Assessing the Security of Privacy Rights and Data Protection in Albania: A Critical Analysis Within the European Legal Framework

Lecturer **Heliona MIÇO BELLANI**[1]
Msc. **Egla LECI**[2]

Abstract

This paper adopts an analytical approach to the regulation of the right to privacy within the normative foundations of the European Union's General Data Protection Regulation (GDPR), offering a comparative perspective with the Albanian legal framework. The paper elucidates the reasons that led to the enforcement of the GDPR and delves into the challenges arising in the field of data protection due to technological advancements. The comprehension of the GDPR approach will serve as a benchmark for comparing the progress of the implementation of data protection in Albania. This discussion will underscore the ongoing process of legislation harmonization with the EU 'Acquis communautaire', aiming to pinpoint potential disparities between the General Data Protection Regulation (GDPR) and the Albanian Law on Data Protection. The paper will scrutinize various data protection breaches occurring from 2021 to 2022 in Albania, events that cast doubt on the legal framework concerning the right to privacy and its practical implementation. These instances of data breaches illuminate the challenges within the legal framework and its execution, underscoring the vulnerability of the state in the face of technological advancements. This emphasizes the imperative for proactive measures to enhance the protection of personal data and the right to privacy.

Keywords: *the right to privacy, GDPR, data protection, European Union, Albania.*

JEL Classification*: K38*

DOI: 10.62768/TBJ/2024/14/4/12

Please cite this article as:	**Article History**
Miço (Bellani), Heliona & Egla Leci, 'Assessing the Security of Privacy Rights and Data Protection in Albania: A Critical Analysis Within the European Legal Framework', *Juridical Tribune – Review of Comparative and International Law* 14, no. 4 (December 2024): 721-748.	Received: 04 September 2024 Revised: 05 October 2024 Accepted: 02 November 2024

1. Introduction

The right to privacy is a fundamental human right recognized and safeguarded by numerous international agreements and legal systems. Historically, privacy has been an intrinsic part of human life, deeply rooted in various cultural, legal, and philosophical

[1] Heliona Miço (Bellani) - lecturer of Public and Constitutional Law in the Faculty of Law and Social Sciences, EPOKA University, Tirana, Albania, and a researcher in the field of human rights, the right to education, quality assurance, and social inclusion. hmico@epoka.edu.al. ORCID 0000-0002-2398-7798.
[2] Egla Leci - Junior Lawyer at Tonucci and Partners Law Firm, Tirana, Albania, egla.leci2000@gmail.com.

traditions. In Western developed nations and the global north, the concept of privacy has evolved through distinct trajectories, often linked to both tangible and intangible dimensions. Initially, privacy was associated with physical spaces, such as the home, where protection was contingent upon accessibility to others[3]. In a broader sense, privacy has also been perceived as secrecy or confidentiality, where an intrusion is defined by a violation of mutual trust[4].

This concept of privacy is not new; it has been discussed since ancient times. For instance, Cicero, in his Treatise of State Offices, pondered the responsibilities of government in protecting the sanctity of both public and private spheres[5]. Ancient Roman law insisted on a sharp distinction between private spaces and state matters, asserting that government power to trespass on private property, search private spaces, or seize personal belongings must be severely limited by law. These restrictions placed privacy within the intellectual framework supporting due process and the rule of law[6].

Remarkably, the right to privacy was recognized as an international human right before it was enshrined in any state constitution. After World War II, as the international human rights system was being devised, state constitutions primarily protected specific aspects of privacy, such as the inviolability of the home, correspondence, and the protection against unreasonable body searches[7]. No state constitution at that time contained a comprehensive guarantee of the right to privacy as an overarching principle. This development was unusual since international human rights typically evolve from well-established national rights. In contrast, the right to privacy emerged on the international stage without a precedent in national constitutions, creating something entirely new[8].

The right to privacy is enshrined in the Universal Declaration of Human Rights, which specifically recognizes and safeguards this right. Privacy rights began to be formally recognized in statutes during the 1970s, particularly through legislation in the United States and Europe[9]. A classic definition was provided by Louis Brandeis and

---

[3] Norberto Nuno Gomes de Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights*"*. *Privacy and Identity Management for Life*: 6th IFIP WG PrimeLife International Summer School, Helsingborg, Sweden, August 2010, Revised Selected Papers. IFIP Advances in ICT, Vol. 352, Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (Eds.), Springer (2011), pp. 90-107. Retrieved from SSRN: https://ssrn.com/abstract=2033225.

[4] Global Privacy Assembly ("GPA") Policy Strategy Workgroup Three ("PSWG3"), *PSWG3: Privacy and data protection as fundamental rights: A narrative*. (2022). https://globalprivacyassembly.org/wp-content/uploads/2022/05/PSWG3-Narrative-Final.pdf.

[5] Cicero, *On Obligations: De Officiis (Oxford World's Classics)*, translated P. G. Walsh. 2008, Book I, sec. 85, p. 30 31.

[6] Bernardo Periñán, "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*"*, *American Journal of Legal History*, Volume 52, Issue 2, April 2012, Pages 183–201, https://doi.org/10.1093/ajlh/52.2.183.

[7] Oliver Diggelmann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", *Human Rights Law Review*, Volume 14, Issue 3, September 2014, Pages 441–458, https://doi.org/10.1093/hrlr/ngu014.

[8] Daniel J. Solove, "Understanding Privacy", (Harvard University Press, May 2008), *GWU Legal Studies Research Paper* No. 420, *GWU Law School Public Law Research Paper* No. 420, Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888.

[9] Daniel J. Solove, "The Limitations of Privacy Rights". *Notre Dame Law Review*. 2023, Vol 98, Issue 3,

Samuel Warren, who described privacy as "the right to be let alone," capturing the fundamental idea that most people associate with privacy and representing its core essence.[10] The legal concept of privacy as a fundamental right and a means to secure other basic rights is rooted in liberal ideas that view privacy primarily as a protective barrier against state intrusions. In addition to this negative, defensive aspect of privacy, Westin[11] proposes a more positive interpretation, where privacy empowers individuals to exercise control over their personal information[12]. There are two fundamental, yet competing concepts of privacy. On one hand, privacy is viewed as the ability to distance oneself from society, emphasizing the right to be left alone (privacy as freedom from societal intrusion). On the other hand, privacy is also seen as a means of safeguarding essential community values, such as those related to intimate relationships or public reputation (privacy as dignity). These core concepts often compete with, and sometimes even contradict, one another[13]. However, a generally recognized definition of privacy does not exist.

Over time, the significance of privacy has only grown, particularly with the advent of the digital age. Individual privacy rights form the foundation of most information privacy and data protection laws[14]. Since the 1970s, legislative bodies in Europe and North America have addressed growing concerns about the effects of computers on data collection, integration, and utilization by enacting protective laws. These laws are primarily designed to regulate how governments collect, use, and share personal information through the implementation of codes of fair information practices[15]. Privacy concerns have escalated rapidly, especially as technological advancements have increasingly threatened individuals' control over their personal information. As nations become more digitally advanced, the likelihood of data breaches and privacy violations inevitably increases[16].

Privacy encompasses various dimensions, including informational privacy, bodily integrity, territorial privacy, and communication confidentiality, making it an overarching concept that protects a broad range of human activities[17]. Informational

Article 1, https://scholarship.law.nd.edu/ndlr/vol98/iss3/1?utm_ source=scholarship.law.nd.edu%2Fndlr%2Fvol98%2Fiss3%2F1&utm_medium=PDF&utm_campaign=PDFCoverPages.

[10] David H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection". *Case Western Reserve Law Review*, Vol. 41, Issue 3, (1991) Retrieved from https://scholarlycommons.law.case.edu/caselrev/vol41/iss3/14.

[11] Alan. F Westin, "Privacy and Freedom", *Washington and Lee Law Review*. Vol 25, Issue 1, Article 20, Spring 3-1-1968. Retrieved from https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com.

[12] Philip Schütz and Michael Friedewald, "Privacy: What Are We Actually Talking About? A Multidisciplinary Approach." *Privacy and Identity Management for Life* 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School Helsingborg, Sweden, August 2-6, 2010. Revised Selected Paper. Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen Ronald Leenes, Ge Zhang (Eds.).

[13] Oliver Diggelmann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", p. 442

[14] Daniel J. Solove, "The Limitations of Privacy Rights". p 977.

[15] David H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection", p. 834.

[16] Jonathan W. Z. Lim and Vrizlynn L. L. Thing, "Toward a Universal and Sustainable Privacy Protection Framework". *Digital Government: Research and Practice*, Vol. 4, No. 4, Article 21. Publication date: December 2023. https://doi.org/10.1145/3609801.

[17] Bart van der Sloot, "Do privacy and data protection rules apply to legal persons and should they? A

privacy, a key aspect closely related to data protection, specifically refers to an individual's right to control their personal data and determine how it is collected, processed, and utilized.[18] However, in the late 20th century, as privacy and data protection came under unprecedented attack[19], this expectation began to seem increasingly quaint. The need to protect privacy and the right to data protection has become more pressing, necessitating robust legal frameworks to guard against the myriad ways in which privacy and data protection can be infringed upon in both the digital and physical realms.

1.1. Methodological framework

The digital era's challenges to data protection vary across different national laws and their implementation. As a candidate for European Union membership since 2014, Albania is required to harmonize the legal framework with the EU's Acquis Communautaire. Therefore, the article aims to analyze the harmonization of Albanian legislation regarding the right to privacy with a special focus on data protection, with the European legal framework and to assess whether Albanian law is aligned with the EU's General Data Protection Regulation (GDPR). The ultimate goal is to identify the underlying causes of the serious data breaches that occurred between 2021 and 2022 in Albania, in the light of legal architecture on data protection and corresponding authorities. By paralleling the evolution of privacy protection within the EU framework in the digital context, this article aims to address the research question: In light of technological advancements, are the challenges related to data protection primarily due to the need for legislative improvements, better implementation of existing laws, or the lack of professionalism of individuals managing the technological systems that store personal data?

The article begins by exploring the evolution of privacy and data protection within the European context, providing an overview of digital privacy protection on both international and European stages. It then examines the reasons behind the implementation of the EU General Data Protection Regulation (GDPR), emphasizing its significance in shaping data protection standards. Next, the focus shifts to Albania, where the legal framework for data protection is critically analyzed. The discussion traces the development of privacy and data protection rights in Albania since the 1990s, followed by a thorough evaluation of the Law "On the Right to Information and Protection of Personal Data." The analysis then compares the Albanian legal framework with the GDPR, assessing how closely aligned or divergent it is from the European standards. The article also delves into significant data breaches in Albania, highlighting

proposal for a two-tiered system.". *Computer Law and Security Review.* Vol 31, Issue 1. February 2015, pp 26-45. Retrieved from https://doi.org/10.1016/j.clsr.2014.11.002.

[18] Paulo Campanha Santana and Faiz Ayat Ansari, "Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India". *Journal of Liberty and International Affairs*. Volume 9, Number 3, 2023. eISSN 1857-9760. DOI: https://doi.org/10.47305/JLIA2393555cs.

[19] Jonathan W. Z. Lim and Vrizlynn L. L. Thing, "Toward a Universal and Sustainable Privacy Protection Framework".

the security failures. The analysis of Albanian data protection legislation in comparison with the European legal framework, along with the examination of data breaches, will highlight the need for aligning Albanian laws more closely with the EU Acquis. This alignment is not only necessary in terms of drafting but, more importantly, in terms of effective implementation and raising awareness. Finally, the article concludes by summarizing the findings and reflecting on the implications of the legal and security issues discussed.

Regarding the methodology, the article employs a comparative legal analysis approach to assess the alignment of Albanian data protection laws with the GDPR and international standards. The research relies on a combination of primary and secondary sources, including legal texts, government reports, case studies of data breaches, and academic literature, to gather comprehensive data. The analysis is guided by an established analytical framework that evaluates the extent of legal harmonization and the effectiveness of implementation, ensuring a thorough examination of how Albanian legislation measures up to European and international benchmarks.

2. The right to privacy and data protection in European context

2.1. A brief overview of the protection of digital privacy on the international and European scene

The protection of privacy is rooted in a multitude of legal acts issued by various international organizations, typically articulated through the proclamation of a bill of rights. These acts, when implemented, enable the safeguarding of privacy at international, regional, and domestic levels. This process occurs through the reception and adaptation of international and regional standards into domestic legal frameworks.

A significant, albeit indirect, affirmation of the right to digital privacy is found in the Universal Declaration of Human Rights (UDHR)[20], which was approved by the United Nations General Assembly in 1948. Article 12 of the UDHR asserts that "No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." This clause has been interpreted to include the right to privacy as a fundamental human right[21].

Preceding the explicit recognition of the right to privacy in international law is the International Covenant on Civil and Political Rights (ICCPR)[22], an international human rights treaty of the United Nations that entered into force in 1976. Article 17 of the ICCPR envisions the right to be free from arbitrary or unlawful interference with one's privacy, family, home, and correspondence. This provision encompasses protection against unlawful surveillance, wiretapping, searches, and other forms of

[20] Universal Declaration of Human Rights, GA Res 217A(III), 10 December 1948, A/810 at 71. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[21] Oliver Diggelmann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", p. 443

[22] International Covenant on Civil and Political Rights, adopted on 16 December 1966, by General Assembly resolution 2200A (XXI). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

interference that infringe upon an individual's right to privacy. The ICCPR also underscores the necessity of legal protection against any attacks on a person's reputation or honor, implying that individuals whose privacy rights are violated have the right to seek legal redress and compensation. Apart from being a legally binding document, Article 17 of the ICCPR not only reiterates the right to privacy but also expands on it by explicitly prohibiting "arbitrary or unlawful interference" with an individual's privacy, family, home, or correspondence. It also emphasizes the need for legal protection against such interferences and attacks on honor and reputation. This detailed language provides clearer obligations for state parties to enact and enforce laws that protect privacy rights[23].

The European Convention on Human Rights (ECHR)[24] explicitly safeguards the right to privacy under Article 8, which guarantees the fundamental human right to respect for one's private and family life, home, and correspondence. This right includes the protection of personal data, positioning the right to privacy as an overarching "umbrella" right that intersects with various legal domains. Any interference with the right to privacy is permissible only when it is authorized by law and necessary to protect broader societal interests[25]. In this article, the right to privacy is analyzed specifically within the context of data protection. Article 8 of the ECHR covers the right to respect for private life, home, and correspondence, with the European Court of Human Rights (ECtHR) interpreting this provision broadly to encompass a wide array of privacy-related issues.

In its case law, the ECtHR has consistently expanded the scope of Article 8 to cover broader interpretations of private life. For instance, in *Denisov v. Ukraine [GC]*[26], the Court asserted that the concept of private life is not confined to an "inner circle" where a person is free to live privately, isolated from the external world. Similarly, in *Bărbulescu v. Romania [GC]*[27] and *Botta v. Italy*[28], the Court emphasized that the right to a "private social life" includes the freedom to form and develop relationships with others and with the outside world. Moreover, in *Axel Springer AG v. Germany [GC]*[29], the Court articulated that the term "private life" is broad and not easily definable,

---

[23] Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties". *International Journal of Law and Information Technology*, Vol 6, Issue 3, pp 247-284, 1998. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=915065#.

[24] The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), as amended. Council of Europe. Rome, 4.XI.1950. Retrieved from https://www.echr.coe.int/ documents/ convention_eng.pdf.

[25] Ali Alibeigi, Abu Bakar Munir and MD. Ershadul Karim, "Right to Privacy, A Complicated Concept to Review" *Library Philosophy and Practice (e-journal).* 2841. (2019). Retrieved from https://digital commons.unl.edu/libphilprac/2841 or https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3537968.

[26] European Court of Human Rights, Case of Denisov v. Ukraine (25 September 2018), Strasbourg Application no. 76639/11.

[27] European Court of Human Rights, Case of Bărbulescu v. Romania (5 September 2017), Strasbourg, (Application no. 61496/08).

[28] European Court of Human Rights, Case of Botta v. Italy (24 February 1998), Strasbourg, (153/1996/772/973).

[29] European Court of Human Rights, Case of Axel Springer AG v. Germany (7 February 2012), Strasbourg, (Application no. 39954/08).

encompassing various aspects of an individual's identity, such as their name, sexual orientation, gender identity, and the right to control their image. This expansive interpretation includes the principle that personal information should not be made public without the individual's consent, which is particularly relevant in the digital age.

Due to the diverse regulatory frameworks across numerous European countries, there was a pressing need for harmonization to ensure compatibility among national data protection laws[30]. To address this, the Council of Europe—an intergovernmental organization based in Strasbourg, France—drafted and adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in 1981[31]. This convention became the first legally binding international instrument dedicated to protecting personal data. Convention No. 108 aims to regulate cross-border data flows and to protect individuals from abuses in data collection and processing. It establishes fundamental rights for individuals, such as the right to access, rectify, or erase their personal data when it has been processed unlawfully. Article 5 of the Convention requires that personal data be processed fairly, securely, and solely for specific and legitimate purposes[32].

In response to the evolving nature of cyber threats, the Convention on Cybercrime (the "Budapest Convention") represents another crucial international treaty addressing both substantive criminal law and procedural law aspects of cybercrime[33]. The Budapest Convention, adopted in 2001, defines several cyber offenses, including unauthorized access, unauthorized interception, data and system interference, computer-related fraud, copyright infringement, and child pornography.

Beyond the instruments of the Council of Europe, the European Union (EU) has developed a comprehensive body of laws to protect privacy and personal data, reflecting its foundational values of human rights and the creation of a single market. The Charter of Fundamental Rights of the European Union (CFR),[34] a key document in the EU's legal framework, outlines the fundamental rights and freedoms of individuals within the Union. Article 8 of the Charter guarantees the right to privacy, including respect for one's home, communications, and family life, and mandates the protection of personal data. The CFR reinforces that personal data must be processed fairly for specified purposes with the consent of the individual concerned, by assigning specific

[30] Oskar J. Gstrein and Anne Beaulieu, "How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches". *Philosophy & Technology* (2022) 35: 3. https://doi.org/10.1007/s13347-022-00497-4.

[31] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe, Strasbourg 28/01/1981, European Treaty Series - No. 108. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

[32] Jörg Ukrow, "Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108." *European Data Protection Law Review*, 2018, 4(2), 239–247. https://doi.org/10.21552/edpl/2018/2/14.

[33] Convention on Cybercrime (ETS No. 185). Council of Europe Budapest 23/11/2001. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

[34] Charter of Fundamental Rights of the European Union 2012/C 326/02. Official Journal of the European Union, 26.10.2012. C 326/391. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

characteristics to the right to data protection, distinguished from the right to privacy[35]. Thus, while the right to data protection can be seen as an extension of the right to privacy, particularly in the context of informational privacy, it addresses specific challenges posed by the digital age and data-centric societies[36]. The relationship between these two rights is complementary; the right to data protection serves as a crucial mechanism to safeguard the broader right to privacy, particularly in contexts involving personal data processing.

Building on these principles, the EU has established a robust data protection framework that includes several landmark regulations and directives. The European Convention on Human Rights (ECHR) serves as a foundational influence, particularly Article 8, which protects the right to privacy and has been extensively interpreted by the European Court of Human Rights to encompass various aspects of private life, such as the right to personal data protection. The principles enshrined in the ECHR have been further developed in the EU's legal framework, including the Directive 95/46/EC[37] and the General Data Protection Regulation (GDPR)[38].

Adopted in 1995, Directive 95/46/EC aimed to harmonize data protection laws across EU Member States, ensuring a common standard of protection for personal data while supporting the free flow of information within the single market. The Directive introduced several key principles of data protection, such as transparency, legitimate purpose, and proportionality, and established the rights of data subjects, the roles and responsibilities of data controllers and processors, and guidelines for cross-border data flows. Moreover, the Directive seeks to ensure a high level of protection within the Union for "the fundamental rights and freedoms of natural persons, and in particular their right to privacy." Without sufficient data protection, the processing of personal information is not permissible[39]. Notable cases, such as the *Rechnungshof*[40] and *Lindquist*[41] cases have demonstrated the Directive's broad applicability and its

---

[35] Yvonne McDermott, "Conceptualising the right to data protection in an era of Big Data". *Big Data & Society*, January-June 2017: 1–7. https://doi.org/10.1177/2053951716686994.

[36] Lee Andrew Bygrave, "Data Privacy Law: An International Perspective*"* (Oxford, 2014; online edn, *Oxford Academic*, 16 April 2014). Retrieved from https://doi.org/10.1093/acprof:oso/9780199675555.001.0001.

[37] Directive 1995/ 46 EC. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119 04.05.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[39] Paul M. Schwartz, "European data protection law and restrictions on international data flows", *Iowa Law Review* 1995 March; 80(3): 471-496. http://hdl.handle.net/10822/882430.

[40] Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk Joined cases C-465/00, C-138/01 and C-139/01**.** *European Court Reports 2003 I-04989.* ECLI identifier: ECLI:EU:C:2003:294. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0465.

[41] Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping [2003] ECLI:EU:C:2003:596. Retrieved from https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62001CJ0101.

significance in shaping the right to privacy within the EU. Additionally, the Directive established independent Data Protection Authorities (DPAs) in each Member State to oversee compliance and enforce data protection laws.

The evolution of data protection in the EU culminated in the adoption of the General Data Protection Regulation (GDPR) in 2016, which became fully enforceable in May 2018. The GDPR represents the most comprehensive and stringent data protection regulation in the world, governing the processing of personal data within the EU and the European Economic Area (EEA), as well as the transfer of personal data outside the EU/EEA. The GDPR enhances individuals' control over their personal data, imposes stricter obligations on data controllers and processors, and introduces significant penalties for non-compliance, making it a cornerstone of digital privacy protection in the region[42]. Many of the GDPR's requirements were already present in its predecessor, the Data Protection Directive, which suffered from weak enforcement and compliance issues. However, the GDPR has significantly heightened awareness among lawyers and the business community due to its provisions for hefty fines—starting at eight figures—and its establishment of both internal and external mechanisms to strengthen enforcement. Consequently, the GDPR represents the most significant regulatory shift in information policy in a generation. It introduces a comprehensive and stringent regulatory framework for the protection of personal data.

2.2. The novelties introduced by the GDPR

The GDPR, adopted in 2016 and effective from May 2018, represents a significant overhaul in data protection regulation across the EU[43]. Comprising 11 chapters and 99 articles, it underscores data protection as a fundamental right. Recital 1 emphasizes the protection of individuals in relation to personal data processing, while Recital 2 extends this protection irrespective of nationality or residence, contributing to an area of freedom, security, justice, and economic progress. Consequently, organizations must ensure personal data is collected legally and securely, with reasonable steps taken to prevent unauthorized use or exploitation[44]. The GDPR, which replaced the Data Protection Directive 95/46/EC, was created to harmonize personal data privacy laws across the European Union. It aims to provide a consistent framework that ensures the protection and empowerment of all EU citizens regarding their data privacy rights. Additionally, the regulation reshapes how organizations throughout the EU handle data privacy, requiring them to adopt new practices that align with this unified standard.[45]

---

[42] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means". *Information & Communications Technology Law*, 2019, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501.

[43] Article 99 GDPR.

[44] Stefano Rodotà, 'Data Protection as Fundamental Human Right,' in S Gutwirth, Y Poullet, P De Hert, C de Terwangne, and S Nouwt (eds), *Reinventing Data Protection?* (Springer, 2009). https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_3.

[45] Marie-Pierre Granger and Kristina Irion, "The right to protection of personal data: the new posterchild of European Union citizenship?". *Civil Rights and EU Citizenship*, Edited by Sybe de Vries, Henri de

The GDPR principles—lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability[46]—are similar to those in the earlier Directive 95/46/EC but with key enhancements[47]. Notably, the GDPR expands the definition of personal data to include digital identifiers like IP addresses and introduces new concepts such as profiling[48] and pseudonymization[49]. It strengthens the requirement for consent[50], enabling data subjects to withdraw consent at any time and obliging controllers to prove that consent was obtained properly[51,52].

The regulation also introduces the "right to be forgotten," allowing individuals to request the deletion of their personal data when it is no longer necessary or when they withdraw consent[53]. In the landmark *Google Spain* case[54], the European Court of Justice affirmed this right, ruling that search engines must remove outdated or irrelevant personal information upon request. Additionally, the GDPR enhances the obligations of data controllers and processors, requiring them to implement appropriate technical and organizational measures to ensure data security, notify authorities and data subjects of breaches, and comply with stricter penalties[55].

While the GDPR has strengthened data protection rights, cases like *Schrems I*[5657], *Schrems II*[58] and *TU and RE v. Google LLC*[59] reveal challenges in its interpretation and implementation, highlighting conflicts between privacy rights and other

Waele, and Marie-Pierre Granger. 2018, 279-302, Retrieved from https://www.elgaronline.com/collection/Social_and_Political_Science_2018.

[46] Article 5 GDPR

[47] Žaklina Spalević and Kosana Vićentijević, "GDPR and Challenges of Personal Data Protection". *The European Journal of Applied Economics.* EJAE 2022, 19(1): 55 – 65. DOI: 10.5937/EJAE19-36596. Retrieved from https://scindeks-clanci.ceon.rs/data/pdf/2406-2588/2022/2406-25882201055S.pdf.

[48] Article 22 GDPR.

[49] Recital 28 GDPR.

[50] Article 7 GDPR.

[51] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means".

[52] Article 7, paragraph 3 GDPR.

[53] Recital 66 GDPR.

[54] Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez, C-131/12, ECLI:EU:C:2014:317, (2014) 3 CMLR 1247. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[55] Anastasia Greenberg, "Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces". May 18, 2018. Retrieved from SSRN: https://ssrn.com/abstract=3180941 or http://dx.doi.org/10.2139/ssrn.3180941.

[56] European Court of Justice, Ruling C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A62014CJ0362.

[57] Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of CJEU's Constitutional Reasoning", *German Law Journal*, 2019, 20. pp 864-883. doi:10.1017/glj.2019.6.

[58] European Court of Justice, Ruling C-311/18, *Schrems II* on 9 May 2020, ECLI:EU: C:2020:559. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2020%3A559.

[59] European Court of Justice, Ruling C-460/20 on 8 December 2022 Re V. Google ECLI:EU: C:2022:962. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CJ0460.

fundamental freedoms. The case of *Schrems I*, involving the activist Max Schrems, highlighted several issues related to the implementation of the GDPR, particularly concerning the validity of Standard Contractual Clauses (SCC) for cross-border data transfers. The subsequent *Schrems II* case further underscored the importance of protecting personal data during international transfers and called for careful assessments, additional safeguards, and oversight to ensure compliance with EU data protection laws. Meanwhile, Case C-*460/20 TU and RE v Google LLC* brought to the forefront a conflict between fundamental rights: the right to freedom of expression and the right to privacy, specifically the right to erasure[60]. The European Court of Justice (ECJ) emphasized that the right to data protection is not absolute; it must be balanced against other fundamental rights in accordance with the principle of proportionality[61]. Consequently, the GDPR clarifies that the right to data deletion is limited when processing is necessary for exercising other rights, such as the freedom of information[62]. The GDPR explicitly acknowledges that the right to privacy is generally balanced equally with other fundamental rights, such as freedom of expression[63]. However, the regulation permits certain limitations on specific rights, particularly those afforded to individuals, when national governments consider such restrictions necessary to protect other fundamental rights or public interests[64].

3. A critical analysis of the legal framework of data protection in Albania

3.1. Development of the right to privacy and data protection after 90's

Albania has a history marked by severe human rights violations, where fundamental freedoms were suppressed, distorted, or reshaped in ways that left individuals unaware of their full scope and entitlements. Under the previous 1976 Constitution, the right to privacy and personal data protection was not recognized, reflecting the broader suppression of fundamental rights during Albania's communist era,[65]which restricted freedoms such as privacy and expression.[66] It was only with the 1998 Constitution, following the fall of communism, that the protection of personal data and the right to privacy were formally acknowledged[67]. The 2016 Constitutional

[60] Article 17 GDPR.
[61] Recital 170 GDPR.
[62] European Agency for Fundamental Rights, 'Handbook on European Data Protection Law' (2018 edition) (Publications Office of the European Union, 2018). https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.
[63] Article 65 GDPR.
[64] Articles 85-91, GDPR.
[65] "Kushtetuta e Republikës Popullore Socialiste të Shqipërisë". (Constitution of Popular, Socialist Republic of Albania). Law no. 5506, dated 28.12.1976. Retrieved from http://licodu.cois.it/?p=383&lang=en.
[66] Heliona Miço, "The right to private and family life and the need for protection against the digital environment". *European Journal of Economics, Law and Social Sciences*, Vol 4, No. 1, 2024. DOI: https://doi.org/10.2478/ejels-2023-0010.
[67] Articles 35-37, Constitution of the Republic of Albania, adapted by the law no. 8417, dated 21.10.1998, as amended. Retrieved from https://qbz.gov.al/preview/635d44bd-96ee-4bc5-8d93-d928cf6f2abd.

amendments further entrenched privacy rights, specifically in Articles 35, 36, and 37, which outline the right to private life and the inviolability of housing. Recognizing that privacy is increasingly threatened by technological advancements, these amendments were essential in establishing constitutional protections against unauthorized intrusions[68]. Article 35, in particular, affirms an individual's right not to disclose personal data unless legally required, emphasizing consent as a prerequisite for lawful data processing, and granting individuals the right to correct or delete inaccurate or unlawfully collected data[69].

Privacy rights are also safeguarded through related provisions, such as Article 32, which protects against self-incrimination, reinforcing an individual's right to withhold certain personal information[70]. The legal framework is further strengthened by international agreements ratified by Albania, including the European Convention on Human Rights[71], the International Covenant on Civil and Political Rights[72], and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[73]. These international instruments, which Albania has incorporated into its legal system, mandate consent for data processing, access rights, rectification or erasure, and safeguards for cross-border data transfers.

Albania's first dedicated data protection law was Law No. 8517 on the Right to Information and Protection of Personal Data, adopted in 1999[74]. Although limited in scope, this law introduced fundamental principles such as data subject notification, data security, consent, and basic provisions on data transfer. This early legislation laid the groundwork for the more comprehensive Law No. 9887/2008[75], which governs data protection in Albania today, aligning national law with international standards to

---

[68] Cristina Elena Popa Tache, "The New International Triangle: Human Rights-Digitalization-Security". *International Investment Law Journal*. Vol 4, Issue 1, February 2023. https://www.ceeol.com/search/article-detail?id=1224141.

[69] Luan Omari and Aurela Anastasi, "E drejta kushtetuese", 2017, Dajti 2000, Tirane ISBN: 978 99956 01 41 6 pp. 136-137.

[70] Heliona Miço and Eralda (Methasani) Çani, "The Right to Information as a Means of Participation in Governance and Administration. Albanian Legislation Alignment with the Council of Europe Standards." *Proceedings of the International Scientific Conference "Social Changes in the Global World";* 2023 1(10), 269-284. ISBN 978-608-244-998-2 (T. 1). Retrieved from https://js.ugd.edu.mk/index.php/scgw/article/view/6139/5012.

[71] "On the Ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms", Law no. 8137, dated 31.07.1996. Retrieved from https://qbz.gov.al/eli/ligj/1996/07/31/8137/bffaa86c-7ecc-48c8-a7f9-8e812cd0a799;q=ligji%20nr.%208137date%2031.07.1996.

[72] "On the Accession of the Republic of Albania to the International Covenant on Civil and Political Rights" Law no. 7510 dated 08.08.1991. Retrieved from: http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=2&Lang=EN.

[73] "On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)", Law No. 9288 dated 07.10.2004. www.qbz.gov.al.

[74] "On the protection of personal data", Law No. 8517, dated 22.07.1999, as amended. Retrieved from https://www.qbz.gov.al/eli/ligj/1999/07/22/8517/1c6ad472-ebfd-417c-89ea-a20291d930e2;q=ligji%208517%20date%2022.07.1999%20per%20mbrojtjene%20e%20te%20dhenave%20personale.

[75] "On the protection of personal data", Law no. 9887, dated 10.03.2008, as amended. Retrieved from https://www.qbz.gov.al/eli/ligj/2008/03/10/9887/41ed4e3c-3dde-4028-9755-11887c48b7f6;q=ligji%208517%20date%2022.07.1999%20per%20mbrojtjene%20e%20te%20dhenave%20personale.

safeguard the right to privacy as a fundamental right.

3.2. A critical examination of the Law on the right to information and protection of personal data

Albania's Law on Personal Data Protection (LPDP), enacted in March 2008 and effective from May 23, 2008, serves as the cornerstone of the country's regulatory framework on personal data processing. The LPDP seeks to safeguard individuals' fundamental rights and freedoms, with a specific emphasis on the right to privacy, thereby positioning data protection as a key element of personal rights. Article 2 of the LPDP explicitly mandates that data processing must respect fundamental human rights, reflecting the Albanian legal system's recognition of data protection as closely intertwined with the right to privacy[76].

The LPDP's scope extends to all personal data processing activities conducted by data controllers and processors based in Albania[77]. Personal data is broadly defined as any information relating to an identifiable natural person, while processing refers to any operation or set of operations performed on such data, whether automated or manual[78]. The LPDP mirrors the principles of the General Data Protection Regulation (GDPR), including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and storage limitation. Consent plays a pivotal role, although the LPDP allows for exceptions in specific cases where legal obligations necessitate processing, such as the financial disclosure requirements imposed on public officials[79].

The LPDP enshrines several rights for data subjects, including the right of access, which allows individuals to confirm whether their data is being processed and to obtain pertinent information about such processing[80]. Additionally, data subjects have the right to rectification, enabling them to correct inaccuracies in their data[81]. The LPDP also provides for the right to erasure[82] under certain conditions, such as when data is no longer necessary for its original purpose, and the right to object, permitting individuals to restrict or halt the processing of their personal information[83]. In instances of perceived violations of their data rights, data subjects can file complaints[84] with the Commissioner for Data Protection and the Right to Information, the administrative body responsible for overseeing data protection compliance, and may seek judicial remedies

[76] Egla Leci, "The Right to Privacy in Albania. Its Compliance with EU GDPR and Current Challenges" *Unpublished Diploma Theses*. Epoka University, Tirana Albania 18.07.2023. Retrieved from https://dspace.epoka.edu.al/handle/1/1637/browse?value=Egla%2C+Leci&type=author.
[77] Article 4, Law no. 9887, dated 10.03.2008, as amended.
[78] Article 3, paragraph 1, LPDP.
[79] Luan Omari, Aurela Anastasi. "E drejta kushtetuese", pp. 138.
[80] Article 12 LPDP.
[81] Article 13 LPDP.
[82] Article 13 LPDP.
[83] Jorida Xhafaj, Krasimir Marinov and Almarin Frakulli, "Economic Consequences of the Right to be Forgotten". *Economic Alternatives*, Issue 2, pp 429-438. DOI:10.37075/EA.2024.2.11.
[84] Article 16, LPDP.

if administrative interventions prove insufficient[85].

The Commissioner for Personal Data Protection (CPDP), established under the LPDP[86,87] as an independent authority, plays a critical role in the law's enforcement. The CPDP is responsible for monitoring compliance, offering guidance, and investigating violations. Its mandate includes conducting administrative investigations, imposing sanctions on non-compliant entities, and providing advisory support on data protection impact assessments[88]. Additionally, the CPDP collaborates with other supervisory bodies domestically and internationally to promote the consistent application of data protection laws[89]. A core aspect of the CPDP's role involves handling complaints and disputes related to data processing, as well as undertaking preventive measures, such as approving data protection impact assessments for high-risk processing activities[90]. The CPDP also engages in public awareness initiatives to enhance understanding of data protection rights and obligations—a crucial task given the relatively low level of legal awareness in Albania.[91] The LPDP also provides for the right to compensation, allowing individuals who have suffered violations of their data protection rights to seek damages.[92] Furthermore, the law imposes specific obligations on data controllers, including the duty to inform data subjects about the nature of data processing and the requirements to ensure the accuracy, rectification, and appropriate storage of data[93,94].

To align with the EU "acquis" on data protection, Albania has undertaken continuous updates to its legal framework. The primary legal safeguard for personal data in Albania remains Law No. 9887/2008, as amended, which is further reinforced by secondary legislation issued by the Council of Ministers and the Commissioner for Personal Data Protection. The legal framework is being revised, with the adoption of amendments to the Law on the Right to Information in 2023. These measures collectively enhance the robustness of Albania's data protection regime, ensuring compliance with evolving international standards. However, a new draft Law on Personal Data Protection is in preparation, which aims to align with the EU's General Data Protection Regulation and the Law Enforcement Directive[95].

---

[85] Article 29 LPDP.
[86] Article 29 LPDP.
[87] Article 9/1 On the Right to Information, Law No. 119/2014, as amended. Retrieved from https://qbz.gov.al/preview/f5b3bd78-80cf-4fb0-8037-7700f3b9e139/cons/20231108.
[88] Article 30 LPDP.
[89] Article 32 LPDP.
[90] Sara Zotaj, "Protection of the Personal Data in Albania in Compliance with The General Data Protection Regulation". *LL.M. Capstone Thesis* 2021. Central European University Private University. Retrieved from https://www.etd.ceu.edu/2021/zotaj_sara.pdf.
[91] Article 31/k LPDP.
[92] Article 17 LPDP.
[93] Evis Garunja, "Protection of Privacy and Personal Data in Albania". *Croatian and Comparative Public Administration*. HKJU-CCPA, 23(1), 91–116, 2022. https://doi.org/10.31297/hkju.23.1.3.
[94] Article 18 LPDP.
[95] Screening Report – Albania, pp 27, 24 July 2023. European Commission, Directorate-General for Neighborhood and Enlargement Negotiations. Retrieved from https://neighbourhood-enlargement.ec.europa.eu/screening-report-albania_en.

3.3. How close or far from the GDPR is the Albanian legal framework?

The extent of Albania's legislative alignment with Regulation 2016/679/EU (GDPR) on the protection of personal data has not yet been comprehensively assessed. A legal gap assessment conducted in 2021 under Chapter 23 of the EU acquis found that significant portions of Albanian law are broadly consistent with EU standards. However, it also highlighted the need for continued efforts to fully harmonize Albania's personal data protection legislation with the GDPR. Complete alignment requires further legislative reforms to bridge the gaps between domestic laws and these key EU regulations.[96] To evaluate the alignment of Albanian legislation on the right to privacy, particularly in terms of data protection, with the European legal framework, various aspects of the GDPR are compared with the Albanian Law on Data Protection, as outlined in Table 1.

Table 1: *Contrasting GDPR with Law 9887/2008 on Data Protection in the Republic of Albania, as amended (LPDP)*

Aspects	General Data Protection Regulation	Law no. 9887/2008 (Albania) LPDP
Scope	Recognizing the critical importance of data protection, the European Union decided to upgrade the data protection directive to a regulation, thereby ensuring uniform applicability across all EU member states. This regulation requires each member state to adopt and enforce the provisions without any alterations, ensuring a strict and consistent application of data protection standards. The regulation's stringent requirements also extend to non-EU organizations that process the data of EU residents, reinforcing comprehensive data protection on a global scale.	The scope of the Albanian Law on Data Protection (Law No. 9887/2008) is to govern the processing of personal data by both public and private entities within the Republic of Albania. Its primary objective is to safeguard the fundamental rights and freedoms of individuals, with a particular focus on the right to privacy in the context of personal data processing.
Data Subject Rights	The GDPR and the Albanian Law on Personal Data Protection (LPDP) share several core rights, including the rights to access, rectify, erase, and restrict the processing of personal data. However, the GDPR introduces key enhancements that address the evolving needs of the digital market and extend beyond it. One significant addition is the "right to be forgotten," which, while related to the right to erasure found in the LPDP,	The Law on Data Protection of the Republic of Albania (LPDP) provides data subjects with several fundamental rights, including the right to access, rectify, and erase their personal information that is processed and stored by data controllers. Additionally, the LPDP grants individuals the right to object to the processing of their data, thereby reinforcing the protection of data subjects' rights.

[96] Chapter 23, National Plan for European Integration 2022-2024. Albanian Ministry of Foreign Affairs, (2021). Retrieved from https://integrimi-ne-be.punetejashtme.gov.al/wp-content/uploads/2022/02/NPEI_2022-2024_EN-.pdf.

	is more expansive and distinct under the GDPR. This right obligates data controllers to erase an individual's personal data when it is no longer necessary for legitimate purposes or after a specified period, thereby broadening the conditions under which data must be deleted. Another notable feature of the GDPR is the right to data portability, which enables individuals to receive their personal data in a structured, commonly used, and machine-readable format. This right also allows data subjects to transfer their data seamlessly from one controller to another, enhancing user control and data mobility. This provision, absent in the LPDP, represents a critical advancement in empowering individuals in the digital economy.	While the right to be forgotten is not explicitly stated in the LPDP, it can be logically inferred from the broader right to erasure, allowing data subjects to request the deletion of their information under specific circumstances.
Accountability and Compliance **Impact Assessment**	The GDPR establishes the principle of accountability, which greatly expands the obligations of data controllers. Under this principle, controllers must actively demonstrate compliance with data protection regulations through detailed documentation, perform Data Protection Impact Assessments (DPIAs) when necessary, and appoint Data Protection Officers (DPOs) in specific cases. Notably, the GDPR shifts the burden of proof to controllers, requiring them to substantiate their adherence to data protection principles and regulations, thereby reinforcing a proactive approach to data privacy and security.	Under the Law on Data Protection of the Republic of Albania (LPDP), data controllers bear the primary responsibility for ensuring compliance with data protection requirements. However, the LPDP places limited emphasis on documentation and accountability measures. Unlike the GDPR, the LPDP does not mandate data controllers to proactively provide evidence of compliance unless specifically requested by the Commissioner or a court. Additionally, there is no requirement for data controllers to conduct regular Data Protection Impact Assessments (DPIAs), reflecting a significant gap in accountability and proactive risk management compared to international standards.
Penalties	The GDPR establishes a robust penalty framework with significantly increased fines, categorized into two levels based on the severity of the infringement. Lower-level fines can reach up to €10 million or 2% of the undertaking's total worldwide annual turnover from the preceding financial year, whichever is higher. For more severe violations, higher-level fines may be imposed, reaching up to €20 million or 4% of the	The LPDP outlines penalties and administrative sanctions for data breaches; however, the fines imposed under Albanian law are significantly lower than those stipulated by the GDPR. The maximum fine under the LPDP reaches up to 5 million ALL (approximately €40,000), highlighting a substantial disparity in the financial deterrents between

	total worldwide annual turnover of the preceding financial year, whichever is greater. This tiered penalty structure underscores the stringent compliance requirements of the GDPR, emphasizing the substantial financial consequences of non-compliance.	the two legal frameworks[97].
Data Breach Notification	The GDPR places a strong emphasis on breach notification requirements, obligating data controllers to report data breaches to supervisory authorities within 72 hours of becoming aware of the incident. In certain cases, where the breach poses a high risk to individuals' rights and freedoms, data controllers are also required to directly inform the affected individuals, ensuring transparency and prompt risk mitigation.	The LPDP does not impose a mandatory breach notification requirement for data controllers in the event of a data breach. This absence of a compulsory notification obligation contrasts with international standards, such as those set by the GDPR, and represents a significant gap in the Albanian data protection framework.
International Data Transfers	The General Data Protection Regulation (GDPR) maintains the necessity for safeguarding data transferred outside the European Union but introduces more complex mechanisms to ensure compliance. These include standard contractual clauses and binding corporate rules, which provide structured frameworks for adhering to the required data protection standards.	LPDP permits international data transfers, provided that adequate measures are in place. However, it does not specify what constitutes these adequate measures, suggesting that they are understood to be aligned with general principles of data protection.
Data Protection by Design and by Default	The GDPR introduced a notable innovation by requiring the integration of protective measures directly into technological infrastructure to keep pace with evolving technologies. This requirement encompasses 'data protection by design' and 'data protection by default,' mandating that privacy considerations are embedded in the design and operational processes of services from their inception.	The LPDP lacks specific digital provisions intended to promote data protection by design and by default. For example, it does not mandate practices such as requiring minimum permissions for apps or setting privacy modes as default settings.
Profiling and Automated Decision-Making; Pseudonymization	The GDPR establishes explicit rights related to profiling and automated decision-making. These processes involve the use of algorithms to analyze personal data and make decisions without human intervention. According to the Regulation, this includes identifiers such as IP addresses or similar digital data that can identify individuals online. Additionally, the	The LPDP lacks specific digital provisions designed to minimize human interaction with data processing, such as those related to Automated Decision Making, Profiling, and Pseudonymization. In its implementation, only general principles of fairness and transparency are applicable.

[97] Gliqiri Riza, "GDPR and Personal Data Protection in non-EU countries: Albanian case of data protection legislation". *Proceedings of RTA-CSIT 2021*, May 2021. Retrieved from http://ceur-ws.org/.

	GDPR introduces new concepts such as profiling and pseudonymization, which involve techniques for transforming data so that individuals cannot be easily identified.	
Territorial Scope	The GDPR has an expansive scope, with no territorial limitations. It applies not only within the territories of EU Member States but also beyond the European Union. The only condition for its applicability is that the data being processed or controlled, or the data controller/processor, must involve EU citizens.	The Law on Data Protection specifies that its territorial application is confined to the Republic of Albania. It also applies to foreign entities, provided that they have their headquarters within Albanian territory. Consequently, its territorial scope is limited to the borders of Albania.
Parental Consent for Minors (Children Data)	The GDPR acknowledges the right of children to consent to the processing of their personal data. It sets the general minimum age for consent at sixteen (16) years old. However, Member States have the option to lower this age to thirteen (13) years in certain circumstances, as permitted by national law.	The Albanian law lacks specific provisions for the protection of minors' or children's data. It does not define a specific age at which parental consent is required or no longer required. Consequently, the LPDP applies general principles without further specification regarding the consent of minors.
Consent	The GDPR stipulates that consent must be both explicit and informed, defining two main characteristics of valid consent. In contrast to the LPDP, the GDPR requires consent even for processing public data, regardless of its availability to the public.	The LPDP requires 'consent' but does not specify the conditions under which consent should be given. It includes a provision allowing the use of public data with consent. In such cases, the data controller may utilize personal data obtained from public sources for business purposes.
Data Protection Authority	The GDPR establishes the role of Data Protection Authorities (DPAs), which are responsible for ensuring the correct application of the Regulation and safeguarding the data of all European citizens.	The LPDP designates an authority responsible for overseeing its implementation and protecting the data of Albanian citizens. This authority is known as 'The Commissioner for the Right to Information and Data Protection'.
Data Protection Officer (DPO)	The GDPR mandates that certain organizations, including public authorities and those processing large-scale sensitive data, must appoint a designated Data Protection Officer (DPO).	The LPDP does not require companies that act as data controllers or processors to appoint a specific entity, such as a Data Protection Officer, to oversee data protection and processing.

The comparative analysis between the Albanian Law on Personal Data Protection (LPDP) and the European Union's General Data Protection Regulation (GDPR) reveals both similarities and critical gaps in compliance, indicating the need for Albania to further harmonize its legal framework with EU standards. Both legal

frameworks share common ground in their protection of data subjects' rights, the responsibilities of data controllers, and mechanisms for data breaches, yet they diverge significantly in areas such as territorial scope, penalties, and specific rights afforded to data subjects.

One of the key disparities lies in the territorial scope. While the GDPR applies to all data controllers and processors handling the personal information of EU citizens, regardless of location[98], Albanian law is limited to entities within its territory[99]. Expanding the scope of Albanian law would enhance data protection for citizens beyond the country's borders, offering a higher level of legal safeguarding.

Moreover, certain rights under GDPR, such as the right to data portability and the right to be forgotten[100], are either absent or inadequately defined in Albanian law.[101] For instance, while the GDPR provides the right to data portability[102], allowing data subjects to transfer their personal data between controllers seamlessly, this right is not explicitly recognized under LPDP, limiting data mobility and control for Albanian citizens. Similarly, the right to be forgotten—a crucial aspect of data protection that enables individuals to request the erasure of their data—lacks detailed provisions in Albanian legislation. The existing law vaguely addresses this through a general right to request correction and erasure[103], which does not fully align with the GDPR's comprehensive approach.

The concept of consent also presents notable differences. Under GDPR, consent must be explicit and informed, particularly when processing personal data, whereas the LPDP's requirements are less stringent and leave room for interpretation. For instance, Albanian law permits data controllers to process publicly available information without seeking explicit consent, a provision that poses a high risk of misuse and could lead to significant privacy violations.

Additionally, the accountability principle under GDPR requires data controllers to demonstrate compliance with data protection obligations proactively. In contrast, Albanian law does not impose a similar burden of proof on controllers unless specifically requested by the Commissioner or courts, thereby weakening the enforcement of compliance.

The analysis also highlights the critical role of the Commissioner for Data Protection in Albania[104], an institution analogous to the GDPR's supervisory authorities[105]. However, limitations in resources and authority impede the Commissioner's ability to enforce compliance effectively, raising concerns about the adequacy of oversight in the current legal framework. The discrepancy in penalties further underscores the need for reform; fines under Albanian law are significantly

[98] Article 3 GDPR.
[99] Article 4/2 LPDP.
[100] Article 17 GDPR.
[101] Article 13 LPDP.
[102] Article 20 GDPR.
[103] Article 13 LPDP.
[104] Article 29 LPDP.
[105] Article 60 GDPR.

lower[106] than those under GDPR, reducing the deterrent effect and the overall impact of enforcement actions.

In conclusion, while the LPDP aligns with the GDPR in many fundamental respects, substantial legislative updates are necessary to close the existing gaps and fully integrate EU data protection standards into the Albanian legal framework. This harmonization is crucial for ensuring that Albanian citizens receive the same level of data protection as their EU counterparts and that the country's legal infrastructure can adequately address the challenges posed by evolving digital and data landscapes.

4. Examining significant data breaches in Albania: a security breakdown

Several significant data breaches and a major cyber-attack between 2021 and 2022 exposed the vulnerabilities of Albania's data protection framework, posing severe threats to citizens' privacy. The first incident, in April 2021, involved the leak of a database containing personal information of 2,070,000 Tirana voters[107], including names, dates of birth, identity card numbers, home addresses, political affiliations, and sensitive data such as religion and family situations. Allegedly owned by the ruling political party, this database raised concerns about its use for political purposes[108].

Nine months later, on December 22, 2021, a data breach exposed the salaries of 630,000 employees, violating their privacy rights as protected under Law No. 9887/2003 on Data Protection. Salaries are considered personal data since they relate to identifiable individuals, making this leak a breach of confidentiality. The National Tax Directorate, where the data was stored, was found responsible for the security failure after two internal employees were identified and arrested for the leak. While the data processing by state institutions was lawful, the breach highlighted significant security lapses, particularly in safeguarding data against unauthorized access and ensuring staff training in data protection protocols as required by Article 27 of the Law on Data Protection. The Commissioner for Data Protection investigated the incident, ultimately fining the National Tax Directorate €25,000 as per Decision No. 52 of November 24, 2022[109].

Although the Commissioner fulfilled his duties by investigating the breach, the incident underscores the need for enhanced resources and preventive measures within the Commissioner's office, including random and periodic audits of institutions. The 2021 annual report reveals a shortage of human resources in the Commissioner's office, further stressing the need for increased support to effectively uphold data protection

[106] Article 39 LPDP.

[107] Recommendation No. 44, dated 19 August 2021, "On the controller "Socialist Party of Albania". Commissioner for the Right to Information and Data Protection. Retrieved from https://idp.al/wp-content/uploads/2024/02/rekomandimi_nr_44_pssh_2021_dmdp.pdf.

[108] Alice Taylor, "Exit Explains: The Leak of Over 910,000 Albanians Personal Data to Politicians and the Public", *Exit News*, 16 April 2021.

[109] Vendimi nr. 52, date 24.12.2022 "Për kontrolluesin Drejtoria e Pergjithshme e Tatimeve" (Decision of Commissioner No.52, dated 24.11.2022, "On the Controller "National Tax Directorate"). Commissioner on the right to information and the protection of personal data. Retrieved from https://idp.al/wp-content/uploads/2024/02/Vendim-TATIME.pdf.

standards[110].

On December 24, 2022, another data breach occurred, exposing 530,452 license plates along with vehicle owner credentials and other detailed information. An administrative investigation by the Commissioner for Data Protection revealed that the data had been sourced from the General Directorate of Road and Transport (DPSHTRR), a government institution responsible for storing and protecting personal data. The investigation concluded that, while the data was legitimately collected, the institution failed to comply with proper data storage protocols, violating Article 5 of Law No. 9887 "On the Protection of Personal Data." The Commissioner fined the institution €8,800,000 as per Decision No. 51 of December 24, 2022[111].

The breach highlighted ongoing issues, including inadequate training of staff, as found in a prior ex officio investigation (Recommendation No. 32, dated July 23, 2022)[112]. This investigation noted that DPSHTRR had not properly trained employees, failed to notify individuals about data processing, and did not adhere to good administration standards, breaching Articles 21 and 22 of the Data Protection Law. These incidents reflect systemic negligence by authorities in adhering to data protection laws, specifically in training staff to ensure the safe processing and storage of personal data[113]. The lack of compliance and understanding of data protection obligations has indirectly contributed to repeated leaks.

The most severe incident occurred in September 2022, when a cyber-attack, allegedly by external forces from Iran, compromised the entire Albanian government's e-governance systems, including e-Albania and TIMS[114]. This attack paralyzed state institutions, led to the shutdown of systems for days, and disrupted services, including border controls, highlighting severe cyber security flaws.

These incidents, occurring over two years, exposed almost all aspects of citizens' personal information, including sensitive data that legally requires special permission to store and process. The leaks highlighted significant violations of Law No. 9887/2008 on Data Protection, specifically Articles 24/1/a and 27, which mandate strict data security measures and consent protocols.

The response to these incidents by Albanian authorities, including the

---

[110] Raporti Vjetor 2021, Komisioneri i së Drejtës së Informimit dhe Mbrojtjes së të Dhënave Personale, p. 47. Retrieved from https://idp.al/wp-content/uploads/2024/01/RAPORTI-VJETOR-2021.pdf.

[111] Vendimi Nr. 51, datë 24.11.2022, "Për Kontrolluesin "Drejtoria e Përgjithshme E Shërbimeve të Transportit Rrugor" (Decision No. 51, Dated 24.11.2022 "On the Controller "General Directorate of Services of Road Transport"). Commissioner on The Right to Information and its Protection Personal Data. Retrieved from https://idp.al/wp-content/uploads/2024/02/Vendim-DPSHTRR.pdf.

[112] Recommendation no. 32, dated 2.07.2022. "On the controller "Special College of Appeal", Commissioner of the Information and Protection of Personal Data. Retrieved from https://idp.al/wp-content/uploads/2024/01/rekomandim_32_2022_kpa_dpmdhp.pdf.

[113] Policy and Position Paper. "Legal and institutional overview of personal data protection and security in the country and their compliance with the acquis", Albanian Helsinki Committee. June 2022. Retrieved from https://ahc.org.al/wp-content/uploads/2022/07/policy-and-position-paper-personal-data-protection-and-security-korrigjime.pdf.

[114] Fiori Sinoruka, "Massive Data Leaks in Albania Pose Public Security Question". 23 December 2021. BIRN. Retrieved from https://balkaninsight.com/2021/12/23/massive-data-leaks-in-albania-pose-public-security-question/.

Commissioner for Data Protection, has been criticized for its inefficacy. Investigations were often delayed or incomplete, failing to hold accountable the entities involved. The Commissioner's limited actions, such as issuing recommendations rather than stronger sanctions, have been deemed insufficient to address the severity of these breaches[115].

Public awareness of data protection rights also appeared inadequate, as evidenced by the low number of complaints from citizens affected by the first data leak. Moreover, despite Albania's obligations under the European Convention on Human Rights (ECHR), no claims were brought to the European Court of Human Rights (ECHR). This underscores a lack of engagement with international legal mechanisms to protect privacy rights[116].

Comparisons with ECHR rulings, such as the 2022 decision against Spain for a similar unauthorized compilation and dissemination of personal data[117], suggest that Albania has failed to fulfill its duty to protect individuals from arbitrary intrusions into their privacy actively. The Albanian government's inability to prevent data leaks and identify the perpetrators has been interpreted as a breach of Article 8 of the ECHR, further emphasizing the urgent need for comprehensive reforms in Albania's data protection regime.

5. Conclusions

The analysis of Albania's legal framework on data protection in comparison to the European Union's GDPR reveals both alignment and critical areas for improvement. Although Albania's legal framework on privacy and data protection shares many principles with the GDPR, substantial gaps remain, particularly in areas such as territorial scope, data subject rights, accountability measures, and penalties. These differences undermine the overall level of data protection in Albania, highlighting the need for further legislative reforms to fully align with EU standards. Institutional weaknesses also pose significant challenges to effective data protection. The Commissioner for Personal Data Protection, despite being central to enforcement, is hindered by limited resources and authority, which affect its ability to conduct comprehensive investigations and enforce compliance. Strengthening the capacity and authority of the Commissioner is essential for improving governance in data protection. Recent data breaches in Albania, including the leaks of voter information, employee salaries, and vehicle registrations, along with the cyber-attack on governmental e-governance systems, underscore severe deficiencies in data security and the implementation of existing regulations. These incidents expose the inadequate institutional response and the lack of effective preventive measures, further

[115] Franziska Klopfer, Ena Bavcic and Laylo Merali, "Cybersecurity and human rights in the Western Balkans: mapping governance and actors". 5 October 2022. Geneva Centre for Security Sector Governance. Retrieved from https://www.dcaf.ch/cybersecurity-and-human-rights-western-balkans-mapping-governance-and-actors.

[116] "Policy and Position Paper..." Albanian Helsinki Committee.

[117] Case of M.D. and Others V. Spain (Application no. 36584/17). Final Judgement 28.09.2022. European Court of Human Rights. Retrieved from https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-218034%22]}.

complicating the data protection landscape. Moreover, the low level of public engagement following these breaches reflects insufficient awareness of data protection rights among citizens. Enhancing digital literacy and educating the public about their rights and available protection mechanisms are critical steps to bolster data privacy and encourage greater civic participation in safeguarding personal information.

The cyber-attacks on Albania's government systems also highlight the need for robust cybersecurity measures as an integral part of the data protection framework. Strengthening cybersecurity protocols and improving coordination between institutions responsible for data protection are essential to mitigating future risks and enhancing the overall resilience of the national data protection infrastructure.

Looking forward, Albania is drafting a new personal data protection law that aims to align more closely with the GDPR. This forthcoming legislation will introduce enhanced accountability measures, expand the Commissioner's role, and include new protections for data subjects, such as safeguards for biometric and genetic data. The effective implementation of this new law is expected to address existing gaps and elevate Albania's data protection standards to meet evolving technological challenges. In conclusion, while Albania's current legal and institutional framework provides a solid foundation, significant reforms are necessary to achieve full harmonization with the GDPR and to effectively respond to the complex challenges of digital privacy and data security in a rapidly changing technological environment.

Bibliography

1. Alibeigi, Ali, Abu Bakar Munir and MD. Ershadul Karim, "Right to Privacy, A Complicated Concept to Review" *Library Philosophy and Practice (e-journal).* 2841. (2019). Retrieved from https://digitalcommons.unl.edu/libphilprac/2841 or https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3537968.
2. Andrade, Norberto Nuno Gomes de. "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights*". Privacy and Identity Management for Life*: 6th IFIP WG PrimeLife International Summer School, Helsingborg, Sweden, August 2010, Revised Selected Papers. IFIP Advances in ICT, Vol. 352, Fischer-Hübner, S.; Duquenoy, P.; Hansen, M.; Leenes, R.; Zhang, G. (Eds.), Springer (2011). Retrieved from SSRN: https://ssrn.com/abstract=2033225.
3. Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of CJEU's Constitutional Reasoning", *German Law Journal,* 2019, 20. doi:10.1017/glj.2019.6.
4. Bygrave, Lee A., "Data Privacy Law: An International Perspective" (Oxford, 2014; online edn, *Oxford Academic*, 16 April 2014), Retrieved from https://doi.org/10.1093/acprof:oso/9780199675555.001.0001.
5. Bygrave, Lee A., "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties". *International Journal of Law and Information Technology*, Vol 6, Issue 3, 1998. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=915065#.
6. Campanha, Santana Paulo and Faiz Ayat Ansari, "Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India". *Journal of Liberty and International Affairs*. Volume 9, Number 3, 2023. eISSN 1857-9760. DOI: https://doi.org/10.47305/JLIA2393555cs.

7. Case C-101/01 Bodil Lindqvist v. Åklagarkammaren i Jönköping [2003] ECLI:EU:C: 2003:596. Retrieved from https://eur-lex.europa.eu/legal-content/GA/TXT/?ur_i=CE LEX:62001CJ0101.
8. Case of M.D. and others V. Spain (Application no. 36584/17). Final Judgement 28.09.2022. European Court of Human Rights. Retrieved from https://hudoc.echr.coe. int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-218034%2 2]}.
9. Chapter 23, National Plan for European Integration 2022-2024. Albanian Ministry of Foreign Affairs, (2021). Retrieved from https://integrimi-ne-be.punetejashtme.gov.al/ wp-content/uploads/2022/02/NPEI_2022-2024_EN-.pdf.
10. Charter of Fundamental Rights of the European Union 2012/C 326/02. Official Journal of the European Union, 26.10.2012. C 326/391. Retrieved from https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.
11. Cicero. *On Obligations: De Officiis (Oxford World's Classics)*, translated P. G. Walsh. 2008, Book I, sec. 85.
12. Constitution of the Republic of Albania, adapted by the law no. 8417, dated 21.10.1998, as amended. Retrieved from https://qbz.gov.al/preview/635d44bd-96ee-4bc5-8d93- d928cf6f2abd.
13. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe, Strasbourg 28/01/1981, European Treaty Series - No. 108. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=tre aty-detail&treatynum=108.
14. Convention on Cybercrime (ETS No. 185). Council of Europe Budapest 23/11/2001. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail &treatynum=185.
15. Diggelmann Oliver and Maria Nicole Cleis. "How the Right to Privacy Became a Human Right", *Human Rights Law Review*, Volume 14, Issue 3, September 2014, https://doi.org/10.1093/hrlr/ngu014.
16. Directive 1995/ 46 EC. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
17. Elena Popa Tache Cristina. "The New International Triangle: Human Rights-Digitalization-Security". *International Investment Law Journal*. Vol 4, Issue 1, February 2023. https://www.ceeol.com/search/article-detail?id=1224141.
18. European Agency for Fundamental Rights, 'Handbook on European Data Protection Law'. Publications Office of the European Union, 2018. https://fra.europa.eu/en/ publication/2018/handbook-european-data-protection-law-2018-edition.
19. European Court of Human Rights, Case of Axel Springer AG v. Germany (7 February 2012), Strasbourg, (Application no. 39954/08).
20. European Court of Human Rights, Case of Bărbulescu v. Romania (5 September 2017), Strasbourg, (Application no. 61496/08).
21. European Court of Human Rights, Case of Botta v. Italy (24 February 1998), Strasbourg, (153/1996/772/973).
22. European Court of Human Rights, Case of Denisov v. Ukraine (25 September 2018), Strasbourg Application no. 76639/11.
23. European Court of Justice, Ruling C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A62014CJ0362.

24. European Court of Justice, Ruling C-311/18, *Schrems II* on 9 May 2020, ECLI:EU: C:2020:559. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=ecli:ECLI%3AEU%3AC%3A2020%3A559.
25. European Court of Justice, Ruling C-460/20 on 8 December 2022 Re V. Google ECLI:EU: C:2022:962. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CJ0460.
26. Flaherty, David H. "On the Utility of Constitutional Rights to Privacy and Data Protection". *Case Western Reserve Law Review*, Vol. 41, Issue 3, (1991) Retrieved from https://scholarlycommons.law.case.edu/caselrev/vol41/iss3/14.
27. Franziska, Klopfer, Ena Bavcic and Laylo Merali. "Cybersecurity and human rights in the Western Balkans: mapping governance and actors". 5 October 2022. Geneva Centre for Security Sector Governance. Retrieved from https://www.dcaf.ch/cybersecurity-and-human-rights-western-balkans-mapping-governance-and-actors.
28. Garunja, Evis. "Protection of Privacy and Personal Data in Albania". *Croatian and Comparative Public Administration*. HKJU-CCPA, 23(1), 2022. https://doi.org/10.31297/hkju.23.1.3.
29. Global Privacy Assembly ("GPA") Policy Strategy Workgroup Three ("PSWG3"). *PSWG3: Privacy and data protection as fundamental rights: A narrative*. (2022). https://globalprivacyassembly.org/wp-content/uploads/2022/05/PSWG3-Narrative-Final.pdf.
30. Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez, C-131/12, ECLI:EU:C:2014:317, (2014) 3 CMLR 1247. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.
31. Granger, Marie-Pierre and Kristina Irion. "The right to protection of personal data: the new posterchild of European Union citizenship?". *Civil Rights and EU Citizenship*, Edited by Vries, Sybe de, Henri de Waele, and Marie-Pierre Granger. 2018. Retrieved from https://www.elgaronline.com/collection/Social_and_Political_Science_2018.
32. Greenberg, Anastasia. "Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces". May 18, 2018. Retrieved from SSRN: https://ssrn.com/abstract=3180941 or http://dx.doi.org/10.2139/ssrn.3180941.
33. Gstrein, Oskar J. and Anne Beaulieu. "How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches". *Philosophy & Technology* (2022) 35: 3. https://doi.org/10.1007/s13347-022-00497-4.
34. Hoofnagle Chris Jay, Bart van der Sloot and Frederik Zuiderveen Borgesius. "The European Union general data protection regulation: what it is and what it means". *Information & Communications Technology Law*, 2019, 28(1). https://doi.org/10.1080/13600834.2019.1573501.
35. International Covenant on Civil and Political Rights, adopted on 16 December 1966, by General Assembly resolution 2200A (XXI). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
36. Jonathan, W. Z. Lim and Vrizlynn L. L. Thing. "Toward a Universal and Sustainable Privacy Protection Framework". *Digital Government: Research and Practice*, Vol. 4, No. 4, Article 21. Publication date: December 2023. https://doi.org/10.1145/3609801.
37. Kushtetuta e Republikës Popullore Socialiste të Shqipërisë. (Constitution of Popular, Socialist Republic of Albania). Law no. 5506, dated 28.12.1976. Retrieved from http://licodu.cois.it/?p=383&lang=en.
38. Leci, Egla. "The Right to Privacy in Albania. Its Compliance with EU GDPR and

Current Challenges" *Unpublished Diploma Theses Epoka University, Tirana Albania*. 18.07.2023. Retrieved from https://dspace.epoka.edu.al/handle/1/1637/browse?value=Egla%2C+Leci&type=author.

39. McDermott, Yvonne. "Conceptualising the right to data protection in an era of Big Data". *Big Data & Society*, January-June 2017: 1–7. https://doi.org/10.1177/2053951716686994.
40. Miço, Heliona and Eralda (Methasani) Çani. "The Right to Information as a Means of Participation in Governance and Administration. Albanian Legislation Alignment with the Council of Europe Standards." *Proceedings of the International Scientific Conference "Social Changes in the Global World";* 2023 1(10). ISBN 978-608-244-998-2 (T. 1). Retrieved from https://js.ugd.edu.mk/index.php/scgw/article/view/6139/5012.
41. Miço, Heliona. "The right to private and family life and the need for protection against the digital environment". *European Journal of Economics, Law and Social Sciences*, Vol 4, No. 1, 2024. DOI: https://doi.org/10.2478/ejels-2023-0010.
42. Omari, Luan and Aurela Anastasi. "E drejta kushtetuese", 2017, Dajti 2000, Tirane ISBN: 978 99956 01 41 6 pp. 136-137.
43. On the Accession of the Republic of Albania to the International Covenant on Civil and Political Rights, Law no. 7510 dated 08.08.1991. Retrieved from: http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=2&Lang=EN.
44. On the protection of personal data, Law No. 8517, dated 22.07.1999, as amended. Retrieved from https://www.qbz.gov.al/eli/ligj/1999/07/22/8517/1c6ad472-ebfd-417c-89eaa20291d930e2;q=ligji%208517%20date%2022.07.1999%20per%20mbrojtjene%20e%20te%20dhenave%20personale.
45. On the protection of personal data, Law no. 9887, dated 10.03.2008, as amended. Retrieved from https://www.qbz.gov.al/eli/ligj/2008/03/10/9887/41ed4e3c-3dde-4028-9755-11887c48b7f6;q=ligji%208517%20date%2022.07.1999%20per%20mbrojtjene%20e%20te%20dhenave%20personale.
46. On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Law No. 9288 dated 07.10.2004. www.qbz.gov.al.
47. On the Ratification of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Law no. 8137, dated 31.07.1996. Retrieved from https://qbz.gov.al/eli/ligj/1996/07/31/8137/bffaa86c-7ecc-48c8-a7f9-8e812cd0a799;q=ligji%20nr.%208137date%2031.07.1996.
48. On the Right to Information, Law No. 119/2014, as amended. Retrieved from https://qbz.gov.al/preview/f5b3bd78-80cf-4fb0-8037-7700f3b9e139/cons/20231108.
49. Periñán, Bernardo. "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law", *American Journal of Legal History*, Volume 52, Issue 2, April 2012, https://doi.org/10.1093/ajlh/52.2.183.
50. Policy and Position Paper. "Legal and institutional overview of personal data protection and security in the country and their compliance with the acquis", Albanian Helsinki Committee. June 2022. Retrieved from https://ahc.org.al/wp-content/uploads/2022/07/policy-and-position-paper-personal-data-protection-and-security-korrigjime.pdf.
51. Raporti Vjetor 2021, Komisioneri i së Drejtës së Informimit dhe Mbrojtjes së të Dhënave Personale. Retrieved from https://idp.al/wp-content/uploads/2024/01/RAPORTI-VJETOR-2021.pdf.
52. Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk Joined cases C-465/00, C-138/01 and

C-139/01**.** *European Court Reports 2003 I-04989.* ECLI identifier: ECLI:EU:C:2003: 294. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3 A62000CJ0465.

53. Recommendation no. 32, dated 2.07.2022. "On the controller "Special College of Appeal", Commissioner of the Information and Protection of Personal Data. Retrieved from https://idp.al/wp-content/uploads/2024/01/rekomandim_32_2022_kpa_dpmdhp. pdf.
54. Recommendation No. 44, dated 19 August 2021, "On the controller "Socialist Party of Albania". Commissioner for the Right to Information and Data Protection. Retrieved from https://idp.al/wp-content/uploads/2024/02/rekomandimi_nr_ 44_pssh_2021_dmd p.pdf.
55. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119 04.05.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
56. Riza, Gliqiri. "GDPR and Personal Data Protection in non-EU countries: Albanian case of data protection legislation". *Proceedings of RTA-CSIT 2021*, May 2021. Retrieved from http://ceur-ws.org/.
57. Rodotà, Stefano. 'Data Protection as Fundamental Human Right,' in Gutwirth, S., Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt (eds), *Reinventing Data Protection?* (Springer, 2009). https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_3.
58. Schütz, Philip and Michael Friedewald. "Privacy: What Are We Actually Talking About? A Multidisciplinary Approach." *Privacy and Identity Management for Life* 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 / PrimeLife International Summer School Helsingborg, Sweden, August 2-6, 2010. Revised Selected Paper. Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen Ronald Leenes, Ge Zhang (Eds.).
59. Schwartz, Paul M. "European data protection law and restrictions on international data flows", *Iowa Law Review* 1995 March; 80(3): 471-496. http://hdl.handle. net/10822/88 2430.
60. Screening Report – Albania, pp 27, 24 July 2023. European Commission, Directorate-General for Neighborhood and Enlargement Negotiations. Retrieved from https://neigh bourhood-enlargement.ec.europa.eu/screening-report-albania_en.
61. Sinoruka, Fiori. "Massive Data Leaks in Albania Pose Public Security Question". 23 December 2021. BIRN. Retrieved from https://balkaninsight.com/2021/12/23/massive-data-leaks-in-albania-pose-public-security-question/.
62. Solove, Daniel J. "Understanding Privacy", (Harvard University Press, May 2008), *GWU Legal Studies Research Paper* No. 420, *GWU Law School Public Law Research Paper* No. 420, Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 1127888.
63. Solove, Daniel J., "The Limitations of Privacy Rights". *Notre Dame Law Review*. 2023, Vol 98, Issue 3, Article 1. https://scholarship.law.nd.edu/ndlr/v_ol98/iss3/1?utm_sour ce=scholarship.law.nd.edu%2Fndlr%2Fvol98%2Fiss3%2F1&utm_medium=PDF&ut m_campaign=PDFCoverPages.
64. Spalević, Žaklina and Kosana Vićentijević. "GDPR and Challenges of Personal Data Protection". *The European Journal of Applied Economics.* EJAE 2022, 19(1). DOI: 10.5937/EJAE19-36596. Retrieved from https://scindeks-clanci.ceon.rs/data/pdf/2406-2588/2022/2406-25882201055S.pdf.

65. Taylor, Alice, "Exit Explains: The Leak of Over 910,000 Albanians Personal Data to Politicians and the Public", *Exit News*, 16 April 2021.
66. The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), as amended. Council of Europe. Rome, 4.XI.1950. Retrieved from https://www.echr.coe.int/documents/convention_eng.pdf.
67. Ukrow, Jörg, "Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108." *European Data Protection Law Review*, 2018, 4(2), 239–247. https://doi.org/10.21552/edpl/2018/2/14.
68. Universal Declaration of Human Rights. GA Res 217A(III), 10 December 1948, A/810 at 71. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
69. Van der Sloot, Bart. "Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system.". *Computer Law and Security Review.* Vol 31, Issue 1. February 2015. Retrieved from https://doi.org/10.1016/j.clsr. 2014.11. 002.
70. Vendimi Nr. 51, datë 24.11.2022, "Për Kontrolluesin "Drejtoria e Përgjithshme E Shërbimeve të Transportit Rrugor" (Decision No. 51, Dated 24.11.2022 "On the Controller "General Directorate of Services of Road Transport"). Commissioner on The Right to Information and its Protection Personal Data. Retrieved from https://idp.al/wp-content/uploads/2024/02/Vendim-DPSHTRR.pdf.
71. Vendimi nr. 52, date 24.12.2022 "Për kontrolluesin Drejtoria e Pergjithshme e Tatimeve" (Decision of Commissioner No.52, dated 24.11.2022, "On the Controller "National Tax Directorate"). Commissioner on the right to information and the protection of personal data. Retrieved from https://idp.al/wp-content/uploads/2024/02/ Vendim-TATIME.pdf.
72. Westin, Alan F. "Privacy and Freedom", *Washington and Lee Law Review*. Vol 25, Issue 1, Article 20, Spring 3-1-1968. Retrieved from https://scholarlycommons.law. wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com.
73. Xhafaj, Jorida, Krasimir Marinov and Almarin Frakulli. "Economic Consequences of the Right to be Forgotten". *Economic Alternatives*, Issue 2. DOI: 10.37075/EA.2024. 2.11.
74. Zotaj, Sara. "Protection of the Personal Data in Albania in Compliance with The General Data Protection Regulation". *LL.M. Capstone Thesis* 2021. Central European University Private University. Retrieved from https://www.etd.ceu.edu/2021/zotaj_ sara.pdf.