



The 17th Year Publication, No.1

June 2025

PROTECTION OF PERSONAL DATA IN A DIGITALIZED JUSTICE SYSTEM

Rialda Xhizdari *, Klevent Xhizdari**, Sibela Ymeraj***

* Albanian University

** Legal Director “Gkam sh.p.k”

*** Law Student, Albanian University

Abstract

The digitalization of the justice system brings significant benefits in efficiency, transparency, and access to legal services. However, it also presents important challenges regarding the protection of citizens' personal data. In Albania, the legal framework for data protection is based on Law No. 9887/2008 “On the Protection of Personal Data.” With the increasing use of electronic systems and artificial intelligence (AI) in the justice sector, the need for additional protective measures arises.

The analysis of key risks is related to the storage, processing, and sharing of personal data within courts, prosecution offices, and automated legal services. Additionally, it examines the impact of the EU's General Data Protection Regulation (GDPR) on Albanian legislation and the need for alignment with European standards.

The focus is on strategies and mechanisms necessary to ensure the security and confidentiality of data in the justice system, while maintaining a balance between technological innovation and the protection of fundamental human rights.

Keywords: *Data protection, justice system digitalization, privacy, GDPR, Albanian legislation.*

1. Introduction

The digital revolution has encompassed every area of public administration, particularly the justice sector, bringing considerable benefits in transparency and efficiency [1]. The digitalization of court procedures, the use of electronic platforms for document submission, the integration of case management systems, as well as the use of artificial intelligence, has reduced bureaucracy and increased access to justice [2].

The advantages of justice system digitalization include:

- Greater transparency in legal processes
- Increased efficiency in judicial procedures
- Improved access to legal services for citizens
- Enhanced monitoring and judicial statistics
- Reduction of administrative costs

- Increased accountability of justice personnel
- Safer data storage
- Facilitation of inter-institutional cooperation

However, these developments have significantly increased the processing of personal data and created the need for strict protective measures, given that the justice system handles sensitive data, including health information, private life, criminal convictions, or individuals' economic status [3].

2. National Legal Framework and the Role of the EU GDPR

2.1. Albanian Legislation

Law No. 9887/2008 “On the Protection of Personal Data” constitutes the legal basis in Albania. It defines the principles of data processing, the rights of individuals, and the obligations of the controller and processor [4]. This law refers to the EU Directive 95/46/EC but does not include all the elements of the GDPR, which came into force in 2018 [5].

2.2. General Data Protection Regulation (GDPR)

The GDPR (Regulation (EU) 2016/679) was adopted by the European Union in 2016 and entered into force on 25 May, 2018. It is the most comprehensive regulation in the world for the protection of personal data and aims to ensure data protection throughout the EU. It also has an extraterritorial effect for entities processing the data of EU citizens [6].

The GDPR modernizes and harmonizes Albanian legislation with EU regulations. Some of the core principles of the GDPR are:

I. Lawfulness, Fairness, and Transparency

Data processing must be:

- In accordance with the law (based on a valid legal ground);
- Fair to individuals (not deceptive or harmful);
- Transparent (individuals must be informed about what data is collected, why, and how it is processed).

II. Purpose Limitation

Personal data must be collected for specified, clear, and legitimate purposes and not further processed in ways incompatible with those purposes.

III. Data Minimization

Only data that is:

- Necessary
- Relevant
- Limited to the purpose for which it is processed, should be collected.

IV. Accuracy

Personal data must be:

- Accurate

- Updated as necessary, with steps taken to correct or delete inaccurate data.

V. Storage Limitation

Personal data must not be kept longer than necessary for the purpose for which it was collected.

VI. Integrity and Confidentiality

Data must be processed in a way that ensures:

- Security;
- Protection against unauthorized or unlawful processing;
- Protection from loss, destruction, or damage.

VII. Accountability

The data controller is responsible for compliance with these principles and must be able to demonstrate such compliance.

These principles are essential for a justice system that respects fundamental rights [7].

3. Challenges in Data Protection in the Justice System

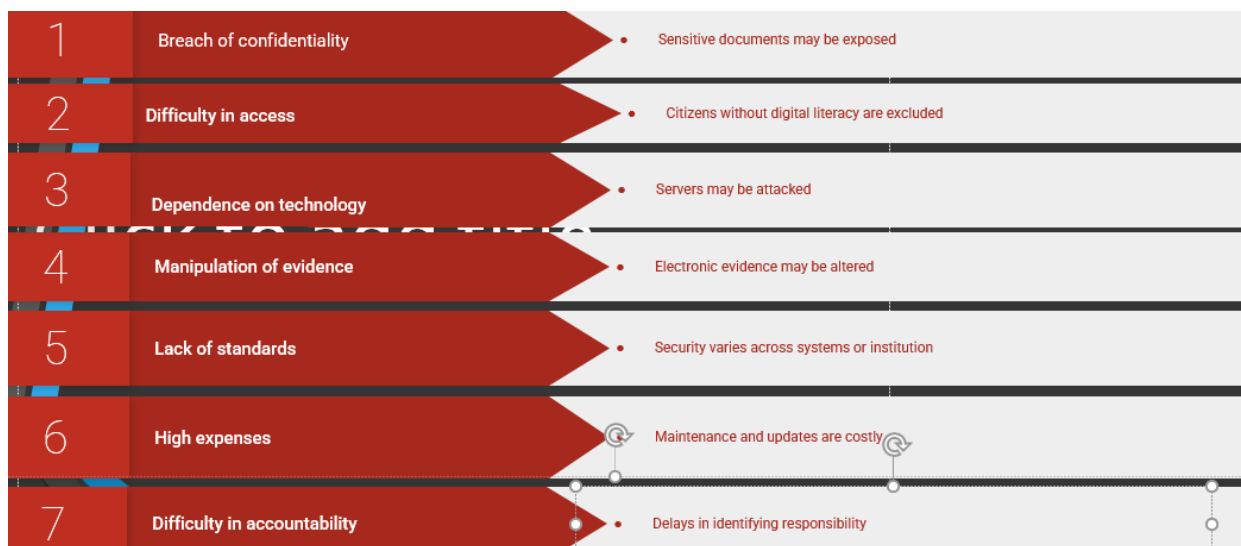
3.1. Processing of Sensitive Data

In the justice system, special categories of data are processed (e.g., criminal records, medical data, minors' personal data), which require special protection. Any leakage or mismanagement of such data poses a serious risk to individuals [8].

3.2. Technological and Institutional Risks

- Cyberattacks: Judicial systems may be targeted by ransomware or malware [9].
- Unauthorized Access: Lack of internal controls creates opportunities for employee-related breaches [10].
- Breach of Confidentiality: Judicial decisions published online often contain identifying data [11].

3.3. Disadvantages of Justice System Digitalization



4. International Cases and Comparative Examples

In France and Germany, the online publication of judicial decisions is subject to strict standards in accordance with existing legislation [12]. In Estonia, judicial systems use artificial intelligence to assist in decision-making for simple administrative cases, always under human oversight [13].

5. Harmonization with GDPR and Recommendations for Albania

5.1. Need for Legal Amendments

Review of Law No. 9887 to incorporate GDPR principles such as Data Protection Impact Assessments (DPIA) and “privacy by design” [14].

- Clear rules for data processing in the justice system and clarification of institutional actors’ roles [15].

5.2. Increased Transparency and Oversight

- Courts and justice institutions should publish their privacy policies.
- Mechanisms for appeals and supervision should be made available to citizens affected by data processing [16].

6. The Role of New Technologies and Additional Risks

6.1. Artificial Intelligence (AI)

The use of AI in justice can improve decision prediction but raises serious concerns about accountability, algorithmic discrimination, and lack of transparency [17].

6.2. Big Data and Surveillance

The processing of large volumes of data for statistical or analytical purposes can threaten privacy if appropriate controls are not enforced [18].

7. Strategies for Data Security in the Justice Sector

7.1. Technical Measures

- Data encryption to protect against unauthorized access
- Multi-factor authentication
- Intrusion detection systems

7.2. Organizational Measures and Training

- Continuous training for judges, prosecutors, and administrative staff on data protection [19]
- Development of internal manuals on confidentiality standards [20]

8. Recommendations

1. Improve the national legal framework:

Review and update Law No. 9887/2008 to further align with GDPR, including specific provisions on AI and emerging technologies in justice.

2. Strengthen technical and organizational measures:

Justice institutions must invest in technical protections such as encryption, access controls, internal audits, and user activity logging to ensure personal data confidentiality.

3. Ongoing staff training:

Judges, prosecutors, and judicial administrative staff should receive regular training on data protection and the risks associated with digital technologies.

4. Establish a dedicated supervisory structure:

A specialized structure for data protection within the justice system should be established to implement and monitor privacy and security policies.

5. Increase public awareness:

Citizens should be better informed about their data protection rights when using digital justice services and how to file complaints in cases of misuse.

6. Apply the “privacy by design” principle:

Any digital platform or database developed for the justice system should consider privacy from the design phase to ensure embedded protection.

7. Continuous monitoring and auditing of digital systems:

Justice system digital platforms should undergo regular audits to identify vulnerabilities and prevent potential data breaches.

9. Conclusion

Protecting personal data in a digitalized justice system requires a careful balance between technological efficiency and fundamental individual rights. Digitalization does not automatically ensure legal security or privacy. Harmonization with GDPR, strengthening institutional capacities, and implementing robust technical measures are essential steps to ensure a secure and trustworthy justice system.

Bibliography

1. UNODC. (2020). Digitalization of Justice Systems: Efficiency and Privacy.
2. Ministry of Justice. (2021). Justice Strategy 2021–2025.
3. ENISA. (2022). Security Guidelines for e-Justice Systems.
4. Parliament of Albania. (2008). Law No. 9887, dated 10.03.2008 On the Protection of Personal Data.
5. European Parliament & Council. (1995). Directive 95/46/EC.
6. European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).
7. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.
8. Commissioner for the Right to Information and Protection of Personal Data. (2023). Annual Report.
9. European Data Protection Board. (n.d.). Guidelines on Data Breach Notifications.
10. CNIL. (2019). Guide on Security of Personal Data. France.
11. European Data Protection Supervisor. (2022). Anonymisation Techniques and Best Practices.

12. Federal Office for Information Security (BSI). (n.d.). IT-Grundschutz Catalogues. Germany.
13. Estonian Ministry of Justice. (n.d.). Digital Justice Strategy.
14. Council of Europe. (2021). Handbook on European Data Protection Law.
15. OECD. (2020). Digital Government in the Justice Sector.
16. FRA. (2020). Fundamental Rights Report.
17. AlgorithmWatch. (2021). AI in Justice Systems: Risks and Ethics.
18. Brkan, M. (2019). AI and GDPR: Impact on Fundamental Rights.
19. OSCE. (2022). Training Manual on Data Protection in the Judiciary.
20. International Association of Privacy Professionals (IAPP). (n.d.). Privacy Program Management.
21. BelenSaglam, R., Altuncu, E., Lu, Y., & Li, S. (2022). A systematic literature review of the tension between the GDPR and public blockchain systems. *arXiv*.
22. Maralbaeva, A. (2024). Evolution of eJustice Platforms: from ICT in Courts Towards ‘Digital Justice’ Portal in Kyrgyzstan. *International Journal for Court Administration*, 15(1), Article 6.
23. Miço Bellani, H., & Leci, E. (2024). Assessing the security of privacy rights and data protection in Albania: A critical analysis within the European legal framework. *Juridical Tribune*, 14(4), 721–748.
24. Trigiante, L., Beneventano, D., & Bergamaschi, S. (2023). PrivacyPreserving Data Integration for Digital Justice. In T. P. Sales et al. (Eds.), *Advances in Conceptual Modeling (LNCS Vol. 14319*, pp. 172–177). Springer.
25. Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *arXiv*.