



PARLIAMENTARY ASSEMBLY OF THE BLACK SEA ECONOMIC COOPERATION
PABSEC

INTERNATIONAL SECRETARIAT

Doc.: GA67/LC67/REP/26

COMMITTEE FOR LEGAL AFFAIRS AND INTERNATIONAL COOPERATION

REPORT*

“Legal Dimensions of Digital Governance and Innovation in the BSEC Region”

Rapporteur: Mr. Irakli Mezurnishvili, Member of the Committee (Georgia)

* *The text was considered by the Sixty Seventh Meeting of the Committee for Legal Affairs and International Cooperation, held in Bucharest, Romania on 17 March 2026 and discussed and approved by the Sixty Seventh Plenary Session of the General Assembly in Georgia, on 1 July 2026*

I. INTRODUCTION

1. The development of contemporary societies and economies is shaped by digital knowledge, innovation, and the expanding use of information and communication technologies (ICTs). The growth of digital networks and the emergence of a global information space are strengthening cross-border interconnections between public institutions, markets and citizens. Digitalisation increasingly permeates most spheres of social life, transforming economic activity, education and research, as well as public administration. It significantly transforms the relations between the state and society, generating heightened expectations regarding efficiency, transparency, participation, and accountability. At the same time, it complicates governance mechanisms, as public decision-making processes are increasingly mediated by data-analytics systems and interconnected digital infrastructures. In this evolving environment, innovation functions not only as a driver of competitiveness, but also as a catalyst for institutional renewal and democratic resilience.

2. Digital governance has emerged as a strategic instrument for modernising public administration, promoting innovation, and supporting sustainable socio-economic development. By reshaping service delivery, automating administrative processes, and strengthening transparency and integrity, digital governance can improve policy effectiveness and institutional performance. At the same time, it extends beyond the deployment of technological solutions, it entails a comprehensive transformation of governance structures, legal frameworks and institutional practices, including the modernisation of administrative law, and the establishment of safeguards for data protection, cybersecurity, procedural fairness and accountability. Effective implementation therefore requires long-term strategies, sustained political commitment, adequate financing, and robust legislative frameworks capable of ensuring legality, public trust and social legitimacy.

3. Given its geopolitical position at the crossroads of major transport corridors, energy routes and trade networks, the Black Sea Region occupies a strategic position in the broader geopolitical landscape. In this context, the development of effective digital governance frameworks is of particular importance, not only as a driver of administrative modernisation and economic competitiveness, but also as an instrument for institutional resilience and societal stability. Secure and interoperable digital infrastructures enhance governments' capacity to ensure uninterrupted service delivery, protect sensitive data flows, and strengthen preparedness against cyber threats and disinformation, thereby contributing to security and regional stability across the Wider Black Sea Region.

4. In recognition of the growing importance of digital governance and innovation for the economic development, the Parliamentary Assembly of the Black Sea Economic Cooperation (PABSEC) has consistently considered issues relating to modern governance and technological progress. Over the years, the Assembly has adopted a number of Reports and Recommendations, including: "E-Government in the BSEC Member States" (Rec. 146/2015) and "The Role of New Technologies in the Development and Strengthening of the Information Society in the BSEC Member States" (Rec. 143/2015). These documents provide a foundation for strengthening legislative cooperation

and demonstrate that progress in digital governance and innovation in the Black Sea Region requires harmonised standards and coordinated policies.

5. Accordingly, the Sixty-Seventh Meeting of the PABSEC Committee on Legal Affairs and International Cooperation, to be held in Bucharest, Romania, on 17 March 2026, will address the topic: “Legal Dimensions of Digital Governance and Innovation in the BSEC Region”. The present Report draws upon contributions from the national delegations of the Republic of Armenia, the Republic of Azerbaijan, the Republic of Bulgaria, Georgia, the Hellenic Republic, the Republic of Moldova, Romania, the Republic of Serbia, the Republic of Türkiye and Ukraine, as well as reference materials obtained from publicly available sources and official websites of relevant international organisations.

II. LEGAL DIMENSIONS OF DIGITAL GOVERNANCE AND INNOVATION IN THE BSEC REGION

6. Digital governance has been defined by various international institutions, each emphasising distinct dimensions of its scope, objectives and implications. These approaches converge in recognising that digital governance should not be understood solely as the digitalisation of administrative procedures. Rather, it involves a comprehensive transformation of governance models through the strategic and systematic use of information and communication technologies (ICTs). In this respect, the Organisation for Economic Co-operation and Development (OECD) define digital government as the strategic use of ICTs to achieve better government outcomes, while the United Nations conceptualises digital governance as the application of digital technologies to transform the internal functioning and external relationships of public authorities with a view to ensuring effective, transparent and accountable governance.

7. Building upon this digital governance may be understood as an integrated institutional framework based on interoperable electronic document management systems and digital service-delivery platforms, which collectively enable public authorities to operate more efficiently, transparently and responsively. A mature digital governance environment is typically organised as a nationwide distributed system providing a wide range of public services through secure digital channels. It encompasses multiple models of interaction, including Government-to-Citizen (G2C), Government-to-Business (G2B), Government-to-Government (G2G) and Government-to-Employees (G2E), each entailing distinct legal, organisational and procedural requirements. Therefore, digital governance constitutes a key pillar of modern public administration and inclusive socio-economic development.

8. The concept of digital governance is becoming more complex and multidimensional with the rapid advancement of artificial intelligence (AI) and the growing convergence of physical and digital governance systems. At the same time, traditional boundaries between sectors, policy domains and jurisdictions are becoming progressively blurred, giving rise to interconnected governance ecosystems. In this regard, the strategic importance of digital transformation has increased significantly. To meet the expectations of increasingly digitally literate populations, improve public-sector performance, and support inclusive and sustainable development, governments must harness digital transformation to strengthen institutional resilience, improve administrative efficiency, foster innovation, and deliver more responsive, citizen-oriented public services.

9. Digital governance advances socio-economic development by enhancing administrative efficiency, reducing transaction costs, improving regulatory quality, and expanding equitable access to public services. Through the digitalisation and automation of administrative procedures, public authorities can simplify workflows, shorten decision-making cycles, and reduce bureaucratic barriers, thereby fostering a more predictable, transparent and business-friendly environment. These improvements contribute to productivity, competitiveness and investment attractiveness, while also enabling more efficient allocation of public resources. At the same time, digital governance strengthens transparency and integrity by enabling traceability of administrative actions, facilitating public oversight, and reducing discretionary space in routine decision-making processes. By reducing opportunities for corruption and strengthening accountability, digital governance contributes significantly to public trust and to the legitimacy of public authority.

10. Digital governance also plays an important role in advancing innovation ecosystems and knowledge-based growth. Predictable regulatory frameworks, resilient digital infrastructure and access to public-sector data create favourable conditions for research and development and support start-ups and small and medium-sized enterprises (SMEs). By lowering entry barriers, facilitating access to relevant information, and enabling cross-sectoral collaboration, digital governance fosters entrepreneurship and accelerates the diffusion of innovative solutions. In this context, the legislative dimension of digital governance performs a dual function: it acts as an enabling framework for technological and organisational innovation, while also serving as a protective mechanism safeguarding fundamental rights, cybersecurity, data integrity, fair competition and the public interest. When properly designed and implemented, digital governance becomes a strategic asset for sustainable growth, technological sovereignty and long-term societal resilience.

11. Beyond efficiency gains, digital governance reshapes democratic participation and civic engagement by expanding opportunities for citizen involvement in policy formulation and public deliberation. Government portals, e-participation platforms and open-data initiatives create channels for structured dialogue between public authorities and society, enabling citizens, civil society organisations and businesses to contribute more meaningfully to public decision-making. These tools contribute to inclusiveness, enhance transparency and reinforce social accountability, thereby promoting more participatory governance models. However, the sustainability of these benefits depends on robust legal and institutional safeguards ensuring data protection, cybersecurity, accessibility, procedural fairness and non-discrimination, so that digital participation remains secure, inclusive and grounded in human-rights principles.

12. E-government constitutes a core component of the broader digital transformation of the public sector and forms one operational dimension of digital governance. In this context, e-government may be defined as the digitalisation of public administration and service delivery using information and communication technologies, with a focus on the provision of online public services, the optimisation of administrative procedures and the facilitation of interaction between public authorities and users. Digital governance encompasses e-government, but extends further to include the legal, institutional and policy frameworks that ensure interoperability, data protection, cybersecurity, transparency, accountability, procedural fairness and the protection of fundamental rights in increasingly data-driven and automated administrative environments.

13. Comparative international indicators demonstrate that digital governance is not merely a matter of political commitment or strategic vision, but also of measurable institutional performance and implementation capacity. Among these indicators, the United Nations E-Government Development Index (EGDI) provides a comprehensive benchmarking tool for assessing national progress. The EGDI is based on three core components: the scope and quality of online public service provision, the development of telecommunication infrastructure, and the level of human capital—particularly digital skills and education. By integrating these dimensions into a composite index, the EGDI offers governments, policymakers and international organisations a analytical basis for monitoring reforms, identifying structural constraints and designing evidence-based public policy.

UN E-Government Development Index (EGDI) in the BSEC Region

Country	Global rank (out of 193)
Albania	62
Armenia	48
Azerbaijan	74
Bulgaria	55
Georgia	69
Greece	36
Moldova	70
North Macedonia	84
Romania	72
Russian Federation	43
Serbia	39
Türkiye	27
Ukraine	30

Source: UN E-Government Knowledgebase (2024) ¹

14. The Black Sea Region occupies a pivotal strategic position at the intersection of key transport and energy corridors, making strong digital governance essential for enhancing regional connectivity, economic resilience, cybersecurity, and coordinated policymaking in an increasingly interconnected and data-driven global environment. Secure and interoperable digital infrastructures enable governments to maintain administrative functionality and strengthen preparedness against cyber threats, disinformation campaigns and disruptions to critical infrastructure. In this respect, digital governance contributes not only to economic development and administrative modernisation, but also to security and regional stability by reinforcing the

¹ The EGDI focuses primarily on the performance of e-government—namely the availability and quality of online services, infrastructure and human capital. While these are essential components of digital governance, they do not fully capture broader governance requirements such as accountability arrangements, procedural safeguards, rights protection, cybersecurity governance and institutional coordination.

capacity of public institutions to protect citizens, preserve democratic processes and uphold the rule of law during periods of increased uncertainty.

15. Despite notable progress in legal frameworks, institutional structures and digital infrastructure, BSEC Member States continue to face complex and interrelated challenges in effective implementation. One of the most common obstacles is the gap between legislative and administrative implementation capacity. While many countries have adopted comprehensive legislation on e-government, electronic public services, data protection, cybersecurity and digital identification, practical implementation is often constrained by limited resources, shortages of specialised expertise, fragmented governance arrangements and uneven levels of digital maturity across public authorities and territorial units. These factors hinder service integration, delay implementation and generate inconsistencies in service quality, thereby weakening institutional credibility and undermining public confidence in digital reforms. Insufficient financing and weak monitoring mechanisms further undermine sustainability.

16. Cybersecurity and the protection of personal and institutional data constitute another major and increasingly critical challenge. As public administrations become more dependent on interconnected digital platforms, cloud infrastructure and data-driven decision-making systems, vulnerabilities to cyberattacks expand significantly. Incidents affecting public services, critical infrastructure or sensitive information can have severe consequences for public trust, economic stability and national security. Effective cybersecurity therefore requires not only technological measures, but also comprehensive legislative frameworks defining institutional responsibilities, prevention and response mechanisms, oversight structures and proportionate sanctions for non-compliance. Strong coordination and international cooperation are equally essential, given the cross-border nature of cyber threats.

17. Digital inclusion represents a further fundamental structural challenge. Despite the growing availability of online public services, persistent disparities in access to reliable internet connectivity, digital devices and digital literacy continue to affect rural areas, disadvantaged groups, older persons, persons with disabilities and economically vulnerable populations. Without targeted public policy and inclusive service design, digital transformation risks exacerbating inequalities and undermining social cohesion and democratic participation. Legislative frameworks should therefore address accessibility and affordability, support digital skills development, and establish requirements for inclusive design, ensuring that digital governance advances social equity and territorial cohesion. In addition, limited uptake of e-services among certain groups remains an operational challenge, reflecting regulatory, cultural and behavioural barriers.

18. In parallel, the rapid expansion of artificial intelligence introduces an additional layer of legal, ethical and institutional complexity. While AI-enabled systems can enhance administrative efficiency and policy effectiveness, they raise concerns regarding transparency, accountability, algorithmic bias, discrimination, data protection and fundamental rights. Ensuring that AI deployment in public administration is governed by a robust legal and ethical framework is indispensable for safeguarding democratic values and the rule of law, while maintaining public trust in innovation-driven governance. Regulatory gaps remain in emerging areas, including the governance of digital platforms, big data analytics, certain blockchain-based applications, and comprehensive AI governance.

The Role of the Parliaments and the legal dimensions

19. Parliaments occupy a central role in shaping digital governance as the primary institutions of democratic legitimacy. By adopting legislation on digital infrastructure, e-services, cybersecurity, data protection, artificial intelligence governance, and digital inclusion, parliaments establish the legal foundations upon which digital systems operate. This function is not merely technical but constitutional in nature, as it determines how rights are protected, how public power is exercised through digital means, and how legality, proportionality and due process are preserved in increasingly automated administrative environments.

20. Parliaments exercise oversight over the implementation of digital governance policies and the use of public resources. Through hearings, committee inquiries, audit procedures and budgetary scrutiny, legislatures assess whether executive authorities deliver interoperable and secure systems, adequately protect citizens' data, ensure integrity in public procurement, and achieve measurable outcomes. This oversight is especially critical in the digital domain, where technological complexity and rapid innovation cycles can heighten the risks of institutional fragmentation, insufficient accountability and uneven service quality across public institutions.

21. Parliaments provide institutional platforms for public dialogue by convening representatives of civil society, academia, technical experts and business stakeholders to deliberate on the ethical, legal and societal implications of digitalisation. In sensitive domains such as artificial intelligence, algorithmic decision-making and the regulation of digital platforms, the deliberative and representative functions of parliament become particularly important, as democratic legitimacy depends on informed public debate, transparency of policy objectives and broad societal consensus regarding the appropriate balance between innovation, security, economic development and the protection of fundamental rights.

22. Parliaments also play a strategic role in aligning national digital reforms with broader regional and international frameworks. As cybersecurity risks, cross-border data flows, disinformation campaigns, and evolving digital market dynamics increasingly transcend national jurisdictions, effective responses require legislative convergence, regulatory coordination, and the systematic exchange of institutional experience.

23. Parliamentary cooperation with global partners enhances access to technical expertise, strengthens institutional interoperability and promotes convergence of governance approaches. Active participation in regional and international initiatives, together with systematic exchanges of best practices, will further assist BSEC Member States in aligning their legislative and regulatory frameworks with international norms and standards. By combining national responsibility with regional cooperation, the BSEC Member States can ensure that digital governance and innovation become drivers of sustainable socio-economic development, democratic resilience, cybersecurity and inclusive growth, fully consistent with the principles of transparency, accountability and respect for human rights.

III. SITUATION IN THE BSEC MEMBER STATES

24. Digital transformation constitutes one of the key factors determining the resilience and competitiveness of states in the 21st century. *The Republic of Azerbaijan* is implementing a comprehensive state policy aimed at the development of the digital economy and the introduction of innovative technologies. Azerbaijan actively participates in interparliamentary formats within the framework of the Black Sea Economic Cooperation (BSEC), promoting the harmonization of legislation, exchanging experience in digital governance, and developing joint initiatives.

25. The ASAN xidmət system, established in 2012, has become one of the most successful examples of digital governance, ensuring the integration of public services into a unified platform, the reduction of administrative barriers, and the enhancement of transparency and public trust. Key initiatives include state digitalization programs (2018–2022), the development of cashless payments (2019–2023), support for innovation ecosystems, and the expansion of digital infrastructure.

26. The Milli Majlis of the Republic of Azerbaijan plays a central role in shaping the legal framework for digital governance. Key legislative acts include: the Law “On Personal Data” (2010, amended in 2020); the Law “On Information, Informatization and Protection of Information” (1998, amended in 2021); the Law “On Electronic Government” (2015); the Law “On Telecommunications” (2005, amended in 2019); and the Law “On Innovation Activity” (2022), aimed at stimulating innovation and startups. These laws establish a systematic legal foundation for digital transformation.

27. The legal aspects of digital governance are a key element of sustainable development for the states of the BSEC region. Azerbaijan’s experience demonstrates that successful digital transformation is not possible without the active role of parliament, which shapes the regulatory and legal framework, ensures oversight of policy implementation, protects the rights of citizens, and contributes to the development of an innovation-driven economy. Strengthening interparliamentary cooperation within the BSEC will serve as an important factor in building a sustainable and interconnected digital future for the region.

28. Promoting digital innovation and developing digital governance in *the Republic of Armenia* are key directions for modernising public administration, enhancing the efficiency of the justice system, and ensuring sustainable socio-economic development. In this context, state policy aims to create an institutional and legal environment that fosters the widespread implementation of digital technologies, expands their accessibility, and improves the quality of services provided to citizens and businesses.

29. Within the framework of reforms in the justice sector, special attention is paid to the development of digital justice solutions, the introduction and modernisation of electronic systems, and the strengthening of cybersecurity capacities. These initiatives are designed to ensure more efficient, transparent, and secure judicial and administrative processes, while simultaneously increasing public trust in the state institutions.

30. To develop skills for working with digital technologies, targeted capacity-building programs are implemented for public servants. These include training in legal drafting, evidence-based

policy formulation, development of project management skills, the use of digital tools, and the improvement of citizen-centric services. An important component is also the exchange of international expertise through various peer-learning formats with partner countries.

31. To ensure the sustainable development of digital innovations, foreign language training programs, specifically in English, are implemented, increasing access for public officials to international professional resources. At the same time, organised trainings ensure continuity and long-term impact of capacity building. In this context, a series of courses were organised for the staff of the Ministry of Justice aimed at developing project management skills and strategic capacities. Additionally, a two-day specialized course titled “Introduction to Artificial Intelligence: Applying AI in the Public Sector” was held to provide employees with fundamental knowledge and practical skills regarding AI technologies.

32. In recent years, *the Republic of Bulgaria* has formulated comprehensive strategic documents aimed at accelerating the penetration of digital innovations across all sectors. At the end of 2025, the Digital Transformation Strategy of the Republic of Bulgaria 2026–2030 was developed, serving as the main guide for state policy in the coming decade. This strategy provides a coherent framework for accelerating national digital development, with the objective of establishing Bulgaria as a connected, secure, and inclusive digital country.

33. The strategy defines measures for modernising the public sector, stimulating innovation, and building a competitive digital economy with the active participation of citizens, businesses, and institutions. It recognizes the importance of digital skills as a key resource for modern society and plans targeted initiatives for their development. Core principles such as “digital by default” in public services, equal digital access for all social groups, ethics and transparency of digital solutions, high security standards, and “green” digitalisation contributing to sustainable development are also envisaged.

34. In early 2026, the Council of Ministers approved an interim monitoring report on the implementation of the Innovation Strategy for Smart Specialisation, tracking progress on strategic and operational objectives for the period 2021–2024. The report identifies key challenges facing the national innovation system and outlines guidelines for further action, taking into account European and global technological dynamics. It provides a basis for informed management decisions and for updating the Strategy so that it remains an effective tool for developing innovation and the high-tech economy by 2027.

35. A number of national programmes and initiatives have been introduced for the practical achievement of the strategic goals. Investments are being made, with the support of European Funds, in digital infrastructure, high-speed connectivity, 5G coverage, and technology start-ups. Under the Recovery and Resilience Plan, over 1,600 SMEs received funding to implement new digital solutions, totalling approximately 29.55 million EUR. Projects are also underway to establish Digital Innovation Hubs, providing expert assistance in fields such as artificial intelligence, robotics, and cybersecurity.

36. *Georgia* has established a comprehensive digital governance framework that links innovation policy with fiscal incentives and regulatory reform, including startup status recognition, preferential tax regimes (0% for startups in their first three years and 5% for IT firms) and aligned

R&D framework. Complemented by nationwide technology parks, acceleration programs, equity-free grants, AI prioritization, simplified residency for foreign IT professionals and partnerships with leading global accelerators, these measures position Georgia as a regional innovation hub and platform for piloting and scaling emerging technologies translating policy into practical tools that support SMEs, empower youth, expand market access and promote inclusive, sustainable growth.

37. At the same time, Georgia continues to focus on priority areas for improvement, including the need to further strengthen advanced digital skills, expand access to finance for early-stage innovators, deepen R&D commercialization and ensure responsible and inclusive adoption of AI and emerging technologies. Addressing these priorities through continued reform and international cooperation remains central to sustaining long-term, inclusive digital transformation.

38. In *the Hellenic Republic*, the Ministry of Digital Governance serves as the competent authority for artificial intelligence and data governance in both the public and private sectors. The development and implementation of artificial intelligence are recognized as key pillars of government policy, reinforced in July 2025 by the establishment of the Special Secretariat for Artificial Intelligence and Data Governance, reporting directly to the Minister and responsible for designing and coordinating a comprehensive policy framework. This institutional reform reflects the state's intention to implement the national AI strategy in a structured manner and in full alignment with European and international regulatory standards.

39. At the regulatory level, Greece actively participated in negotiations on Regulation (EU) 2024/1689 (the Artificial Intelligence Act), supporting a risk-based regulatory approach and enhanced protection of fundamental rights. Following its adoption, national representatives were appointed to the European Artificial Intelligence Board, and a special working group was established to coordinate the adaptation of national legislation and define the national AI governance model. Competent national authorities for rights protection in the context of AI systems were also designated. Greece, however, faces some legal and regulatory challenges in implementing digital governance.

40. Ensuring that national legislation is aligned with EU frameworks, such as the AI Act and the Data Governance Act, requires careful coordination to avoid gaps or overlaps, while ensuring the protection of fundamental rights in the use of AI and public sector data. Moreover, EU initiatives such as the Digital Omnibus highlight additional challenges, as the consolidation and simplification of digital rules aims to reduce legal complexity and administrative burdens that could otherwise create compliance risks for public authorities and private actors. Implementing AI-enabled e-government services also requires the establishment of clear governance procedures and responsibilities for the effective management of operational, ethical, and legal risks.

41. Despite the challenges, policies such as the AIGov digital assistant and AI applications in the Hellenic Cadastre have enabled the deployment of AI and e-government systems and services, which altogether improve efficiency, reduce administrative burdens and enhance transparency. Additionally, several initiatives have been adopted aiming at promoting digital innovation, fostering digital inclusion and developing digital skills. Moreover, the Ministry of Digital Governance actively promotes the development of a modern, powerful, and innovative AI ecosystem in Greece through two flagship projects: the “Daedalus” Supercomputer and the “Pharos” AI Factory.

42. Within the framework of the National Digital Transformation Strategy for 2023–2030 of *the Republic of Moldova*, the Digital Transformation Program of the Justice Sector 2025–2030 has the main objective to ensure the transparency, accessibility and efficiency of the act of justice. The program aims to implement electronic platforms for submitting applications, transmitting documents, consulting the status of files and scheduling hearings, thus facilitating access of citizens, lawyers and the business environment to efficient and secure judicial services, in accordance with the objectives of the National Digitisation Strategy.

43. In the healthcare field, a package of measures for health services digitisation was initiated and is being currently implemented. The approval of the National Program for Digitisation and Innovation in Health for 2025–2030 lays down the strategic framework for medical services modernisation by using digital technologies. The already fulfilled actions include the development and extension of health information systems, administrative and medical processes digitization, introduction of electronic networks, used especially for compensated medicines and the modernisation of mechanisms for medical services reporting and monitoring. These solutions contribute to reducing bureaucracy, downsizing administrative errors and increasing the efficiency of the medical act.

44. Within the framework of the National Program for Digitisation and Innovation in Health 2025–2030, the authorities have initiated the processes of creating and implementing the Electronic Health Record, which will allow secure access to patients' medical history and ensure data interoperability between medical institutions. At the same time, the program provides for the promotion and expansion of telemedicine solutions and remote consultations, to facilitate, in particular, access to medical services in rural or underserved areas.

45. In parallel, the Republic of Moldova is implementing sectoral digital transformation programs, including the Program for the Digital Transformation of the Energy Sector for 2026–2030, approved by the Government. The program aims to implement smart meters, develop a National Energy Management Platform, strengthen the cybersecurity of critical infrastructure and create an interoperable smart energy infrastructure. These measures aim to optimise energy consumption and production, ensure transparency and operational efficiency, as well as support the integration of renewable sources and the digitization of public services in the energy sector.

46. *Romania* considers digital governance a fundamental component of rule-of-law–based digital transformation, ensuring that technological innovation develops within a coherent, secure and rights-respecting legal framework. The national institutional architecture is coordinated by the Authority for the Digitalization of Romania, operating under Government Decision no. 89/2020, with responsibilities in e-government platforms, interoperability, digital identity and trust services. The legal framework has been strengthened through Law no. 242/2022 on data exchange and the National Interoperability Platform, and Law no. 214/2024 on electronic signatures and trust services, aligning national legislation with the Regulation (EU) No 910/2014.

47. From a governance perspective, Romania's approach integrates digital innovation with regulatory safeguards. The implementation of the General Data Protection Regulation through Law no. 190/2018 ensures robust data protection standards consistent with the General Data Protection Regulation, while national cybersecurity legislation reinforces institutional resilience against evolving digital threats. The launch of the Government Cloud and the operationalisation

of the National Interoperability Platform represent structural reforms designed to standardise data exchange, increase transparency and improve administrative efficiency.

48. National strategies promote innovation, digital inclusion and competitiveness in parallel with regulatory consolidation. The National Strategy on Artificial Intelligence (2024–2027) establishes principles for ethical AI deployment, risk assessment and public sector innovation. Broader policy instruments support digital skills development, digital entrepreneurship and the digitalisation of public services, including through investments under the National Recovery and Resilience Plan (PNRR). These initiatives contribute to building a digitally competent workforce and fostering a dynamic digital economy, while ensuring that innovation remains anchored in legal accountability and fundamental rights protection.

49. Romania's digital governance framework is closely integrated with European and international developments. National legislation reflects the objectives of the Digital Governance Act and the Data Act, facilitating secure data sharing and equitable access to data resources. Alignment with the policy objectives of the Digital Decade 2030 further guides national reforms. Within the BSEC framework, Romania supports enhanced regional cooperation through exchange of best practices in interoperability, harmonisation of standards for digital identity and trust services, and collaborative initiatives to strengthen cybersecurity and legal preparedness in the digital domain.

50. *The Republic of Serbia* is implementing digital transformation through a strategic and programmatic framework that includes the development of digital skills and inclusion, the promotion of digital innovation and the digital economy, as well as the improvement of information security as a precondition for trust in digital processes. Particular emphasis is put on strengthening the capacity of citizens, businesses and institutions to use modern technologies in a safe and sustainable way, with support for the development of the digital market and the international competitiveness of the ICT sector.

51. A key framework in this area is the Strategy for the Development of the Information Society and Information Security in the Republic of Serbia for the period 2021-2026, as well as the accompanying Action Plan (2024-2026), whose priorities are organised through three interlinked specific objectives: development of digital knowledge, skills and digital infrastructure in educational institutions; encouraging the digitisation of business, the development of the digital economy and innovation; improving information security as a foundation of trust and sustainable digital transformation.

52. At the regional level, cooperation takes place primarily within the framework of the Western Balkans, where digital transformation is recognized as one of the key drivers of economic growth and regional integration. Of particular importance is the Republic of Serbia's participation in initiatives stemming from the Western Balkans Digital Agenda, aimed at improving digital connectivity, developing digital skills, supporting digital innovation and enhancing cyber security. Within this framework, cooperation is developing in the areas of electronic communications, reduction of roaming costs, interoperability of the system, as well as exchange of good practices in the application of digital technologies.

53. At the international level, the Republic of Serbia actively participates in the activities of relevant organizations and initiatives such as the International Telecommunications Union (ITU),

the Organization for European Security and Cooperation (OSCE), the United Nations, as well as other multilateral formats dealing with the development of digital policies, Internet governance and information security. Cooperation with European Union institutions and bodies is of particular importance, including aligning the national framework with relevant EU policies and regulations in the field of electronic communications, digital services and information security.

54. The digital transformation process in the **Republic of Türkiye** is addressed within a multi-actor public structure under the 12th Development Plan (2024–2028), in a coordinated manner, focusing on legal infrastructure, industrial policies, digital infrastructure investments, and modernization of public services. As strategic policy areas, digital transformation and innovation support sustainable development by increasing Türkiye’s global competitiveness and the efficiency of public services. This holistic integration of digital technologies into public, industrial, and social sectors is facilitated by central coordination, legal regulations, and strategic developments in implementation

55. The legal infrastructure of the Republic of Türkiye’s digital transformation and e-government system is based on a comprehensive legislative framework created over the last twenty years. In addition to the “Electronic Signature Law” enacted in 2004, the “Law on the Regulation of Publications Made on the Internet” implemented in 2007, and the “Personal Data Protection Law” adopted in 2016, significant regulations strengthening the legal dimension of digital transformation have been implemented through changes in the judicial field incorporating digitalization and technological innovations.

56. The “National Artificial Intelligence Strategy” published in 2021, serves as the fundamental reference document for artificial intelligence policies in Türkiye. The strategy aims to develop artificial intelligence in a way that increases economic and social benefits, to implement it within the framework of ethical and legal principles, to ensure compliance with regulations on the protection of personal data, and to strengthen public-private sector collaborations. Within the scope of the strategy, the goal is to develop artificial intelligence within ethical and legal frameworks, to bring it into compliance with data protection regulations, and to ensure that artificial intelligence applications are used for the benefit of society.

57. The Information and Communication Technologies Authority (BTK) assumes the regulatory and supervisory role in the electronic communications sector. Electronic communication services are provided by operators authorized by the BTK. In this context, the aim is to support domestic data center operators, improve security and service delivery standards, and integrate data into the economy in a way that generates higher added value. On the other hand, cybersecurity is considered a fundamental policy area for the safe and sustainable advancement of digitalization. Within this scope, the protection of critical infrastructure, increasing the capacity to combat cyber threats, and the widespread adoption of domestic solutions are targeted. With this approach, the Cybersecurity Directorate has been established.

58. Over the past decade, **Ukraine** has consistently developed a comprehensive legal and institutional framework aimed at advancing digital governance, modernising public administration and supporting technological innovation. Digital transformation has become one of the key priorities of state policy, aimed at increasing transparency, efficiency and accessibility of public services for citizens and businesses. The legal basis for digital governance in Ukraine includes the

Laws of Ukraine "On Electronic Documents and Electronic Document Management", "On Electronic Trust Services", "On Electronic Communications", and "On Personal Data Protection".

59. The institutional development of digital governance is coordinated by the Ministry of Digital Transformation of Ukraine, which is responsible for implementing national digital policies, developing digital infrastructure and promoting innovation in the public and private sectors. In addition, Ukraine has adopted several strategic documents aimed at strengthening digital transformation, including the Concept for the Development of Digital Economy and Society and sectoral programmes related to digitalisation of public services. Overall, Ukraine's regulatory and institutional framework reflects the country's commitment to building an open, efficient and citizen-oriented digital governance system aligned with European standards and international best practices.

60. A key element of Ukraine's digital governance system is the development of e-government services through the national digital platform Diia. This integrated platform provides citizens with access to a wide range of public services online, including digital identification documents, business registration, social services and administrative procedures. The legal framework regulating the functioning of digital public services continues to evolve in order to ensure security, reliability and accessibility.

61. Ukraine actively participates in regional and international cooperation aimed at promoting digital governance, innovation and digital transformation. The country aligns its digital policies with European standards and regulatory frameworks, particularly in the context of Ukraine's European integration process. Cooperation with the European Union supports the harmonisation of legislation in areas such as electronic communications, data protection, cybersecurity and digital services. Ukraine also participates in international initiatives related to open government, digital innovation and the development of digital infrastructure. Partnerships with international organisations and technology institutions contribute to the exchange of best practices, capacity building and the development of joint digital projects.

IV. INTERNATIONAL FRAMEWORK AND EXPERIENCE

United Nations (UN)

62. At the global level, the United Nations has consistently emphasised digital transformation as a catalyst for good governance, sustainable development, and inclusive growth. Within the 2030 Agenda for Sustainable Development, digital governance contributes directly to Sustainable Development Goal 9 (industry, innovation, and infrastructure) and Goal 16 (peace, justice, and strong institutions), which recognize the role of ICTs in strengthening institutional capacity, improving access to public services, and enhancing transparency, accountability, and access to justice.

63. The World Summit on the Information Society (2003) established e-government as a priority domain for ICT-enabled development. The Geneva Declaration of Principles and the Tunis Agenda underscored the importance of modernising public administration, strengthening democratic participation, improving the efficiency and quality of public service delivery, and promoting international cooperation. These principles continue to provide guidance for national

legislative reforms, particularly in ensuring that technological progress remains aligned with social inclusion, human rights protection, ethical governance, and democratic accountability.

64. The United Nations University Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV), based in Portugal, is a policy-oriented think tank dedicated to Electronic Governance, a core centre for research, advisory services and training and a key partner within the UN system and its Member States with a particular focus on sustainable development, social inclusion, and active citizenship. The UNU-EGOV Strategy 2025–2029 seeks to respond to these realities and advance the Unit’s vision of becoming a global leader in digital governance, particularly in addressing challenges faced by the countries.

Council of Europe (CoE)

65. The Council of Europe is committed to protecting human rights, democracy, and the rule of law in the digital environment. The Council of Europe safeguards and promotes the rights to privacy and data protection through the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention on Cybercrime provides its Parties with a framework for domestic action and international co-operation for criminalisation of offences against and by means of computers, procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime, and international cooperation on cybercrime and electronic evidence.

66. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, is the first international legally binding instrument in this field, opened for signature in Vilnius on 5 September 2024. It aims to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy, and the rule of law, while being conducive to technological progress and innovation.

European Union (EU)

67. At the European level, the EU Digital Decade 2030 strategy and the new generation of digital legislation addressing data governance, cybersecurity, digital markets, digital services, and artificial intelligence constitute a comprehensive regulatory framework shaping digital transformation. This strategic framework establishes common objectives for digital infrastructure, digital skills, public service digitalisation, and business innovation, embedded in a coherent legal framework based on risk management, rights protection, and institutional resilience.

68. Legislative instruments such as the Artificial Intelligence Act, the Data Governance Act, the Digital Services Act, the Digital Markets Act, the EU cybersecurity framework, and the revised eIDAS Regulation introduce advanced regulatory models combining enabling innovation with safeguards for fundamental rights, competition, transparency, and systemic security. For EU Member States within the BSEC, these instruments generate binding obligations; for non-EU members, they serve as influential reference standards facilitating legal convergence, interoperability, and international cooperation.

69. At the EU level, the “Digital Omnibus” package constitutes a legislative initiative of the European Commission, which was presented on 19 November 2025 with the proposal for a

Regulation COM (2025), aiming to simplify the EU's digital legislative framework. This initiative represents the first step in the Commission's digital simplification agenda, with the main objectives of reducing administrative burdens. The key elements of this proposal include the consolidation of the Data Acquis, adjustments to the General Data Protection Regulation (GDPR), the introduction of a Single Incident Reporting Point (Incident Reporting), targeted amendments to the Artificial Intelligence Act (AI Act) and to the cookies policy (e Privacy) and the repeal of the Platform-to-Business (P2B) Regulation.

Organisation of the Black Sea Economic Cooperation (BSEC)

70. At the regional level, the relevance of digital governance and innovation is reflected in the BSEC Economic Agenda: Towards a Sustainable Future of the Wider Black Sea Area (2023). In particular, Goal 15 – “Good Governance and the Rule of Law: Strengthening the capacity of the Member States in conducting civil service and public administration reforms in line with best governance and administrative practices” provides a framework for public administration reform, including measures related to digital government, integrity, transparency, and institutional capacity-building.

71. The BSEC Working Group on Institutional Renewal and Good Governance serves as a platform for policy dialogue, exchange of experiences and coordination of activities among Member States in the areas of civil service reform and modernization of public administration. In this context, the Working Group organised, inter alia, a Webinar on “The role of E-Governance as a Citizen-Centric and Effective Approach to Public Service Delivery” (3 November 2022) and a Webinar on “Exploring the Role of Innovations in Driving Public Service Development” (14 June 2023), during which participants shared national practices and approaches related to e-governance and innovation in public service delivery.

V. CONCLUSIONS

72. Digital governance has become a key driver of socio-economic transformation in the twenty-first century, reshaping public administration, economic development, democratic participation and institutional resilience across the BSEC Region. Through the strategic deployment of digital technologies, governments can enhance administrative efficiency, service quality, transparency and accountability, while fostering innovation-led growth and more inclusive public services. At the same time, digital transformation generates complex legal, ethical and security challenges, including risks related to data protection, cybersecurity, algorithmic opacity and limited explainability, institutional accountability, digital exclusion and the increasing concentration of technological power. Addressing these challenges requires governance frameworks firmly grounded in democratic values, fundamental rights, legality, social equity and sustainable development, ensuring that technological progress strengthens, rather than undermines, public trust and democratic legitimacy.

73. The BSEC Member States have made progress in developing legislative frameworks, national digital strategies and regulatory regimes aligned with international and regional standards, particularly in areas such as e-government, cybersecurity, personal data protection, digital identification and artificial intelligence. In the absence of coherent legal frameworks, sustainable financing mechanisms and effective monitoring systems, digital transformation may reinforce

existing inequalities, weakening accountability and undermining public confidence. Bridging these gaps therefore requires comprehensive legislative reform, integrated strategic planning, strengthened institutional coordination and sustained investment in administrative, technical and human capacity.

74. Strengthening cybersecurity and personal data protection represents another key policy priority. Enhanced information sharing, joint response mechanisms and closer collaboration among national cybersecurity institutions within the BSEC framework can substantially strengthen collective resilience. Maintaining an appropriate balance between innovation and security remains essential to ensure that digital public services are trustworthy and that citizens' rights—particularly the right to privacy—are fully protected.

75. Promoting digital inclusion through legislative and policy measures should remain a core objective of digital governance reforms. Legal frameworks should guarantee equal access to e-government, embed accessibility and usability standards, and support infrastructure development in underserved regions. Equally important is sustained legal support for digital literacy, education and workforce reskilling initiatives. Strengthening digital competencies across society will increase service uptake, reinforce social cohesion and ensure that public investment in digital governance generates broad and equitable social and economic value.

76. Given the transnational nature of digital markets, cross-border data flows, cybersecurity risks and innovation ecosystems, deeper regional cooperation within the BSEC framework is indispensable. The development of a common regional roadmap for digital transformation, guided by shared strategic objectives while respecting national specificities, would strengthen coherence, predictability and mutual accountability. Harmonisation of legislative frameworks, mutual recognition of electronic identities and trust services, and convergence of technical standards would facilitate cross-border digital services, stimulate trade and innovation, and reinforce regional economic integration and collective resilience.

77. National parliaments play a significant role in shaping, legitimising and overseeing digital governance frameworks. Through legislative action, democratic deliberation and structured oversight mechanisms, parliaments ensure that digital transformation remains transparent, accountable, inclusive and firmly grounded in fundamental rights. By fostering public dialogue and engaging civil society, academia and the private sector, parliament enhances social legitimacy and ethical reflection. Within the framework of PABSEC, strengthened parliamentary cooperation promotes legislative convergence, knowledge sharing and coordinated responses to shared digital challenges, thereby reinforcing democratic resilience and regional cohesion.

78. The legal dimensions of digital governance and innovation constitute a strategic priority for sustainable development, democratic stability and economic competitiveness in the Wider Black Sea Region. By aligning national reforms with adaptive legislation, strong cybersecurity and data protection regimes, inclusive public policies, effective institutional coordination and enhanced regional cooperation, the BSEC Member States can harness digital transformation as an important driver of innovation, social cohesion, institutional trust and long-term resilience. Such a comprehensive and cooperative approach will enable the Black Sea Region to remain an active and competitive participant in the evolving global digital order, firmly anchored in the principles of transparency, accountability and respect for fundamental rights.