



Privacy and Data Protection in the Age of AI-Powered Cybersecurity: A Comparative Legal Approach

Gentian Koci¹

Emirjana Dimo²

Mariya Valkova Hristozova³

¹PhD., Lecturer, Faculty of Political Science and Law,
University "Aleksander Moisiu", Durrës, Albania;
Member of the Union of Scientists of Bulgaria

²Magistrate, Judge at the Court of First Instance of General Jurisdiction of Elbasan,
Elbasan, Albania

³Associate Professor, Faculty of Public Health,
Medical university of Plovdiv, Plovdiv, Bulgaria

Received: 17 January 2026 / Revised: 24 February 2026 / Accepted: 7 March 2026 / Published: 25 March 2026
© 2026 Koci et al.

Doi: 10.56345/ijrdv13n129

Abstract

The development of artificial intelligence-based cybersecurity systems has changed how public and private organisations identify, prevent, and manage digital threats. However, the use of these systems leads to a marked increase in the processing of personal data, often using persistent monitoring, profiling, and automated decision-making, that directly tests the boundaries set by data protection law. This article contends that the operational logic of AI-powered cybersecurity, which favours large-scale, uninterrupted data collection and predictive risk profiling for maximum security gains, generates acute conflict with key principles of the General Data Protection Regulation (GDPR), such as data minimisation (Article 5(1)(c)) and restrictions on automated decision-making (Article 22). By specifying these structural points of friction in the abstract, the paper anchors its normative claim and clarifies the stakes of the debate from the outset. This analysis is carried out using a doctrinal and comparative approach, comparing the legal framework of the European Union with Albanian legislation. The focus is on the General Data Protection Regulation (GDPR), the EU Regulation on Artificial Intelligence (AI Act), the Data Act, the new eIDAS framework, and the Albanian Law no. 124/2024 "On the Protection of Personal Data". The article claims that the current regulatory framework only partially reconciles the operational logic of AI-powered cybersecurity with the normative logic of personal data protection. In this sense, privacy should not be understood solely as a limitation on technological monitoring, but as a structural prerequisite for the legitimacy, credibility, and sustainability of cybersecurity systems based on artificial intelligence. The paper concludes with proposals *de lege ferenda* for strengthening normative coherence, algorithmic accountability, and human oversight in the use of AI in cybersecurity. Key policy recommendations include the introduction of a dedicated regulatory framework for the use of AI in cybersecurity in Albania, the establishment of mandatory augmented Data Protection Impact Assessments (DPIAs) for high-impact AI-driven systems, the adoption of clear standards on transparency, auditability, and human monitoring, and the separation of security and investigative functions in the use of AI-produced data for criminal procedures. GDPR is Regulation (EU) 2016/679, AI Act is Regulation (EU) 2024/1689, Data Act is Regulation (EU) 2023/2854, the new eIDAS rules were adopted with Regulation (EU) 2024/1183, while in Albania, the central basis is Law no. 124/2024.

Keywords: Artificial intelligence; privacy; personal data protection; cybersecurity; GDPR; AI Act ;comparative law

1. Introduction

In the context of accelerated digitalisation, the protection of personal data and cybersecurity have become closely interdependent legal areas. The increase in data volume, the use of cloud infrastructure, and the expansion of automated systems have simultaneously increased the need for security and the risk of privacy breaches. In this context, artificial intelligence is taking on a central role in digital security, used for anomaly detection, user behaviour analysis, and automated incident response. These functions increase the technical strength of systems, but also the intensity of personal data processing, making it more difficult to maintain the balance between the effectiveness of security and the protection of fundamental rights (European Parliament and Council, 2016, 2024a; Novelli et al, 2024).

This analysis is primarily addressed to policymakers, legal practitioners, and institutional decision-makers in the fields of data protection, cybersecurity, and information governance, both within the European Union and in Albania. It is also relevant for data protection officers, compliance professionals, and regulatory authorities who are responsible for implementing or supervising the intersection of AI-based cybersecurity and privacy regulation. By explicitly directing attention to these audiences, the paper aims to inform both strategic policy development and practical regulatory action amid accelerated digital transformation. Furthermore, the findings seek to guide policymakers in identifying concrete areas for regulatory reform, such as clarifying compliance obligations, strengthening oversight mechanisms, and establishing procedural safeguards for the responsible use of AI in cybersecurity. By highlighting where current legal provisions fall short and offering targeted recommendations, the analysis offers a practical foundation for decisions on future legislation, institutional guidelines, and operational measures.

The use of AI in cybersecurity is not only a technical development. It is also a legal transformation. This technology affects principles like lawfulness, data minimisation, purpose limitation, transparency, proportionality, and accountability. In the European Union, this tension is addressed by many laws. The GDPR is the primary act governing the protection of personal data. The AI Act creates a risk-based regime for AI systems. The Data Act governs data access and use. eIDAS strengthens electronic identity and trust services. NIS2 Directive sets high cybersecurity requirements (European Parliament and Council, 2016, 2022, 2023, 2024a, 2024b). Still, these laws, while many, are not fully coherent (Levitina, 2024; Novelli et al, 2024). For this comparative study, the key criterion is the level of rights protection achieved by the EU's legal framework. By assessing how well these laws together protect privacy and data, the analysis offers a critical look at their strengths and weaknesses.

Albania provides a valuable example, as it meets European standards. With Law No. 124/2024 on Personal Data Protection and the National Cybersecurity Strategy 2025–2030, Albania has begun harmonising with the GDPR and EU cybersecurity standards (Assembly of the Republic of Albania, 2024; National Cybersecurity Authority, 2025). Still, questions remain about whether this system is ready for advanced algorithmic monitoring, risk assessment, and automated response.

This article analyses the conflict between privacy and AI-empowered cybersecurity using doctrinal and comparative approaches. It compares European Union law and the Albanian legal system. The main thesis is that the existing legal framework only partly reconciles AI-based cybersecurity with privacy protection; that is, current laws provide limited consistency and coherence among these domains. Therefore, a more integrated regulatory approach is normatively required to guarantee both solid privacy protection and effective cybersecurity. This should include increased transparency, algorithmic accountability, human monitoring, and stronger guarantees (European Parliament and Council, 2016, 2024a; Parliament of the Republic of Albania, 2024). To test this thesis, the doctrinal analysis closely examines the GDPR (especially Articles 5, 22, 32), the AI Act, and Law no. 124/2024. It reviews their requirements for processing personal data for AI-powered cybersecurity. The comparative study then checks how the frameworks converge or diverge on the privacy-cybersecurity tension. Attention is given to safeguards, oversight, and regulatory deficiencies. This transparent methodology is intended to justify and support the findings and recommendations.

This issue also affects criminal law. AI-driven systems can help identify possible criminal behaviour, generate electronic traces, and provide potential evidence. Therefore, analysing the relationship between privacy and cybersecurity must also include criminal law guarantees. This is especially important for surveillance proportionality, suspicion individualisation, and the reliability of electronic evidence (Council of Europe, 2001, 2022; Dushi & Bërdufi, 2017).

2. Literature Review

Contemporary literature on privacy, data protection, artificial intelligence, and cybersecurity shows that these fields have developed into distinct subfields. In practice, however, they are progressively interconnected. As cybersecurity systems

powered by artificial intelligence proliferate, fragmented analyses are clearly insufficient. Recent literature notes that interaction among data protection laws, AI regulation, and information security measures requires an integrated approach. Each area directly affects the legitimacy and limits of automated security systems (Negara, 2024; Novelli et al., 2024). Nevertheless, recent scholarship shows a growing convergence around the idea that principles such as trust, transparency, and accountability form the basis of privacy, AI, and cybersecurity governance. Calls for risk-based approaches, multi-layered safeguards, and recognition that technological progress must be anchored in individual rights reflect this emerging consensus. These shared threads provide a basis for the integrated analytical viewpoint adopted in this paper.

From a theoretical point of view, privacy and data protection are closely related but not identical concepts. Privacy involves individual autonomy and the limits of interference in the personal sphere, while data protection focuses on the conditions, legal bases, and procedures for processing personal data (European Parliament and Council, 2016). This division is particularly important for analysing AI-driven systems. cybersecurity, as these systems can not merely expand surveillance but also violate the principles of legality, transparency, data minimisation, and purpose limitation.

An important strand of modern literature focuses on automated decision-making and profiling. Lukács and Vári point out that the European data protection framework faces serious challenges when AI systems are used for automated decision-making, notably in environments lacking transparency and a high risk of discrimination (Lukács & Vári, 2023). Along the same lines, Christodoulou argues that the use of machine learning algorithms in automated systems creates a dual tension between the requirement for accuracy and productivity, on the one hand, and the obligation to guarantee privacy, data protection, and human control, on the other (Christodoulou, 2024). This is particularly important for cybersecurity systems, which rely precisely on profiling, behavioural analysis and automated anomaly detection.

Another segment of the literature concerns the legal governance of artificial intelligence in the European Union. Novelli and co-authors point out that the legal obstacles to AI in the EU are not limited to civil liability or intellectual property, but also include privacy, cybersecurity, and the normative compliance of complex models (Novelli et al., 2024). This literature becomes even more important after the adoption of the AI Act, which aims to create a harmonised, risk-based regime for the use of AI in the EU (European Parliament and Council, 2024a). However, here too, it is noted that the AI Act does not replace the GDPR but coexists with it, creating a multi-layered architecture that requires systemic interpretation (Levitina, 2024).

Another important idea in the literature is that cybersecurity and privacy should not be treated as necessarily opposing objectives. Some authors argue that privacy should also be understood as a structural condition of faith in digital systems, including AI systems used for security. In this sense, a strong data protection regime is not an obstacle to cybersecurity but a prerequisite for its legitimacy (European Data Protection Supervisor, 2025; Levitina, 2024).

However, despite considerable development in the literature, there is still a significant gap in the analysis of AI-powered cybersecurity as a field where data protection, artificial intelligence regulation, and cybersecurity law collide (Bai, X., Zhang, Z., Zhang, Z., Li, Z., & Zhang, J. (2023). Also, there is still insufficient comparative work examining this conflict in relation to jurisdictions in the process of approximation to the European Union *acquis*, such as Albania. It is precisely this gap that justifies the importance of this paper, which aims to build an integrated analysis between the EU framework and Albanian law. 124/2024 (Parliament of the Republic of Albania, 2024).

3. Study Methodology

This paper relies on a **doctrinal, comparative, and normative approach**. The doctrinal method is used to analyse the main legal sources of the European Union and Albania, in particular the GDPR, the AI Act, the Data Act, eIDAS 2, NIS2 and Law no. 124/2024 (European Parliament and Council, 2016, 2022, 2023, 2024a, 2024b; Parliament of the Republic of Albania, 2024).

The comparative method is applied to identify similarities, differences and gaps between the European Union and Albanian frameworks at the principal, functional and institutional levels. While the normative method is used to formulate **de lege ferenda** proposals, the current framework is assessed to determine whether it is sufficient to meet the challenges presented by artificial intelligence systems. cybersecurity, especially in relation to immediate monitoring, large-scale processing and automated decision-making (Levitina, 2024; Novelli et al, 2024).

The study is based on primary legal sources and secondary scientific literature. It is not empirical in the classical sense, as it does not use interviews or statistical data, but aims to analyse the legal legitimacy of these systems and the capacity of the normative framework to regulate them. In this regard, the paper aims to make a theoretical and comparative contribution to the debate on the relationship between privacy and cybersecurity in the era of artificial intelligence.

3.1 *Conceptual framework : privacy, data protection and AI- powered cybersecurity*

Privacy and data protection are related concepts, but not the same. Privacy involves individual autonomy and the limits of interference in private life, while data protection focuses on the conditions, purpose, and lawfulness of the processing of personal information (Gellert & Gutwirth, 2013; European Parliament and Council, 2016). In the digital environment, this separation becomes essential because formally lawful processing can produce serious consequences for the individual. The GDPR bases this protection on principles such as lawfulness, transparency, purpose limitation, data minimisation, and accountability (European Parliament and Council, 2016).

AI-powered cybersecurity refers to the use of artificial intelligence systems to detect, analyse, and manage cyber attacks. These systems depend on large-scale data analysis, profiling, and risk classification, which increases technical efficiency yet also raises the potential for persistent monitoring and privacy violations (Novelli et al., 2024; Christodoulou, 2024). For example, an AI-driven intrusion detection tool may monitor all employee network activity in real time, looking for patterns that resemble malicious behaviour. In practice, this could mean that a legitimate but unusual access by an employee late at night is flagged as suspicious, leading to the collection of extensive metadata, triggering internal reviews, and perhaps even the automated restriction of the employee's access. Such scenarios make clear how the operational drive for extensive data gathering in pursuit of greater security accuracy can create risks of excessive data retention, lack of transparency, or unjustified profiling. This is where the main tension arises: the more security relies on the logic of "more data, more accuracy", the more the respect for proportionality, openness, and necessity is put to the test (European Parliament and Council, 2016; Gonçalves, 2025).

A central element in this debate is automated decision-making. Many security systems do not limit themselves to analysis, but can block access, categorise users as "high risk", or activate security measures absent instant human involvement. For this reason, human monitoring must be real and effective, not merely formal, otherwise automation increases the risk of a lack of transparency and a weakening of judicial accountability (Levitina, 2024; European Data Protection Supervisor, 2025), (Prasetyoningsih, N. (2024).

3.2 *The legal framework of the European Union*

The European Union legal framework on the relationship between privacy, personal data protection and AI-based cybersecurity is built on a multi-layered architecture. At its centre is the GDPR, which sets out the basic principles of personal data processing, the entitlements of data subjects, and the obligations of controllers and processors (European Parliament and Council, 2016). Alongside it, the AI Act regulates artificial intelligence according to a risk-based approach; the Data Act addresses access to and use of data; eIDAS 2 strengthens electronic identity and trust services; while NIS2 imposes strengthened cybersecurity obligations in essential sectors (European Parliament and Council, 2022, 2023, 2024a, 2024b). This makes the European framework normatively rich, but not fully coherent.

The GDPR remains the fundamental instrument for assessing the lawfulness of cybersecurity systems that process personal data. The principles of Article 5, such as lawfulness, transparency, purpose limitation, data minimisation, and accountability, are important for AI security systems because they regularly operate on the logic of collecting large amounts of data to attain more accurate threat detection (European Parliament and Council, 2016). However, the existence of a legal basis, such as legitimate interest or legal obligation, is not sufficient in itself: processing must remain proportionate, necessary and limited to the specific security purpose. Equally important is Article 32 of the GDPR, which treats the security of processing as part of the very logic of data protection, rather than as an external field to it (European Parliament and Council, 2016).

Cybersecurity for powered systems also poses important questions regarding Article 22 of the GDPR on automated decision-making. Here, it is critical to distinguish between technical risks—such as threats to system integrity, data availability, and operational continuity—and risks to fundamental rights, such as privacy, fairness, and due process for persons affected by automated actions. Although not every security system makes "decisions" in the strict legal sense, many carry out risk classification processes, restrict access, or activate alerts that may significantly affect individuals (European Parliament and Council, 2016). This twofold framing sharpens the analysis by clarifying that while technical risk management focuses on preventing intrusions or disruptions, Article 22 primarily addresses protections against adverse effects on individuals resulting from fully automated processing. In these cases, the legal analysis should go beyond the security of the processing, and explicitly reinforce GDPR safeguards by examining the transparency of the logic used, the rights of the subject, and the existence of real human control (Levitina, 2024; European Data Protection Supervisor, 2025). The problem becomes even more acute when using incompletely explanatory models, because

algorithmic opacity makes it more difficult to contest or correct the results (Christodoulou, 2024; Gonçalves, 2025).

The adoption of the AI Act constitutes the most important development in recent years in European artificial intelligence law. It establishes harmonised rules for AI systems and adds requirements for risk management, data quality, technical documentation, human monitoring, accuracy, and system security (European Parliament and Council, 2024a). However, the AI Act does not replace the GDPR; rather, it complements it. At the same time, the Data Act and eIDAS 2 extend the analysis to data flows, electronic identity, and digital trust infrastructures, while NIS2 strengthens obligations for risk management and cybersecurity incident reporting (European Parliament and Council, 2022, 2023, 2024b).

This analysis shows that the European Union has built an advanced framework for privacy, artificial intelligence, data, and cybersecurity, but it remains functionally fragmented. GDPR regulates the lawfulness of processing; the AI Act governs the risks posed by AI systems; the Data Act addresses the use of data; eIDAS 2 supports digital identity and trust; while NIS2 imposes security obligations. The difficulty emerges when all these instruments have to be implemented simultaneously within the same AI-powered system. For this reason, a systemic reading of them and a comparative study with national jurisdictions, such as Albania, is required.

3.3 Albanian legal framework

The Albanian legal framework for the protection of personal data has entered a new phase with the adoption of Law No. 124/2024 "On the Protection of Personal Data", which constitutes the central basis for the analysis of the relationship between privacy, data processing and the utilisation of advanced technologies in cybersecurity (Assembly of the Republic of Albania, 2024). The scope of the law itself makes it clear that it covers the fully or partially automated processing of personal data, which renders it especially relevant for AI-driven systems. cybersecurity .

From a structural perspective, Law No. 124/2024 is clearly aligned with the GDPR model. It regulates the processing of personal data, the rights of subjects, the obligations of controllers and processors, the security of processing, and institutional oversight (Assembly of the Republic of Albania, 2024; European Parliament and Council, 2016). An important indicator of this approach is the role of the data protection officer (DPO), especially in cases of regular and systematic large-scale monitoring, a standard that is directly relevant to the use of AI in cybersecurity (Information and Data Protection Commissioner, 2025a, 2025b).

Albanian law treats security of processing as part of the very logic of data protection, in line with the GDPR model. This means that the use of AI in security functions should not be seen as a field outside data protection, but as part of it whenever personal data is involved (Assembly of the Republic of Albania, 2024). This direction is additionally reinforced by developments in secondary legislation: the Commissioner's Office has commenced consultations on secondary legislation and issued guidelines on areas such as video surveillance, which show that the new framework is gradually being operationalised (Information and Data Protection Commissioner, 2025c, 2025d).

Although Law No. 124/2024 creates a stronger basis for the protection of personal data, it does not establish a special regime for artificial intelligence (AI) or AI-driven systems in cybersecurity. As a result, issues such as algorithmic clarity, explainability, model auditability, classification errors, and effective human monitoring still remain without specific treatment. This gap becomes more apparent compared to the European Union, where the GDPR, AI Act, NIS2, Data Act, and eIDAS 2 together create at least a readable architecture. In Albania, meanwhile, controllers must be guided primarily by general privacy protection standards and administrative practice, which creates interpretative uncertainty. Without AI-specific guidance, Albanian controllers face a considerable compliance burden, as they are left to interpret general obligations in complex, quickly evolving technical contexts, thereby increasing legal risk and resource investment.

Given these problems, it is important for Albanian authorities to take immediate, practical interim measures while thorough regulatory solutions are developed. As a first step, the Information and Data Protection Commissioner and the National Cyber Security Authority could jointly issue interim guidelines clarifying how existing data protection principles apply to AI-based cybersecurity systems, with an emphasis on core areas such as mandatory data minimisation, transparency, and human oversight. In parallel, authorities could organise targeted training sessions and information campaigns for data protection officers, IT staff, and compliance professionals to build capacity to identify and manage emerging AI-powered cybersecurity risks. Additionally, launching a pilot program to upgrade Data Protection Impact Assessments for selected public or private sector entities that implement AI-based security solutions could yield valuable practical insights into future regulation. These interim measures would help bridge the current regulatory gap, improve compliance, and reduce interpretative uncertainty, while setting the foundation for a more specific and complete legal framework in the near future.

In the institutional plan, effective implementation of the law does not require only a normative basis but also

bylaws, thematic guidelines, training and auditing standards. Public data from 2025 show that the process of institutional consolidation has begun but is still in development (Information and Data Protection Commissioner, 2025a, 2025b, 2025c). For this reason, the Albanian framework constitutes an important step forward, but the lack of a specific AI layer in cybersecurity is a key gap that will also be reflected in the relative analysis.

3.4 *Comparative study: the structural conflict between privacy and AI-powered cybersecurity, with aspects of criminal law*

The comparative study of the European and Albanian frameworks shows that the conflict between privacy and AI-based cybersecurity is not simply technical or administrative, but structural. It arises because these systems depend on uninterrupted monitoring, extensive data processing, and risk classification, while privacy and data protection require limitation, proportionality, openness, and control over processing (European Parliament and Council, 2016, 2024a; Parliament of the Republic of Albania, 2024). In the criminal sphere, the tension becomes even more acute because the same technologies can be used both for prevention and for the production of electronic traces and evidence.

The most obvious form of this conflict lies in the relationship between persistent oversight and data minimisation. AI security systems operate on logs, metadata, user behaviour, and anomaly signals, increasing the potential for early threat detection while also increasing the risk of exceeding the limits of necessity (European Parliament and Council, 2016). At the same time, purpose limitation is put to the test when data originally collected for technical security is reused for internal investigations, disciplinary measures or criminal prosecution. This shifts the debate from data security to criminal intelligence and calls for clear rules on the preservation, integrity, and chain of evidence (Council of Europe, 2001; European Parliament and Council, 2016).

Another sensitive element is profiling. AI systems can classify behaviour as “anomalous” or “high risk” based on statistical correlations, but in criminal law, a probabilistic profile cannot replace individualised legal suspicion. This is where the importance of the AI Act becomes more apparent, as it places stronger limits and safeguards on certain uses of AI in sensitive areas, including those related to law enforcement and justice (European Parliament and Council, 2024a). From this perspective, AI systems can serve as aids for early warning, but not as an automatic basis for restricting freedoms or generating criminal suspicion.

Equally important is the electronic evidence dimension. AI-powered cybersecurity systems can generate automated logs, alerts, and reports that are later used in investigations or trials. This elicits concerns about the reliability, integrity, verifiability, and transparency of the algorithmic model. While all evidentiary principles, integrity, authenticity, and admissibility constitute challenges, authenticity is the most unresolved issue in practice when logs from automated systems are used as criminal evidence. Guaranteeing the authenticity of digital logs generated with limited human monitoring is particularly problematic, given the risks of undetected manipulation, insufficient documentation of the system's operation, and difficulties in duplicating or challenging how an algorithm reached a conclusion. If authenticity cannot be clearly established, subsequent efforts to demonstrate integrity or satisfy admissibility criteria become much less meaningful. The Budapest Convention and its explanatory instruments emphasise the role of criminal justice in securing electronic evidence while observing fundamental rights, which makes this debate essential for Albania as well (Council of Europe, 2001, 2022). In the absence of clear standards on documentation, auditing and human control, there is a risk that technology will enter the criminal process with high technical authority but insufficient legal guarantees.

From a fundamental rights perspective, the analysis should also be linked to Article 8 of the ECHR. The jurisprudence of the European Court of Human Rights has stressed that surveillance regimes must be based on law, necessary, and proportionate, even when justified on grounds of security (European Court of Human Rights, 2010, 2017, 2021). This has direct relevance for AI-powered cybersecurity, because systematic, automated monitoring can easily turn into intensive surveillance with administrative and criminal consequences.

The EU–Albania comparison shows that the European Union has a more developed and differentiated architecture, where the GDPR, AI Act, NIS2, Data Act, and eIDAS 2 can be read together, although not without fragmentation. Albania, meanwhile, has made important steps with Law no. 124/2024 and the first sub-legal acts, but still does not have a separate regulatory layer for AI in security functions (Parliament of the Republic of Albania, 2024; Information and Data Protection Commissioner, 2025a, 2025c, 2025d). In the criminal field, this gap is even more acute, because the relationship among algorithmic security, electronic evidence and procedural guarantees remains underdeveloped.

In conclusion, the conflict between privacy and AI-based cybersecurity is structural and not accidental. This core dilemma can be encapsulated as the “surveil-privacy paradox”: the more we deploy continuous monitoring and

algorithmic vigilance to ensure digital security, the more we expose privacy and fundamental rights to possible erosion. In the civil-administrative sphere, it appears as a tension with the principles of data protection; in the criminal sphere, it is linked to the risk that monitoring, profiling, and algorithmic products assume an excessive role in the production of suspicion and evidence. The recognisable signature of the surveil-privacy paradox suggests that this is not a transient trade-off but a recurring challenge wherever AI-powered security systems operate. Precisely for this reason, clearer guarantees of transparency, auditing, human oversight, and limits on the criminal use of AI-driven systems are needed. cybersecurity .

3.5 *Proposals de lege ferenda , with special focus on Albania*

The analysis shows that the main problem in Albania is not the absolute lack of norms, but the lack of an integrated architecture that connects the protection of personal data, the use of artificial intelligence and cybersecurity. Although Law No. 124/2024, Law No. 25/2024, and the National Cybersecurity Strategy 2025–2030 have substantially reinforced the normative-institutional basis, a specific approach to AI-driven systems is still missing. cybersecurity (Assembly of the Republic of Albania, 2024, 2024a; National Cyber Security Authority , 2025a, 2025b). For this reason, the first recommendation is to draft an integrated framework, through a joint guideline or a sub-legal act by the Commissioner and the National Cyber Security Authority, to define minimum standards for the use of AI in monitoring, anomaly analysis, risk classification and automated response (Information and Data Protection Commissioner , 2025a, 2025c; National Cyber Security Authority , 2025c).

A second necessary step is to establish enhanced DPIAs for AI-powered cybersecurity systems. In addition to classic privacy elements, these assessments should include the model's logic, data categories, the risk of algorithmic error, human monitoring mechanisms, and the possibility of data reuse in disciplinary or criminal proceedings (European Parliament and Council, 2016; National Cyber Security Authority, 2025d). To clarify compliance obligations and avoid uncertainty, two objective criteria should be set to trigger the requirement for an enhanced DPIA: (1) the scale of the dataset processed, for example, if an AI-powered system processes data relating to over 10,000 individuals or involves cross-sectoral data integration, and (2) the level of automation, in particular where the system enables automated decision-making without real-time human involvement that may impact data subjects' rights or access to critical services. Requiring an enhanced DPIA for systems meeting either or both of these thresholds makes certain that controllers apply higher standards of risk assessment and accountability in higher-impact scenarios. Equally important is the establishment of minimum standards for transparency, explainability, and auditability, including technical documentation, recording automated interventions, retaining *audit trails*, and periodic testing of models (Information and Data Protection Commissioner, 2025c; National Cyber Security Authority, 2025b).

In practice, authorities should implement a clear, actionable DPIA process. First, regulatory bodies can develop and circulate standardised DPIA templates specifically created for AI-powered cybersecurity systems, detailing required information and risk assessment checkpoints. Second, pilot projects should be initiated within selected public or private sector organisations to apply these templates in practical situations, with findings used to improve the process and address practical obstacles. Third, targeted capacity development programs, such as specialised workshops and e-learning modules, should be provided for data protection officers and compliance professionals to strengthen their understanding of AI-specific risks and the application of enhanced DPIAs. At the institutional level, this should be accompanied by stronger cooperation between the Commissioner and AKSK, sectoral guidance on highly sensitive areas, and strengthened training for DPOs and public institutions (Information and Data Protection Commissioner, 2025b).

In the criminal and procedural dimension, even clearer guarantees are needed. First, the security function should be clearly separated from the investigative function, so that data collected for security purposes is not automatically reused for criminal purposes. Second, specific standards are needed for the admissibility and dependability of electronic evidence produced by AI, including authenticity, integrity, *chain of custody*, and verifiability of the system logic (Council of Europe, 2001, 2022). Third, algorithmic profiling should not serve as the sole basis for measures with criminal or legal effect, but only as a preliminary technical signal subject to human verification (European Parliament and Council, 2024a). To further guard against automation bias in criminal proceedings, it is proposed that any AI-generated alert or output used in a criminal context should require mandatory human corroboration before it can have legal or evidentiary consequences. Such a safeguard would ensure that prosecutors and investigators treat AI outputs as leads requiring independent validation, rather than as conclusive evidence, supporting more reliable and rights-respecting criminal processes. Finally, the procedural guarantees of the individual should be strengthened, including the right to information,

human review and challenge of the algorithmic result, as well as the specialisation of prosecutors, judges and experts in electronic evidence and the use of AI in the procedure (European Court of Human Rights, 2010, 2017, 2021).

In conclusion, if Albania aims to build a modern and secure framework for AI-powered cybersecurity, formal coordination with the EU *acquis* is not sufficient. Operationalisation of standards through common guidelines, enhanced DPIAs, openness and audit standards, and clear rules on the criminal use of data is required. security data. Only in this way can a model be built that guarantees not only greater security but also greater legal legitimacy and societal trust.

4. Conclusions

This paper showed that the relationship between privacy, personal data protection and cybersecurity based on artificial intelligence cannot be understood as a simple balancing act between two competing interests. AI-powered cybersecurity constitutes a complex meeting point among several legal regimes: data protection, artificial intelligence regulation, cybersecurity, and, in certain circumstances, criminal law and criminal procedure. The more security relies on uninterrupted monitoring, profiling, and automated intervention, the greater the risk of violating the principles of legality, minimisation, transparency, and accountability (European Parliament and Council, 2016, 2024a).

The analysis of the European Union framework showed that the EU has built an advanced and multi-layered regulatory architecture. The GDPR remains the main pillar for the lawfulness of the processing of personal data, while the AI Act provides a new layer of risk-based control. The Data Act, eIDAS 2, and NIS2 complement this system by regulating data use, digital trust infrastructures, and cybersecurity obligations (European Parliament and Council, 2016, 2022, 2023, 2024a, 2024b). However, the article showed that this architecture remains functionally fragmented and does not yet provide a single regime for AI-powered cybersecurity.

In comparative terms, Albania has taken an important step forward with the adoption of Law No. 124/2024 and with developments in the field of cybersecurity, especially through Law No. 25/2024 and the National Cybersecurity Strategy 2025–2030 (Assembly of the Republic of Albania, 2024; National Cyber Security Authority, 2025a, 2025b). However, a specific normative layer for the use of artificial intelligence in security functions remains missing, leaving issues such as algorithmic transparency, auditability, human control, and data reuse for investigative purposes without clear treatment.

One of the main conclusions of the paper is that privacy should not be seen as an obstacle to cybersecurity, but as a structural condition of its legitimacy. An AI-powered cybersecurity system may be technically efficient, but it remains legally vulnerable if transparency, proportionality, audit, and real human monitoring are lacking (Levitina, 2024; European Data Protection Supervisor, 2025). For this reason, the central question is not whether AI should be used in cybersecurity, but rather under what statutory and procedural conditions this use can be considered lawful and compatible with fundamental rights.

Given the vital need for policy action, the most immediate and influential next step would be to introduce a mandatory audit obligation for AI-powered cybersecurity systems. In designing such audit obligations, legislators can draw on established audit frameworks from the European Union, such as the EU's Guidelines regarding Data Protection Impact Assessments and the regular audit provisions in the GDPR. Best practices can also be observed in the risk-based audit requirements set out in the AI Act, as well as in frameworks developed by the European Union Agency for Cybersecurity (ENISA), which provides thorough methodologies for technical and organisational audits in high-risk digital environments. Internationally, the NIST AI Risk Management Framework in the United States and the ISO/IEC 27001 standard on information security management offer widely recognised benchmarks for audit structure, transparency, and accountability in technology-driven sectors. By referencing such models, legislators and regulators can establish clear, enforceable requirements for routine technical, legal, and procedural audits tailored to the specific challenges of AI-powered cybersecurity. In this way, oversight would be strengthened, functional transparency improved, and human rights safeguards systematically checked in practice. This single reform would provide a practical foundation for accountability and a concrete starting point for legislators seeking to address gaps in the current regulatory system. From a final and procedural perspective, the paper highlighted that AI-powered cybersecurity systems can produce logs, alerts, and reports that can later be used as electronic evidence or as preliminary grounds for criminal suspicion. This makes it necessary to form clear standards for *the chain of custody*, the verifiability of the algorithmic product, the limits of profiling, and the separation between the security and investigative functions (Council of Europe, 2001, 2022). In the absence of these guarantees, there is a risk that algorithmic products will carry disproportionate weight in investigations or legal decision-making.

In conclusion, the article's main thesis is confirmed: the current legal framework only partially reconciles the operational logic of cybersecurity based on artificial intelligence with the normative logic of privacy and personal data

protection. The European Union has built an advanced, but not yet fully integrated, foundation; Albania has created important foundations, but needs to take further steps to make this system truly functional for the AI era. Consequently, *the de lege ferenda direction* should aim to build a common model of legal governance in which security, privacy, algorithmic accountability, and procedural guarantees exist together in a coherent manner. Only such an approach can ensure that the digital transformation produces not only greater technical efficiency, but also greater legality, institutional trust, and real protection of fundamental rights.

References

- Bai, X., Zhang, Z., Zhang, Z., Li, Z., & Zhang, J. (2023). Spatial Heterogeneity and Formation Mechanism of Eco-Environmental Quality in the Yellow River Basin. *Sustainability*, 15(14), 10878.
- Berisha, IS, Kerka, EP, & Andersons, A. (2026). Personal data protection and privacy. *European Journal of Economics, Law and Social Sciences*, 10 (1), 84–94. <https://doi.org/10.2478/ejels-2026-0009>
- Ceko, E. (2023). Cyber security issues in Albanian higher education institution curriculum. *Canadian Research Journal*, 1 (1). <https://doi.org/10.59380/crj.v1i1.2728>
- Christodoulou, P. (2024). Data protection issues in automated decision-making systems using machine learning algorithms. *AI*, 4 (1), 74–90.
- Council of Europe. (nd.). *The Budapest Convention him Cybercrime*.
- Council of Europe. (2001). *Explanatory report to the Convention him Cybercrime (ETS No. 185)*
- Council of Europe. (2022). *Explanatory report to the Second Additional Protocol to the Convention him Cybercrime him enhanced cooperation and disclosure of electronic evidence (CETS No. 224)*.
- Dushi, D., & Bërdufi, N. (2017). Law enforcement and investigation of cybercrime in Albania. *European Scientific Journal*, 13 (12), 576–588. <https://doi.org/10.19044/esj.2017.v13n12p576>
- European Court of Human Rights. (2010). *Kennedy v. the United Kingdom* (Application) no. 26839/05).
- European Court of Human Rights. (2017). *Antović and Mirković v. Montenegro* (Application no. 70838/13).
- European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom* (Applications) nose 58170/13, 62322/14, and 24960/15).
- European Data Protection Supervisor. (2025). *TechDispatch #2/2025: Human oversight of automated decision-making*. European Data Protection Supervisor.
- European Parliament and Council. (2016). *Regulation (EU) 2016/679 of 27 April 2016 on the protection of Sports person with regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88.
- European Parliament and Council. (2022). *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. *Official Journal of the European Union*.
- European Parliament and Council. (2023). *Regulation (EU) 2023/2854 of 13 December 2023 on harmonized rules him fair access to and use of data (Data Act)*. *Official Journal of the European Union*.
- European Parliament and Council. (2024a). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*.
- European Parliament and Council. (2024b). *Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. *Official Journal of the European Union*.
- Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law & Security Review*, 29 (5), 522–530. <https://doi.org/10.1016/j.clsr.2013.07.002>
- Gonçalves, A. (2025). Engineering explainable AI systems for GDPR- aligned automated decision-making : Legal and technical challenges under the GDPR and the EU AI Act. *Standards*, 6 (1), Article 7.
- Hulok, M. (2025). The EU model of AI governance : Regulating artificial intelligence in a multi-layered legal framework. *International Review of Law, Computers & Technology*.
- Information and Data Protection Commissioner. (2025a, July 3). *Data Protection Officer legal obligation for the public and private sector*.
- Information and Data Protection Commissioner. (2025b, July 28). *The trainings for strengthening the capacities of the Data Protection Officer (DPO) has commenced*.
- Information and Data Protection Commissioner. (2025c, April 15). *Public consultation on the set of bylaws drafted by the Office of the Commissioner*.
- Information and Data Protection Commissioner. (2025d, April 30). *Instruction no. 03, dated 30.04.2025, on the processing of personal data from video surveillance systems*.
- Information and Data Protection Commissioner. (2025e, October 6). *Law no. 124/2024 approximates Albanian legislation with the GDPR and the Police Directive*.
- Levitina, A. (2024). Humans in automated decision-making under the GDPR and AI Act. *CIDOB Notes International*.
- Lukács, A., & Vári, G. (2023). GDPR- compliant AI- based automated decision-making in the employment context. *Computer Law & Security Review*, 49.

- National Cyber Security Authority . (2025a, October 24). *The National Cyber Security Strategy 2025–2030 and Action plans are approved* .
- National Cyber Security Authority . (2025b). *National Cyber Security Strategy 2025–2030* .
- National Cyber Security Authority . (2025c). *About us : National Cyber Security Authority* .
- National Cyber Security Authority . (2025d), June 11). *Directive No. 1 on the methodology for risk assessment of information infrastructure following a cyber incident* .
- National Cyber Security Authority. (2025). *National Cyber Security Strategy 2025–2030* .
- Negara , DS (2024). The legal implications of data protection laws , AI regulation , and cybersecurity measures him privacy rights in 2024. *Global International Journal of Innovative Research* , 2 (7).
- Novelli , C., Casolari , F., Hacker , P., Spedicato , G., & Floridi , L. (2024). Generative AI in EU law : Liability , privacy , intellectual property , and cybersecurity . *Computer Law & Security Review* , 55 , 106066. <https://doi.org/10.1016/j.clsr.2024.106066>
- Parliament of the Republic of Albania. (2024). *Law no. 124/2024 On the protection of personal data* .
- Parliament of the Republic of Albania. (2024a). *Law no. 25/2024 On Cybersecurity* .
- Prasetyoningsih, N. (2024). The Potential and Challenges of Implementing the Omnibus Method in Indonesia: Lessons from Other Countries. <https://doi.org/10.56444/jidh.v9i1.5389>