



INTERNATIONAL INSTITUTE FOR PRIVATE
COMMERCIAL AND COMPETITION LAW
(IIPCC - AUSTRIA)

Research Article

© 2026 Ina Shënplaku

This is an open access article licensed under the Creative Commons
Attribution-NonCommercial 4.0 International License
(<https://creativecommons.org/licenses/by-nc/4.0/>)

Cyberbullying and Data Protection: A Comparative Legal Analysis of the EU and Albanian Frameworks

PhD (C.) Ina Shënplaku

DOI: <https://doi.org/10.2478/ajbals-2026-0016>

Abstract

Cyberbullying has emerged as one of the most pressing challenges of the digital age, affecting millions of individuals globally. While increasingly recognized as a harmful phenomenon warranting legal intervention, most existing frameworks approach it primarily through criminal law, overlooking its fundamental dimension as a privacy and data protection issue. Cyberbullying inherently involves the unauthorized processing and dissemination of personal data, making data protection law a critical but underutilized tool for victim protection. This paper conducts a comparative legal analysis of the European Union and Albanian frameworks governing cyberbullying through the lens of privacy and data protection. The EU, through the GDPR and the Digital Services Act, offers the most developed rights-based model globally, yet lacks unified cyberbullying-specific legislation. Albania, as an EU candidate state, has fully transposed the GDPR through Law No. 124/2024, yet faces critical gaps in cyberbullying-specific legislation, platform accountability, and enforcement capacity. The paper identifies structural gaps common to both frameworks and advances concrete recommendations, arguing that effective protection requires not merely rights on paper, but robust enforcement infrastructure, meaningful platform accountability, and cross-border legal cooperation.

Keywords: Cyberbullying, Data Protection, Right to Privacy, GDPR, Platform Accountability.

1. Introduction

The proliferation of digital technologies and social media platforms has fundamentally transformed the landscape of interpersonal harm. Cyberbullying, broadly understood as the use of digital technologies to repeatedly harass, threaten, humiliate, or harm individuals, has become a phenomenon with severe psychological, social, and legal consequences, disproportionately affecting women and minority groups. Beyond emotional distress, its consequences encompass reputational damage, social exclusion, professional harm, and in the most severe cases, self-harm and suicide. What distinguishes cyberbullying from its offline counterpart is its structural

relationship with personal data. Every act of cyberbullying involves the processing of personal information, the sharing of intimate images without consent, the public disclosure of private facts, digital impersonation, or the coordinated amplification of harmful content across platforms. Cyberbullying is therefore not only a behavioral or criminal problem; it is inherently a data protection problem. Victims lose control over their own personal data, often irreversibly, across platforms headquartered in jurisdictions far removed from their own. This paper addresses that gap through a comparative legal analysis of the European Union and Albania. The EU represents the most comprehensive rights-based data protection model globally, anchored in the GDPR and supplemented by the Digital Services Act (DSA). Albania, an official EU candidate state since 2014, has fully transposed the GDPR through Law No. 124/2024, yet lacks specific cyberbullying legislation and faces profound challenges in translating formal rights into effective victim protection. The EU–Albania relationship creates a direct normative link, making this comparison both legally significant and practically important for transitional legal systems navigating EU accession. Three research questions guide the analysis: How do the EU and Albanian frameworks address cyberbullying through the lens of privacy and data protection? What are the key structural gaps in each framework? And what concrete reforms can Albania adopt, drawing on EU law and practice, to strengthen victim protection as part of its accession process?

2. Context

2.1 Defining Cyberbullying

The definition of cyberbullying has been the subject of considerable legal debate. The most widely cited academic definition, advanced by Hinduja and Patchin, characterizes cyberbullying as willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices. From a legal perspective, however, no universally accepted definition exists. Different jurisdictions have adopted varying terminological and conceptual approaches, often conflating cyberbullying with related but distinct phenomena such as cyberstalking, online harassment, hate speech, and electronic intimidation. For the purposes of this paper, cyberbullying is understood as a pattern of digitally-mediated conduct intended to harm, humiliate, threaten, or control another individual, carried out through electronic communications platforms, and involving the processing or dissemination of personal data relating to the victim. This definition is deliberately oriented toward the data protection dimension. It encompasses the principal forms of cyberbullying most relevant to privacy law: doxxing, which involves the public disclosure of private personal information such as home addresses or financial details; non-consensual sharing of intimate images; digital impersonation, in which perpetrators create false profiles using the victim's identity and personal data; coordinated harassment campaigns that aggregate and amplify personal information across multiple platforms; and the use of location data or other sensitive personal information to

target, track, or intimidate victims. This framing is not merely academic. It has direct legal consequences: by identifying cyberbullying as conduct involving the processing of personal data, it brings such conduct within the normative scope of data protection law and the rights and remedies that flow from it.

2.2 The Nexus: Why Cyberbullying Is a Data Protection Issue

The conceptual link between cyberbullying and data protection rests on a straightforward but legally consequential observation: every act of cyberbullying involves the processing of personal data. Whether the conduct takes the form of sharing intimate images, disclosing a victim's personal details, creating impersonation profiles, or coordinating targeted harassment campaigns, the perpetrator necessarily processes information that relates to an identifiable individual — the legal definition of personal data under Article 4(1) GDPR. Recognizing this nexus opens significant legal possibilities. It enables victims to invoke data subject rights — particularly the right to erasure under Article 17 GDPR, to compel the removal of harmful content. It engages the supervisory and enforcement powers of data protection authorities, providing victims with an administrative avenue for redress that operates independently of criminal prosecution or civil litigation. It is within this framework that the EU and Albanian legal responses to cyberbullying must be evaluated.

3. The GDPR as the Primary Instrument

The General Data Protection Regulation, in force since May 2018, constitutes the cornerstone of the EU's response to privacy and data protection challenges in the digital environment. While the GDPR was not designed specifically to address cyberbullying, its scope and the rights it confers upon data subjects make it a powerful instrument for victim protection. The GDPR applies to the processing of personal data by controllers and processors established in the EU, as well as to controllers established outside the EU where the processing relates to the offering of goods or services to individuals in the EU or the monitoring of their behavior — a provision of critical importance given that the major social media platforms enabling cyberbullying are predominantly headquartered outside the EU. The foundational principles of Article 5, including lawfulness, fairness, transparency, purpose limitation, data minimization, and integrity and confidentiality, apply to all processing operations, including the hosting and dissemination of personal data by perpetrators of cyberbullying through platform infrastructures. From the victim's perspective, the most practically relevant provisions are those establishing data subject rights. The right to erasure under Article 17 entitles data subjects to demand the deletion of personal data where, among other grounds, the data is no longer necessary for the purpose for which it was collected, or where the data subject withdraws consent and no other legal basis applies. In the cyberbullying context, this right can be invoked to compel the removal of intimate images, doxxing content, or impersonation profiles — provided the request is directed to the data controller

responsible for the processing. The right to restriction of processing under Article 18 allows data subjects to limit the use of their data pending the resolution of a dispute, while the right to object under Article 21 enables data subjects to oppose processing carried out on the basis of legitimate interests — a ground frequently invoked by platforms to justify content hosting. The right not to be subject to solely automated decision-making under Article 22 is increasingly relevant as platforms deploy algorithmic systems to moderate, amplify, or suppress content involving cyberbullying. Enforcement of these rights is entrusted to national Data Protection Authorities, which are empowered under Article 58 GDPR to investigate complaints, issue binding orders, and impose administrative fines of up to €20 million or 4% of global annual turnover. The availability of a low-cost administrative complaint mechanism is particularly significant for cyberbullying victims, who may lack the resources or legal knowledge to pursue judicial remedies.

3.1 The Digital Services Act

The Digital Services Act (DSA), which became fully applicable in February 2024, represents a paradigm shift in the EU's approach to platform accountability. Where the GDPR governs the processing of personal data, the DSA governs the conditions under which platforms may host, amplify, and moderate user-generated content, including content that constitutes or enables cyberbullying. The DSA introduces a tiered system of obligations calibrated to platform size and risk. All platforms, regardless of size, are required to establish accessible and transparent mechanisms through which users can flag illegal content including content that violates privacy or constitutes harassment and to process such notices diligently. Very large online platforms (VLOPs), defined as those with more than 45 million monthly active users in the EU, are subject to additional obligations including annual systemic risk assessments, independent audits, and enhanced transparency reporting. Of particular relevance to cyberbullying is the DSA's requirement that VLOPs assess and mitigate systemic risks arising from the design and functioning of their services, including risks related to gender-based violence and online harassment. Platforms are further required to provide victims with effective redress mechanisms including internal complaint systems and access to out-of-court dispute settlement. The DSA also addresses the opacity of algorithmic recommendation systems, requiring VLOPs to offer users options that are not based on profiling, and to provide meaningful transparency about how content is ranked and amplified.

3.2 The EU Charter of Fundamental Rights and the ECHR

The legal framework governing cyberbullying in the EU is further shaped by the fundamental rights architecture of the EU Charter and the European Convention on Human Rights. Article 7 of the EU Charter guarantees the right to respect for private and family life, while Article 8 establishes data protection as an autonomous fundamental right. These provisions impose positive obligations on EU institutions and Member States to ensure that legislation and its application genuinely protect

individuals from digital harm. The European Court of Human Rights has developed a substantial body of jurisprudence directly relevant to cyberbullying and online privacy. In *K.U. v. Finland*, the Court held that states have a positive obligation under Article 8 ECHR to establish legal frameworks capable of protecting individuals from serious online privacy violations, even where this requires compelling platforms to disclose the identity of anonymous perpetrators. In *Delfi AS v. Estonia*, the Court addressed platform liability for harmful user-generated content, affirming that states may legitimately impose obligations on platforms to prevent and remedy serious online harm without violating freedom of expression. In *Bărbulescu v. Romania*, the Court elaborated on the scope of digital privacy protection, emphasizing that reasonable expectations of privacy in digital communications must be legally safeguarded. The balancing of privacy and data protection rights against freedom of expression, guaranteed under Article 11 of the EU Charter and Article 10 ECHR, remains one of the most contested dimensions of cyberbullying law. Content that constitutes harassment or privacy violation from the victim's perspective may be claimed as expression by the perpetrator or as protected speech by the platform. EU law requires that this balance be struck in a manner that gives genuine effect to both sets of rights, with proportionality as the governing principle.

3.3 Gaps in the EU Framework

Despite the sophistication of the EU legal framework, significant gaps remain. Most fundamentally, the EU has not adopted cyberbullying-specific legislation at the supranational level. The GDPR and the DSA operate as horizontal instruments applicable across a wide range of contexts, and while they provide meaningful tools for cyberbullying victims, they were not designed with cyberbullying as a primary concern. The result is that the application of these instruments to cyberbullying scenarios often requires legal interpretation and advocacy that many victims are not positioned to undertake. Cross-border cyberbullying in which perpetrators, victims, and platforms are located in different jurisdictions, creates complex questions of competence and coordination that the GDPR's one-stop-shop mechanism only partially resolves. Finally, the practical accountability of global platforms remains a structural challenge. Despite the significant advances, enforcement against major platforms requires substantial institutional capacity and political will. Victims frequently report that takedown requests are ignored, that complaint mechanisms are inaccessible, and that meaningful redress is effectively unavailable without legal representation.

4. Albania's Legal Context

The Republic of Albania was granted official EU candidate status in 2014, and accession negotiations have progressed steadily across multiple chapters of the EU acquis. Albania's digital landscape has undergone rapid transformation in recent years. Social media penetration is high, with platforms such as Facebook, Instagram,

TikTok, and YouTube widely used across age and demographic groups. This digital expansion has been accompanied by a significant rise in reported cyberbullying incidents, particularly affecting women and individuals in public life. Yet legal awareness among victims remains limited, digital literacy is uneven, and institutional responses have struggled to keep pace with the scale and complexity of online harm. A landmark development in Albanian data protection law is the adoption of Law No. 124/2024 on the Protection of Personal Data, which entered into force in 2024. This law represents a full and comprehensive transposition of the GDPR into Albanian national law, making Albania's data protection framework one of the most formally advanced among EU candidate states. The law enshrines the full suite of GDPR-equivalent data subject rights in Albanian law. Victims of cyberbullying now have formal access to the right to erasure, enabling them to demand the deletion of harmful personal data processed without a lawful basis, including intimate images shared without consent, doxxing content, and impersonation profiles. The right to restriction of processing, the right to object, and the right not to be subject to solely automated decision-making are equally available under Albanian law, on terms substantively identical to those established by the GDPR. Law No. 124/2024 also replicates the GDPR's accountability framework, imposing obligations on data controllers and processors regarding lawfulness of processing, data minimization, purpose limitation, security, and transparency. The principles of Article 5 GDPR, are reproduced in Albanian law, establishing a common normative baseline between the two systems. The significance of this development for cyberbullying cannot be overstated. A cyberbullying victim in Albania now has access, at least formally, to the same data protection rights as a victim in an EU Member State. The right to demand takedown of harmful content, to restrict its further dissemination, and to lodge a complaint with the supervisory authority are all legally available — representing a substantial advance on the fragmented protections available under the previous legislative framework. The institutional architecture of Albanian data protection law centers on the Information and Data Protection Commissioner (IDPC), an independent supervisory authority established under the data protection framework and now operating under the strengthened mandate conferred by Law No. 124/2024. The IDPC is empowered to receive and investigate complaints from data subjects, issue binding orders to data controllers, impose administrative sanctions, and engage in public awareness and educational activities. In the context of cyberbullying, the IDPC represents the primary administrative avenue for victim redress. A victim whose personal data has been processed unlawfully — through the dissemination of intimate images, the publication of private information, or the operation of impersonation profiles may lodge a complaint with the IDPC, which has the authority to order the responsible controller to erase the data, restrict its processing, or pay administrative fines. In practice, however, the IDPC faces significant institutional constraints. Its resources both financial and in terms of specialized technical personnel remain limited relative to the volume and complexity of cases arising in a rapidly digitizing society. The IDPC's enforcement capacity against foreign data controllers, particularly the major

social media platforms that host the majority of cyberbullying content, is structurally constrained: while Law No. 124/2024 replicates the GDPR's extraterritorial scope provisions, the practical ability to enforce orders against platforms headquartered outside Albania remains highly limited without bilateral cooperation mechanisms or integration into EU enforcement networks.

4.1 Cyberbullying in Albanian Criminal and Civil Law

Notwithstanding the advances in data protection law, Albanian law still lacks a dedicated cyberbullying statute. The legal response to cyberbullying is therefore constructed from a patchwork of provisions in criminal law, civil law, and sector-specific legislation that were not designed with digital conduct in mind. The Albanian Criminal Code contains several provisions that may be applied to cyberbullying conduct. Article 119 criminalizes insult, Article 120 criminalizes defamation, and Article 121 criminalizes threats. These provisions are in principle applicable to conduct carried out through digital means, and prosecutors have on occasion relied on them to address online harassment. However, their application to cyberbullying is structurally imperfect: the provisions are drafted with offline conduct in mind, do not capture the specific harms associated with digital harassment such as the viral amplification of harmful content, the permanence of digital records, or the anonymity of perpetrators and carry penalties that may not reflect the severity of online harm. Civil law remedies are similarly available in principle but limited in practice. Albanian civil law recognizes personality rights, including the right to honor, reputation, and private life and provides for compensation of moral damages in cases of unlawful interference with these rights. A cyberbullying victim may in principle bring a civil action for damages against an identified perpetrator. In practice, however, civil litigation in Albania is expensive, slow, and procedurally demanding, placing it beyond the realistic reach of many victims. The identification of anonymous online perpetrators presents additional procedural and technical challenges that Albanian courts are not yet well-equipped to address.

4.2 Platform Accountability in Albania

One of the most consequential gaps in the Albanian framework is the absence of any domestic equivalent to the EU's Digital Services Act. Albanian law imposes no specific obligations on social media platforms regarding the detection, notification, or removal of cyberbullying content. There is no mandatory notice-and-action mechanism, no requirement for platforms to conduct systemic risk assessments, and no obligation to provide accessible redress mechanisms for Albanian users. In practical terms, this means that a cyberbullying victim in Albania seeking the removal of harmful content from a major platform such as Facebook, Instagram, or TikTok is entirely dependent on the platform's own voluntary content moderation policies — policies that are designed and applied by companies headquartered in the United States and subject primarily to US law, EU law where applicable, and the platforms' own commercial

interests. Albanian law provides no enforceable legal basis through which the IDPC or Albanian courts could compel a foreign platform to remove content or provide victim redress. This gap is partially mitigated by the GDPR's extraterritorial reach for platforms operating in EU markets, and by the DSA's application to platforms with significant EU user bases, since major platforms are subject to EU obligations that may incidentally benefit Albanian users. However, this indirect protection is structurally inadequate: it depends on EU enforcement action rather than Albanian legal remedies, and it provides no direct accountability mechanism under Albanian national law.

4.3 EU Harmonization Obligations and Progress

Albania's EU accession process creates both an obligation and an opportunity in the field of cyberbullying and data protection law. The adoption of Law No. 124/2024 represents a significant milestone in formal legal harmonization, demonstrating Albania's capacity to transpose complex EU legislative instruments into national law. European Commission progress reports have consistently acknowledged advances in the data protection field while identifying enforcement capacity and institutional independence as areas requiring further development. The harmonization agenda ahead remains substantial. Albania will need to align with the Digital Services Act as part of its accession obligations, introducing platform accountability mechanisms that are currently absent from national law. The development of cyberbullying-specific legislation — drawing on the experience of EU Member States that have enacted such laws — is an identified priority that has not yet been acted upon. Strengthening the IDPC's resources and technical capacity, and developing cooperation mechanisms with EU DPAs and enforcement networks, are further prerequisites for effective protection in practice.

5. Comparative Findings

The adoption of Law No. 124/2024 has fundamentally altered the comparative picture between the EU and Albanian frameworks. Albania is no longer a system that merely approximates EU data protection standards — it is a system that has formally replicated them in their entirety. This represents a significant convergence that distinguishes Albania from many other EU candidate states and creates a genuine common normative foundation between the two systems. However, formal legal convergence has not produced practical equivalence. The central divergence between the EU and Albanian frameworks lies not in the text of the law but in the institutional and regulatory ecosystem surrounding it. EU Member States benefit from well-resourced, experienced, and institutionally independent Data Protection Authorities; enforcement networks enabling cross-border cooperation; and a platform accountability regime — the DSA — that imposes binding obligations on the major platforms through which cyberbullying predominantly occurs. Albania lacks to varying degrees, all of these surrounding conditions. Both systems share the absence

of cyberbullying-specific legislation, but the consequences of this gap are more severe in Albania. In the EU, the gap is partially compensated by the GDPR's horizontal application, the DSA's platform obligations, the ECtHR's positive obligation jurisprudence, and the growing body of DPA guidance and case law addressing online harassment. In Albania, the gap is largely uncompensated: without specific legislation, without platform obligations, and with limited enforcement capacity, victims are left with formal rights that are difficult to exercise in practice. The most consequential shared structural failure of both frameworks is the incomplete resolution of platform accountability. Cyberbullying predominantly occurs on platforms operated by companies headquartered outside the EU and Albania, whose cooperation with national legal orders is inconsistent and frequently inadequate. The EU has made the most significant global advance in addressing this through the DSA, which imposes binding obligations on very large platforms and provides enforcement mechanisms through the European Commission and national Digital Services Coordinators. Yet even within the EU, enforcement against major platforms has proven slow and contested. For Albania, the platform accountability gap is near-total. Without a DSA equivalent and without integration into EU enforcement networks, Albanian victims are structurally dependent on the voluntary policies of foreign platforms, an entirely inadequate basis for legal protection. This gap is the single most urgent regulatory priority for Albanian cyberbullying law, and aligning with DSA standards should be treated as an immediate accession-related obligation rather than a medium-term aspiration. One dimension of the comparative analysis that is frequently overlooked is the significance of Albania's membership in the Council of Europe and its ratification of the ECHR. ECtHR jurisprudence on privacy, online harm, and state positive obligations, including the landmark decisions in *K.U. v. Finland* and *Delfi AS v. Estonia* — is directly applicable in Albanian law. Albanian courts and the IDPC are entitled, and indeed obligated, to interpret national law in conformity with the Convention as construed by the Court in Strasbourg. This represents a significant but underutilized legal resource. Greater engagement by Albanian courts and practitioners with ECtHR jurisprudence on digital privacy and online harm could meaningfully extend the practical protection available to cyberbullying victims under existing law and would simultaneously advance Albania's alignment with European legal standards.

6. Recommendation

The most urgent legislative priority is the enactment of a dedicated cyberbullying law that integrates data protection remedies, criminal sanctions, and civil redress mechanisms within a coherent and digitally-adapted framework. Such a law should provide a clear legal definition of cyberbullying applicable in both criminal and civil proceedings; establish specific criminal offenses covering online harassment, non-consensual sharing of intimate images, doxxing, and digital impersonation; and create explicit procedural mechanisms enabling victims to invoke their data subject rights

— particularly the right to erasure — in the context of cyberbullying complaints. Albania should further enact a platform notification and takedown mechanism aligned with DSA standards, requiring platforms operating in Albania to establish accessible reporting systems, process takedown requests within defined timeframes, and cooperate with the IDPC in the investigation of cyberbullying complaints. While the extraterritorial enforcement of such obligations against foreign platforms will remain challenging, a domestic legal framework creates the normative foundation for bilateral cooperation agreements and future integration into EU enforcement networks. The Criminal Code should be amended to introduce digitally-specific offenses that capture the distinctive features of online harassment, including the elements of anonymity, viral amplification, and cross-platform coordination, rather than relying on the imperfect application of provisions designed for offline conduct. The IDPC must be substantially strengthened if Law No. 124/2024's formal rights are to produce real-world protection for cyberbullying victims. This requires meaningful investment in the IDPC's financial resources, technical personnel, and cybersecurity expertise. A dedicated unit within the IDPC or established in formal cooperation between the IDPC and law enforcement should be tasked specifically with cyberbullying complaints, enabling the development of institutional expertise, consistent practice, and effective victim support. Albanian prosecutors and judges require systematic training in digital evidence, data protection law, and cyberbullying-specific legal issues. The identification of anonymous online perpetrators requires technical investigative capacity and legal frameworks for compelling platforms to disclose user information that Albanian law enforcement currently lacks. Formal cooperation protocols with major platforms, negotiated at the governmental level, would represent a significant practical advance.

7. Conclusion

This paper has examined the legal frameworks governing cyberbullying through the lens of privacy and data protection in the European Union and Albania, with the aim of identifying structural gaps, comparative divergences, and pathways for reform. The analysis reveals a picture of significant formal progress accompanied by persistent practical inadequacy — a pattern that characterizes both systems, though in markedly different ways and to markedly different degrees. The EU framework, anchored in the GDPR and increasingly supplemented by the Digital Services Act, represents the most advanced rights-based data protection model globally. It provides cyberbullying victims with a meaningful suite of legal rights, accessible administrative remedies, and an evolving platform accountability architecture. Yet it too falls short: the absence of cyberbullying-specific legislation at the EU level, inconsistent enforcement across Member States, and the enduring difficulty of holding global platforms genuinely accountable are structural limitations that the existing framework has not fully resolved. Albania's position has been transformed by the adoption of Law No. 124/2024, which constitutes a full

and comprehensive transposition of the GDPR into Albanian national law. This is a landmark achievement that places Albania's formal data protection framework on par with EU Member States — a significant advance that should be recognized and built upon. Yet formal legal convergence has not produced practical equivalence. The absence of cyberbullying-specific legislation, the lack of a DSA equivalent, the limited enforcement capacity of the IDPC, and the structural inability to hold foreign platforms accountable mean that Albanian victims face a profound gap between the rights formally available to them and the protection they can realistically obtain. The central argument of this paper is that effective legal protection against cyberbullying requires more than rights on paper. It requires enforcement infrastructure capable of giving those rights real effect; platform accountability mechanisms that impose binding obligations on the digital intermediaries through which cyberbullying occurs; institutional capacity to investigate, adjudicate, and remedy complaints; and cross-border cooperation frameworks adequate to the inherently transnational character of online harm. These are challenges shared by both the EU and Albania — but they are challenges whose resolution is more urgent, and whose costs of failure are more severe, in a transitional system still building the foundations of its digital governance architecture. Looking ahead, the growing role of artificial intelligence in online environments introduces new dimensions of legal complexity that both frameworks must urgently address. Algorithmic recommendation systems amplify cyberbullying content, extending its reach and harm far beyond what perpetrators could achieve alone. Generative AI enables the creation of deepfakes and synthetic intimate images that weaponize victims' likenesses without any direct perpetrator-victim interaction. These developments challenge the foundational assumptions of existing data protection and platform liability frameworks — assumptions designed for a world of human-generated content and identifiable controllers — and demand a new generation of legal responses that place the right to privacy and the right to protection from digital harm at their center. For Albania, the path forward is clear in outline if demanding in execution: enact specific cyberbullying legislation, align with DSA standards, strengthen the IDPC, and invest in the institutional and human capital needed to translate formal legal rights into genuine victim protection. The EU accession process provides both the normative framework and the political incentive to pursue this agenda with urgency. The adoption of Law No. 124/2024 demonstrates that Albania possesses the legislative capacity to undertake ambitious legal reform. What remains is the sustained political will and institutional investment to ensure that the law serves not merely as a formal commitment, but as a living guarantee of the right to privacy and dignity in the digital age.

References

Council of Europe. (1981, as amended 2018). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+)*. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

- European Commission. (2021). *Albania 2021 report*. <https://ec.europa.eu>
- European Commission. (2022). *Albania 2022 report*. <https://ec.europa.eu>
- European Commission. (2023). *Albania 2023 report*. <https://ec.europa.eu>
- European Commission. (2024). *Albania 2024 report*. <https://ec.europa.eu>
- European Parliament & Council of the European Union. (2012). *Charter of Fundamental Rights of the European Union* (OJ C 326, 26 October 2012, pp. 391–407). <https://eur-lex.europa.eu>
- European Parliament & Council of the European Union. (2016). *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)*. Official Journal of the European Union, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Official Journal of the European Union, L 277, 1–102. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- European Court of Human Rights. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), as amended by Protocol No. 11*. <https://www.echr.coe.int>
- Bărbulescu v. Romania*, Application No. 61496/08 (European Court of Human Rights, Grand Chamber, September 5, 2017).
- Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.
- Delfi AS v. Estonia*, Application No. 64569/09 (European Court of Human Rights, Grand Chamber, June 16, 2015).
- Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin.
- K.U. v. Finland*, Application No. 2872/02 (European Court of Human Rights, December 2, 2008).
- Republic of Albania. (2024). *Law No. 124/2024 on the Protection of Personal Data*.
- Republic of Albania. (1995, as amended). *Criminal Code of the Republic of Albania* (Articles 119–121).
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376–385. <https://doi.org/10.1111/j.1469-7610.2007.01846.x>
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Tambou, O. (2021). *European data protection law*. Bruylant.
- Vogiatzoglou, P. (2019). The impact of the GDPR on fundamental rights protection. *European Law Journal*.