http://dx.doi.org/10.18623/rvd.v23.6722

PERSONAL DATA GOVERNANCE IN ALBANIA'S E-JUSTICE SYSTEM. PRIVACY, ETHICS AND EU APPROXIMATION IN THE DIGITAL TRANSFORMATION OF JUSTICE

GOVERNANÇA DE DADOS PESSOAIS NO SISTEMA DE JUSTIÇA ELETRÔNICA DA ALBÂNIA: PRIVACIDADE, ÉTICA E APROXIMAÇÃO À UNIÃO EUROPEIA NA TRANSFORMAÇÃO DIGITAL DA JUSTIÇA

Article received on: 1/23/2026
Article accepted on: 4/24/2026

Gentian Koci*
*Aleksandër Moisiu University, Durrës, Albania
Orcid: https://orcid.org/0009-0001-5369-4785
gentiankoci@uamd.edu.al

Loren Lico*
*Aleksandër Moisiu University, Durrës, Albania
Orcid: https://orcid.org/0009-0004-1998-4449
lorenlico@uamd.edu.al

The authors declare that there is no conflict of interest

Abstract
The digital transformation of justice has become a central component of institutional modernisation, access to justice, and rule of law reforms. In Albania, the need for e-Justice has become particularly urgent following the judicial reform and the implementation of the New Judicial Map, which reorganised the judicial system and centralised appellate jurisdiction in a single Court of Appeal with General Jurisdiction in Tirana. This article examines the governance of personal data in the Albanian e-Justice system through the perspective of privacy, ethics, and EU approximation, arguing that the digitalisation of justice in its entirety should not be understood only as a technical modernisation, but as an institutional obligation to structural changes in the judicial system, procedural delays, adjournments of hearings, and the costs of physical access to courts. The article analyses Law no. 124/2024 on the Protection of Personal Data, EU standards, the European e-Justice Strategy 2024–2028, the e-CODEX framework, CEPEJ ethical standards and European good practices. Particular attention is paid to real-time notifications, access control, anonymisation, cybersecurity, audit trails and the supervisory role of the Commissioner. The article concludes that e-Justice increases efficiency, accessibility and public trust only if personal data governance is integrated into every stage of digital justice platforms.

Resumo
A transformação digital da justiça tornou-se um componente central da modernização institucional, do acesso à justiça e das reformas do Estado de Direito. Na Albânia, a necessidade de e-Justiça tornou-se particularmente urgente após a reforma judicial e a implementação do Novo Mapa Judiciário, que reorganizou o sistema judicial e centralizou a jurisdição recursal em um único Tribunal de Apelação de Jurisdição Geral, localizado em Tirana. Este artigo examina a governança de dados pessoais no sistema albanês de e-Justiça sob a perspectiva da privacidade, da ética e da aproximação com a União Europeia, argumentando que a digitalização da justiça como um todo não deve ser compreendida apenas como uma modernização técnica, mas como uma resposta institucional às mudanças estruturais no sistema judicial, aos atrasos processuais, ao adiamento de audiências e aos custos do acesso físico aos tribunais. O artigo analisa a Lei n.º 124/2024 sobre Proteção de Dados Pessoais, os padrões da União Europeia, a Estratégia Europeia de e-Justiça 2024–2028, a estrutura e-CODEX, os padrões éticos da CEPEJ e boas práticas europeias. Dá-se atenção especial às notificações em tempo real, ao controle de acesso, à anonimização, à cibersegurança, às trilhas de auditoria e ao papel supervisor do Comissário. O artigo conclui que a e-Justiça aumenta a eficiência, a acessibilidade e a confiança pública somente se a governança de dados pessoais for integrada

Keywords: E-Justice. Albania. Personal Data Governance. Judicial Reform. Data Protection. EU Approximation. Cybersecurity. Rule of Law.

Palavras-chave: *E-Justiça. Albânia. Governança de Dados Pessoais. Reforma Judicial. Proteção de Dados. Aproximação à União Europeia. Cibersegurança. Estado de Direito.*

1 INTRODUCTION

The digital transformation of justice has become one of the most important dimensions of institutional modernisation, access to justice and strengthening the rule of law. Electronic case management systems, digital communication with parties, the use of electronic hearing calendars, online publication of court decisions and inter-institutional interaction through digital platforms aim to increase the efficiency, transparency and credibility of judicial services. At the European level, the European e-Justice Strategy 2024–2028 links the digitalisation of justice with improving access to justice, increasing the effectiveness and efficiency of the judicial system and developing digital services in the field of justice (Council of the European Union, 2025).

In the case of Albania, the digitalisation of justice should not be seen only as an objective of technical modernisation, but as an institutional necessity stemming from the structural developments of the judicial reform. The implementation of the New Judicial Map brought about a profound reorganisation of the judicial system and significantly reduced the number of functional courts. According to a Council of Europe document on Albania, the implementation of the New Judicial Map was completed on 1 July 2023, and the reform reduced the number of operational courts in the Republic of Albania from 38 to 20 (Council of Europe, 2025). This change is not only of organisational importance, but also directly affects the way in which citizens, lawyers and litigants access courts, procedural information and justice services. One of the most important consequences of this reorganisation is the concentration of appellate jurisdiction. The European Commission has noted that the New Judicial Map reorganised the appellate courts into a single general court of appeal and that this has created several problems, including the lack of infrastructure (European Commission, 2025, p. 5). This focus makes the

development of electronic systems for case management, notification of parties and real-time communication even more necessary, especially for lawyers and citizens located outside Tirana.

In this context, practical issues of judicial administration show that the lack of timely digital notification can produce unnecessary costs for parties and their representatives. Postponement of hearings due to the absence of a judge, annual leaves, training, overload or other organisational reasons is not only an internal administrative issue. It can directly affect effective access to justice, especially when parties or lawyers from the districts travel to Tirana or other judicial centres and are notified late about the non-conduct of the hearing. In these cases, the lack of a reliable electronic notification system causes loss of time, travel costs, additional expenses for legal representation and reduced confidence in the administration of justice.

For this reason, e-Justice in Albania should be understood as a practical instrument to reduce procedural costs and improve access to justice. Electronic calendar of hearings, automatic notifications for postponement or change of hearing dates, electronic communication with parties and lawyers, as well as secure access to the status of the court case, should be considered integral parts of a modern justice model. The EU4Digital Justice project aims precisely to address such challenges in the provision of justice services in Albania, including outdated processes, fragmented case management and limited use of technology (European Union External Action Service, 2026). Within the framework of this project, Albania is expected to create an integrated case management system for the judiciary, which will serve around 550 users in 20 offices and aims to strengthen efficiency, transparency, effectiveness and approximation with EU standards (European Union External Action Service, 2025). In the European model, the single electronic access point approach is seen as a way to make judicial information more understandable and accessible to citizens, businesses and legal professionals (European Commission, n.d.).

However, as justice moves towards electronic platforms, the management of personal data becomes more important. e-Justice systems process broad categories of data: identification data of parties, procedural data, data of lawyers, experts and witnesses, financial, family, health, criminal and electronic evidence. These data are often sensitive not only due to their nature, but also due to the judicial context in which they are

processed. Therefore, e-Justice cannot be designed solely as an infrastructure for administrative efficiency; it must be built on the principles of legality, data minimisation, purpose limitation, security, transparency and accountability.

Law no. 124/2024 "On Personal Data Protection" constitutes the main normative basis for this analysis. This law establishes rules for the protection of individuals with regard to the processing of personal data and aims to protect fundamental rights and freedoms, in particular the right to the protection of personal data (Republic of Albania, 2024, p. 1). The law applies to the processing of personal data by fully or partly automatic means, as well as to non-automatic processing when the data are part of a filing system (Republic of Albania, 2024, p. 1).

For this reason, it is directly relevant for electronic case management platforms, digital notification systems, court registers and the online publication of court decisions. In this context, the Commissioner for the Right to Information and Personal Data Protection has a special role. Law no. 124/2024 defines the Commissioner as an independent authority that monitors and supervises the right to the protection of personal data in accordance with the law (Republic of Albania, 2024, p. 2). The law also stipulates that the Commissioner is a public legal person and an independent supervisory authority, responsible for monitoring and supervising the implementation of the law, with the aim of protecting the fundamental rights and freedoms of natural persons with regard to the processing of personal data (Republic of Albania, 2024, p. 53). This makes the role of the Commissioner essential not only after the establishment of violations, but also in the drafting of preliminary standards for digital justice systems, including anonymisation, data retention, access auditing and security of electronic notifications. From an ethical perspective, the digitalisation of justice should be guided by principles that guarantee not only efficiency, but also procedural fairness, equality, non-discrimination, transparency and human control. If not carefully designed, e-justice systems can create new risks to the privacy, security and integrity of the judicial process. These systems can create scope for unauthorised access to files, exposure of sensitive data through electronic notifications, excessive publication of information in judicial decisions, lack of sufficient traceability of actions, and vulnerability to cyberattacks. For this reason, the ethical dimension of e-justice must necessarily be intertwined with the governance of personal data and institutional oversight.

This article argues that the digitalisation of justice in Albania is an institutional and practical necessity following the justice reform and the reorganisation of the judicial map. The concentration of courts, the creation of a Court of Appeal of General Jurisdiction in Tirana and the increase in physical distances for some parties make the use of electronic systems for case management, timely notification and procedural communication necessary. However, this transformation can only be sustainable if it is accompanied by a clear model of personal data governance, in line with the principles of privacy, ethics, security and approximation with the European Union.

2 E-JUSTICE AS A NECESSITY AFTER THE JUDICIAL REFORM IN ALBANIA

2.1 New judicial map and institutional concentration

The judicial reform in Albania has not only produced changes at the constitutional, institutional and procedural level, but has also brought about a reconfiguration of the way in which citizens and legal professionals physically access the courts. The implementation of the New Judicial Map significantly reduced the number of operational courts and created a more centralised judicial structure. According to the Council of Europe document for Albania, the New Judicial Map was finalised on 1 July 2023, and the number of operational courts in the Republic of Albania was reduced from 38 to 20 (Council of Europe, 2025, p. 1). This fact shows that the digitalisation of justice is no longer just a matter of administrative efficiency, but a direct need to maintain effective access to justice in the conditions of a more centralised judicial system.

Institutional concentration is particularly evident at the appeal level. The reorganisation of the courts led to the creation of a Court of Appeal of General Jurisdiction based in Tirana, replacing the previous structure with several territorial appeal courts. The European Commission has noted that the New Judicial Map reorganised the appeal courts into a single court of appeal of general jurisdiction and that this change has created several practical difficulties, including issues related to infrastructure (European Commission, 2025, p. 5). In this sense, the digitalisation of justice should be seen as a means to compensate for the practical effects of the physical concentration of courts and to avoid

the territorial reorganisation becoming a real barrier for the parties. This dimension is particularly important for lawyers, citizens, experts and litigants located outside Tirana. If judicial services remain dependent on physical presence and traditional communication, the concentration of courts may increase the cost of access to justice. On the contrary, if coupled with functional electronic systems, it can alleviate the financial and organisational burden on parties. Therefore, the New Judicial Map creates a strong argument for the development of an e-justice model that supports timely notification, digital case management, and secure procedural communication.

2.2 Court hearing postponements and procedural costs

One of the most obvious problems of judicial administration is related to the postponement of court hearings. Postponements can occur for various reasons: the absence of the judge, his participation in training, annual leaves, health reasons, overload of the judicial body, the absence of the parties or other organisational problems. In itself, the postponement of the hearing is not necessarily a procedural violation; it can be justified by objective circumstances. The problem arises when the parties and their representatives are not notified in time and are forced to travel to the court for a hearing that will not take place.

This problem is particularly serious for district attorneys and parties who do not live near the centre where the competent court is located. In cases where a lawyer or party travels from another city to Tirana for an appeal hearing and is only notified at the court that the hearing has been postponed, the cost is not only economic. It includes lost time, transportation costs, and the inability to participate in other professional commitments, as well as increased negative perceptions of the effectiveness of the judicial system. In this sense, the lack of timely notification affects not only procedural convenience but also the real quality of access to justice.

Digitalisation can provide a direct solution to this problem. An electronic case management system, linked to an electronic hearing calendar and automatic notification mechanisms, would enable parties and lawyers to be informed in a timely manner of any change in the date, time, panel or procedural status of the case. This would not eliminate

all reasons for postponing hearings, but it would significantly reduce unnecessary costs arising from the lack of fast and reliable information.

In this regard, e-Justice should be understood as an instrument for the rational administration of judicial time. If the judicial system cannot always guarantee the holding of the hearing on the scheduled date, it should at least guarantee accurate, documented and timely notification. Electronic notification, accompanied by traceability of its receipt, creates a higher standard of institutional accountability and reduces procedural uncertainty for the parties. This approach is consistent with the logic of the digitalisation of judicial cooperation in the EU, where electronic communication aims to increase the speed, security and predictability of procedures (European Parliament & Council of the European Union, 2023).

2.3 Real-time notification and digital access to justice

Real-time electronic notification should be seen as a functional element of the right to effective access to justice. In a centralised judicial system, access to justice is not measured only by the formal existence of the competent court, but also by the practical possibility of the parties to receive accurate, rapid and reliable information on their case. For this reason, the electronic calendar of hearings, automatic notification of procedural changes and a secure portal for parties and lawyers should be considered part of the basic infrastructure of modern justice.

In practice, such a system should enable several minimum functions. First, each party and legal representative should have secure access to basic information on the status of the case. Second, any change of the hearing date should be registered in the system and accompanied by automatic notification. Third, the system should generate electronic proof of sending and receiving the notification. Fourth, information sent via email, SMS or portal should be limited to what is necessary for the procedural purpose. This means that electronic notification should avoid exposing sensitive data and use, where possible, secure case references and authenticated access to the portal.

This model is directly related to the governance of personal data. An electronic notification system that sends excessive data, that does not verify the identity of the recipient, that does not maintain audit trails, or that uses insecure communication

channels may create more risks than benefits. For this reason, the digitalisation of court notifications should be built on the principle of data minimisation, communication security, controlled access and documentation of actions.

The EU4Digital Justice project is important precisely because it aims to address the limited use of technology and the fragmented management of cases in the Albanian justice system (European Union External Action Service, 2026). If implemented with strong personal data protection standards, an integrated case management system can serve not only to increase efficiency but also to improve practical access to justice, reduce costs, and strengthen public trust.

2.4 The privacy-efficiency balance

The digitalisation of justice produces a natural tension between procedural efficiency and privacy protection. On the one hand, electronic platforms can significantly improve the speed of communication, case management, administrative coordination and institutional transparency. On the other hand, they create new risks for the processing of personal data, especially when court files, decisions, evidence, data on children, health data, financial data or criminal data are involved.

Precisely for this reason, efficiency should not be achieved at the expense of privacy. In an e-Justice system, any technological solution must be assessed not only according to its ability to speed up procedures, but also according to its ability to protect the personal data of the parties. This requires clear rules on access, storage, deletion, anonymisation, auditing and use of data. If an electronic calendar or notification system publicly exposes more information than necessary, it can infringe on privacy. If, on the contrary, the system is closed, secure, authenticated and traceable, it can simultaneously strengthen efficiency and data protection.

In this sense, the governance of personal data should be integrated from the design phase of e-justice systems. Data protection principles should not be added after the construction of the platform, but should be part of its institutional and technical architecture. Law no. 124/2024 is important in this regard, as it applies to the processing of personal data by wholly or partly automated means and imposes obligations on how controllers and processors must ensure the protection of personal data (Republic of

Albania, 2024, p. 1). The EDPB guidelines on data protection by design and by default emphasise that the obligation to protect data should be implemented from the design phase of processing operations and not as a subsequent corrective measure (European Data Protection Board, 2020, pp. 4–6).

The role of the Commissioner for the Right to Information and Personal Data Protection becomes essential in this balance. The Commissioner should not be seen only as an authority that reacts to violations, but also as an institution that can guide the standards of design, use and supervision of e-Justice systems. This includes guidelines for electronic notifications, standards for anonymising decisions, protocols for storing logs, rules for authorised access and recommendations for data protection impact assessments.

Consequently, the e-Justice model in Albania should be built on a double premise: on the one hand, to guarantee efficiency, timely notification and reduction of procedural costs; on the other hand, to protect the privacy, security and integrity of personal data. Only such a model can turn digitalisation from a technical solution into a genuine instrument of the rule of law.

3 PERSONAL DATA GOVERNANCE IN ALBANIA'S E-JUSTICE SYSTEM

3.1 The meaning of personal data governance in digital justice

Personal data governance in the e-justice system does not only mean the technical storage of information on an electronic platform. It includes the set of rules, roles, responsibilities, control mechanisms and technical and organisational measures that determine the way in which personal data is collected, used, accessed, stored, transmitted, published, anonymised, and deleted in the context of judicial activity. In this sense, data governance is a legal, institutional, technological and ethical issue at the same time.

In the justice system, the processing of personal data has a special nature. Data is not processed simply for administrative purposes, but is related to the exercise of the judicial function, guaranteeing due process, administering evidence and resolving disputes. For this reason, any electronic system used for the management of judicial cases

must guarantee not only technical functionality, but also the protection of the fundamental rights of the persons involved in the process.

In an e-Justice platform, personal data can circulate at several levels. They can be entered by the judicial administration, accessed by judges, used by parties and lawyers, exchanged with other institutions, stored in electronic registers, included in judicial decisions and, in some cases, made public through online portals. This variety of operations requires a clear governance model, because each processing link can create risks for the privacy, security and integrity of the data.

For this reason, e-justice must be built on some very practical questions:

-*what data is really needed for the judicial process; who should see it;*

-*how long should it be stored; what can be made public;*

-*how is access controlled and documented; how is unauthorised use avoided; and*

-*how are the rights of individuals protected without hindering the functioning of the courts?*

These questions show that data governance is not a side issue, but one of the main conditions that makes e-justice legal, safe and trustworthy.

3.2 Categories of personal data processed in e-Justice

E-justice systems process a wide range of personal data. At the most basic level, they include identification data of the parties, such as name, surname, father's name, date of birth, personal identification number, address, contact details and other data that enable the identification of the person. These data are necessary for the administration of the case, the notification of the parties and the linking of procedural documents with the relevant entities.

In addition to identification data, judicial systems also process procedural data. These include the case number, the subject of the claim, the litigants, the panel, the dates of the hearings, interim decisions, procedural acts, the status of the case, the appeal, the recourse and other data related to the progress of the process. Although these data may seem formal, they often reveal important information about the private, economic or professional life of the individual.

In many cases, court cases also contain highly sensitive categories of data. In family proceedings, data on marriage, divorce, custody, maintenance obligations, domestic violence or minors may be processed. In criminal cases, data on suspicions, charges, convictions, security measures, witnesses, victims and evidence may be processed. In civil and administrative cases, financial, tax, property, health or employment data may be processed. For this reason, the digital court file should be considered a high-risk environment for the protection of personal data.

A special category is the data of professionals involved in the process: judges, prosecutors, lawyers, experts, translators, bailiffs, administrators and employees of the court administration. These data are necessary for the transparency and functioning of the process, but they must also be processed in a proportionate manner. For instance, the publication of a judge's or lawyer's name may be justified by procedural transparency and the need to ensure public confidence in judicial proceedings. By contrast, publishing contact details or additional personal information that is not necessary for the conduct of the proceedings would be disproportionate and unjustified. In this regard, the principle of data minimisation is particularly important. Law No. 124/2024 requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Republic of Albania, 2024, p. 8). In the context of e-Justice, this requires digital justice systems to collect and display only the data strictly necessary for the relevant procedural function. Accordingly, a public electronic court calendar should not disclose the same level of information as a secure portal accessed by a party or an authorised lawyer.

3.3 Processing purposes and the risk of function creep

Any processing of personal data in e-Justice must be linked to a clear and legitimate purpose. In judicial systems, the main purposes may include registering the case, assigning the panel, notifying the parties, taking evidence, conducting hearings, issuing decisions, publishing case law and institutional archiving. These purposes are linked to the functioning of justice and may justify the processing of personal data.

However, a risk arises when data collected for a procedural purpose are subsequently used for other, not clearly defined purposes. This phenomenon is known in

the data governance literature as a functional extension of data use, or "function creep". In the context of e-Justice, this risk may arise when court file data are used for statistical analysis without sufficient anonymisation, when access is granted to other institutions without a clear legal basis, when they are published excessively on public portals or when they are stored beyond the necessary time limits.

This risk is particularly relevant in a system where electronic platforms enable inter-institutional interaction. Interaction between courts, prosecution, police, civil registries, tax institutions, bailiffs or other public institutions can increase efficiency, but can also create complex processing chains. The more institutions have access to court data, the greater the need for clear rules on authorisation, purpose, access limitation and auditing.

In this regard, the principle of purpose limitation is essential. Personal data should not be processed in a manner incompatible with the purpose for which they were collected. In practice, this requires that any new functionality of an e-Justice platform be assessed in advance as necessary, proportionate and based on a legal basis. For example, a system initially used only for case registration cannot be automatically extended to profiling, performance analysis or extensive data sharing without a clear legal and ethical assessment.

If this limitation is not respected, the risk is not only formal. Parties to proceedings may lose control over how their data circulate, institutions may create extensive databases without sufficient oversight, and public trust in e-Justice may be undermined. For this reason, any functional extension of e-Justice systems should be accompanied by a data protection impact assessment, institutional consultation and oversight by the Commissioner.

3.4 Access control and institutional accountability

Access control is one of the most important elements of personal data governance in e-justice. In a traditional physical system, access to the court file is limited by procedural rules, physical space and document management. In a digital system, access can be achieved faster, by more users and remotely. This increases efficiency, but at the same time increases the risk of unauthorised or unnecessary access.

For this reason, e-Justice platforms should use role-based access control. This means that each user should only have those access rights that are necessary for their function. The judge should access the cases assigned to him; the court secretary should have access to administrative functions related to the case; the lawyer should only have access to the cases where he is authorised; the party should only see information related to his case; while technical users should not have access to the material content of the file, unless absolutely necessary and controlled.

Access control should be accompanied by full traceability. Every login to the system, every document opening, every session date change, every notification sent, and every document download should be recorded in secure logs. These logs are not just a technical element; they are an institutional accountability mechanism. In case of suspected misuse, logs enable the identification of the user, the time of the action and the nature of the action taken.

However, logs themselves are also data that require governance. They can reveal information about user behaviour, the items accessed, working hours and other sensitive actions. Therefore, the retention of logs should have clear deadlines, limited access and a defined purpose. They should be used for auditing, security and incident investigation, not for unlimited monitoring or other unauthorised purposes.

Institutional accountability requires that each court or institution using e-justice systems have a clear responsibility for how personal data is processed. In this model, it is not enough to say that "the system" processes data. It must be determined who is the controller, who is the processor, who manages the infrastructure, who authorises access, who responds to incidents, and who is liable for violations. Without this division of responsibilities, digitalisation can create an unclear zone where institutional responsibility is diffused and becomes difficult to exercise.

3.5 Anonymisation, publication of judicial decisions and open justice

The publication of judicial decisions is an important part of the transparency of the judicial system. It helps to develop jurisprudence, increases the predictability of decision-making and strengthens public control over the courts. However, the online

publication of decisions creates particular risks to privacy, because decisions may contain personal data of parties, witnesses, victims, children or third parties.

In a digital environment, the publication of a decision does not have the same effect as reading it in a physical register or in a courtroom. A decision published online can be indexed by search engines, copied, distributed, stored by third parties and used in contexts other than the judicial one. For this reason, anonymisation should not be seen as a technical formality, but as a condition for balancing judicial transparency and the protection of personal data.

Effective anonymisation requires more than the removal of first and last names. In many cases, a person can be identified by a combination of other data: place of residence, profession, family relationships, circumstances of the case, date of the event or specific factual details. For this reason, anonymisation should be based on a contextual assessment of the risk of re-identification. This is particularly important for family cases, cases involving minors, criminal cases, health cases and cases involving victims or vulnerable persons. This is in line with the data protection approach according to which the risk of re-identification should be assessed based on the context and combination of data, not only on the presence of the person's formal name (European Data Protection Board, 2020, pp. 19–21).

In the Albanian e-Justice system, it would be necessary to develop a unified standard for the anonymisation of court decisions. This standard should define which data are always removed, which data may be retained for reasons of public interest, how special categories of data are treated, how children are protected and how the quality of anonymisation is checked before publication. Without a unified standard, courts may follow different anonymisation practices, which would create uncertainty and unequal protection of privacy from one court to another. This is where the role of the Commissioner becomes important, as he can guide justice institutions towards clearer, more consistent and more uniform rules for the protection of personal data. As the supervisory authority for the protection of personal data, the Commissioner could contribute to the drafting of guidelines on anonymisation, in cooperation with the High Judicial Council, the Ministry of Justice and the institutions managing electronic justice platforms. This would ensure a better balance between judicial transparency and the protection of privacy.

3.6 Data retention, archiving and the limits of digital memory

Another key issue of personal data governance in e-Justice is data retention. Digital systems tend to retain large amounts of information for long periods, often because technical retention is easier than selective deletion. However, from a data protection perspective, unlimited retention is not neutral. The longer data is retained, the greater the risk of unauthorised access, inappropriate use, information leakage or misinterpretation of old data.

In justice, data retention has a particular specificity. Court files can be important for the rights of parties, for the enforcement of decisions, for procedural history, for public archives and for scientific or institutional interest. For this reason, a simple deletion logic cannot be applied. However, the fact that court files can be stored for legal reasons does not mean that all data should remain accessible in the same way and to the same users forever.

A good e-Justice model should distinguish between several levels of storage: active case data, archived data, published data, anonymised data and technical logs. Active cases require broader procedural access for judges, administration and parties. After the case is concluded, access should be gradually restricted. Published decisions should be anonymised. Logs should be stored for a sufficient period for audit and security, but not indefinitely. Archiving should follow clear legal and technical rules.

In this respect, the limitation of storage does not contradict the need for judicial archiving. On the contrary, it requires that archiving be organised, proportionate and controlled. An archived file should not have the same level of access as an active file. A published decision should not contain the same data as the full decision in the court file. A security log should not be used for purposes other than those for which it was created.

This approach is particularly important for Albania, where the development of new digital systems should avoid the creation of uncontrolled electronic archives. If clear rules for storage, archiving, access restriction and deletion are established at the design stage, the system can avoid many future problems. Conversely, if platforms are built without clear retention policies, the risk is that e-justice will create an unlimited “digital memory”, which could violate privacy and proportionality.

4 PRIVACY, ETHICS AND EU APPROXIMATION IN ALBANIA'S DIGITAL JUSTICE SYSTEM

4.1 Privacy as a condition of effective access to justice

Privacy in e-justice should not be treated as an obstacle to transparency, but as a condition for a trustworthy judicial system. In judicial proceedings, individuals are often forced to present very personal information: family, financial, health, criminal, professional or data on private relationships. If these data are processed without clear boundaries, published excessively or made accessible to unauthorised persons, the justice system no longer guarantees only the resolution of the dispute, but itself becomes a source of risk for fundamental rights.

In this sense, privacy is directly linked to effective access to justice. Citizens may hesitate to use the courts if they believe that their personal data will be exposed in an uncontrolled manner. This risk is even greater in family matters, cases involving minors, criminal cases, domestic violence cases, health matters or cases involving vulnerable categories. Therefore, a modern e-Justice system should guarantee not only faster access to the court, but also the certainty that personal information will be processed only to the extent necessary and for lawful purposes.

This approach is consistent with the logic of Law No. 124/2024, which places the protection of individuals with regard to the processing of personal data and their right to data protection at the centre. The Law applies to automatic and partially automatic processing of personal data, which makes its relevance for electronic case management systems, electronic notifications and digital court registers direct (Republic of Albania, 2024, p. 1). In this context, privacy is not an additional element of e-Justice, but an integral part of its legality.

4.2 Ethical principles in digital justice

The ethics of digital justice require that technology is not used only to speed up procedures, but to strengthen the quality, fairness and accountability of the judicial system. An electronic system may be technically efficient, but ethically problematic if it

creates inequalities in access, exposes personal data, does not allow for sufficient human control or operates in a way that is unclear to users.

The first ethical principle is transparency. Parties should know how the system is used, what data is processed, who accesses it and what consequences electronic actions create. For example, if an electronic notification is considered received at the moment of opening it on the portal, this should be clear to the user. If a document is uploaded to the system and made accessible to other parties, there should be a clear mechanism for information and traceability.

The second principle is procedural fairness. Digitalisation should not create an advantage for parties with more technological capabilities or more economic resources. An e-Justice system should be accessible, understandable and functional even for citizens who do not have advanced digital knowledge. On the contrary, digitalisation can create a new form of exclusion, where formal access exists, but real access becomes more difficult.

The third principle is non-discrimination. If, in the future, justice systems use analytical tools or artificial intelligence for case management, workload distribution, prioritisation, or statistical analysis, it must be guaranteed that these tools do not produce discriminatory results. The CEPEJ has emphasised that the use of artificial intelligence in judicial systems can contribute to increasing efficiency and quality, but it must be implemented responsibly and in compliance with fundamental rights and data protection standards (Council of Europe, 2018).

The fourth principle is human control. Justice cannot be reduced to automation. Even when technology helps in the management of files, notifications, calendars or procedural analyses, judicial decision-making should remain the responsibility of the judge and the relevant institutions. In the case of AI tools, the CEPEJ emphasises that legal professionals should be able to review the decisions and data used to produce an outcome and should not necessarily be bound by it (Council of Europe, 2018, p. 12).

4.3 EU approximation and the European model of e-Justice

Albania’s approximation with the European Union in the field of digital justice should not be understood only as a formal adoption of laws similar to those of the EU. It

also requires practical compliance with the way the EU conceives the digitalisation of justice: as an instrument for better access to justice, greater efficiency, institutional cooperation and the protection of fundamental rights.

The European e-Justice Strategy 2024–2028 establishes an important framework for the development of digital services in justice. The strategy aims to guide the digital transformation in the field of justice in the EU and to support the development of digital tools that improve access, effectiveness and cross-border cooperation (Council of the European Union, 2025). For Albania, this strategy is important not because it is automatically implemented as an internal act, but because it provides a guiding standard for the European integration process and for the construction of future e-Justice systems.

At the same time, Albania has taken important steps in approximating the personal data protection framework. Law No. 124/2024 on the protection of personal data was adopted following the European model and establishes important principles for the processing of personal data, including lawfulness, transparency, purpose limitation, minimisation, accuracy, storage limitation, integrity and confidentiality (Republic of Albania, 2024, pp. 7–9). These principles need to be translated into concrete requirements for e-justice platforms.

Approximation with the EU also requires Albania to avoid a purely technical approach to digitalisation. An integrated case management system should not be assessed solely by the number of users, processing speed or the amount of documents scanned. It should also be assessed according to data protection guarantees, auditability, quality of electronic notifications, access security, anonymisation standards and institutional accountability mechanisms.

4.4 The role of the Commissioner in the digital justice ecosystem

In the digital justice ecosystem, the Commissioner for the Right to Information and Personal Data Protection has a central role. This role should not be reduced only to reviewing complaints or imposing measures following a violation. In the context of e-Justice, the Commissioner should also be seen as an institution that guides, standardises, and supervises the practices of processing personal data by justice institutions.

Law no. 124/2024 defines the Commissioner as an independent authority that monitors and supervises the right to the protection of personal data (Republic of Albania, 2024, p. 2). The law also provides that the Commissioner is an independent supervisory authority, responsible for monitoring and supervising the implementation of the law, in order to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data (Republic of Albania, 2024, p. 53). In the e-Justice system, this competence takes on particular importance because the processing of data is massive, interconnected and often high-risk.

The Commissioner can play a practical role in several directions. First, he can draft or co-draft guidelines for electronic judicial notifications, determining what data can be included in an email, SMS or portal. Second, he can contribute to standards for the anonymisation of judicial decisions. Third, he can guide institutions on log storage, access auditing and incident reporting. Fourth, he can require the performance of data protection impact assessments for new e-Justice systems.

This role should be built in cooperation with the High Judicial Council, the Ministry of Justice, the courts, the prosecution and the technical administrators of the systems. Only a collaborative approach can avoid two extremes: on the one hand, uncontrolled digitalisation that violates privacy; on the other hand, formal data protection blocks necessary innovation. The goal should be a model where privacy and efficiency are not mutually exclusive, but built together.

4.5 European comparative practices and lessons for Albania

European practices show that e-Justice should not be developed as an isolated technological project, but as an integrated ecosystem of information, communication and procedural guarantees. The European e-Justice Portal represents an important example of the single point of access approach, as it provides information on judicial systems, procedures and judicial cooperation tools in the EU (European Commission, n.d.). For Albania, the main lesson is that a national e-Justice portal should be simple for citizens and secure for authorised users, offering a calendar of hearings, notifications, case status and anonymised decisions.

Another important practice is the e-CODEX system. Regulation (EU) 2022/850 establishes the legal framework for a computerised system for the electronic exchange of data in the field of judicial cooperation in civil and criminal matters (European Parliament & Council of the European Union, 2022). The lesson for Albania is that electronic communication in justice must be based on clear technical standards, security, traceability and interoperability, so that different institutional platforms do not produce new digital fragmentation.

Similarly, Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters confirms the EU's orientation towards structured electronic communication between competent authorities and between natural or legal persons and competent authorities (European Parliament & Council of the European Union, 2023). Although Albania is not yet an EU member state, this standard has guiding value for legal and institutional approximation, because it shows that new digital justice systems should be designed with the logic of European interoperability.

The Estonian e-File model provides a practical example of full integration of the procedural cycle. According to e-Estonia, e-File is the heart of the Estonian judicial system, enabling electronic case management, electronic communication, creation and delivery of summonses, minutes and decisions, as well as electronic monitoring of proceedings by parties (e-Estonia, n.d.). For Albania, this model shows that e-Justice should not be limited to document scanning, but should include registration, scheduling of hearings, notifications, acts, decisions, auditing and archiving in a single controlled chain. However, European practices should be read in conjunction with Albanian cybersecurity risks. Cyberattacks on Albanian public systems in 2022 showed that public digital infrastructure can be the subject of sophisticated attacks. CISA has reported cyber operations by Iranian actors against the Albanian government (Cybersecurity and Infrastructure Security Agency, 2022), while Microsoft has analysed the campaign against Albanian government infrastructure (Microsoft, 2022). For e-Justice, this Albanian case implies that cybersecurity is a condition for the integrity of the judicial process and not just a technical issue of system administration.

5 DISCUSSION AND PRACTICAL IMPLICATIONS

5.1 Digital court calendar and real-time notification system

One of the most important practical implications of this paper is the need for a reliable and real-time updated electronic court calendar. In the conditions of the New Judicial Map and the concentration of a significant part of judicial services in more limited territorial centres, parties and lawyers need accurate information on the date, time, courtroom, status and changes of the session.

An electronic calendar should not be simply an online information board. It should be connected to the case management system, to the registration of procedural decisions and to the electronic notification system. When a session is postponed due to the absence of a judge, training, permission or other organisational reasons, the system should automatically generate a notification for the parties and authorised lawyers. This would reduce unnecessary costs, avoid useless trips and increase the accountability of the judicial administration.

However, such a system should be carefully designed, with privacy and personal data protection at its core. A public court calendar should not display unnecessary data or sensitive information for the parties. It can be limited to minimal procedural data, while full case information should be accessible only to authenticated and authorised users. In this way, the system can guarantee procedural transparency without violating the parties' privacy.

5.2 Secure digital communication with parties and lawyers

Digital communication with parties and lawyers should be done through secure, documented and controlled channels. Email and SMS can be used as notification tools, but should not contain excessive data. For example, an SMS could announce that there is a change in the status of the case and invite the user to log in to the secure portal for details. This is more secure than sending full procedural information through a channel that can be read by other people.

The portal for lawyers and parties should rely on strong authentication. Access should be linked to the procedural role of the user and to the authorisation in the specific case. The lawyer should only see cases where his representation is officially registered. The party should only have access to its own case. The judicial administration should have access according to its function and responsibility.

In this model, the electronic notification should also have evidentiary value. The system should record the time of sending, the time of receipt or opening, the user who accessed the notification and the channel used. This traceability helps both the administration of the process and the resolution of disputes over the validity of the notification. But even these logs should be stored with clear deadlines and purposes, as they constitute personal data or data related to the user's procedural behaviour.

5.3 Case management system and audit trails

The integrated case management system is the central element of e-Justice. It should enable the registration, tracking, administration and archiving of judicial cases in a standardised manner. In Albania, the importance of such a system has also been emphasised in the framework of the EU4Digital Justice project, which envisages the establishment of an integrated system for the Albanian judiciary, which will serve around 550 users in 20 offices and will aim to increase efficiency, transparency and effectiveness in accordance with EU standards (European Union External Action Service, 2025).

From the point of view of personal data governance, the case management system should contain strong audit mechanisms. Every important action must be traceable: case registration, change of panel, scheduling of hearing, postponement of hearing, sending of notification, access to documents, uploading of acts, publication of decision and archiving of file. Without traceability, it is difficult to determine responsibility in case of abuse or an incident.

Audit trails are not just a matter of technical security. They are institutional guarantees for the accountability of judicial administration. If a party claims that they were not notified, the system must show when the notification was sent, through which channel and whether it was accessed. If there is a suspicion of unauthorised viewing of

the file, the system must show who accessed it, when and what documents they opened. This increases trust in e-justice and reduces the scope for abuse.

5.4 Data minimisation in judicial notifications

Minimisation of personal data is one of the most important principles for judicial notification systems. The notification should only contain the information that is necessary for the procedural purpose. If the purpose is to inform that a hearing has been postponed, it is not necessary for the notification to contain all the details of the case, sensitive data, the content of the acts or unnecessary information for third parties.

This principle is particularly important for notifications by SMS or email. These channels can be practical, but do not always have the same level of security as an authenticated portal. Therefore, notifications should use limited wording, such as "There is a change in the calendar of your case; please log in to the portal for details". Full information should only be provided after the user has been authenticated.

Minimisation should also be applied to public calendars. If a public calendar displays the names of the parties, the full scope of the case, or data that could reveal private circumstances, it may infringe on privacy. A more balanced model would be to publish general information about hearings, while leaving detailed information accessible only to the parties and authorised representatives.

5.5 Anonymisation and publication of judicial decisions

The publication of judicial decisions should continue to serve as an instrument of transparency, but in a digital environment, it should be accompanied by strong anonymisation. Judicial decisions often contain data that, even when they do not directly identify the person by name, may allow their identification through a combination of factual circumstances.

For this reason, Albania should develop a unified standard for the anonymisation of judicial decisions. This standard should provide for special rules for family matters, minors, victims, criminal cases, health matters and cases where the publication of details

could harm the privacy or security of persons. The standard should also define the institutional responsibility for quality control of anonymisation before publication.

Such a standard should be drafted in cooperation with the Commissioner, the High Judicial Council and the institutions responsible for the administration of digital systems. The aim should not be to limit transparency, but to make it compatible with the protection of personal data. In a state governed by the rule of law, judicial transparency and privacy should not be treated as absolute opponents, but as principles requiring a proportionate balance.

5.6 Data retention, cybersecurity and incident response

The retention of data in e-Justice systems should be based on clear deadlines, purposes and levels of access. Active files, archived files, published decisions and technical logs should not be treated the same. Active cases require functional access by the judge, the administration and the parties. Closed cases require a more limited regime. Published decisions require anonymisation. Logs require retention for security and audit purposes, but not unlimited use.

Cybersecurity is an integral part of the governance of personal data. An insecure e-Justice system can compromise not only privacy, but also the integrity of the judicial process. Minimum measures should include strong authentication, encryption, backups, disaster recovery plans, clear separation of roles, access monitoring and periodic security testing.

Security incidents should be handled through clear protocols. Institutions should know when an incident constitutes a personal data breach, who should be notified, within what timeframe, how the incident is documented and what corrective measures are taken. In this regard, cooperation with the Commissioner is essential, especially when the incident affects sensitive judicial data or a large number of subjects.

5.7 Institutional training and digital culture

One of the most important conditions for the success of e-Justice is institutional culture. The best technical system can fail if users do not understand their responsibilities.

Judges, court administration, prosecutors, lawyers and technical staff should be trained not only on the use of the platform, but also on the protection of personal data, information security and digital ethics.

The training should be practical. It should include concrete cases: how to send an electronic notification; what data should not be placed in an email; how to control lawyer access; how to anonymise decisions; what to do when a document is sent incorrectly; how to report an incident; and how to avoid using data for purposes outside the procedure.

This institutional culture is essential to ensure that data protection remains a mere formal obligation. It should not exist only as an approved document or as a procedure filed in a file, but should become part of the daily practice of administering justice. Only when judges, court administration, lawyers and other actors in the system understand that privacy and information security directly affect the quality of justice can e-Justice function as a credible instrument of the rule of law.

5.8 Data Protection Impact Assessment and privacy by design

Any new e-justice platform in Albania should undergo a Data Protection Impact Assessment before being put into use. This assessment should analyse the categories of data, the purposes of processing, the legal basis, the users, the accesses, the retention periods, the security risks, the possibility of re-identification and the technical and organisational measures. In judicial systems, the DPIA is of particular importance because the processing is often on a large scale and includes data that may be sensitive for parties, witnesses, victims, children or third parties.

The DPIA should not be a formal document drafted after the system has been built. It should be part of the design phase, together with the principle of privacy by design and by default. The EDPB emphasises that data protection by design and by default requires appropriate technical and organisational measures that make the data protection principles effective throughout the processing cycle (European Data Protection Board, 2020, pp. 4–6). For e-Justice, this means that data minimisation, access control, auditing, anonymisation and communication security should be part of the initial architecture of the system. In practice, this requires the involvement of the Commissioner in the early stages of platform development, especially when the system aims to process case data,

interact with other public registers or publish decisions online. Such a model would avoid a situation where the technology is built first, and privacy issues are addressed only after the risk has materialised.

6 CONCLUSION

The digitalisation of justice in Albania is an institutional and practical necessity following the justice reform and the implementation of the New Judicial Map. The reduction in the number of courts, the concentration of appeals in Tirana and the increase in physical distances for some parties create a clear need for electronic systems that facilitate access to justice. Electronic calendars, real-time notifications, a portal for lawyers and parties, as well as an integrated case management system, can reduce costs, avoid unnecessary appearances and increase procedural predictability.

However, e-Justice cannot be just a technical project. It processes highly sensitive personal data and, therefore, requires strong data governance. Any system must be based on legality, minimisation, purpose limitation, security, transparency, auditability and accountability. Without these guarantees, digitalisation can increase the risk of privacy violations and reduce public trust.

European practices, including the European e-Justice Portal, e-CODEX, the EU Digitalisation Regulation and the Estonian e-File model, show that the digitalisation of justice should be secure, interoperable, accessible and rights-oriented. For Albania, these practices provide guiding models, but need to be adapted to the Albanian context, in particular to the practical consequences of the New Judicial Map, the need for timely notifications and the challenges of cybersecurity.

The role of the Commissioner for the Right to Information and Personal Data Protection is essential to ensure that e-Justice is developed in accordance with personal data protection standards. The Commissioner should be involved not only in post-breach supervision, but also in the drafting of standards for electronic notifications, anonymisation, auditing, DPIA, log retention and security incidents.

Finally, approximation with the European Union should not be limited to formal legal harmonisation. It must be reflected in the way digital systems are designed, used and supervised. Only such a model can turn e-Justice into a true instrument of the rule of

law, reducing costs for citizens, increasing judicial efficiency, protecting personal data and strengthening public trust in justice.

AUTHOR CONTRIBUTIONS

Conceptualisation, methodology and literature analysis: Gentian Koci had the primary role in the conceptualisation of the study, the methodological design and the analysis of the relevant legal, institutional and academic literature. Loren Lico contributed to the refinement of the research framework and the review of the relevant literature.

Investigation, formal analysis, and draft preparation: Gentian Koci had the leading role in the legal and institutional investigation, the formal analysis of the research problem and the preparation of the initial draft of the manuscript. Loren Lico contributed to the discussion of the findings, the organisation of arguments and the improvement of the draft.

Final draft preparation: Gentian Koci prepared and revised the final version of the manuscript. Loren Lico reviewed the final draft and contributed to its final approval.

ETHICS STATEMENT

This study is based exclusively on legal, institutional and academic sources. It does not involve human participants, interviews, surveys, experiments or the processing of identifiable personal data. Therefore, no ethics committee approval was required.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

FUNDING

This research received no external funding.

REFERENCES

Council of Europe. (2025). *Support to the implementation of the judicial map in Albania: Deliverable 2*. Council of Europe.

Council of Europe, European Commission for the Efficiency of Justice. (2018). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. Council of Europe.

Council of the European Union. (2025). European e-Justice Strategy 2024–2028. *Official Journal of the European Union*, C/2025/437.

Cybersecurity and Infrastructure Security Agency. (2022). *Iranian state actors conduct cyber operations against the Government of Albania*. CISA.

e-Estonia. (n.d.). Justice and public safety. e-Estonia.

European Commission. (n.d.). European e-Justice Portal. European Commission.

European Commission. (2025). *2025 Rule of Law Report: Country chapter on the rule of law situation in Albania*. European Commission.

European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25: Data protection by design and by default* (version 2.0). EDPB.

European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/850 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system). *Official Journal of the European Union*.

European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters. *Official Journal of the European Union*.

European Union External Action Service. (2025). *EU4Digital Justice: An integrated case management system for the judiciary in Albania*. European Union.

European Union External Action Service. (2026). *EU4Digital Justice: Support to the rule of law through digital transformation — Advancing case management and access to justice in Albania*. European Union.

Katsh, E., & Rabinovich-Einy, O. (2017). *Digital justice: Technology and the internet of disputes*. Oxford University Press.

Microsoft. (2022). Microsoft investigates Iranian attacks against the Albanian government. *Microsoft Security Blog*.

National Authority for Electronic Certification and Cyber Security. (2023). *Governance report: NAECCS 2023*. NAECCS.

Republic of Albania. (2024). Law No. 124/2024 on personal data protection. *Official Gazette of the Republic of Albania*.

United Nations Albania. (2025). EU and UNOPS launch the EU4Digital Justice project: Support to the rule of law through digital transformation. United Nations Albania.

United Nations Development Programme. (2022). *E-justice: Digital transformation to close the justice gap*. UNDP.

Véliz, C. (Ed.). (2023). *The Oxford handbook of digital ethics*. Oxford University Press.