data Protection Challenges for Non-EU Citizens: Comparative Insights from the Western Balkans' (2026) 9(3) Access to Justice in Eastern Europe 1-32 <https://doi.org/10.33327/AJEE-18-9.3-a0001992> Published Online 12 June 2026

DOI: https://doi.org/10.33327/AJEE-18-9.3-a0001992

***Keywords*:** *artificial intelligence, EU legislation, data protection rights, risk, privacy.*

DETAILS FOR PUBLICATION

Date of submission: 04 Feb 2026
Date of acceptance: 27 Apr 2026
Online First Publication: 12 June 2026
Publication: Aug 2026
Was the manuscript fast-tracked? - No
Number of reviewer reports submitted in the first round: 2 reports
Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The author confirms that no artificial intelligence tools or services were used at any stage of writing, translating, editing, or analysing content for this manuscript.

FUNDING AND APC STATEMENT

The author received no specific grant or external funding for the research and publication of this article. Consequently, the APC was partially waived (50%) by the publisher under the AIP funding strategy, in accordance with the AJEE Charges Policy for authors from Lower-Middle-Income countries (as per the World Bank classification). The balance was covered by the author.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

АКТ ЄС ПРО ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРОБЛЕМИ ЗАХИСТУ ДАНИХ ДЛЯ ГРОМАДЯН КРАЇН, ЩО НЕ ВХОДЯТЬ ДО ЄС: ПОРІВНЯЛЬНИЙ ДОСВІД ЗАХІДНИХ БАЛКАН

Фйорида Баллаурі

АНОТАЦІЯ

Вступ. *В епоху штучного інтелекту захист даних та права на приватність стали критично важливими компонентами правового порядку Європейського Союзу. Це дослідження розглядає взаємодію між Актом ЄС про штучний інтелект 2024 року та Загальним регламентом про захист даних, зосереджуючись на їхньому впливі на країни, що не входять до ЄС, зокрема Албанію. Ухвалення Акту ЄС про штучний інтелект змінило правову базу, що регулює ШІ та захист персональних даних у Європі. Однак*

практичні наслідки цих інструментів для громадян країн, що не входять до ЄС, особливо країн Західних Балкан як країн-кандидатів на вступ до ЄС, залишаються недостатньо вивченими.

Методи. *У дослідженні використано комбіновану порівняльно-правову та емпіричну методологію. Воно поєднує порівняльно-правовий аналіз для оцінки ступеня узгодженості національного законодавства зі стандартами ЄС, анкетне опитування 178 респондентів для оцінки обізнаності громадськості та сприйняття прав на приватність, а також аналіз ставлення до ризиків, пов'язаних зі штучним інтелектом та обробкою персональних даних. Воно надає кількісні докази, що доповнюють правовий аналіз, ілюструючи, як регуляторні межі сприймаються та використовуються на практиці. На основі даних анкети, які визначають Meta Platforms як найпоширенішу платформу соціальних мереж в Албанії, у статті було проведено тематичне дослідження, розроблене як експериментальний тест на здійснення прав, що містить запит на доступ до даних, поданий компанії, з метою вивчення транскордонної можливості забезпечення виконання прав суб'єктів даних.*

Результати та висновки. *Результати дослідження виявляють значний розрив між формальною гармонізацією законодавства зі стандартами ЄС щодо захисту даних та штучного інтелекту та їх ефективним впровадженням у країнах-кандидатах Західних Балкан. Дані опитування 178 албанських респондентів свідчать про обмежену обізнаність щодо прав на персональні дані, низьку довіру до інституційного захисту та широку невизначеність щодо профілювання та використання даних на основі штучного інтелекту. Тематичне дослідження також демонструє проблеми, що пов'язані з дотриманням прав щодо іноземних організацій. Для забезпечення ефективного захисту персональних даних у країнах-кандидатах рекомендується посилення механізмів нагляду та впровадження ризик-орієнтованого підходу ЄС до регулювання ШІ. Ефективні заходи захисту даних для громадян країн, що не входять до ЄС, вимагають посилення співпраці у сфері нагляду, посилення правоохоронних можливостей та впровадження ризик-орієнтованої моделі управління Акт ЄС про ШІ у внутрішньому законодавстві.*

Ключові слова. *Штучний інтелект, законодавство ЄС, права на захист даних, ризик, конфіденційність.*