



© 2026 Puravelli et al. This article follows the  Open Access policy of CC BY NC under CC v 4.0.



Submitted: 24/03/2026 - Accepted: 10/05/2026 - Published: 28/09/2026

The Social Fabric of Cybersecurity: Trust, Digital Literacy, and Policy in the Albanian Context

Folitjona Puravelli¹, Anni Dasho Sharko¹, and Agim Alia¹

¹Department of Information and Innovation Technology, Luarasi University, Tirana, Albania
*folitjona.puraveli@luarasi-univ.edu.al

DOI: 10.26417/twg1m37q

Abstract

In the era of surveillance and rapid digital transformation, the protection of personal data has evolved from a technical requirement into a foundational element of social trust and democratic integrity. This article uses Albania as a case study to look at these problems. It talks about big events when personal data was stolen, like the "*patronage database*," the "*salary leaks*", and the "*exposing of vehicle registration details*". The research adopts a qualitative approach, combining legal and policy analysis with an extensive literature review. This framework allows for an in-depth examination of how national legislation aligns or conflicts with the educational and social realities of data protection. The findings show that even while Albania has made progress in aligning its laws, enforcement remains inconsistent and lacks the institutional rigor required for effective implementation, and institutions don't have enough technical and organizational protections. Consequently, individuals continue to be susceptible to the exploitation of personal data for political and economic objectives. This article examines how major data breaches in Albania, uncovered vulnerabilities that extend beyond technical infrastructure. These events reveal deficits in institutional accountability and a politicization of data that erodes trust in public governance. While Albania has sought alignment with European data protection standards, gaps in enforcement and digital literacy persist. This study argues that digital resilience in Albania requires a transition from purely technical fixes to a socio-institutional approach that reinforces transparency, empowers citizens, and protects democratic values.

Keywords: Information Politicization · Institutional Accountability · EU Acquis Alignment · Privacy Rights · State Legitimacy ·

Introduction

Digital transformation has notably reshaped the social, educational, and institutional landscape of contemporary societies. As digital technologies become part of daily life, shaping how people learn, access services, and participate in public life, they also affect the way individuals form trust, relate to institutions, and engage as citizens. Today, global reports highlight that digital change plays a decisive role in shaping social progress, making it essential for societies to develop new skills and adapt their governance and education systems to this evolving context. *"Improving education and skills is a key part of the overall vision for digital transformation in Europe.* (European Commission, 2020, p. 4). *"Ensuring data security and privacy builds trust among stakeholders and complies with legal and ethical standards".* (UNESCO, 2024, p. 22). In this context, cybersecurity is no longer solely a technical matter; it has become a deeply social issue shaped by norms, institutional practices, and the digital skills of citizens.

For developing countries such as Albania, these social dimensions of cybersecurity are especially important. Rapid digitalization has expanded access to information, modernized public administration, and introduced new tools for education and economic participation. Yet research shows that societies with uneven digital literacy and weak institutional safeguards are more vulnerable to cyber harms and data misuse. Data protection is just one aspect of data governance though. One important question relates to the relationship between governments, the data subjects, and the private sector that usually develops the smart education technologies. (OECD, 2021, p.32). In Albania, these vulnerabilities were dramatically revealed through a series of major data breaches, triggering public concern and exposing structural weaknesses in data governance. Reports from both national and international bodies highlight persistent challenges in institutional accountability, transparency, and the enforcement of data protection standards (Commissioner for Personal Data Protection, 2022).

From a social science perspective, these incidents illustrate how digital infrastructures intersect with issues of governance, public trust, and civic responsibility. Theories of social trust emphasize that institutional reliability and transparency are essential for enabling citizens to engage confidently in digital environments. *"General social trust is translated into politically relevant trust. Social life is pervaded with new and expanding threats and hazards of our own making. The more technology is applied to nature and society; the more life becomes unpredictable. The complex interactions of technology as they bear upon nature and society create an ever-larger number of unintended consequences"* (Sztompka, 1999, pp. 12–14).

Zuboff, 2015 (p.75) argues that "big data" is not simply a technological development but a socially constructed system of economic power that forms the basis of surveillance capitalism, a logic of accumulation in which personal data are extracted, analysed, and used to predict and shape human behaviour for profit.

This paper situates the Albanian case within broader debates on the sociology of technology, digital governance, and social trust. It argues that cybersecurity should not be viewed solely as a technical infrastructure, but as a component of the social fabric, shaped by individual competencies, institutional reliability, and societal expectations. By examining the interaction between trust, digital literacy, and policy in Albania, the study highlights the importance of integrated approaches that combine education, institutional reform, and community-level engagement. In this context, Law No. 124/2024 provides a necessary legal framework, yet the shift from “regulation” to “protection” represents a significant social and educational challenge. This paper explores the gap between the law’s objectives and the level of digital literacy required for citizens to effectively enact these protections, emphasizing the need to foster a culture of trust and strengthen competencies to ensure that digital transformation supports democratic development rather than creating new vulnerabilities.

Methodology

This study uses a qualitative case study design to examine the gap between Law No. 124/2024 and the digital skills citizens need to use it effectively. The research is based on: document analysis of the law, and literature on digital literacy and cybersecurity; and thematic analysis of key ideas, regulation, protection, and citizen competence, through sociology of law and digital literacy perspectives. This approach looks at both the law itself and the social and educational conditions needed for it to work. My research question in this paper is to what extent does the gap between Albania’s advanced legal framework (Law No. 124/2024) and the low level of citizen digital literacy affect social trust and the practical protection of personal data?

Literature Review

Digitalization has brought important transformations to public administration, education, and civic life. While it expands access to services and information, research consistently shows that societies with weak institutions, limited digital skills, and low levels of trust face significantly higher exposure to cyber risks, privacy violations, and data misuse.

Theoretical Framework

From a sociological view, Law No. 124/2024 only work if people understand and accept them, as laws alone cannot ensure protection. Digital literacy shows that citizens need not just technical skills but also the ability to think critically and stay safe online. Together, these ideas point to a “protection gap”, where legal rules exist but people lack the skills to use them. Closing this gap requires education and social programs that turn rules into real protection. The “*Patronage Database*” case shows what happens when data is politicized and citizens do not have the knowledge to hold institutions accountable for privacy issues.

Digital Governance, Institutional Capacity, and Trust

The OECD (2020) posits that the quality of digital service delivery is a primary determinant of state-citizen relations. When public institutions fail to meet the digital expectations of the population, the resulting dissatisfaction can significantly diminish trust in government integrity and the efficacy of public policy (p. 14).

Waller & Weerakkody (2016) argue that in order to understand how digitally-enabled transformation can occur, it is important to examine how ICT affects the selection and implementation of policy instruments, shaping both their design and effectiveness. Technology can influence the choice, calibration, and operational use of instruments, reduce costs and enable real-time management information to support policy review and adjustment (p. 5).

According to UNESCO (2019, p. 32), the adoption of artificial intelligence must align with the principles of Internet Universality, which prioritizes human rights and transparency. Without these reference points, digital governance risks alienating the public and facilitating systemic abuses of power, particularly in emerging digital landscapes like Albania's.

"A 2018 report on privacy in the digital age by the High Commissioner for Human Rights defined privacy as: "[...] the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."

1.2. Digital Literacy, Inequality, and Cyber Vulnerability

Digital literacy acts as the primary defence mechanism for both the individual and the state in an increasingly connected society. DiMaggio & Hargittai (2001, p.18) observe that the concept of the *"digital divide"* was useful for scholars and policymakers in the early stages of Internet adoption. However, as Internet access has grown and institutions have evolved, it is necessary to go beyond this framework to fully capture and explain the evolving aspects of digital inequality that persist even as Internet penetration becomes more widespread. This disparity creates vulnerabilities, as citizens with limited skills are more exposed to fraud, manipulation, and data exploitation.

World Bank findings also suggest that populations lacking digital competencies are disproportionately targeted by cyberattacks and scams. The World Development Report 2021 notes that an effective Integrated National Data System (INDS) relies on skilled people at every level: those who generate, manage, and ensure the quality of data; those who staff institutions responsible for safeguarding it; and those who develop, implement, and enforce data strategies, policies, and regulations. Equally important is ensuring that all stakeholders, including government agencies, the private sector, and citizens possess the knowledge and skills to use data responsibly

and hold public and private entities accountable. Achieving this requires strong data literacy across institutions and society as a whole.” (World Bank, 2021, pp. 41–42).

The European Commission (2022, pp. 6-7) further identifies digital skills as a protective factor, showing that countries with more digitally literate populations report fewer cyber incidents and higher levels of trust in e-government services. The DESI 2022 report indicates that although many EU Member States are advancing in digital transformation, the use of critical technologies like artificial intelligence and big data by businesses remains limited, even among leading countries. Low levels of digital skills continue to hinder growth, exacerbate the digital divide, and increase the risk of excluding citizens as essential services move online.

1.3. Cybersecurity as a Social and Institutional Problem

Singer and Friedman (2014) argue that cybersecurity is more about people and institutions than just technology, challenging the idea that software alone can solve the problem (pp. 9–10). This perspective is vital for the Albanian context, where technical software upgrades often outpace the development of human digital competencies.

UNESCO (2023, pp. 11-14). warns that inadequate regulation of digital platforms can lead to privacy violations, political profiling, and large-scale data manipulation. It notes that cyber risks intensify when states lack transparency, strong oversight bodies, and clear accountability mechanisms. Digital platform regulation involves a diverse range of bodies, from existing media regulators to newly established independent authorities, and must be tailored to local contexts while remaining open, transparent, and inclusive of multiple stakeholders. Effective regulatory systems require independence from political and economic pressures, secure and transparent funding, merit-based appointments, accountability mechanisms, and expertise in international human rights law. To maintain impartiality and public trust, regulators should report regularly, disclose conflicts of interest, and avoid post-mandate employment with entities they have supervised. These structural issues are especially relevant for emerging democracies, where institutional independence is still developing. All these factors and structures are very relevant to Albanian context.

1.4. Digitalization, Education, and Societal Capacity

Education is the most effective way to build a society that is resilient against digital threats. Selwyn (2016, p.16) argues that meaningful digital transformation in education can occur only when institutions ensure “equitable access, inclusion, and critical digital pedagogy”. In essence, the term ‘educational technology’ goes beyond the physical tools and devices used in learning environments. Digital technologies should not be considered merely as background equipment in schools or classrooms. Rather, these technologies are deeply intertwined with social, cultural, economic, and political dimensions, meaning they are not neutral instruments and their use in

education is shaped by broader societal factors. Without these conditions, digital tools may widen social inequalities rather than reduce them.

The European Commission's Digital Education Action Plan similarly emphasizes that cybersecurity awareness, data protection literacy, and digital citizenship should be integrated into all levels of education to prepare students for safe participation in a digital society. Initiated in 2021, the EU's Structured Dialogue on digital skills aims to harmonize Member State policies to reach 2030 targets: ensuring 80% of the population possesses basic digital literacy and expanding the ICT workforce to 20 million specialists ((European Commission 2022, p. 27).

World Bank studies highlight that education systems without coordinated strategies for digital transformation face gaps in access, privacy protection, and online safety. The pandemic has highlighted the urgent need to address digital divides and the crucial roles of teachers and parents in supporting learning. Many countries were unprepared for such a crisis, revealing gaps in connectivity, access to devices, and teacher training. Closing these divides requires investments in technology, professional development, and ensuring equitable access to devices and internet at home or in the community. Additionally, resilience in education depends on actively involving parents, providing them with guidance and support to help their children learn effectively. Strengthening these elements can make education systems more equitable, flexible, and capable of supporting learning for all students, everywhere (World Bank, 2020, p. 9). This suggests that Albania's cybersecurity challenges are directly linked not only to institutional weaknesses but also to limited public digital awareness.

The Albanian legal framework for the protection of personal data

2.1. Legal and Constitutional Architecture of Data Protection in Albania

Albania's cybersecurity challenges cannot be understood without examining the legal and constitutional framework governing privacy and personal data. The Albanian Constitution establishes privacy as a fundamental right, placing the protection of personal data at the heart of democratic governance. Article 35 guarantees that no individual may be compelled to disclose personal information except as provided by law, and it affirms citizens' rights to access, correct, or delete personal data collected unlawfully. Article 36 further secures the confidentiality of all forms of communication, recognizing that data protection is inseparable from communication privacy in a digital society (Constitution of the Republic of Albania, 1998).

Albania's commitment to privacy is reinforced by its ratification of key European instruments, including the European Convention on Human Rights and the Convention on automatic processing of personal data. Over the past decade, this framework has evolved through extensive legislative alignment with EU standards.

2.2 Law No. 124/2024: Modernizing Albania's Data Protection Regime

The adoption of Law No. 124/2024 "On the Protection of Personal Data" represents the most significant reform in Albania's data-governance landscape. The law repeals the outdated Law No. 9887/2008, which had been based on Directive 95/46/EC, a framework repealed long ago in the EU. The new law and the Law 49/2022 harmonize Albania's legislation with the General Data Protection Regulation (GDPR), the Law Enforcement Directive (Directive (EU) 2016/680), and the Regulation (EU) 2016/679) thereby strengthening transparency, accountability, controller obligations, and citizens' rights (European Commission, 2023). Law no. 124/2024 serves as a critical sociotechnical case study; while it achieves high legislative maturity by aligning with the GDPR, it simultaneously exposes a profound 'protection gap' between formal state obligations and the actual digital literacy of the citizenry. The implementation of Law no. 124/2024 serves as a focal point for this analysis, where several factors made the reform essential:

Alignment with EU standards. European Commission progress reports (2018–2023) consistently found gaps in Albania's data-protection regime, emphasizing the need for harmonization to ensure adequate safeguards and compatibility with EU data-exchange systems.

Expansion of individual rights. The old law lacked modern guarantees, including the right to erasure, data portability, and clear rules governing profiling and automated decision-making.

Weak enforcement powers. The supervisory authority lacked the mandate and sanctioning capacity necessary to deter violations or investigate systemic breaches.

Outdated institutional obligations. Public and private controllers were not required to conduct data-protection impact assessments, implement privacy-by-design, notify breaches, or appoint Data Protection Officers.

The transition from the outdated Law no. 9887/2008 to the modernized Law no. 124/2024 highlights the paradox of digital governance in post-transition Albania: the law provides the tools for transparency, yet the *'Patronage and 'Salary'* leaks demonstrate that without institutional accountability and public awareness, these legal tools remain symbolic. Law no. 124/2024 addresses these gaps by introducing GDPR equivalent obligations, expanding the definition of sensitive data (e.g., genetic, biometric, sexual orientation), strengthening rules for data transfers, and enhancing the powers of the Commissioner for the Right to Information and Personal Data Protection. The new regime also establishes a modernized system of administrative sanctions calibrated to the Albanian economic context.

2.3 A Framework Misaligned with Practice

Despite this strong legal framework, the series of large-scale data breaches in 2021, *patronage lists*, *salary leaks*, and *vehicle-registration leaks*, illustrated a profound

implementation gap. While the law is robust on paper, enforcement remains inconsistent, and institutional accountability is weak. The Commissioner has the legal authority to investigate and sanction institutions, as demonstrated in Decision No. 41 of August 23, 2021, which fined the General Directorate of Taxes for failing to comply with data-protection obligations. Yet, in no major incident were individual perpetrators definitively identified or prosecuted.

This disconnects between formal legal guarantees and practical implementation has contributed to declining public trust in digital governance. It illustrates a broader pattern: cybersecurity failures in Albania are not solely technological but deeply institutional, political, and social. Without consistent enforcement, the constitutional right to privacy remains vulnerable, and digitalization risks undermining rather than strengthening democratic legitimacy.

This legal analysis reinforces the central thesis of the article: cybersecurity in Albania must be understood as part of a social fabric shaped by trust, literacy, and governance. Albania possesses an advanced legislative framework aligned with European norms, yet systemic vulnerabilities persist due to limited institutional capacity, insufficient cyber-awareness, and politicization of data governance. The gap between law and practice mirrors gaps in public trust, digital literacy, and policy enforcement, all of which interact to shape citizens' behaviour and overall cyber-resilience.

The Albanian Data-Leak Scandals as Evidence of Systemic Vulnerabilities

3.1. The Patronage Database Controversy

One of the most serious data-protection failures in Albania emerged days before the April 2021 parliamentary elections, when a database containing personal information on nearly 900,000 citizens was leaked to the public. The 2021 '*patronageists*' leak, involving nearly 900,000 citizens, serves as a stark example of what Transparency International (2021) characterizes as the weaponization of state data for political gain. Rather than a mere data breach, this incident represented a systemic failure of privacy, where sensitive personal identifiers were converted into tools for political profiling.

The leak triggered widespread public outrage, given that it violated the right to privacy and raised concerns about the integrity of the electoral process. More than 160 citizens filed legal complaints accusing the Socialist Party of unlawful processing of personal data, while the Prosecutor's Office opened a criminal investigation into unauthorized access to state databases. Civil society organizations argued that the database was likely extracted from public institutions, most notably the tax administration, for political profiling purposes.

The scandal gained significant international attention. Amnesty International (2022) reported that the Socialist Party used the illegally obtained dataset for electoral purposes, while Transparency International (2021) warned that the creation of a

political-profiling database containing information on more than 910,000 voters constituted a misuse of state resources and called for immediate investigation.

Domestically, the incident exposed major institutional shortcomings. An investigation by the Commissioner for the Right to Information and Personal Data Protection concluded that the General Directorate of Taxes (GDT) had shown a “lack of cooperation” and a “marked ignorance” of data-protection legislation. In Decision No. 41 of August 23, 2021, the Commissioner fined the GDT 1,000,000 lekë for violating Article 32 of the Law on Personal Data Protection and ordered the implementation of ISO/IEC 27001 standards and other organizational safeguards. Nevertheless, the investigation did not identify any individual perpetrators, reinforcing the perception that violations of data protection laws in Albania rarely result in personal accountability. Despite being cited internationally as a major human-rights breach, the case ended without a full criminal resolution.

3.2. Leak of Salary Information

In late 2021, Albania faced an even more extensive breach when a database containing salary information for approximately 630,000 citizens was leaked through social media and messaging apps. The dataset included names, gross monthly salaries, job titles, employer names, and, in some cases, social security numbers. A second file containing mobile phone numbers for nearly 900,000 individuals circulated shortly afterward.

Investigations revealed that the salary data corresponded to internal records of the Tax Administration, specifically the Directorate of Large Taxpayers. The Tirana Prosecutor’s Office initiated criminal proceedings for “abuse of office” and “interference with computer data,” leading to the arrest of four individuals, two IT specialists and two collaborators, accused of downloading and selling the data to private companies.

From the perspective of citizen security, the leak generated multiple risks. Public exposure of salary and identification data can facilitate identity theft, extortion, financial fraud, and highly detailed economic profiling. Several individuals listed were employees of national security institutions, thereby increasing the severity of the breach.

Institutionally, the incident revealed profound deficiencies in Albania’s digital governance: weak access controls, lack of audit trails, minimal internal monitoring, and an inability to determine where the data originated or how it was disseminated. The breach severely damaged public trust in state digital systems and exposed the urgent need for a coordinated national cybersecurity strategy.

3.3. Leak of Vehicle License-plate Information

In December 2021, a third major cybersecurity incident occurred when a file containing personal and vehicular information on more than 530,000 car owners was

leaked online. The dataset included names, license-plate numbers, car models, colours, and chassis numbers; some accounts claimed identity-card details were also included. Coming after the patronage and salary leaks, the incident intensified public uncertainty and weakened confidence in state institutions.

The Tirana Prosecutor's Office seized servers from several agencies with access to vehicle-registration data, while the General Directorate of Road Transport Services denied that the leak originated from its system. The National Agency for the Information Society (AKSHI), responsible for managing government IT infrastructure, drew criticism for inadequate safeguards. AKSHI representatives stated that the platform used Microsoft technologies and announced measures such as blockchain-based access tracking to strengthen system security.

This leak demonstrated how the exposure of combined personal and vehicle data could facilitate profiling, tracking, fraud, and other criminal activities. Moreover, the fact that the case remains unresolved illustrates ongoing deficiencies in institutional transparency and accountability, further eroding public trust.

Taken together, these three consecutive data scandals were not isolated technological failures but manifestations of deeper structural issues at the intersection of public trust, digital literacy, institutional capacity, and cybersecurity governance in Albania. They revealed a social ecosystem in which weak data governance, limited public awareness, and politicization of digital systems combine to generate widespread vulnerability. The following sections examine how these breaches shape citizens' trust in digital governance, influence digital literacy and risk perception, and expose critical policy gaps in the Albanian cybersecurity framework.

Discussion and Conclusion

This study illustrates that while Albania has made significant progress in developing a legal and institutional framework for data protection and cybersecurity, the broader social and educational dimensions remain underexplored. As a case study in this article, Law no. 124/2024 reveals that regulatory alignment is insufficient for cyber-resilience. The recurring scandals involving vehicle registration and personal IDs suggest that the protection gap is not a failure of the legal text itself, but a failure of the social and educational systems to embed these rights into everyday practice. Laws and regulations, such as the recent Law no. 124/2024 on the protection of personal data, provide a formal structure for safeguarding individual rights. However, the effectiveness of these measures is closely tied to public awareness, digital literacy, and the capacity of individuals and institutions to apply these protections in daily life.

From this article I noticed that the social impact of data protection extends beyond compliance: breaches of personal data can erode community trust and influence citizens' willingness to engage with digital services. Likewise, integrating cybersecurity and data protection topics into educational curricula can empower students to navigate the digital world safely, fostering both personal responsibility

and collective resilience. The covid 2019 highlighted the urgency of addressing digital inequalities, showing that access to devices, connectivity, and digital skills is critical for educational participation and for maintaining equitable learning opportunities.

Albania's experience can serve as a case study for global discussions on cybersecurity and digital education, and this case shows that while legal and technical structures are necessary, they are not sufficient. Policies must also engage social and educational considerations, emphasizing the development of digital competencies, public awareness campaigns, and institutional accountability. By linking legal frameworks with educational initiatives, societies can build trust, reduce vulnerabilities, and promote inclusive digital participation.

The findings of this study demonstrate that in a post-transition society like Albania, legislative maturity does not automatically result in a resilient cybersecurity ecosystem. While the implementation of Law No. 124/2024 represents a high degree of legal maturity by aligning with the EU GDPR, a significant protection gap remains due to the lagging state of public digital literacy and institutional accountability.

The protection gap identified through this qualitative analysis manifests within the Albanian cybersecurity ecosystem through three distinct mechanisms:

Erosion of Social Trust: Frequent leaks of personal data, ranging from political lists to private salaries have turned digital tools into a source of public anxiety. This study finds that when laws exist but fail to catch or punish violators, the public views these regulations as just for show, which severely damages trust in government institutions.

The Literacy-Vulnerability Loop: High-level legislation assumes a "digitally competent" citizen. However, without integrated educational strategies, the complexity of modern data rights leaves the average citizen unable to enact the protections the law provides, creating a landscape where technical infrastructure is secure but the human element remains a critical vulnerability.

Politicization of Data: In post-transition contexts, the lack of digital literacy allows for the politicization of information. The patronage database controversy proves that without a socially embedded culture of privacy, personal data can be weaponized for political objectives, undermining democratic legitimacy.

In conclusion, ensuring the effectiveness of data protection and cybersecurity requires an integrated approach that combines legal reform with social and educational strategies. Digital literacy, public engagement, and institutional capacity-building are essential to transform legislation into meaningful protections and to prepare citizens for a rapidly evolving digital landscape. Albania's reforms provide valuable insights, but their true impact will be determined by the ability of society to embed these protections into everyday practice, education, and public understanding.

Recommendations for Policy and Education

To transition from a paper-based protection regime to a resilient ecosystem, this study proposes an integrated approach:

Pedagogical Integration: Building on Selwyn's (2016, p. 171) observation that teaching is shifting towards a mentoring and networking role, curricula should integrate cybersecurity and data privacy through Critical Digital Pedagogy to empower students as active participants in digital networks and responsible digital citizens."

Institutional Transparency: Digital governance must include "privacy-by-design" and blockchain-based audit trails to restore public trust through technical accountability.

Community-Level Awareness: Public campaigns should focus on the social impact of data protection, moving beyond legal jargon to explain how privacy safeguards community-level resilience.

Ultimately, Albania's experience serves as a global case study: technical and legal structures are necessary, but they are not sufficient. Ultimately, the efficacy of Albania's digital transformation hinges not on the complexity of its code, but on the depth of its social and educational integration

Bibliography

- [1] Amnesty International. (2022). *Amnesty International report 2021/22: The state of the world's human rights*. <https://www.amnesty.org>
- [2] Commissioner for Personal Data Protection. (2022). *Annual report on the state of personal data protection in Albania*. <https://idp.al>
- [3] Constitution of the Republic of Albania. (1998). *Law No. 8417, dated 21.10.1998*. <http://www.qbz.gov.al>
- [4] DiMaggio, P., & Hargittai, E. (2001). *From the 'digital divide' to 'digital inequality': Studying internet use as penetration increases* (Working Paper No. 15). Princeton University Center for Arts and Cultural Policy Studies. <https://www.princeton.edu/~artspol/workpap15.html>
- [5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals by competent authorities for law enforcement purposes. (2016). *Official Journal of the European Union*, L 119.
- [6] European Commission. (2018–2023). *Albania 2018–2023 progress reports*. <https://neighbourhood-enlargement.ec.europa.eu>
- [7] European Commission. (2020). *Shaping Europe's digital future*. Publications Office of the European Union. <https://doi.org/10.2759/091014>
- [8] European Commission. (2022). *Digital Economy and Society Index (DESI) 2022*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=100504
- [9] Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale. (2021). *Vendimi nr. 41, datë 23.08.2021*. <https://www.idp.al>

- [10] Law no. 49/2022 on the ratification of the amending protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (2022). <http://www.qbz.gov.al>
- [11] Law no. 124/2024 on the protection of personal data. (2024). <http://www.qbz.gov.al>
- [12] OECD. (2020). *Digital government index: 2019 results* (OECD Public Governance Policy Papers No. 03). OECD Publishing. <http://dx.doi.org/10.1787/4de9f5bb-en>
- [13] OECD. (2021). *OECD digital education outlook 2021: Pushing the frontiers with AI, blockchain, and robots*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/06/oecd-digital-education-outlook-2021_0f1487d9/589b283f-en.pdf
- [14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119.
- [15] Selwyn, N. (2016). *Education and technology: Key issues and debates* (2nd ed.). Bloomsbury Academic.
- [16] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- [17] Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.
- [18] Transparency International. (2021). *Albania: 2021 country report*. <https://www.transparency.org>
- [19] UNESCO. (2019). *Steering AI and advanced ICTs for knowledge societies: Brochure* [Brochure].
- [20] UNESCO. (2023). *Guidelines for regulating digital platforms*. <https://unesdoc.unesco.org/ark:/48223/pf0000386740>
- [21] UNESCO. (2024). *Six pillars for the digital transformation of education: A common framework* (ED-2024/WS/23). <https://unesdoc.unesco.org/ark:/48223/pf0000391299>
- [22] Waller, P., & Weerakkody, V. (2016). *Digital government: Overcoming the systemic failure of transformation* (Working Paper No. 2). Brunel University Press. <https://bura.brunel.ac.uk/bitstream/2438/12732/4/FullText.pdf>
- [23] World Bank. (2020). *Realizing the future of learning: From learning poverty to learning for everyone, everywhere*. <https://openknowledge.worldbank.org/handle/10986/34165>
- [24] World Bank. (2021). *World Development Report 2021: Data for better lives*. <https://openknowledge.worldbank.org/entities/publication/11f58a71-4b43-59c4-9e5b-c11abd4c5350>

- [25] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89.
<https://doi.org/10.1057/jit.2015.5>