Western Balkans Digital Rights Cooperation Project

Digital Services Act (DSA), Digital Markets Act (DMA), and AI Act Policy Paper

Background

The adoption of EU regulations for the Digital Services Act (DSA), Digital Markets Act (DMA), and AI Act, which follow the landmark GDPR regulation, marks a significant milestone in the EU's efforts to regulate the digital sphere. Stemming from concerns about online harms, market dominance, and ethical AI, these regulations aim to create a safer, fairer, and more transparent digital environment for EU citizens.

The need for these regulations arose from the rapid evolution of the digital landscape, where traditional laws struggled to keep pace with emerging challenges such as misinformation, hate speech, and unfair competition practices. The DSA addresses issues related to online content moderation, platform liability, and user rights, aiming to establish clear rules for digital service providers while safeguarding freedom of expression.

Meanwhile, the DMA targets digital gatekeepers, such as large tech companies, to prevent unfair practices that stifle competition and innovation. By imposing obligations on these platforms regarding data sharing, interoperability, and self-preference, the DMA seeks to level the playing field and foster a more competitive digital market.

Additionally, the AI Act sets out comprehensive rules for the development, deployment, and use of artificial intelligence systems within the EU, while particular focus remained on the use of biometric identification and mass surveillance systems.

Overall, the adoption of these regulations represents a proactive approach by the EU to address the challenges and opportunities brought by the digital revolution, aiming to strike a balance between the protection of fundamental rights and freedoms while protecting citizens and businesses in the digital single market. However, the issue will remain its implementation, in particular with regards to the big platforms as well as the oversight of the limited use of BMS technology in modern era.

New EU Legal Framework for the Digital Environment: DSA-DMA-AIA

Digital Services Act (DSA)

The essential reasoning behind the DSA rules is to make new and appropriate legal rules that would enable prevention of dangerous and/or illegal internet activities, or the dissemination of false information. The new challenges in this sense are recognized in the power gathered by online intermediaries and platforms, who are main obligors of the DSA rules. These are differentiated in four groups based on risks and obligations they bear: very large online platforms and search engines, online platforms (marketplaces, app stores, collaborative economy or social media platforms), hosting services and intermediary services offering network infrastructure. On the other hand, beneficiaries of these rules are online content users, be it consumers or smaller platforms or start-ups. The promise of the DSA is that it will provide fair rules for everyone in environment where online platforms play pivotal role, but also to ensure online safety and to uphold fundamental rights in digital environment.

On the other hand, it raises serious concerns regarding enforcement of censorship and selective suppression of particular information that can be of public interest.

Digital Markets Act (DMA)

DMA rules focuses on competition issues in digital markets. It recognises that certain online platforms that are providing core platform services have a potential to disrupt digital market, and that these situations cannot be appropriately addressed by traditional competition law rules. These platforms are called "gatekeepers" in DMA text. DMA prescribes in rather detailed in concrete terms what kind of practices these platforms must follow when they are provided services in their B2B relations, but also to end users (consumers). These practices include variety of obligations for gatekeepers, with the aim to prevent them to abuse their market power in apparent, or less obvious ways (for example, obligation to provide interoperability of their services, freedom of choice, reporting and transparency obligations, restrictions of favouring their own products and services).

Artificial Intelligence Act (AIA)

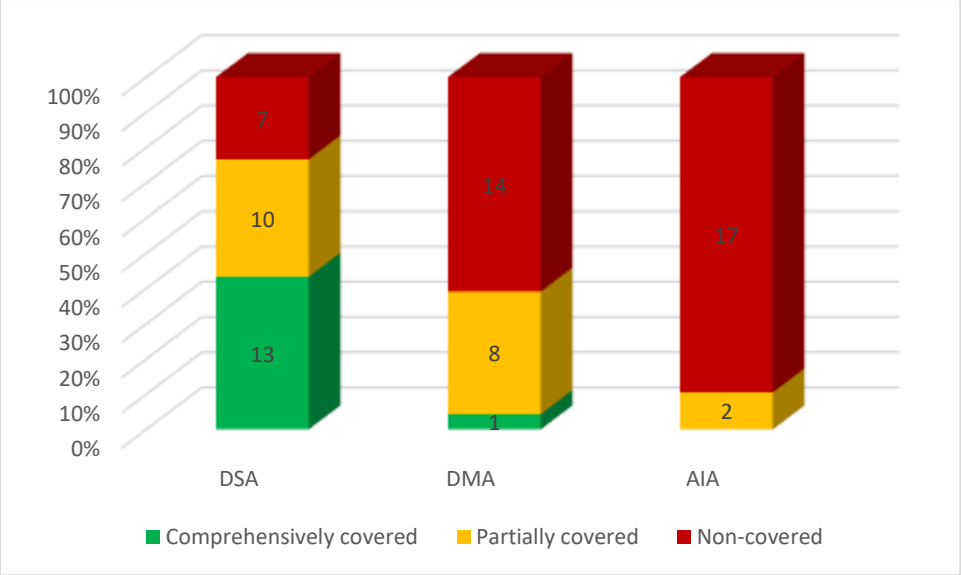
The AI Act is EU's all-encompassing legal framework for artificial intelligence. The definition of AI systems is drafted to be technology-neutral and uniform, although some systems such are remote biometric identification are specifically regulated. Its proclaimed aims are to ensure fair and transparent conditions for the development and use of AI systems, as well as respect for ethical standards, health, safety and fundamental rights. In the words of AI Act preamble, the goal is an uptake of human centric and trustworthy artificial intelligence. The AI Act uses risk-based approach, which means that AI systems that bear the unacceptable risks for people and society are forbidden, those that bear high risks are heavily regulated, while those with limited or minimal risks must comply with some basic transparency related rules. The regulation of the high-risk AI systems in a complex set of rules, legal and technical, that apply throughout the whole life-cycle of the system i.e. from its initial development, testing, any updates or changes till full implementation and use in concrete scenarios.

DSA-DMA-AIA Compliance in the Western Balkans Legal Frameworks: State of the Ecosystem in North Macedonia[1]

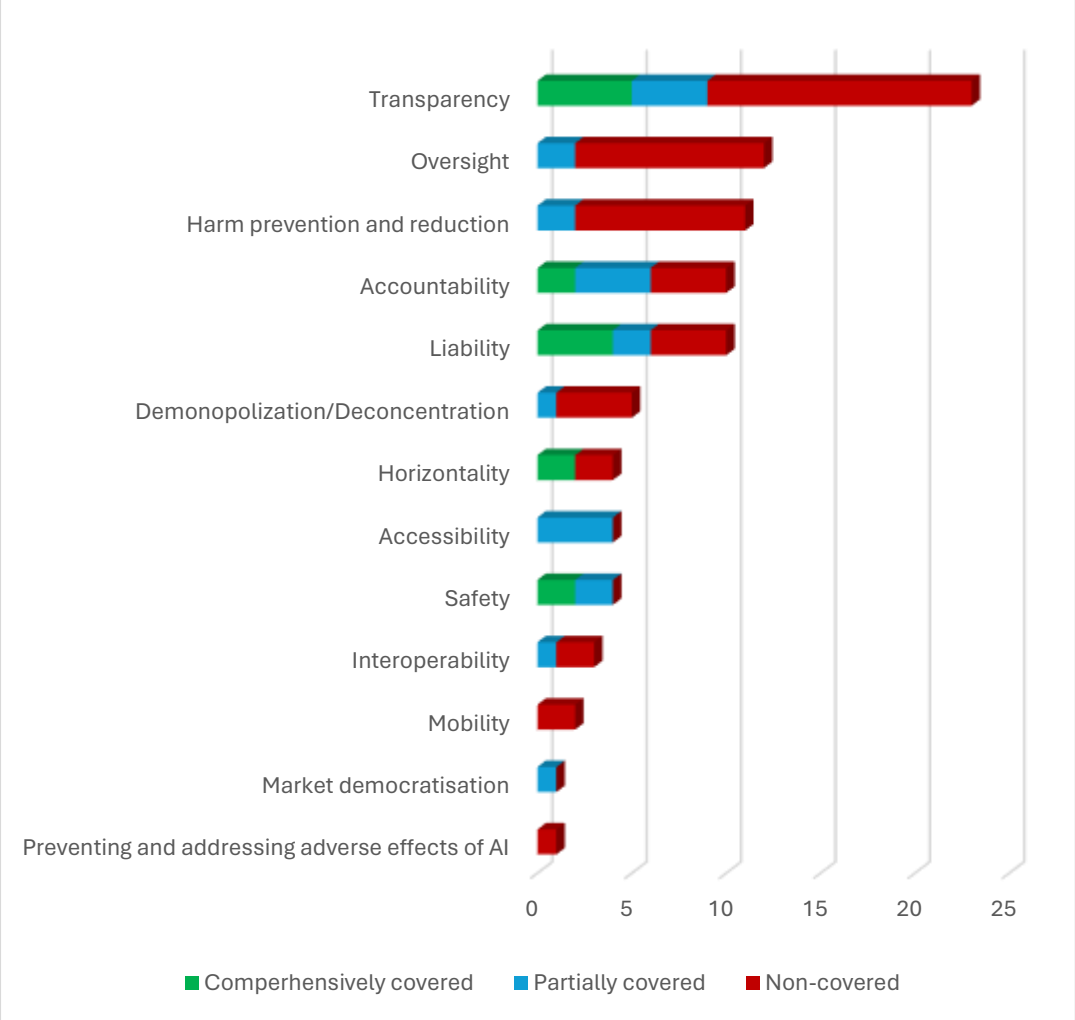
Finding 1: Out of the 72 DSA-DMA-AIA rules analyzed for their incorporation into the N. Macedonia regulatory framework, 34 were found in hard law, demonstrating a certain level of compliance, while 2 were identified in soft law.

Finding 2: More than 75% of DSA rules are partially or comprehensively recognized in N. Macedonia regulations. Some rules from the DMA are widely acknowledged but in a more general and indirect way. However, the rules from the AIA are covered, at the very least. (Graph 1)

[1] Hereinafter: N. Macedonia, or simply, Macedonia.



Finding 3: The normative analysis of DSA-DMA-AIA mapped 13 values as key pillars supporting the new European regulation. The graphic illustrates that the N. Macedonia regulation recognizes rules concerning transparency, accountability, liability, horizontality, and safety more comprehensively, while other values are partially covered or are not addressed by the existing rules. (Graph 2)



Regulation references - N. Macedonia

The Constitution
Law on electronic communications
Law on the provision of remote financial services
Law on electronic commerce
Criminal code
Law on violations
Law on commerce
Communications surveillance law
Personal data protection law
Bylaws and related legal acts
Law on mediation
Law on the security of networks and informational systems
Law on protection of consumers

As a general overview, the current level of legal conformity between Macedonian law and the three EU acts (the DSA, DMA and AI Act) is sporadic at best, ranging from the strongest (first) to weakest (last). Most of the actual conformity is a result of alignment lawmaking activity in the past with previous EU regulations (one example would be the EU Directive on Electronic Commerce). Other conformity arises out of lawmaking in compliance with other more general obligations undertaken by Macedonia in the scope of the United Nations, regional, multilateral, and bilateral agreements. Finally, some conformity arises out of native Macedonian lawmaking.

This approach results in a patchwork of legal instruments that often conform to some of the provisions of these three acts in spirit but not in actual wording or formality. The same patchwork is spread across different laws, bylaws, and other regulations, and often lacks structure or a unified approach. This conforms to the findings presented above.

Conformity with the Digital Services Act

Conformity with the DSA is partial. The provision of digital and intermediary services is tangentially regulated by several acts, starting with the Constitution and including the Law on electronic communications, Law on the provision of remote financial services, Law on electronic commerce, and by extension, the Criminal code, the Law on violations, the Law on commerce, the Communications surveillance law, the Personal data protection law, their bylaws and related legal acts, and some other legal acts. Content moderation is initially regulated from within the Law on electronic communications, which specifies a bylaw that is focused (amongst other topics) on the obligation of ISPs to inform consumers on the common methods in which electronic communications are used to cause illegal or IP infringement acts.

However, aside from specifying particular acts and violations in the Criminal code and the Law on violations (such as incitement of national, religious and ethnic hatred or discrimination, calls for genocide or the performance of a criminal act, and similar), and aside from the general stipulations in the Constitution which forbids censorship and supports free expression, content moderation is only tangentially regulated in a dedicated legal act on the level of a law. The most concrete stipulation can be found in the Law on electronic commerce, where responsibility of ISPs is regulated in regards of (illegal) content that they serve i.e. they are not responsible for any illegal content only if they are not aware that the content is illegal, they did not modify it while transferring it to the requestor (end user), and they were not the initiator of the request.

In general, content moderation is left generally unregulated as of yet. Notable exceptions are content moderation in relation to lawful surveillance of communications for the purposes of criminal investigation, management of security incidents and risks, and regarding issues of technical nature.

Regarding obligations for ISPs to designate single points of contact or representatives, there are legal rules as a general requirement (typically for dispute settlement and cooperation with authorities), not in relation to content moderation. ISPs are required to be transparent about content restrictions and moderation practices, by publishing their terms of services.

ISPs and online platforms are required to withhold data the process and create for a certain period and provide it to competent authorities on the basis of a request. Yet, whether this request can include regular notifications and proactivity on the part of ISPs in respect of reporting is unclear.

ISPs and online platforms are also obliged to suspend services under certain conditions (DSA art. 23), provide basic information about advertisements they display, be transparent about online advertisement, general obligation for verification and traceability of traders on their platforms, perform mandatory risk assessment, implement mandatory measures on addressing identified and regulated risks (especially regarding stability and security of networks), and monitor compliance with mandatory rules (but not related with very large online platforms or search engines *in particular*). Additionally, recipients of services have the legal means to file a complaint against ISPs with an authority and can pursue compensation for damage or loss, either through mediation dispute settlement or through a court procedure.

However, there are many key provisions from the DSA that are not implement. The identified ones are non-existent obligations for:

- establishing mechanisms that enable users to report existence of specific information (e.g. Illegal content) on platforms,
- establishment of internal complaint-handling systems,
- creation of interfaces to online platform providers or other ISPs,
- regulation of recommender systems,
- mandatory design of interfaces for online stores,
- informing consumers about the sale of illegal products or services on their platform, and
- establishment of independent compliance function.

All in all, the above paints a complex picture of conformity with the DSA act, and further lawmaking activity will be required to improve this patchwork by taking a structured and focused approach in enacting conformance laws in Macedonia.

Probably the best approach would be to enact a new law that will follow both the title, structure, and the spirit of the DSA, and unify provisions in a single instrument with its accompanying bylaws. This act would, of course, need to be compliant with overarching Macedonian and international acts, such as the Constitution, international conventions, documents and agreements, and other *leges generales* – e.g. in respect of the prohibition of censorship and support for free expression.

Conformity with the Digital Markets Act

When it comes to the DMA, conformity is similarly sporadic. The provision of information society services (ISS) is regulated with the Law on electronic commerce. However, no mention of *core platform services* is present in particular. B2B relations are also sporadically mentioned and regulated, not in particular to conformity of the DMA. The protection of personal data is covered with the general Law on the protection of personal data and the Law on electronic commerce.

End users have a stipulated right to file a complaint on ISS providers' practices. Transparency of advertisement is tangentially covered in the Law on electronic commerce and the Law on the protection of consumers. On non-discrimination obligation for ISS providers, the Law on consumer protection stipulates the obligation to provide access to public services under non-discriminatory conditions.

Interoperability of services is also covered tangentially in the Law on electronic communications, by stipulating such an obligation for operators of electronic communication. Finally, on the subject of compliance and reporting, there are some provisions in the Law on electronic commerce, albeit not directly aimed at CPSs. The provisions stipulate auditing obligations and rights, and additionally assigned competent authorities (Ministry of economic affairs, Ministry for electronic communications, Agency for electronic communications) that have the right to perform compliance audits. Non-compliance for ISSs with the above auditing obligations is subject to penalties.

However, as already mentioned above, Macedonian law as of yet does not specifically cover many specific cases that are subject of the DMA. These are:

- rules regulating usage of, or access to, business data in B2B relations in the digital sector,
- rules or practices (e.g. issued by antitrust or competition authorities) on marketing offers addressed *in particular* to end users of any CPS, including contracts and the right to access their online content,
- bundling of services on digital platforms or restriction to use third-party providers,
- rights of users to change settings or install and remove features of digital services or products,
- ranking obligations for ISS providers in the context of CPS provision,
- rights of end users to use a different ISS provider,
- interoperability of hardware and software in provision of CPS (tangentially covered, see above), and of messaging services,
- data portability rights for end users,
- availability of online search results,
- terms and conditions in B2B relations regarding ISS provision,
- reporting obligations regarding profiling practices done by ISS providers, and
- obligation to establish compliance body, or a body with similar function.

From the above can be seen that conformity to the DMA is even less powerful in comparison to the DSA act, and also is a patchwork of provisions. Similarly to the DSA, the conformity here can be significantly improved by enacting a new law that will follow both the title, structure, and the spirit of the DMA, and unify provisions in a single instrument with its accompanying bylaws, while taking care to be compliant with overarching Macedonian and international acts.

Conformity with the AI Act

Finally, conformity with the AI act is very low. Even though there was an initiative by the National Fund for Innovations and Startups for the creation of the first Macedonian AI Strategy a few years ago, it has not resulted in anything substantial in terms of policy. Thus, conformity regarding AI ethics, liability, responsibility, and accountability, as stipulated by the AI act, does not exist in Macedonian law as of yet.

This includes (non-)conformity with: differentiation of AI systems based on risk, prohibition of AI systems, compliance of AI systems with pre-determined set of requirements, compliance of general-purpose AI models, risk management, technical documentation, log keeping, use of personal data for training in particular to AI systems, human oversight on the AI systems functioning, conformity or compliance assessments of certain AI systems, obligations for AI systems importers, distributors and

deployers, transparency around functioning of AI systems, registration in databases, post-market phase obligations, reporting of AI systems incidents, and penalties for non-compliance. The only topic covered, albeit tangentially, is on fundamental rights (impact assessment). The Law on consumer protection stipulates that consumers have the right of satisfaction of 'basic needs', which tangentially fit many fundamental rights. There is no particular obligation for an *impact assesment*, however.

The silver lining is conformity with data protection, protection of biometric data, and prohibition of real-time biometric identification. Personal data protection is covered with the general Law on personal data protection, a legal document conforming to the GDPR. Within the provisions of the same Law biometric data is treated as 'special personal data category', and benefits from enhanced protection, including prohibitions and protections regarding real-time biometric identification (with exceptions for criminal investigation) and collation of personal data in databases.

On the subject of conformity with the AI Act, the path forward is clearly to enact specific and structured legislation that will convert AI Act's provisions into applicable law within the Macedonian legal system, while taking care to be compliant with overarching Macedonian and international acts.

Way Forward

As the EU enlargement has stalled over the last decade, many ideas were floated around how to frontload the EU membership benefits before the actual accession to the EU takes place. Thus, the concepts of gradual integration/phasing in of the Western Balkans to the EU have been developed which essentially mean that once a country meets certain criteria in a given area, it will be able to access those EU programmes and funds.

Of particular importance would be opening up of Union's policies pertaining to the digital area, as the Western Balkans digital ecosystems are intrinsically linked with the EU's ones whilst left out from the umbrella of EU digital acquis and platform regulations.

The underlying issue for the Western Balkans's Digital Single market membership is the legal framework. The legal instruments for WB (Stabilisation and Association Agreements) are less detailed than Ukraine or Moldova's DCFTAs and thus do not provide for carving out of EU's single market as they immediately aimed for the full EU membership of WB Given the complexity of amending the SAAs (as it would require adoption in all EU 27 national parliaments), this could be overcome by the general Annex to the SAP which would be adopted by EU-only and WB Six.

The benefits of the EU's digital single market for the Western Balkans would be indeed mutual. The EU can ensure the safe digital environment and enhance the economic convergence by opening up its market for booming digital sector in the region, while the Western Balkans can ensure EU's tools and protection mechanisms for the complex legislative initiatives (i.e. DSA, AI Act, Code of Conduct for Disinformation).

OPEN SOCIETY FOUNDATIONS
WESTERN BALKANS

This policy paper was produced with the financial support of the Open Society Foundations – Western Balkans. Its contents are the sole responsibility of the Institute of Communication Studies and do not necessarily reflect the views of the Open Society Foundations – Western Balkans.