RESEARCH ARTICLE

AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

NAVIGATING LEGAL FRONTIERS: ADDRESSING CHALLENGES IN REGULATING THE DIGITAL ECONOMY

Liridon Dalipi and Agim Zuzaku*

ABSTRACT

Background: *The integration of digital technologies into various facets of society has given rise to the digital economy, transforming the economic landscape. Western Balkan nations face challenges from this digital transformation, necessitating effective regulatory frameworks. Recognising and addressing regulatory gaps is crucial for fostering a secure and innovative digital environment. This study examines regulatory challenges in the Western Balkans' digital economy, focusing on public-private partnerships (PPPs) in cybersecurity. The research question revolves around identifying gaps in legal frameworks, understanding PPP dynamics in countering cyber threats, and assessing the potential impact of the EU's Digital Market Act and Digital Services Act on the Western Balkan regulatory sphere.*

Methods: *The research employs a qualitative approach, analysing the legal and policy frameworks of six Western Balkan countries. Data is gathered through an in-depth examination of cybersecurity laws, strategies, and action plans, with a specific emphasis on provisions related to PPPs. Comparative analysis is utilised to discern patterns and variations across the countries while also considering the potential impact of the Digital Market Act and Digital Services Act.*

Results and conclusions: *The analysis reveals a common challenge – the lack of specific regulations for the digital economy, creating a legal vacuum. Varying PPP integration levels exist across the Western Balkans. Significant findings include ethical considerations, challenges related to data privacy, and the need for robust competition regulations. Examination of the Digital Market Act and Digital Services Act highlights potential harmonisation opportunities and challenges. In conclusion, the research underscores the urgency for comprehensive regulatory reforms in the Western Balkans to address the challenges of the digital economy. The study advocates for developing specific laws governing digital platforms, strengthening PPPs to enhance cybersecurity, and incorporating ethical considerations in legal frameworks. The findings offer valuable insights for policymakers and stakeholders, emphasising the necessity of adaptive and forward-looking regulatory approaches in the ever-evolving digital landscape, considering the potential impact of EU initiatives such as the Digital Market Act and Digital Services Act.*

1 INTRODUCTION

In this era of rapid technological change, digital platforms have gained a key role in the economic and social structure, bringing about major developments in citizens' awareness of electronic services, which their governments now provide. The Western Balkans and the countries of the European Union are subject to this great transition towards the use of digital technology to improve the provision of services and to facilitate citizens' access to them.

In recent years, the governments of countries of the Western Balkans and the European Union have shown an increased commitment to the development of digital infrastructure and the broader use of online services. However, their use has not yet reached the desired levels, although there is an increase compared to other years.

To address this issue and understand the potential and challenges of using online services in these countries, this research will focus on the analysis of the legal basis, technological challenges, and impact of online services on the economy of these regions. By analysing legal instruments such as the Digital Markets Act (DMA), we will examine efforts to regulate digital platforms and improve citizens' use of online services.

The use of online services in the countries of the Western Balkans by a large part of citizens started with the spread of the Covid-19 virus. Prior to this, online services were primarily used by businesses for banking, tax services, e-commerce and other online services.[1] However, the state shutdown in mid-2020 accelerated the shift towards online platforms, leading to a significant increase in the adoption of digital services across various sectors.

The heightened adoption of ICT technology within the judicial community was encouraging. The first online trial was successfully conducted,[2] accompanied by webinars, consultations, and meetings held in a virtual environment. With continued support, these advancements hold the potential for positive, long-term impacts.[3]

With the focus on the use of online services, the countries of the Western Balkans have experienced a rapid transition towards a more digitised economy and society.[4] This has

1 Xiao Xiao and other, 'ICT Innovation in Emerging Economies: A Review of the Existing Literature and a Framework for Future Research' (2013) 28(4) Journal of Information Technology 264, doi:10.1057/jit.2013.20.

2 The first online trial in North Macedonia was held in the Basic Court Kavadarci, which found a way to hold trials with all involved participants without their joint physical presence in the court premises. See: Center for Legal Research and Analysis. *Challenges of the Judiciary During a State of Emergency* (CLRA 2020) 26.

3 Arbëresha Loxha Stublla and Njomza Arifi, 'The Western Balkans and the Covid-19: Effects on good Governance Rule of Law and Civil Society' (*Group for Legal and Political Studies*, 21 June 2020) <https://www.legalpoliticalstudies.org/the-western-balkans-and-covid-19-effects-on-good-governance-rule-of-law-and-civil-society/> accessed 24 January 2024.

4 Berat Rukiqi, *Covid-19 dhe Ndikimi në Ekonomi: Mundësitë për rimëkëmbje dhe transformim ekonomik* (Oda Ekonomike e Kosovës, Fondacioni Konrad Adenauer 2020).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

brought fundamental changes in how citizens follow services and businesses operate. This transition has brought new challenges, including the need for an appropriate legal and regulatory framework to support the development and use of online services in these countries.

The emergence of the COVID-19 pandemic in early 2020 triggered a significant shift in various aspects of daily life. With the need to prioritise public health and safety, traditional activities came to a halt, prompting a surge in the adoption of digital alternatives. In response to the challenges posed by the pandemic, numerous webinars were conducted, suggesting innovative approaches to advisory services.

The education sector swiftly adapted to the new normal, with schools and universities transitioning to online teaching methodologies facilitated by information technology. Similarly, remote work became a prevalent practice in professions where it was feasible. This paradigm shift was not only limited to the educational and professional realms but also extended to consulting services. Many organisations, recognising the potential of information technology applications, advocated for the delivery of their services through digital platforms.[5]

Amid the disruptions caused by the pandemic, the Information and Communication Technology (ICT) infrastructure played a pivotal role in sustaining economic activities. E-commerce experienced notable growth, reflecting the increased reliance of citizens and businesses on the Internet. The adaptability of individuals and enterprises to leverage ICT further underscored its significance during these challenging times.

1.1. The methodology

This study's methodology was developed through a qualitative approach. It used an interpretive framework to deeply understand the legal and political context of cyber security and the digital economy in Western Balkan countries, and compare them with EU countries. This methodology has followed several main steps in defining and analysing the key aspects of the study.

Various legal documents, policies, and strategies are reviewed to understand the interaction between the public and private sectors in cyber security and the digital economy. Starting with a detailed description of the legal, political and economic context in which the countries of the Western Balkans operate, we followed the identification of the main themes and categories of responsibilities.

5 Agim Zuzaku, Ilir Murtezaj and Valon Grabovci, 'The Role of ict During the Covid 19 Pandemic in the Advisory Service in Kosovo' in L Parijkova and Z Gancheva (eds), *Knowledge Society and 21st Century Humanism: 18th International Scientific Conference, Sofia, 1-2 November 2020* (Za Bukvite – O Pismeneh 2020) 816.

Extensive research has been used to deepen understanding and gather the views of key actors in the field. The use of this method has improved the consistency and depth of the analysis, enabling a deeper understanding of how the public-private partnership works in the development of policies and legal measures related to the challenges of cyber security and the development of the digital economy in the region.

1.2. Defining the problem

In a period of accelerated technological development, the digital economy has transformed economic paradigms, bringing new challenges to regulators and legislators. In this context, one of the main problems is the lack of an adequate and appropriate legal framework to efficiently address the various aspects of the digital economy.

Despite the rapid growth of digital markets and their substantial impact on the global economy, most current laws are still designed for a traditional economy and cannot cope with the specific challenges of this digital revolution. The appearance of the platforms and model of the collaborative economy has highlighted the lack of a dedicated legal basis to address the complex and specific challenges of this sector.

The problem is further highlighted by the insufficient response at the international level, despite some legal efforts like the Digital Markets Act. Thus, this lack of a global legal framework causes legal uncertainty and deficiencies in the protection of consumer rights, privacy and data security in the context of this new form of commerce.

In this context, addressing the problem focuses on the need to develop an appropriate legal framework capable of effectively addressing the challenges posed by the expansion of the digital economy while ensuring adequate protection for participants in this transformed and technologically advanced market.

2 LEGAL REGULATION AND THE DIGITAL ECONOMY

The literature review identified a link between legal regulation and the development of the digital economy.

Nowadays, the rapid development of information technology has announced the arrival of a new concept that is creating a new development paradigm for countries – the concept of "Digital Economy". This trend is an inevitable force shaping the trajectory of economic activities with the evolving technological landscape.

However, due to the rapid advancement of technological platforms, the massive widespread use of the Internet, and constant innovations, there is still no precise and universal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

definition of the digital economy. Various technological applications have caused major changes in the way companies, institutions and markets operate and function.[6]

In this context, efforts to deeply understand what is involved in measuring the digital economy are still in their infancy. Some efforts have included using online platforms, e-commerce, digital services, and automation of business processes. However, the scale and variability of these activities are such that they do not allow a clear and appropriate definition of the concept.

One of the main challenges is that the digital economy includes many different and diversified areas, causing difficulties in drawing up a general definition. In addition, the rapid changes and innovations in this field make it difficult to define boundaries and common terminology.

Therefore, continuing discussions and research to determine what the digital economy means in practice is necessary to understand the potential and challenges of this paradigm shift in the economic world.

The dangers of the digital economy have brought about political and policy controversy over the digital economy and e-commerce, examining its limits and how best to regulate it. Policy discussions on this topic, however, do not take into account the true distribution of digital commerce, which includes hardware, software, networks, platforms, applications and data as key elements, pushing the boundaries of e-commerce policies towards trade-in utility, services and intellectual property protection.[7]

The concept of a fully digital enterprise, blending people, technology, and organisational agility, stands as a formidable force in the contemporary economic and social landscape. However, embarking on the journey toward a digital future is a complex undertaking, fraught with challenges and considerations.

Organisations grapple with the fundamental question of whether they possess the capacity to confront the multifaceted challenges posed by digitalisation. This encompasses the ability to validate, assimilate, and effectively commercialise the wealth of knowledge generated by the digital landscape.[8]

6 Nguyen Thi Thanh Van and Nguyen Thien Duy, 'Digital Economy: Overview of Definition and Measurement' (2020 5th International Conference on Green Technology and Sustainable Development (GTSD), Ho Chi Minh City, Vietnam, 27-28 November 2020) 593, doi:10.1109/GTSD50082.2020.9303166.

7 Padmashree Gehl Sampath, 'Regulating the Digital Economy: Are We Heading for a Win-Win or a Lose Lose?' (*SSRN*, 18 December 2018) <https://ssrn.com/abstract=3107688> accessed 24 January 2024.

8 Agim Zuzaku and Blerton Abazi, 'Digital Transformation in the Western Balkans as an Opportunity for Managing Innovation in Small and Medium Businesses - Challenges and Opportunities' (2022) 55(39) IFAC-PapersOnLine 60, doi:10.1016/j.ifacol.2022.12.011.

The intricacies of IT work are formidable, especially for organisations lacking independent IT systems that can compete effectively in a dynamic digital environment. The sophistication, dynamism, and complexity of IT work pose hurdles for unprepared entities.

Many organisations encounter a trifecta of challenges – a dearth of resources, a shortage of talent, and competing priorities. The scarcity of resources, coupled with the distraction from other pressing matters, hinders their ability to concentrate on digital transformation. This often leads to a hopeful yet passive expectation that digital evolution will occur spontaneously with a stroke of luck.

The reality unfolds starkly – either companies and their inter-organisational networks proactively engage with digital transformation or risk being weakened by their own delays. The idea that digital evolution will materialise without conscious efforts proves to be a fallacy.

The digital future demands a strategic and concerted effort from organisations. While challenges loom large, the imperative for digital transformation necessitates a departure from passive anticipation to proactive engagement. Embracing the complexities of digitalisation, overcoming resource constraints, and fostering a commitment to innovation are essential steps for organisations aspiring to thrive in the digital era.

3 THE DIGITAL MARKETS ACT

The primary legal texts for the Digital Markets Act (DMA) are Regulation (EU) 2022/1925 of the European Parliament and the Council, dated 14 September 2022, regarding contestable and fair markets in the digital sector and the Procedural Implementing Regulation.[9]

The Digital Markets Act (DMA) serves as a crucial supplement to existing competition laws, aiming to curtail the power wielded by major digital entities. This chapter delves into the DMA's key provisions, shedding light on its obligations for designated gatekeepers and the consequences of non-compliance.

One of the central tenets of the DMA is the imposition of specific obligations on gatekeeper platforms. These mandates are designed to foster fair competition and create a level playing field within the digital ecosystem. For instance, gatekeepers are required to allow business users on their platforms to promote their offerings and engage in transactions with customers outside the confines of the gatekeeper's platform. Moreover, the DMA prohibits gatekeepers from displaying preferential treatment to their own services and products over those of third parties on their platforms, ensuring a more impartial ranking.

9 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 'On Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828' (Digital Markets Act) (Text with EEA relevance) [2022] OB L 265/1.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

To ensure adherence to the DMA, robust enforcement mechanisms are in place. Non-compliance with the established obligations can result in severe consequences for the implicated digital companies. Fines, constituting up to 10% of the company's total worldwide annual turnover (or up to 20% for repeated infringements), serve as a potent deterrent. Additionally, periodic penalty payments of up to 5% of the average daily turnover may be imposed. In cases of systematic infringements identified after market investigations, the DMA empowers authorities to institute additional remedial measures.[10]

The DMA officially came into force on 1 November 2022, following its publication in the Official Journal on 12 October 2022. Its practical application commenced on 2 May 2023. From this date, potential gatekeepers must notify the Commission within a two-month window if their platform surpasses specified thresholds. Gatekeepers are broadly defined as entities providing core platform services, meeting criteria such as having at least 45 million monthly active end users, 10,000 yearly active business users in the Union, or a minimum annual turnover of €7.5 billion over the last three financial years.[11] Following notification, the Commission assesses and designates the platform as a gatekeeper. Once designated, gatekeepers have a six-month grace period to align with the obligations outlined in the DMA.[12]

The DMA is an important regulatory tool for enforcing control over the power of large digital companies. By defining and imposing criteria and restrictions on gatekeepers, this act aims to ensure a fairer, more transparent and more competitive environment in digital markets. It is important to note that the DMA does not change the competition rules in the European Union; rather, it serves as an addition and improvement to address the specific challenges of digital markets.[13]

4 THE DIGITAL SERVICES ACT

The Digital Services Act (DSA), spearheading a comprehensive regulatory overhaul, ushers in a new era of digital governance within the European Union. This chapter delves into the DSA's intricacies, focusing on the regulatory cornerstone – Regulation (EU) 2022/2065 of the European Parliament and the Council, dated 19 October 2022.[14]

10 Anna Pingen and Thomas Wahl, 'New EU Rules for Online Platforms' (2022) 4 EUCRIM 228.
11 ibid.
12 Regulation (EU) 2022/1925 (n 9).
13 'About the Digital Markets Act' (*European Commission: Digital Markets Act (DMA)*, 2022) <https://digital-markets-act.ec.europa.eu/about-dma_en> accessed 24 January 2024.
14 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) (Text with EEA relevance) [2022] OJ L 277/1.

Born out of the necessity to adapt to the dynamic digital landscape, the DSA seeks to complement and modernise the existing E-Commerce Directive, a document now two decades old. The DSA introduces a set of uniform and horizontal regulations, primarily centred around due diligence obligations and conditional exemptions from liability for online intermediary services.

The DSA casts a wide net, encompassing all online intermediaries offering services in the single market, irrespective of their location within or outside the EU. Tailoring obligations to the size and type of intermediary services, the DSA classifies large online platforms as those with a significant societal and economic impact, meeting specific user numbers and annual turnover criteria.

At the heart of the DSA lies a robust framework for countering illegal content online. The Digital Services Act (DSA) complements existing consumer protection laws by mandating that service providers inform affected users or recipients about the reasons behind removing user-generated content. This requirement also extends to cases involving suspending or terminating services provided to the respective user's account. The aim is to enhance transparency and accountability in digital service provision, ensuring that users are informed about actions taken concerning their content and accounts. Specific due diligence obligations are placed on hosting services, including online platforms such as social networks, content-sharing platforms, app stores, and online marketplaces.

The DSA empowers users by facilitating the reporting of illegal content and challenging platforms' content moderation decisions. Transparency measures are introduced, mandating online platforms to disclose information on algorithms, terms and conditions, and advertising systems. Specific obligations target very large platforms, necessitating risk-based actions and independent audits of their risk management systems.

Effective enforcement mechanisms form a cornerstone of the DSA. It introduces fines, periodic penalty payments, and remedial measures for non-compliance. The oversight structure involves EU countries appointing a Digital Services Coordinator, supported by the European Board for Digital Services. Very large platforms fall under the direct supervision of the Commission, equipped with enforcement powers akin to anti-trust proceedings.[15]

Enacted on 19 October 2022, the DSA outlines a phased implementation approach. Very large online platforms, directly supervised by the Commission, are given a three-month window to publish user numbers. Following designation, these platforms have four months to comply with the DSA. From 17 February 2024, smaller platforms fall under DSA rules, with Member States empowered to enforce regulations.

15 'The Digital Services Act package' (*European Commission: Shaping Europe's digital future*, 2022) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 24 January 2024.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

The DSA emerges not just as a regulatory document but as a catalyst for transforming the digital landscape. Striking a balance between user empowerment, platform accountability, and regulatory oversight, the DSA sets a precedent for safer, more predictable, and trustworthy online interactions within the EU.[16]

5 NAVIGATING DIGITAL PLATFORMS IN THE WESTERN BALKANS

The European Union's neighbouring countries, particularly those in the Western Balkan region, undergo profound social, economic, and technological changes. These shifts have not only intensified international competition but have also fostered increased flexibility in the labour market.

Central to these transformations is the pivotal role played by technological advancements and digitalisation, which have led to the rise of novel employment structures such as remote and freelance work facilitated by international labour platforms. The prevalence of digital labour platforms in the region has become particularly noteworthy, serving as a dynamic mechanism for aligning labour and skill demand with their respective supplies.[17]

Platform work, defined as labour provided through or mediated by online platforms across diverse sectors, has gained prominence in all six Western Balkan countries. This work involves breaking down jobs into tasks, often contracted out for on-demand services, with at least three primary stakeholders: online platforms, workers, and clients. The matching process is digitally mediated, and the administration may involve varying degrees of algorithmic management.[18]

Two main categories of platform work are observed in the Western Balkans:

- **Digital Labour Platforms for Remote Services** - Involving the remote delivery of electronically transmittable services, dominated by international platforms such as Upwork, Freelancer, Guru, Fiverr, and People per Hour.[19]
- **Digital Labour Platforms for On-location Services** - Encompassing the physical delivery of services with digital matching and administration, particularly represented by local platforms offering ride-hailing and delivery services.[20]

Local labour markets in the region, often marked by underperformance and high entry barriers, especially for the youth demographic, have influenced individuals to explore new

16 Pingen and Wahl (n 10) 228-9.
17 European Training Foundation, *Embracing the Digital Age : The future of work in the Western Balkans: New forms of employment and platform work* (ETF 2022).
18 ibid 7.
19 ibid 8-9.
20 ibid 10-1.

forms of employment perceived as alternative job opportunities. The limited options in traditional labour markets have increased participation in the digital economy.[21]

Moreover, the economic repercussions of the full-scale Russian invasion of Ukraine have further shaped the landscape, prompting heightened engagement in new employment forms and platform work. In this context, the European Commission's proposed Directive on improving working conditions in platform work, currently under negotiation, is poised to significantly influence regulatory frameworks in the Western Balkans. This is particularly relevant in the context of EU accession and alignment with the International Labour Organization's principles of decent work.[22]

6 DIGITAL ECONOMY GROWTH IN THE WESTERN BALKANS

In contemplating the surge of new forms of work in the digital realm, understanding the factors propelling the expansion of the digital economy becomes paramount. Several crucial elements contribute to this phenomenon, with a country's broadband infrastructure, internet penetration, and digital competencies emerging as pivotal facilitators.

A nation's broadband infrastructure forms the backbone of digital progress. Robust and widespread broadband networks lay the foundation for leveraging innovative business models, contributing to enhanced competitiveness and employment growth. Access to high-speed internet is integral to seizing opportunities presented by the evolving digital landscape.

The extent of internet penetration within a country is a critical determinant of its readiness for digital transformation. Countries with higher levels of internet access are better positioned to harness the benefits of emerging digital trends.

Between 2012 and 2022, the Western Balkan countries, notably Serbia, closely followed with a remarkable 56.5% rise. Montenegro and North Macedonia have also displayed notable growth, with a 39.1% and 36.6% increase in daily internet usage, respectively.[23]

In 2022, Kosovo stood out with the highest proportion of individuals aged 16-74 years using the Internet daily, reaching an impressive 92.9%. Bosnia and Herzegovina and Albania maintained acceptable figures with 71.4% and 72.8% daily usage in 2021, respectively.

21 ibid 4-5.

22 Transforming our World: the 2030 Agenda for Sustainable Development (adopted 25 September 2015 UNGA Res 70/1) Goal 8 <https://sdgs.un.org/2030agenda> accessed 24 January 2024.

23 Eurostat, 'Enlargement countries – information and communication technology statistics' (*Eurostat*, May 2023) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Enlargement_countries_-_information_and_communication_technology_statistics> accessed 24 January 2024.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Despite these positive trends, there is a concern regarding the decline in weekly internet usage (but not daily) to below 10% in all countries in 2022. Serbia recorded the lowest share with 1.8%, followed by Kosovo (2.2% – 2020 data).[24]

These statistics underscore the increasing depth and reach of internet usage in the Western Balkans. However, there is a need for special attention to address potential disparities among countries and ensure fair and equal access for all citizens in this region.

Moving forward, there is a compelling argument for states to orient themselves towards online services. The burgeoning trend of internet usage highlights its growing importance in daily life. Strengthening the legal framework to support and regulate online services is imperative to ensure secure and equitable access for all citizens. By doing so, governments can harness the benefits of the digital age and propel their nations toward a more inclusive and technologically advanced future.

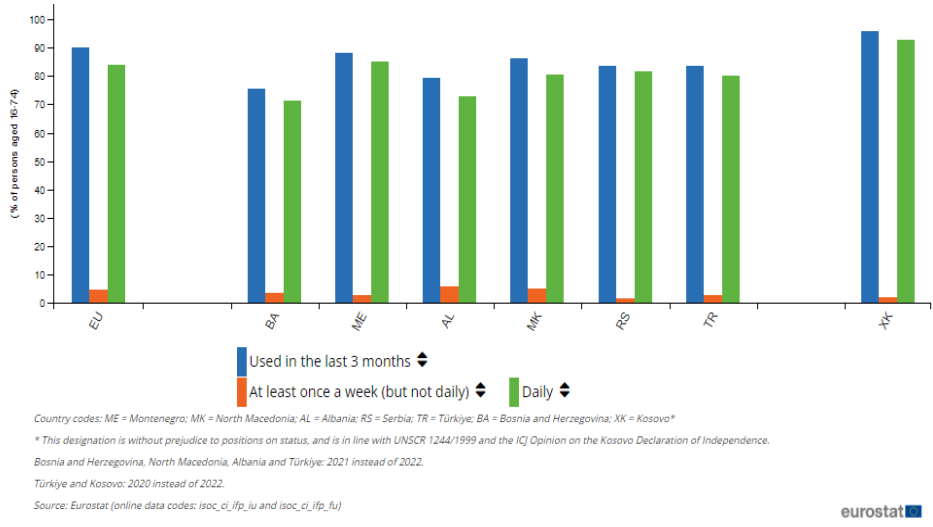

Figure 1. Frequency of internet use, 2022 (EUROSTAT, May 2023)

The proficiency of a population in digital skills is a key factor influencing its engagement in the digital economy. Digital competencies empower individuals to participate in new entrepreneurial activities and navigate the evolving employment landscape. Disparities in digital skills across the region highlight the need for targeted initiatives to bridge these gaps. Serbia and Montenegro exhibit comparatively better performance in this regard.

24 ibid.

The European Union, recognising the transformative potential of the digital economy, has been actively supporting the Western Balkans through initiatives like the Digital Agenda for the Western Balkans. These endeavours aim to accelerate the region's transition into a digital economy, ensuring that the benefits of digital transformation are widespread.

In alignment with broader EU initiatives, individual Western Balkan countries have crafted their national digital strategic frameworks. These frameworks serve as roadmaps for advancing digitalisation, fostering innovation, and enhancing the digital capabilities of their populations.

Flagship 8 within the Economic and Investment Plan for the Western Balkans 2021-2027 is a pivotal driver for digitalisation and the enhancement of human capital. This strategic initiative, encapsulated by the plan, includes key programs such as the Digital Agenda for the Western Balkans and the Youth Guarantee. These initiatives are poised to significantly accelerate the region's progress in the digital realm. The Economic and Investment Plan, a comprehensive strategy, outlines ten investment flagships backed by a substantial financial commitment of up to €9 billion in EU funds. Additionally, there is a potential to leverage an impressive €20 billion in investments through the Western Balkan Guarantee Facility.[25]

This ambitious plan is designed to bolster various sectors, including sustainable transport, clean energy, environment and climate, digital innovation, and the competitiveness of the business sector. Furthermore, it strongly emphasises human capital development, ensuring that the region is equipped with the necessary skills and capabilities to thrive in the digital future.

By targeting these strategic areas, the Economic and Investment Plan for the Western Balkans not only catalyses economic growth but also fosters sustainability, innovation, and human development. It represents a substantial commitment from the EU to support the Western Balkans in navigating the challenges and opportunities of the evolving digital landscape.

As the Western Balkans navigate the complexities of the digital economy, the synergy between infrastructure development, digital literacy initiatives, and strategic EU-backed interventions becomes instrumental in shaping a sustainable and inclusive digital future for the region.[26]

25 Western Balkans Investment Framework, 'Economic and Investment Plan for the Western Balkans 2021-2027' (*WBIF*, 2021) <https://www.wbif.eu/eip> accessed 24 January 2024.

26 Eurostat (n 23).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

7 LEGAL AND POLICY FRAMEWORKS ON PUBLIC-PRIVATE PARTNERSHIPS IN CYBERSECURITY: A COMPARATIVE OVERVIEW OF WESTERN BALKAN ECONOMIES

These efforts to regulate and coordinate cyber security measures cannot be seen separately from the general context of digital developments in these countries. In this era of the digital economy, the increased use of information and communication technology has brought about a number of challenges in various fields, including the digital economy. As these countries tackle cybersecurity challenges head-on, it is also important to consider how these measures impact the growth and development of the digital economy in their national and regional context. In this light, the analysis of public-private partnerships in cybersecurity serves as a key element in understanding the connections between economic development and digital security, paving the way for deeper research and actionable strategies for the sustainable future of technology and the economy in this region.

7.1. Albania

The Law on Cybersecurity, adopted in 2017, aims to establish a robust framework for achieving a high level of cybersecurity.[27] This legislation delineates specific security measures, rights, and obligations and outlines mutual cooperation between entities involved in the realm of cybersecurity. The overarching objective is to enhance the overall resilience and security of digital systems and networks by providing a clear legal foundation for addressing cyber threats and vulnerabilities. The law sets the stage for effective collaboration and coordination among various stakeholders, fostering a comprehensive approach to cybersecurity that safeguards critical infrastructure, data, and digital communication. The National Strategy for Cyber Security 2020-2025 of Albania is a key instrument defined by the Albanian Government, which aims to increase the security of networks and information systems at the national level. This strategy is approved by Decision no. 1084, dated 24 December 2020, of the Council of Ministers and is an essential priority of the Albanian Government.[28]

In accordance with the basic values in the physical and digital world, the strategy aims to guarantee cyber security in the Republic of Albania through the establishment of cooperative institutional mechanisms and legal and technical instruments. These are critical elements of defence in cyberspace and include digital infrastructures, transactions and electronic communications.

27 Law of the Republic of Albania no 2/2017 of 26 January 2017 'On Cyber Security' [2017] Buletini i Njoftimeve ZyrtareI Republikës së Shqipërisë 22/1751.

28 Decision of the Council of Ministers of the Republic of Albania no 1084 of 24 Desember 2020 'On the Approval of the National Strategy for Cyber Security and the 2020-2025 action plan' [2020] Buletini i Njoftimeve ZyrtareI Republikës së Shqipërisë 233/19696.

The strategy also focuses on building professional capacities, increasing nationwide awareness and strengthening national and international collaborations to ensure a secure digital environment. The core values of the strategy include the protection of fundamental rights, freedom of expression, personal data and privacy, access for all, democratic and efficient governance, as well as shared responsibility in ensuring cyber security.

The Strategy is regularly monitored by Albania through monitoring reports, with the aim of evaluating its implementation according to the policy goals and objectives for the period January - December 2021. The Action Plan of the Strategy contains 125 basic activities for its implementation in the coming years.[29]

The National Authority on Electronic Certification and Cyber Security (AKCESK) in Albania holds the crucial responsibility of overseeing the enforcement of three key laws: Law Nr.9880/2008 "On Electronic Signature," Law Nr.107/2015 "On Electronic Identification and Trusted Services," and Law Nr. 2/2017 "On Cyber Security." These legislative frameworks provide the basis for securing electronic transactions, establishing electronic identification standards, and addressing cybersecurity concerns in the digital landscape of Albania. AKCESK's mission, aligned with these laws, is to ensure the security of trusted services, bolstering reliability in electronic transactions among citizens, businesses, and public authorities while enhancing the efficiency of public and private services, including electronic commerce. Additionally, AKCESK defines minimum technical requirements for Critical Information Infrastructure (CII) operators in adherence to international standards, contributing to creating a secure electronic environment as part of its broader goal.[30]

In the Albanian cybersecurity landscape, notable aspects include the absence of specific frameworks delineating public-private cooperation. This absence suggests a potential gap in the collaborative mechanisms between governmental entities and private enterprises in addressing cyber threats. However, the law places emphasis on coordination with security institutions and sector-specific Computer Emergency Response Teams (CERTs), aiming to establish a network of collaboration and information exchange within the national cybersecurity framework. Moreover, the legislation underscores the importance of international cooperation, indicating a commitment to aligning Albania's cybersecurity efforts with global standards and best practices. The narrative here unfolds as a tale of a nation navigating the complexities of cyber threats, seeking coordination within its borders and beyond to bolster its resilience against evolving digital challenges.[31]

29 National Authority on Electronic Certificaton and Cyber Security, *Monitoring the "National Strategy for Cyber Security 2020-2025"* (AKCESK 2023).

30 *National Authority on Electronic Certificaton and Cyber Security (AKCESK)* (2024) <https://cesk.gov.al> accessed 24 January 2024.

31 Irina Rizmal, *Legal and Policy Frameworks in Western Balkan Economies on PPPs in Cybersecurity* (DCAF 2021).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

In conclusion, Albania's cybersecurity landscape reflects the country's efforts to tackle challenges in the digital realm. However, the absence of specific frameworks for public-private cooperation signals the need to enhance collaborative mechanisms. The Cybersecurity Law emphasises coordination with security institutions, sector-specific Computer Emergency Response Teams (CERTs), and international authorities. Albania is grappling with the challenges of an insecure digital environment, aiming to fortify partnerships and improve international collaboration to prepare for future digital challenges.

7.2. Bosnia and Herzegovina

The Policy of Electronic Communications of Bosnia and Herzegovina, adopted in May 2017, serves as a crucial document aligning the country with the Digital Agenda of Europe. It sets forth a comprehensive vision for Bosnia and Herzegovina's ICT ecosystem, emphasising support for the ICT sector as a central driver for economic growth. The policy envisions enhancing competitiveness, increasing business productivity, and improving public and e-government services. However, challenges persist in the segmented regulatory environment, with structural divisions across state, entity, cantonal, and local levels, leading to a lack of effective coordination. The public sector acknowledges its role and the need for collaboration but faces delays in law adoption and implementation at the state level. Despite these challenges, as a potential EU candidate, Bosnia has shown a growing commitment to advancing its digital and cyber capabilities, aligning with EU priorities. The Policy of Electronic Communications lays the foundation for Bosnia's digital society, representing a milestone in the country's cyber diplomatic efforts to align with European standards. However, progress is hindered by the complex distribution of powers between the central government and entities, requiring further development of the institutional and regulatory framework.[32]

In conclusion, Bosnia and Herzegovina stands at a pivotal juncture in shaping its digital and cybersecurity landscape. Adopting the Policy of Electronic Communications in 2017 reflects a commitment to advancing the ICT sector and aligning with European digital priorities. However, the absence of explicit references to public-private cooperation poses a notable gap, hindering the establishment of effective partnerships crucial for addressing cybersecurity challenges. The complex distribution of powers among the central government and entities further complicates policy implementation. While the country shows ambition in enhancing its digital capabilities, the nascent institutional and regulatory framework requires further development to realise these aspirations. Bridging these gaps and fostering collaboration between public and private entities will be imperative for Bosnia and Herzegovina to navigate the evolving digital landscape successfully.

32 'Bosnia and Herzegovina' (*EU Cyber Direct*, 2022) <https://eucyberdirect.eu/atlas/country/bosnia-and-herzegovina> accessed 24 January 2024.

7.3. Kosovo

The increasing frequency of cyberattacks in Kosovo has prompted the development of a new policy framework addressing cybersecurity concerns. Consequently, the Kosovo government adopted the National Cyber Security Strategy and Action Plan 2016–2019.[33] The Strategy positions public-private partnerships (PPPs) as both a "strategic principle" and a "strategic objective," emphasising their importance in enhancing the nation's cybersecurity posture. Establishing the National Cybersecurity Council dedicated to collaborating with the private sector underscores Kosovo's recognition of the vital role played by non-governmental entities in bolstering cyber defences. Additionally, the engagement of non-governmental organisations (NGOs) in educational initiatives and awareness campaigns reflects a holistic approach to cybersecurity.

Acknowledging the growing challenge of cybersecurity, the Program of the Kosovo Government 2021–2025[34] emphasises professional capacity building for cyberattack prevention, enhancing the legal framework, and modernising cyber protection equipment. Moreover, the Kosovo Security Strategy 2022–2027[35] prioritises bolstering Kosovo's cybersecurity capacities and pledges investments in cybersecurity, critical infrastructure, innovation, and technology alongside capacity-building efforts.

The legal framework for electronic services was laid in 2012 with the enactment of the Law on Information Society Services No.04/L-094[36] and the Law on Electronic Communications No. 04/L-109.[37] The former grants legal equivalence to electronic documentation, facilitating various electronic services, including e-commerce, e-banking, e-payment, e-government, and e-procurement, while also recognising the validity of electronic signatures. Kosovo's strategic approach and legal foundation position it to navigate the evolving digital landscape effectively and foster a secure and innovative digital environment. The Law on Electronic Communications in Kosovo regulates electronic communications activities with a commitment to technological neutrality and adherence to the EU regulatory framework for electronic communications. The overarching goal is to

33 Government of the Republic of Kosovo, *National Cyber Security Strategy and Action Plan 2016-2019* (Ministry of Internal Affairs 2015) <https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Kosovo%202016-2019%20Cyber%20Security%20Strategy-EN.pdf> accessed 24 January 2024.

34 Government of the Republic of Kosovo, *Program of the Government of Kosovo 2021-2025* (Office of the Prime Minister of Kosovo 2021) <https://kryeministri.rks-gov.net/wp-content/uploads/2022/04/Programi-i-Qeverise-se-Kosoves-2021-2025.pdf> accessed 24 January 2024.

35 Government of the Republic of Kosovo, *Kosovo Security Strategy 2022-2027* (Office of the Prime Minister of Kosovo 2022) <https://kryeministri.rks-gov.net/en/blog/kosovo-security-strategy-2022-2027/> accessed 24 January 2024.

36 Law of the Republic of Kosovo no 04/L-094 of 15 March2012 'On Information Society Services' [2012] Official Gazette of the Republic of Kosovo 6/1.

37 Law of the Republic of Kosovo no 04/L-109 of 4 October 2012 'On Electronic Communications' [2012] Official Gazette of the Republic of Kosovo 30/1.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

foster competition, ensure the efficiency of electronic communications infrastructure, and guarantee the provision of appropriate services within the territory of the Republic of Kosovo. This legislative initiative aligns Kosovo's electronic communications regulations with international standards, emphasising fairness, competitiveness, and the delivery of quality services to the citizens of Kosovo. By embracing the principle of technological neutrality, the law seeks to create a regulatory environment that accommodates advancements in communication technologies, thus promoting innovation and ensuring the continued development of the electronic communications sector in Kosovo.

Law No. 04/L-109 on Electronic Communications in Kosovo is a comprehensive legal framework designed to govern social relations within the realm of electronic communications networks and services. This legislation encompasses various aspects, including the regulation of associated services and facilities, the utilisation of electronic communications resources, and the management of social relations tied to radio equipment, terminal equipment, and electromagnetic compatibility. A crucial emphasis of this law is the provision of equal protection for personal data rights, particularly safeguarding the right to privacy in processing personal data within the electronic communications sector. By addressing these multifaceted dimensions, the law aims to ensure a fair and secure electronic communications environment, fostering the responsible and lawful use of technology while prioritising the protection of individuals' privacy and personal data.

In 2023, the Kosovo Assembly passed Law No. 08/L-173 on Cyber Security,[38] which mandates the establishment of the Cyber Security Agency and partially aligns with Directive (EU) 2013/40, focusing on attacks against information systems.

In conclusion, Kosovo has responded to cyber security challenges by adopting policies and laws to strengthen information protection and its cyber infrastructure. Adopting the National Strategy for Cyber Security, the Action Plan and creating the Agency for Cyber Security shows a commitment to capacity building and network security. However, efforts must continue to include Kosovo in international cyber security initiatives and strengthen cooperation with regional and international partners to address cyber security threats effectively.

7.4. Montenegro

Montenegro has actively strengthened its information security framework, notably with the adoption of the first Law on Information Security in 2010 and subsequent amendments in 2016 and 2020.[39] The more recent Law on Information Security in 2021 reaffirms and augments measures for achieving a high level of information security in networks and

38 Law of the Republic of Kosovo no 08/L-173 of 2 February 2023 'On Cyber Security' [2023] Official Gazette of the Republic of Kosovo 4/1.

39 Decree of Montenegro no 01-755/2 of 15 March 2010 'On the Promulgation of the Law on Information Security' [2010] Službenom listu Crne Gore 14/114.

information systems.[40] This legal framework establishes protocols for recognising and designating key entities, creating a national cybersecurity framework, managing cybersecurity procedures, and overseeing critical entities. It addresses vital aspects of information security, encapsulating confidentiality, integrity, and data accessibility.

Furthermore, Montenegro recognises the strategic importance of public-private partnerships (PPPs) by establishing the National Cybersecurity Council. This collaborative approach aims to secure critical information infrastructure, with a strong emphasis on cooperation with the private sector. The second National Cybersecurity Strategy (2018–2021) enshrines PPPs as a strategic goal, highlighting their pivotal role in enhancing the overall cybersecurity posture of Montenegro.

As the country navigates the burgeoning landscape of online services, the partnership between the public and private sectors emerges as a national priority, ensuring a resilient and secure cyberspace.[41] The recent findings from the analysis of laws and strategies in Montenegro indicate that the country is developing a positive trajectory in its cyber and information security environment. Legal improvements, such as the 2021 law on information security and the emphasis on collaboration with the private sector, reflect a commitment to strengthening cyber capabilities. Recognising the significance of the public-private partnership, this stance is acknowledged as a priority in Montenegro's Cyber Security Strategy for 2018–2021.

7.5. North Macedonia

North Macedonia adopted its National Cybersecurity Strategy 2018–2022 along with an Action Plan in 2018, marking a significant milestone in the nation's cyber defence and resilience efforts. The strategy and its accompanying action plan serve as foundational frameworks aimed at enhancing the country's cyber defence capabilities, fostering a safer digital environment, and fortifying national resilience against cyber threats. With a strategic focus on strengthening cyber defence mechanisms, enhancing incident response capabilities, and promoting cyber awareness and education initiatives, North Macedonia is poised to address evolving cyber challenges and safeguard its digital infrastructure effectively. Through strategic planning and collaborative efforts, the country seeks to uphold cyber resilience and ensure the security and integrity of its digital ecosystem.[42]

40 Laws on amendments to the Law on Information Security, see the link <http://sluzbenilist.me/pregled-dokumenta-2/?id=%7bC707AE79-3025-4387-B59B-34E5979FBC3E%7d> accessed 24 January 2024.

41 Government of Montenegro, *Cyber Security Strategy of Montenegro 2018-2021* (Ministry of Public Administration 2017) <https://www.gov.me/en/documents/fa4f3ed4-d059-4958-8847-d6111360a477> accessed 24 January 2024.

42 Government of the Republic of Macedonia, *National Cyber Security Strategy 2018-2022* (July 2018) <https://eucyberdirect.eu/atlas/sources/republic-of-macedonia-national-cyber-strategy-2018-2022> accessed 24 January 2024.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

In the Republic of North Macedonia, the Ministry of Information Society and Administration (MISA) plays a central role in formulating and implementing digital public administration policies, particularly concerning IT, eGovernment, and public administration modernisation. Government ministries and state bodies oversee sectorial ICT and eGovernment projects, with the National ICT Council established to monitor the implementation of the National ICT Strategy and guide public procurement plans. Supported by an Operational Body, the Council assists in strategic document preparation, reviews good practices, and collaborates with relevant stakeholders. Additionally, the National Cybersecurity Council, formed under the National Cybersecurity Strategy and pending Law on the Security of Network and Information Systems, coordinates cybersecurity efforts.

Furthermore, the establishment of the Broadband Competence Office aims to enhance broadband infrastructure efficiency, while the Digital Forum facilitates cooperation among diverse sectors for information society development. The Personal Data Protection Agency, established under the new Law on Personal Data Protection, ensures the lawful processing of personal data and safeguards individuals' rights and freedoms. Through these administrative bodies and agencies, North Macedonia is actively pursuing digital transformation and cybersecurity initiatives to foster a safe, resilient, and inclusive digital environment.[43]

In summary, North Macedonia acknowledges the importance of a multi-stakeholder approach in addressing cybersecurity challenges, highlighting the involvement of various actors, such as universities, the private sector, and civil society, in developing and implementing the national cybersecurity framework. The establishment of the National Cybersecurity Council further emphasises the commitment to fostering permanent cooperation between the public and private sectors, enhancing coordination, and ensuring comprehensive cybersecurity measures. This inclusive approach not only strengthens cybersecurity resilience but also promotes collaboration, innovation, and collective efforts to safeguard digital infrastructure and protect citizens' rights in North Macedonia's evolving digital landscape.

7.6. Serbia

The Law on Information Security, adopted by the Republic of Serbia on 26 January 26 2016,[44] represents a pivotal step in regulating measures to mitigate security risks in information and communication systems. This comprehensive legislation delineates the responsibilities of legal entities in managing and operating such systems while designating

43 'Governance - Republic of North Macedonia' (*European Commision: Joinup*, 2024) <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/governance-republic-north-macedonia> accessed 20 January 2024.

44 Law of the Republic of Serbia of 26 January 2016 'On Information Security' [2016] Official Gazette of the Republic of Serbia 6.

competent authorities for the implementation of protection measures. Serving as the first umbrella law of its kind, it establishes a framework to safeguard critical information infrastructure and enhance cybersecurity resilience across various sectors in Serbia.

The establishment of the Body for Coordination of Information Security Affairs marks a significant step towards enhancing the national information security framework in the Republic of Serbia. Envisioned as a cooperative platform for engaging in coordinated efforts and implementing preventive measures, this body plays a pivotal role in fostering collaboration across various sectors. While primarily serving as an advisory body, the Law recognises the potential for broader engagement by allowing the participation of representatives from public institutions, the private sector, the academic community, and civil society in expert working groups. This inclusion reflects a noteworthy display of political will to cultivate public-private partnerships in addressing information security challenges, a concept not widely prevalent in Serbia. Providing such space within the legal framework underscores a progressive approach towards information security governance in the country.

The National Strategy for the Development of Information Security (2017–2020)[45] in the Republic of Serbia underscores the importance of multi-stakeholder cooperation in enhancing cybersecurity measures. Adopted on 29 May 2017, this strategy delineates a roadmap for bolstering information security across various sectors. It articulates fundamental principles and delineates priority areas, such as securing information and communication systems, safeguarding citizens' digital interactions, combating high-tech crime, and fortifying the nation's information security framework. Through its comprehensive approach, the strategy aims to foster collaboration among stakeholders and advance Serbia's resilience against evolving cyber threats.

The Strategy sets the stage for the potential institutionalisation of public-private cooperation through specialised working groups within the Body for Coordination of Information Security Affairs, as mandated by the Law. Furthermore, it underscores the importance of establishing public-private partnerships (PPPs) within this framework to facilitate effective communication and optimise future activities. Emphasising the timely exchange of information and resource sharing, the Strategy prioritises the development of information security in the Republic of Serbia by leveraging collaborative efforts between the public and private sectors.[46]

In conclusion, Serbia has taken significant steps towards bolstering its information security framework through the enactment of the Law on Information Security and the establishment of the National Strategy for the Development of Information Security. These

45 Govenment of the Republic of Serbia, Strategy for the Development of Information Security in the Republic of Serbia for the period from 2017 to 2020 [2017] Official Gazette of the Republic of Serbia 53.

46 Irina Rizmal, *Guide Through Information Security in the Republic of Serbia 2.0* (OSCE Mission to Serbia, Unicom Telecom, IBM, Juniper 2018) 36.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

legislative measures highlight the country's commitment to addressing security risks in information and communication systems while emphasising the importance of multi-stakeholder cooperation. The creation of the Body for Coordination of Information Security Affairs further underscores Serbia's efforts to foster collaboration between public and private entities, marking a crucial milestone in its journey towards enhancing information security at both national and institutional levels. Through the recognition of public-private partnerships as a priority, Serbia demonstrates a proactive approach to addressing contemporary challenges in the digital landscape and strives to ensure the efficient exchange of information and resources for the collective benefit of its citizens and stakeholders. These summaries highlight key points from the legal and policy frameworks in Western Balkan economies regarding public-private partnerships in cybersecurity. The emphasis on multi-stakeholder cooperation, the role of national councils, and strategic goals for PPPs are common themes across these countries.

8 ONLINE SERVICES AS PART OF E-GOVERNMENT

In recent years, the use of Information and Communication Technology (ICT) has rapidly changed e-government services and business models and has largely met citizens' needs of citizens in terms of efficiency and quality of delivery of services by the government.

E-government refers to the use of government Information and Communication Technology to work more efficiently, disseminate information, and provide better services to the public. E-Government is more about government service delivery - the process of public administration reform - than technology.

Benefits resulting from the application of e-government include increasing the efficiency of better-functioning governments, greater trust between government and citizens by increasing transparency, empowering citizens through access to information and contributing to overall economic growth.

"E-Government relates to the use of ICT by government agencies for any or all of the following reasons:

- Exchange of information with citizens, businesses, or other government departments;
- Providing faster and more efficient public services;
- Improving internal efficiency;
- Reducing costs and increasing revenues;
- Restructuring of administrative processes."[47]

47 Agim Zuzaku, 'Communication and Transparency of Public Administration Through Electronic Governance' (master's thesis, University of Southeast Europe 2010).

9 CHALLENGES OF REGULATING THE DIGITAL ECONOMY: TOWARDS A COMPREHENSIVE LEGAL FRAMEWORK

The challenges of regulating the digital economy have emerged as a complex enigma, posing a formidable test to existing legal frameworks. The absence of specific laws governing digital platforms has created a legal vacuum, allowing for unclear practices and ineffective enforcement. In the quest for a solution, a model embraced by European Union member states is seen as a crucial first step towards an appropriate regulation.

The primary challenge stems from the lack of specific regulations, leading to an inability to address new issues and added complexities arising from the digital economy. Existing legal acts focus on specific aspects, often necessitating a comprehensive and adaptable intervention.

One major challenge is the risk to privacy and data security in a robust digital environment. The development of new technologies brings along new risks, emphasising the need for laws and regulations that address these issues with care and precision.

At a time when traditional industries undergo significant transformations and sectors reshape, the regulatory challenge is to adapt to their evolution and ensure a level playing field for all market players.

Monopolisation and barriers created for competition are other challenges stemming from the rapid development of digital markets. A robust regulation is required to prevent the development of monopolies and encourage healthy competition.

Ethical concerns, especially regarding autonomous decisions of systems and emerging technologies, constitute another layer of regulatory challenges. In this context, laws must be updated to address these concerns and ensure an appropriate use of new technologies.

While the benefits of new technologies are immense, they also come with challenges. Legal regulations must be prepared to protect consumer rights and privacy, ensuring a sustainable and fair digital environment. In this process, the search for an appropriate and flexible legal framework becomes essential to effectively and fairly tackle the challenges of the digital economy.

10 CONCLUSION

In conclusion, this research underscores the immediate need for comprehensive regulatory reforms in the Western Balkans to effectively address the challenges the digital economy poses. Specifically, there is a critical call for the development of tailored laws governing digital platforms, a reinforcement of public-private partnerships (PPPs) to bolster cybersecurity efforts, and the integration of ethical considerations within the legal frameworks.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

The study's insights extend beyond the mere identification of issues; they advocate for proactive measures and adaptive regulatory strategies. Policymakers and stakeholders are urged to prioritise the establishment of specific regulations for the digital economy to eliminate existing legal vacuums. Furthermore, strengthening PPPs is imperative for enhancing cybersecurity measures collaboratively. The findings also stress the importance of incorporating ethical considerations into legal frameworks to navigate the ethical dilemmas posed by advancing technologies.

In light of the European Union's proposed Digital Market Act and Digital Services Act, the research highlights both potential harmonisation opportunities and challenges for Western Balkan nations. Policymakers are encouraged to leverage these EU initiatives to align regional regulations, fostering a harmonious digital landscape. These conclusions present actionable recommendations, providing a roadmap for adaptive and forward-looking regulatory approaches in the ever-evolving digital realm. The study serves as a timely resource for guiding stakeholders toward effective regulatory responses in a rapidly transforming digital environment.

An examination of the digital economy and its legal frameworks across various countries reveals that while digitalisation brings numerous benefits, it also presents significant challenges. The digital economy, characterised by increased efficiency, global connectivity, and innovation, offers vast opportunities for businesses, governments, and individuals. However, alongside its advantages come inherent risks, including cybersecurity threats, privacy concerns, and the widening digital divide.

Across different nations, the legal frameworks governing the digital economy play a crucial role in shaping its trajectory. These frameworks vary in their effectiveness, with some countries prioritizing cybersecurity regulations, data protection laws, and measures to promote digital inclusion, while others struggle to keep pace with rapid technological advancements. Regulatory challenges often arise due to the complex nature of digital ecosystems, requiring agile approaches to address emerging issues while balancing innovation and consumer protection.

Several recommendations emerge to enhance the legal framework for the digital economy. Strengthening cybersecurity regulations is paramount to mitigate risks and safeguard digital infrastructure. Privacy legislation is essential to protect individuals' rights and ensure responsible data practices by businesses and governments. Moreover, promoting digital inclusion through affordable access to technology and digital literacy programs can bridge the digital divide and empower marginalised communities.

Support for innovation is vital to foster a dynamic digital economy, requiring regulatory frameworks that encourage entrepreneurship, investment in emerging technologies, and collaboration between industry stakeholders and policymakers. Additionally, an agile regulatory approach is necessary to adapt to the ever-evolving digital landscape, enabling

timely responses to new challenges while fostering an environment of trust, accountability, and ethical use of technology.

In conclusion, while the digital economy presents both opportunities and challenges, proactive measures within the legal framework can ensure its sustainable growth and equitable benefits for all stakeholders. By addressing cybersecurity risks, promoting digital inclusion, enacting robust privacy laws, and fostering innovation through agile regulation, countries can harness the transformative power of the digital economy while mitigating its inherent risks.

REFERENCES

1. Loxha Stublla A and Arifi N, 'The Western Balkans and the COVID-19: Effects on good Governance Rule of Law and Civil Society' (*Group for Legal and Political Studies*, 21 June 2020).
2. Pingen A and Wahl T, 'New EU Rules for Online Platforms' (2022) 4 EUCRIM 228.
3. Rizmal I, *Guide Through Information Security in the Republic of Serbia 2.0* (OSCE Mission to Serbia, Unicom Telecom, IBM, Juniper 2018).
4. Rizmal I, *Legal and Policy Frameworks in Western Balkan Economies on PPPs in Cybersecurity* (DCAF 2021).
5. Rukiqi B, *Covid-19 dhe Ndikimi në Ekonomi: Mundësitë për rimëkëmbje dhe transformim ekonomik* (Oda Ekonomike e Kosovës, Fondacioni Konrad Adenauer 2020).
6. Sampath PG, 'Regulating the Digital Economy: Are We Heading for a Win-Win or a Lose Lose?' (*SSRN*, 18 December 2018) doi:10.2139/ssrn.3107688.
7. Van NTT and Duy NT, 'Digital Economy: Overview of Definition and Measurement' (2020 5th International Conference on Green Technology and Sustainable Development (GTSD), Ho Chi Minh City, Vietnam, 27-28 November 2020) 593, doi:10.1109/GTSD50082.2020.9303166.
8. Xiao X and other, 'ICT Innovation in Emerging Economies: A Review of the Existing Literature and a Framework for Future Research' (2013) 28(4) Journal of Information Technology 264, doi:10.1057/jit.2013.20.
9. Zuzaku A and Abazi B, 'Digital Transformation in the Western Balkans as an Opportunity for Managing Innovation in Small and Medium Businesses - Challenges and Opportunities' (2022) 55(39) IFAC-PapersOnLine 60, doi:10.1016/j.ifacol.2022.12.011.
10. Zuzaku A, 'Communication and Transparency of Public Administration Through Electronic Governance' (Master's Thesis, University of Southeast Europe 2010).

11. Zuzaku A, Murtezaj I and Grabovci V, 'The Role of ICT During the Covid 19 Pandemic in the Advisory Service in Kosovo' in Parijkova L and Gancheva Z (eds), *Knowledge Society and 21st Century Humanism: 18th International Scientific Conference, Sofia, 1-2 November 2020* (Za Bukvite – O Pismeneh 2020) 816.

AUTHORS INFORMATION

Liridon Dalipi
Dr.Sc. (Law), Associate Professor, Faculty of Law, University "Kadri Zeka", Gjilan, Republic of Kosovo
liridon.dalipi@uni-gjilan.net
https://orcid.org/0009-0000-9372-104X
Co-author, responsible for research methodology, data collection, writing, and supervising.

Agim Zuzaku*
Dr.Sc. (Information Systems), Assistant Professor, University for Business and Technology, Prishtina, Republic of Kosovo
agim.zuzaku@ubt-uni.net
https://orcid.org/0000-0003-3811-9093
Corresponding author, responsible for conceptualization, writing, and data collection.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organizations.

ABOUT THIS ARTICLE

Cite this article
Dalipi L and Zuzaku A, 'Navigating Legal Frontiers: Addressing Challenges in Regulating Digital Economy' (2024) 7(2) Access to Justice in Eastern Europe 112-37 <https://doi.org/10.33327/AJEE-18-7.2-a000205> Last Published 1 May 2024

Submitted on 13 Jan 2024 / Revised 26 Jan 2024 / Approved 10 Feb 2024
Published ONLINE: 1 Apr 2024
DOI https://doi.org/10.33327/AJEE-18-7.2-a000205

Managing editor – Mag. Yuliia Hartman. **English Editor** – Julie Bold.

Keywords: *digital economy, legal framework, cybersecurity, public private partnership, Western Balkans.*

RIGHTS AND PERMISSIONS