EUROPEAN MOVEMENT ALBANIA

BEYOND COMPLIANCE: BUILDING A FUNCTIONAL DIGITAL SERVICES ACT FRAMEWORK IN ALBANIA

Petra Kováčiková

Funded by the European Union

EUROPEAN MOVEMENT ALBANIA

SFPA Slovak Foreign Policy Association

PUBLISHER

European Movement Albania (EMA)
Rr. Milto Tutulani, Nd.1, Ap. 4.
Tirana 1019, Albania
Tel: +355 44 104 247
E-mail: info@em-al.org
Web: www.em-al.org

AUTHORS:

Petra Kováčiková

YEAR OF PUBLICATION:

February 2026

This publication was funded by the European Union. Its contents are the sole responsibility of European Movement Albania and its authors and do not necessarily reflect the views of the European Union.

The action "Building Partnership on Fundamentals: Empowering CSOs for the EU accession process", is being implemented by the European Movement in Albania, with the financial support of the European Union - IPA Civil Society Facility 2021, and in cooperation with the Academy of European Integration and Negotiations (AIEN), Slovak Foreign Policy Association (SFPA) and the Center for Transparency and Freedom of Information (CTFI).

Funded by
the European Union

EUROPEAN MOVEMENT ALBANIA

SFPA
Slovak Foreign Policy Association

Executive Summary

As Albania rapidly aligns its legal framework with the EU acquis across multiple accession chapters, it faces a recurring implementation risk: European legislation may be adopted formally, but remain weak in practice. This risk is particularly pronounced for governance-heavy regulations such as the Digital Services Act, where effectiveness depends not only on legal alignment but also on institutional readiness and sustained cooperation among public authorities, private actors, and civil society.

Without early preparation and a clear allocation of responsibilities, DSA alignment risks becoming a compliance exercise on paper rather than a functioning system that improves online safety, protects users' rights, and strengthens trust in the digital environment. For a candidate country, this distinction is critical. The DSA is not a symbolic commitment to a "safer internet"; it is an operational framework that reshapes how responsibility, accountability, and oversight are exercised in the online space.

The DSA represents one of the EU's most ambitious responses to systemic risks in the digital space. At the same time, its layered design makes it challenging to understand and implement. It introduces new institutional roles, complex cooperation mechanisms, and differentiated obligations that vary by type and scale of digital service. In a candidate country, this complexity can lead to misunderstandings about what the DSA does and does not regulate, and may open space for unnecessary politicisation of a framework that is designed to remain independent. Addressed early and consistently, however, Albania can prevent such misunderstandings, safeguard institutional independence, and strengthen public trust from the outset.

Albania's digital landscape

According to national data, more than 86% of Albania's population uses the internet. Furthermore, around 82% are active on social media on a daily basis, with Facebook as the dominant platform, hosting an estimated 1.8 million Albanian users (INSTAT, 2024; Media Ownership Monitor Albania, 2023). As a result, the vast majority of Albanian citizens – including minors and other vulnerable groups – interact daily in digital environments.

The risks addressed by the Digital Services Act (DSA) are therefore not abstract. Albanian users face the same categories of online harm observed across the EU, including online scams, fraud, online hate speech targeting vulnerable minorities, cyberbullying, and targeted manipulation in e-commerce environments. These risks disproportionately affect people with lower levels of digital literacy, as well as youth, and especially minors. Compared to older and less represented age groups online, 99% of Albanian youth aged 16–29 use the internet daily, which can significantly increase their exposure to harmful content (Eurostat, 2025).

Digital harms do not remain confined to the online environment. Digital marketplaces offering illegal goods, as well as online hate and radicalising or violent content, can spill over into broader societal risks, and potentially escalate into threats to public security and real-world violence. Young people, in particular, are more vulnerable to radicalisation online due to their developmental stage (Bilewicz & Soral, 2020).

At the same time, Albania's digital transformation has been uneven. While internet and social media use is relatively high, the uptake of certain ICT services – such as online banking and e-commerce – lags significantly behind EU averages. Only around 25% of Albanians can use online banking according to the latest statistics (Eurostat, 2026). As more public and private services move online, this gap becomes increasingly consequential. The launch of the e-Albania portal in 2012 and the gradual closure of offline contact points have highlighted how lower digital skills can limit access to essential services – and potentially increase vulnerability to online scams, fraud, manipulative design practices, and other digital threats (European Commission, 2023; The World Bank, 2024). According to data from Albania's Financial Intelligence Agency, reported cases of online fraud targeting citizens have doubled in recent years (FIU, n.d.), which in turn negatively affects public trust in institutions.

Although national data from 2024 indicate that digital literacy in Albania is improving, overall levels remain low, with a score of 39 out of 100 (IDRA, 2024). Recent Eurostat data (2026) present an even more critical picture, indicating that only around 27.65% of the population is digitally literate – the lowest level among European countries. Notably, levels remain limited even among young people, with only 59% demonstrating at least basic digital skills (Eurostat, 2026). While this is comparatively stronger within the regional context of the Western Balkans, it remains far below EU frontrunners such as Denmark or Finland, where the digital literacy of this population segment approaches 90% (Eurostat, 2026).

The situation is particularly severe among Albanians over 55, where the rate drops to approximately 4.8% (Eurostat, 2026), making this group especially vulnerable to online fraud, scams, and other forms of digital harm.

This context is directly relevant for the DSA implementation. Where digital literacy is uneven, the protection of user rights risks remaining formal rather than effective unless accompanied by targeted communication, guidance, and support. Early and structured preparation is therefore essential. The DSA requires Albania to address not only which obligations apply, but also who implements them, how responsibilities are coordinated, and which institutional capacities must be built or strengthened. These decisions need to precede – not follow – formal alignment, if the regulation is to generate tangible impact on citizens' lives as intended.

The core objectives of the Digital Services Act

The DSA is the EU's central regulatory response to systemic risks arising from the functioning of digital intermediary services. Its overarching objective is to create a safer, more transparent, and more accountable digital environment in which fundamental rights are safeguarded. To this end, it addresses a broad range of online harms that users may encounter, with a primary focus on illegal content, such as illegal hate speech, content infringing intellectual property rights, child sexual abuse material, terrorist content, or illegal goods promoted or sold online.

In parallel, the DSA also targets systemic risks linked to how providers design, operate, and govern their services. This includes manipulative design practices and deceptive interface features – commonly referred to as dark patterns – that undermine users' ability to make informed and autonomous decisions, such as misleading subscription flows, hidden costs, or obstructive cancellation mechanisms (Deceptive Design, n.d.).

A defining feature of the DSA is its explicit recognition that these challenges are not incidental to the digital environment, but structural and systemic. The Regulation frames the governance of online spaces as a shared societal responsibility and moves beyond purely reactive approaches focused on individual pieces of content.

The DSA applies horizontally to a wide range of intermediary services, including providers of internet access, cloud and web hosting providers, online platforms, online marketplaces, certain auxiliary services, among others. While baseline obligations apply across this spectrum, the most extensive regulatory requirements apply to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), whose scale, reach, and societal impact justify enhanced scrutiny. Importantly, this category includes not only "classic" social media platforms such as Facebook or YouTube, together with the most popular search engines such as Google Search, but also major e-commerce platforms and app stores, including Amazon, Booking.com, Shein, and Apple's App Store (European Commission, 2026a). The European Commission continuously revisits who falls and who does not fall under the VLOP and VLOSE

categories. Recently WhatsApp has been designated a VLOP, namely with its 'Channels' feature (European Commission, 2026b).

From a bigger-picture perspective – what is the DSA aiming to do?

The DSA aims to protect users from illegal content while safeguarding their digital rights through clear and enforceable procedures. It governs how platforms must act when addressing illegal content, without defining what content is legal or illegal. Determinations of illegality remain exclusively within the scope of national law.

The Regulation's focus is therefore procedural. It seeks to ensure consistent standards of due process across digital services and to protect fundamental rights, in particular freedom of expression, access to information, non-discrimination, and the rights of the child.

For example, providers are obliged to:

- ensure that users can easily report content they believe to be illegal or in breach of the service's terms and conditions;
- provide clear explanations when content or accounts are removed or restricted;
- guarantee access to redress mechanisms where users believe content has been wrongfully removed or insufficiently addressed;
- design and operate content moderation processes in a manner that limits the over-removal of lawful content, particularly where automated tools or third-party notices are used.

Together, these safeguards shift users from passive recipients of platform decisions to active rights-holders with access to remedies.

The DSA strengthens transparency and accountability in the governance of digital services. Decisions affecting content visibility, recommender systems, profiling, or online advertising have significant societal consequences, yet have traditionally been taken with limited external scrutiny.

To address this, the DSA introduces obligations aimed at:

- making platforms' terms and conditions clear and enforceable;
- requiring regular transparency reporting on content moderation practices;
- increasing visibility into recommender systems and advertising practices, particularly for VLOPs and VLOSEs;
- banning the profiling of minors,
- enabling oversight and independent scrutiny, including access to data for competent authorities and researchers.

These obligations are not intended to micro-manage providers' business decisions, but to ensure that decisions with systemic impact are reviewable and subject to accountability mechanisms.

The DSA establishes a risk-based governance model. Obligations are differentiated according to the function, scale, and societal impact of digital services, reflecting the principle that not all services pose the same level of risk. Regulatory intensity therefore increases with scale, reach, and influence.

On this basis, VLOPs and VLOSEs are subject to enhanced obligations. These include requirements to regularly assess systemic risks, such as those stemming from the dissemination of illegal content, manipulation of public discourse, risks affecting minors, or impacts on public security and electoral processes. They must also implement appropriate risk mitigation measures and undergo independent audits. Audit methodology, requirements for auditors and their reports are specified in the Regulations' Delegated act which covers what the audit should address, how to evaluate systemic risks and what standards the auditor is to apply.

Risk mitigation must be embedded in platform design, internal policies, recommender systems, and content moderation practices. This shifts attention from intervention in individual cases to the systems that shape user exposure and behaviour.

Finally, the DSA establishes a coherent and enforceable governance framework. It addresses previous fragmentation by harmonising core rules, clarifying supervisory competences, and embedding cooperation mechanisms into the regulatory architecture.

Key elements of this framework include:

- national Digital Services Coordinators as central points of supervision and coordination;
- structured cooperation between national authorities and the European Commission;
- EU-level oversight exercised by the European Commission over systemic risks posed by VLOPs and VLOSEs.

The Regulation establishes channels of interaction between national authorities, the European Commission, law enforcement bodies, and civil society actors. For candidate countries such as Albania, the DSA is therefore not merely a set of rules to be transposed, but a model of regulatory coordination that presupposes institutional preparedness, procedural discipline, and effective cross-border cooperation.

Understanding the core logic of the Digital Services Act

Frequently presented as a law about illegal speech, the core logic of the Regulation is often misunderstood. Building on the previous chapter, this section clarifies how the DSA should be approached during implementation.

Procedural governance, not content control

The DSA does not introduce new rules defining what content is legal or illegal, nor does it aim to adjudicate individual speech decisions. Instead, it establishes procedural requirements governing how providers organise their systems, moderate content in practice, and ensure that decisions can be reviewed.

The emphasis is therefore on whether platforms have appropriate processes in place – such as transparency obligations, risk assessments, audits, and oversight mechanisms – rather than on individual pieces of content.

This reflects a deliberate shift towards governing the systems that shape how content is managed and amplified.

User orientation, not only institutional compliance

While the DSA creates obligations for providers and supervisory authorities, these obligations are intended to translate into concrete protections for users. The Regulation strengthens users' procedural position by requiring clear explanations for moderation decisions, access to complaint and redress mechanisms, and greater transparency regarding the algorithmic systems that shape user experience.

In this way, the DSA treats users as rights-holders with enforceable guarantees, rather than as passive subjects of platform rules. This user-oriented logic should be reflected not only in national implementation, but also in public communication.

Practical tools for day-to-day governance

The DSA is designed to be operational, not merely declaratory. It introduces practical governance 'tools' intended to function in everyday practice, including:

- Trusted Flaggers – designated organisations with recognised expertise in reporting illegal content;
- Platforms' internal reporting mechanisms – channels enabling users to report content they believe breaches national legislation or platform rules;
- Out-of-court dispute settlement bodies – independent bodies allowing users to challenge content moderation decisions.

The effectiveness of these depends not only on formal designation, but on institutional capacity, clear procedures, and active cooperation among stakeholders.

Clarifying responsibility: mapping the digital ecosystem

A further practical function of the DSA is to reduce uncertainty about responsibility in the digital environment. It does so by clearly defining categories of intermediary services and calibrating obligations according to their function and scale, with enhanced requirements for VLOPs and VLOSEs.

For Albania, identification and correct classification of services will be essential for effective implementation. This task falls to the national Digital Services Coordinator and includes assessing where domestic or regionally relevant services – such as the e-Albania platform or the Gjirafa search engine – fit within the DSA framework.

The Digital Services Coordinator: Base of the functional system

The Digital Services Coordinator (DSC) is the central authority responsible for supervising and enforcing the DSA at the national level. Neither a political regulator of online speech nor a body tasked with determining the legality of online content per se, the DSC does not replace courts or criminal law enforcement authorities.

Those bodies retain responsibility for determining the illegality of specific content and for investigating and prosecuting criminal offences, such as offences related to extremist content or child sexual abuse material.

The function of the DSC is distinct. It oversees compliance with the procedural and systemic obligations established by the DSA, ensuring that the regulatory framework operates effectively in practice and that users' rights are protected and enforceable within a coherent supervisory system. In carrying out this role, the DSC is equipped with investigatory and enforcement powers under the Regulation, including the power to request information, conduct investigations, adopt binding decisions, and ensure effective enforcement, including the imposition of sanctions in line with national institutional arrangements. Where relevant, the DSC may also cooperate with judicial or law enforcement authorities within the limits of its mandate, but it does not adjudicate criminal liability or impose criminal sanctions.

A formally designated but weak or passive DSC does not fulfil the purpose of the DSA. For Albania, the DSC must be understood as an operational hub: a body that connects users, platforms, civil society, and eventually the EU-level supervisory structures, into a functioning governance framework.

From a user perspective, the DSC should serve as a clear and intelligible entry point into the DSA system. It receives complaints concerning potential breaches of DSA obligations and ensures that cases are channelled into appropriate supervisory and coordination mechanisms.

It also plays an active role in supporting users through awareness-raising, the provision of information, and by facilitating access to complaint-handling mechanisms and available redress tools.

The value of user complaints lies not primarily in resolving individual disputes. Their strategic importance is in revealing recurring patterns, structural deficiencies, or systemic failures in platform practices. A functional DSC treats complaints as signals, not only as cases, and integrates them into broader risk assessment and enforcement activities.

Mandates: bringing independent expertise into the system

One of the DSC's key functions is the granting and supervision of mandates that integrate specialised expertise into the DSA framework. These mandates are not formalities; they directly affect the quality of oversight and the credibility of the system.

In particular, the DSC is responsible for:

Trusted flaggers: expert organisations authorised to report specific categories of illegal content, whose notices must be prioritised by platforms. Their value lies in accuracy and expertise, not reporting volume. The DSC must continuously assess performance, require transparent reporting, and withdraw status where accuracy or independence is compromised.

Vetted researchers: researchers and research institutions with granted access to internal data of VLOPs and VLOSEs to study systemic risks.

The DSC evaluates research proposals and ensures that research contributes meaningfully to understanding platform systems and societal impacts.

Out-of-court dispute settlement (ODS) bodies: organisations assisting users in challenging platform decisions, particularly content removals (or non-removals) and account suspensions. The DSC must oversee not only formal eligibility, but also independence, quality of decision-making, and practical accessibility for users.

Institutional design requirements

While the Digital Services Act allows flexibility in institutional design, it sets clear qualitative expectations. In practice, a functional DSC must operate as a single central authority with a clear legal mandate and coordination role. It must be independent from digital service providers and protected from political interference, and it must have adequate human, financial, and technical resources proportionate to the size and complexity of the national digital market.

In addition to its national supervisory role, the DSC participates in EU-level cooperation mechanisms, including coordination through the European Board for Digital Services. It must be capable of engaging in cross-border cases, exchanging information with other DSCs and the European Commission, and contributing to consistent enforcement across the Union.

Article 111 of the DSA does not prescribe a fixed institutional model for the DSC. Instead, it requires that the size, resources, and organisational setup of the DSC be proportionate to the scope and complexity of the tasks it is expected to perform, in particular in relation to digital service providers established in the country. The DSA also allows for an existing authority to be designated as the DSC, provided that it meets the Regulation's requirements, notably with regard to independence from digital service providers and from political or public influence. Independence and capacity are not abstract principles; they are practical preconditions for trust and effectiveness. Member States may appoint existing authorities with relevant expertise, such as telecommunications, media, consumer protection, data protection, or competition regulators. In practice, this has resulted in a heterogeneous landscape, with some systems centralising functions within a single authority, while others distribute responsibilities across multiple bodies, with the DSC acting as a coordinator (Cleynenbreugel and Mattioli, 2023).

A practical illustration of the DSC model can be found in the Council of Media Services in Slovakia. Slovakia adopted an adaptive approach by assigning the role to an existing regulator with prior competence in audiovisual media. Its integration into the DSA framework was gradual: participation in the informal DSC network in 2023, observer status in the European Board for Digital Services following the full applicability of the DSA in early 2024, and formal designation after the adoption of national implementing legislation in mid-2024. Institutionally, the authority combines a collegial decision-making body with an executive office providing legal, technical, and analytical support; the Council, composed of nine members including a Chair, acts as the

statutory body and appoints the Director, who oversees the functioning of the office (Council of Media Services, 2024b). This model demonstrates how an existing authority can be repurposed to fulfil DSC functions, ensuring institutional continuity and early alignment with EU structures.

In practice, the DSC functions as a litmus test of DSA implementation: how it is designed, resourced, and used will determine whether the DSA becomes a practical tool for user protection or remains largely a formal regulatory framework.

Who does what: Enforcement, supervision, and coordination in the DSA system

The DSA establishes a multi-level enforcement model that allocates competences between national authorities and the EU level according to the type of service provider, the nature of the alleged infringement, and its societal impact. The effectiveness of this system depends on a clear understanding of who acts, in which situations, and with which powers.

The country-of-establishment principle

The foundational principle of DSA enforcement is the country-of-establishment rule. Primary supervisory responsibility lies with the DSC in the Member State where a provider has its main establishment or, where applicable, its legal representative. This approach aims to ensure legal certainty for providers and to avoid fragmented enforcement across multiple jurisdictions.

This model leads to an uneven distribution of supervisory workload, with a disproportionate burden on countries hosting a high concentration of digital service providers. This is the case of countries such as Ireland, which hosts Meta, TikTok, X, Google, among several other VLOPs and VLOSEs, such as Shein or Temu (European Commission, 2026a). This context has direct implications for capacity planning.

Exclusive role of the European Commission

A key structural distinction within the DSA enforcement model is between ordinary supervisory activity and the oversight of systemic risks. For VLOPs and VLOSEs, the European Commission holds exclusive supervisory and enforcement powers. This centralisation is deliberate. Systemic risks – such as large-scale manipulation of public discourse or structural harms to fundamental rights – by definition transcend national borders and affect large groups of users. Concentrating enforcement at EU level reduces duplication and enables a consistent response to cross-border risks.

The relationship between national authorities and the Commission is therefore complementary and non-duplicative. DSCs address national and individual aspects of compliance, while the Commission handles cases with a systemic, repeated, or clearly cross-border dimension. Once the Commission opens proceedings against a VLOP or VLOSE, national authorities refrain from parallel action in the same matter.

Cross-border cooperation

Cross-border cooperation is an integral part of the enforcement model. When an issue manifests in one country but the provider is established elsewhere, the DSC in the country of destination does not assume direct supervisory authority. Instead, it activates cooperation mechanisms by collecting evidence and transmitting it to the DSC in the country of establishment, or, where justified, involving the European Commission.

Coordination between DSCs is facilitated through the European Board for Digital Services, which supports information exchange, alignment of interpretations, and the resolution of disagreements between authorities. While the Board's opinions are not legally binding, they play a significant role in shaping consistent application of the DSA.

Implications for Albania: Acting effectively within a networked system

For Albania, this architecture has concrete implications. Effective participation in the DSA system will depend less on national coercive powers and more on the ability to function credibly within a cross-border enforcement network. In practice, many high-impact cases will fall under the supervision of other DSCs or the European Commission. This does not marginalise Albania's role. Instead, it shifts it toward early detection, evidence preparation, and structured escalation.

To be effective, Albania requires an internal enforcement pipeline aligned with EU-level cooperation logic. This includes:

- systematic intake of user complaints and exchanges with civil society and research,
- internal system distinguishing national-only issues from cross-border or systemic concerns,
- structured evidence collection consistent with DSA procedural standards,
- disciplined escalation through formal cooperation channels.

In practice, the DSA tests the ability of public administration to operate in a networked regulatory model rather than a hierarchical one. Clear internal mapping of competences, decision-making thresholds, and cooperation pathways is a prerequisite for enforcement that is effective, predictable, and credible.

What can go wrong – and how to do better?

Early experience with the application of the DSA in EU Member States shows that the key implementation risks stem not from the legal text itself, but from how it is explained to the public and operationalised through early institutional decisions. The preparatory phase is decisive in determining whether the DSA becomes a functional tool for protecting users or a largely formal regulatory framework with limited visible impact.

Strategic communication as a safeguard against delegitimisation

One of the earliest and most significant challenges is strategic communication. At the international level, narratives portraying the DSA as a censorship instrument or as a politically motivated regulation targeting foreign technology companies have been actively promoted. These narratives, coming especially strongly from the United States, where many of the tech companies are based (Inserra, 2025; Pamuk, 2025), have also fed disinformation and polarised discourse within the EU (Corporate Europe Observatory, 2026; Kremidas-Courtney, 2025). Although they ignore the core architecture of the DSA, they can resonate strongly in candidate countries, creating resistance or public anxiety even before implementation begins.

For Albania, it is essential to communicate clearly and consistently from the outset the user-focused advantages and innovations of the Regulation. Communication should also consistently explain that the DSA does not define what content is illegal. Illegality is determined exclusively by national law, and the DSA does not amend Albanian criminal law. Platforms will be required to act only in relation to content that violates Albanian legislation. The DSA regulates procedures and responsibilities – not opinions or political positions.

Without proactive communication, there is a real risk that the DSA will be perceived as an infringement on freedom of expression and become politicised.

Strategic communication should therefore begin during the preparatory phase, not only as a reaction to controversy, and should be handled continuously, with the DSC playing a central role. However, this also extends to establishing proactive communication with the local digital service providers. Communication strategy about rights and obligations can commonly lag behind or be based on a knowledge asymmetry. While DSCs often presume the service providers to understand the regulation, these expect a more patient explanation of their duties provided by their national coordinator.

The position and protection of non-state actors

Effective DSA implementation depends on the active involvement of non-state actors, particularly civil society organisations and research institutions. As a matter of good practice, the Slovak coordinator has established an informal network of expert organisations in the field of online safety, the Trust and Safety Network, which convenes regularly to discuss relevant developments and exchange expertise on topics such as minors' safety online, election integrity, and artificial intelligence. The network also serves as a communication channel through which the national coordinator can share updates and invite input on emerging regulatory and policy developments (Council of Media Services, 2024a).

At the same time, early experience indicates that the non-state actors cooperating on DSA may be among the most exposed and vulnerable components of the system.

Entities designated as out-of-court dispute settlement bodies or, in particular, trusted flaggers, may become targets of disinformation campaigns, intimidation, or political pressure (Guo, 2026; Lenoir, 2024), despite being selected through transparent procedures, subject to ongoing performance assessment, and liable to withdrawal of their status in cases of underperformance or compromised independence. A notable escalation of such campaigns has been observed in Germany, where trusted flagger organisations have been accused of "totalitarian" practices (Beppler-Spahl, 2025; Smith, 2025), alongside cases of targeted defamation against individual members of civil society organisations, potentially affecting both operational capacity and personal safety.

Against this backdrop, the role of the DSC extends beyond the mere designation and supervision of mandates. It also encompasses the active protection of the legitimacy of these actors through transparent decision-making, clear public communication of their function, and the reinforcement of trust in their role within the enforcement ecosystem.

Balancing control and support in cooperative mechanisms

While cooperation with other actors – such as trusted flaggers, vetted researchers, and out-of-court dispute settlement bodies – must be governed by clear and transparent rules, implementation practice must avoid excessive procedural or financial barriers (Lenoir, 2024). If selection criteria and administrative requirements are set unreasonably high, organisations with substantial expertise but limited administrative capacity may be effectively excluded.

This would undermine the functioning of the DSA, which relies on these actors to support oversight of systemic risks. The DSC should therefore combine supervision with procedural support, treating these entities as partners in implementation rather than primarily as compliance risks. Delays in activating these mechanisms risk rendering one of the DSA's key innovations largely theoretical, weakening trust among civil society and the research community. The European Commission is preparing guidelines on trusted flaggers to help DSCs streamline the designation process, with adoption expected by the end of 2026 (European Commission, 2026c).

The risk of procedural compliance without real impact

Supervision under the DSA must go beyond verifying the formal existence of mechanisms "on paper". Otherwise, there is a risk of procedural compliance: situations in which platforms meet formal requirements without delivering meaningful improvements for users. This risk is particularly pronounced as DSA presents a governance-focused regulation.

Early practice from the DSA implementation highlights examples such as complaint mechanisms that exist in theory but are inaccessible in practice, generic or opaque explanations of moderation decisions, or extensive transparency reports that lack analytical value. To avoid this outcome, DSC supervision should focus on usability, accessibility, and sustained qualitative assessment over time. Without such qualitative scrutiny, the DSA risks being reduced to a bureaucratic exercise.

Complaint overload and the need for active case management

The DSA significantly expands the ability of individuals and organisations to submit complaints, both to platforms and to DSCs. While this reflects a deliberate policy choice, early experience points to a risk of overload through incomplete, duplicative, or politically motivated submissions.

Without clear internal procedures, a DSC risks becoming a passive intake body rather than an active supervisory authority. Early establishment of complaint-handling rules should therefore be accompanied by clear public guidance explaining which issues fall within the DSC's remit and which do not. Active case management is essential to ensure that complaints contribute to effective supervision rather than administrative congestion.

Next steps: sequencing and timing of DSA implementation

Under the DSA, most obligations apply on an ongoing basis from the date the Regulation becomes applicable in a country. For EU Member States, this date was 17 February 2024; for Albania, the same logic should apply once national legislation aligning with the DSA becomes applicable. This general rule is set out in Article 93(2) DSA. Unless the Regulation explicitly provides for a different deadline or transition period, obligations apply from the application date.

This has direct implementation consequences: the DSA provides no extended preparatory phase after it becomes applicable. Institutional, procedural, and enforcement readiness must therefore precede or coincide with legal alignment.

Institutional priorities at national level

The designation of the DSC and other competent authorities is the single most critical early task. For EU Member States, this obligation applied by 17 February 2024. For Albania, alignment with the DSA requires treating DSC designation as a front-loaded priority. Experience from EU Member States where DSC designation was, or remains, significantly delayed – such as Poland, Spain, or the Czech Republic (European Commission, 2025) – shows that without a functioning DSC, core mechanisms of the DSA, including complaint handling, trusted flaggers, vetted researchers, and enforcement cooperation, cannot operate effectively in practice.

At the same time, Member States were required to ensure that effective sanctions were available from the date of application. For Albania, this means that the sanctions framework – including fines and enforcement procedures – must be defined and operational when DSA-aligned legislation becomes applicable.

Once operational, the DSC must also comply with recurring reporting obligations. Under Article 55(1), DSCs must publish annual activity reports, including data on complaints received under Article 53 and the follow-up actions taken. While no fixed first reporting date is specified, the obligation applies on an annual basis once the authority is operational.

In addition, effective implementation requires readiness for cross-border cooperation. The DSC must be capable of participating in EU-level coordination mechanisms, including cooperation with other DSCs and the European Commission, and handling cross-border cases from the outset. Operational protocols for information exchange and cooperation should therefore be established early.

Platform-side obligations: Immediate and recurring duties

For intermediary services that are not designated as VLOPs or VLOSEs, most obligations apply from the date of application and continue on a recurring basis in accordance with the Regulation. All intermediary service providers must publish transparency reports at least once per year under Article 15(1), subject to applicable exemptions for micro and small enterprises. Hosting service providers, including online platforms, marketplaces, and e-mail or web hosting services, must have functioning notice-and-action mechanisms in place from the application date (Article 16).

Hosting providers are also subject to an ongoing obligation to inform competent law enforcement authorities where they become aware of information giving rise to suspicion of certain serious criminal offences involving threats to life or safety (Article 18(1)). This requires clear internal escalation and reporting procedures from the outset.

Finally, implementation is shaped not only by the Regulation itself, but also by evolving Commission guidelines, implementing acts, and supervisory practice at the EU level. Albania's preparation should therefore include continuous monitoring of EU-level interpretative developments to ensure alignment with the emerging enforcement landscape.

Discussion: How will Albanian citizens experience the DSA?

The DSA does not automatically make the online environment safer. It creates a framework within which safety, accountability, and user protection can be achieved. If users do not experience clearer decisions, effective remedies, and visible improvements in platform behaviour, the Regulation will be judged not by its ambition, but by its practical impact. Early implementation choices are therefore decisive. They determine whether the DSA is perceived as a living instrument that protects rights, or as a distant regulatory obligation with little relevance to everyday online experience.

For users, the DSA is not about EU institutions or national regulators in the abstract. It is about how platforms treat them when they use social media, marketplaces, or other online services.

First, users gain clearer decisions and enforceable remedies. When content is removed, an account is restricted, or visibility is reduced, platforms must explain why the decision was taken, whether it is based on national law or platform rules, and what redress options are available (Article 17).

Users can submit structured notices for content they believe is illegal (Article 16), use internal complaint-handling systems (Article 20), escalate disputes to out-of-court dispute settlement bodies (Article 21), and ultimately lodge complaints with the DSC alleging breaches of the DSA (Article 53). Where damage results from infringements, users may also seek compensation (Article 54).

Second, users should experience greater safety and transparency in everyday use. On online marketplaces, platforms must collect and display trader identity information and notify users if products they purchased are later identified as illegal (Articles 30–32). Advertising must be clearly labelled, including information on whose behalf it is shown and the main targeting parameters used (Article 26). Recommender systems must become more transparent, with users informed about ranking logic and given options to adjust key parameters (Article 27). VLOPs and VLOSEs must additionally offer at least one recommender option not based on profiling (Article 38). For children and teenagers, platforms accessible to minors must ensure a high level of privacy, safety, and security, including restrictions on targeting and protective default settings (Article 28).

For Albania, effective DSA implementation will depend less on formal transposition and more on early institutional design, capacity-building, and credible communication with the public. The Regulation offers an opportunity to strengthen trust in digital governance and improve users' everyday experience online. Realising this potential requires moving beyond formal compliance and ensuring that the DSA functions, from the outset, as a practical and user-centred system.

BIBLIOGRAPHY

Beppler-Spahl, S. (2025, June 19). German censorship machine in action: The police's shadow war on free speech. European Conservative. https://europeanconservative.com/articles/commentary/german-censorship-police-anonymous-functionaries-intimidation-chilling-free-speech/

Bilewicz, M., & Soral, W. (2020). Hate speech epidemic: The dynamic effects of derogatory language on intergroup relations and political radicalization. Political Psychology, 41(1), 3–33. https://doi.org/10.1111/pops.12670

Cleynenbreugel, P. Van, & Mattioli, P. (2023). Digital Services Coordinators and other competent authorities in the Digital Services Act: Streamlined enforcement, coordination lost? European Law Blog. https://www.europeanlawblog.eu/pub/digital-services-coordinators-and-other-competent-authorities-in-the-digital-services-act-streamlined-enforcement-coordination-lost/release/1

Corporate Europe Observatory. (2026, 25 March). Inside the far-right network targeting Europe's digital rules. https://corporateeurope.org/en/2026/03/inside-far-right-network-targeting-europes-digital-rules

Council of Media Services. (2024a). Pracovný materiál Kancelárie Rady na zasadnutie Rady pre mediálne služby dňa 24. 4. 2024. https://rpms.sk/sites/default/files/2024-04/2024-04-24_bod3.pdf

Council of Media Services. (2024b). Statute of the Council for Media Services. https://rpms.sk/sites/default/files/2024-10/Statut.pdf

Deceptive Design. (n.d.). Types of deceptive design. https://www.deceptive.design/types

European Commission. (2023). Albania 2023 report. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/8181fd61-7eee-11ee-99ba-01aa75ed71a1/language-en

European Commission. (2025, May 7). Commission decides to refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to lack of effective implementation of the Digital Services Act. Press Release. https://digital-strategy.ec.europa.eu/en/news/commission-decides-refer-czechia-spain-cyprus-poland-and-portugal-court-justice-european-union-due

European Commission. (2026a, February 17). Supervision of the designated very large online platforms and search engines under the DSA. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

European Commission. (2026b, January 26). Commission designates WhatsApp as a very large online platform under the Digital Services Act. https://digital-strategy.ec.europa.eu/en/news/commission-designates-whatsapp-very-large-online-platform-under-digital-services-act

European Commission. (2026c). Trusted Flaggers under the Digital Services Act. https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

European Union. (2022). Regulation (EU) 2022/2065 (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

Eurostat. (2025). Young people – digital world. Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world

Eurostat. (2026). Individuals' level of digital skills (from 2021 onwards). https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21__custom_21182119/default/table

Financial Intelligence Agency (FIU). (n.d.). Protection against computer fraud. https://fiu.gov.al/en/protection-against-computer-fraud/

Guo, E. (2026, January 19). What it's like to be banned from the US for fighting online hate. MIT Technology Review. https://www.technologyreview.com/2026/01/19/1131384/what-its-like-to-be-banned-from-the-us-for-fighting-online-hate/

Inserra, D. (2025, August 27). Trump administration rightly attacks EU tech regulations but tariffs and censorship at home harm Americans. Cato Institute. https://www.cato.org/blog/trump-administration-rightly-attacks-eu-tech-regulations-tariffs-censorship-home-harm

Institute for Development Research & Alternatives (IDRA). (2024, February). Assessing municipal and public e-readiness in Albania: National report. United Nations Development Programme (UNDP) Albania. https://www.undp.org/sites/g/files/zskgke326/files/2024-09/dra_national_report_final_eng.pdf

Institute of Statistics (INSTAT). (2024). Survey on information and communication technologies (ICT) usage in households and by individuals, 2024. https://www.instat.gov.al/en/themes/social-condition/information-and-communication-technologies-ict-usage-in-households-and-by-individuals/publication/2024/survey-on-information-and-communication-technologies-ict-usage-in-households-and-by-individuals-in-2024/

Kremidas-Courtney, Chris. (2025, 8 August). The US GOP's disinformation on Europe's Digital Rules. European Policy Centre. https://www.epc.eu/publication/the-us-gops-disinformation-on-europes-digital-rules/

Lenoir, T. (2024, May 28). The difficult life of trusted flaggers. Tech Policy Press. https://www.techpolicy.press/the-difficult-life-of-trusted-flaggers/

Media Ownership Monitor Albania. (2023). Online media. https://albania.mom-gmr.org/en/media/online/

Pamuk, H. (2025, August 7). Rubio orders U.S. diplomats to launch lobbying blitz against Europe's tech law. Reuters. https://www.reuters.com/sustainability/society-equity/rubio-orders-us-diplomats-launch-lobbying-blitz-against-europes-tech-law-2025-08-07/

Smith, L. (2025, December 8). The EU's censorship regime is coming for X – again. European Conservative. https://europeanconservative.com/articles/commentary/eu-censorship-regime-x-jd-vance-dsa/#:~:text=Another%20example%20from%20Germany%20is%20REspekt

The World Bank. (2024). Inclusive and user-centred services in Albania: Project brief. https://thedocs.worldbank.org/en/doc/5f5d7ed374b0dfd5945b469bbb8c6504-0080012024/original/Albania-Inclusive-Services-Project-Brief-July-2024-FINAL.pdf