



PARLIAMENTARY ASSEMBLY OF THE BLACK SEA ECONOMIC COOPERATION
PABSEC

INTERNATIONAL SECRETARIAT

Doc.: GA67/LC67/REC209/26

RECOMMENDATION 209/2026*

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

1. The Parliamentary Assembly of the Black Sea Economic Cooperation (PABSEC) stresses that digital governance and innovation are central drivers of socio-economic transformation, institutional modernisation, democratic participation, and sustainable development in the XXI century. The Assembly reiterates its commitment to promoting a people-centred, inclusive, transparent, and rights-based digital society, in which all citizens can effectively access, use, and benefit from digital public services and emerging technologies. Such a society enables states to strengthen democratic legitimacy, improve public trust, enhance competitiveness, and ensure long-term socio-economic resilience.
2. The PABSEC underlines that digital governance extends beyond the mere digitalisation of administrative procedures and entails a comprehensive transformation of governance structures, legal frameworks, and institutional practices. By reshaping service delivery, automating administrative processes, and strengthening transparency and accountability, digital governance enhances policy effectiveness and public-sector performance. At the same time, it requires robust legal safeguards to protect fundamental rights, ensure cybersecurity, preserve procedural fairness, and guarantee responsible, ethical and transparent use of digital technologies.
3. The PABSEC recalls its previous Reports and Recommendations, including “The Role of New Technologies in the Development and Strengthening of the Information Society in the BSEC Member States” (Rec. 143/2015) and “E-Government in the BSEC Member States” (Rec. 146/2015), which further strengthen the parliamentary framework for legislative cooperation, policy convergence, and institutional reform in digital governance across the BSEC Region.
4. The PABSEC emphasizes the strategic significance of the Black Sea Region, situated at the crossroads of major transport corridors, energy routes, and trade networks, and increasingly exposed to cybersecurity risks, hybrid threats, and systemic vulnerabilities. In this context, digital governance assumes significant importance as an instrument for institutional resilience, continuity of public services, crisis preparedness, and societal stability. Secure, interoperable and trustworthy digital infrastructures strengthen

Assembly’s debate in June 2026 (see Doc. GA67/LC67/REP/27, Report of the Committee for Legal Affairs and International cooperation discussed on 17 March 2026 in Bucharest, Romania; Rapporteur: Mr. Irakli Mezurnishvili, Member of the Committee (Georgia).

The text is to be adopted at the General Assembly in Georgia, on 1 July 2026

governments' capacity to protect citizens, preserve democratic processes, and uphold the rule of law, thereby contributing to security, and regional stability.

5. The PABSEC recognizes that, despite notable progress in national digital strategies, legislative frameworks, and institutional arrangements, BSEC Member States still face complex and interrelated challenges. These include regulatory fragmentation, limited interoperability, uneven institutional capacity, insufficient coordination among public authorities, shortages of skilled personnel, cybersecurity vulnerabilities, and persistent digital divides. The Assembly emphasizes that the effective implementation of digital governance requires coherent legal frameworks, up-to-date innovation approaches, sustainable financing mechanisms, robust monitoring systems, and strengthened regional cooperation.

6. The PABSEC notes that the rapid development of emerging technologies, including artificial intelligence, digital platforms, big data analytics, and blockchain solutions, creates both unprecedented opportunities and significant legal, ethical, and security risks. The Assembly emphasizes that timely legislative adaptation, proactive regulatory approaches, and comprehensive governance frameworks are essential to stimulate innovation, provide legal certainty, and safeguard public interests and fundamental rights.

7. The PABSEC stresses that national parliaments play a central role in shaping, legitimising, and overseeing digital governance frameworks as the primary institutions of democratic representation and constitutional authority. Through legislative action and structured oversight mechanisms, parliaments establish the legal foundations governing digital transformation, ensure transparency, accountability, inclusiveness, and respect for fundamental rights. By fostering broad-based public dialogue and facilitating the participation of civil society, academia, technical experts, and the private sector, parliaments enhance social legitimacy and public trust, thereby ensuring that digital transformation remains citizen-centred and firmly grounded in democratic values.

8. The PABSEC further stresses that strengthened regional and international cooperation constitutes a key prerequisite for effective, secure, and inclusive digital governance. Given the transboundary nature of digital markets, cross-border data flows, cybersecurity threats, disinformation risks, and emerging technologies, closer cooperation among the BSEC Member States, as well as with relevant international organisations, is indispensable. Enhanced coordination, exchange of best practices and joint capacity-building initiatives contribute to reducing regulatory fragmentation, strengthening interoperability, improving cybersecurity preparedness, and promoting innovation-driven growth. In this respect, PABSEC plays a pivotal role in fostering mutual trust, advancing common strategic objectives, and reinforcing regional digital resilience, while aligning national reforms with international norms and standards.

9. Therefore, the Assembly recommends that the Parliaments and Governments of the BSEC Member States:

i. regularly review and update national legislation and policies to address emerging technologies, including artificial intelligence and digital platforms;

ii. ensure legal certainty and responsible innovation through technology-neutral, adaptive and forward-looking regulatory frameworks;

iii. adopt risk-based legal frameworks for digital governance ensuring transparency, human oversight, accountability and protection of fundamental rights;

iv. strengthen institutional coordination for digital transformation through sustainable governance mechanisms and long-term strategic planning;

v. *establish* independent regulatory authorities in areas such as data protection, digital commerce and cybersecurity and ensure their supervisory and enforcement powers through clear legislative mandates;

vi. *improve* legal and institutional frameworks for cybersecurity and personal data protection in line with international standards and evolving technological risks including through strengthened supervisory authorities, monitoring systems and proportionate sanctions;

vii. *introduce* sustainable financing and investment mechanisms to support the development of digital public infrastructure and services;

viii. *guarantee* equal access to e-government and digital public services through binding accessibility and usability standards;

ix. *support* secure infrastructure development in rural, remote and underserved areas to reduce digital divides;

x. *enhance* digital literacy, education and workforce reskilling as a core component of lifelong learning;

xi. *promote* open government tools, including open data policies and e-participation platforms, to strengthen public trust and democratic participation;

xii. *strengthen* transparency and accountability in digital governance, including oversight of algorithmic decision-making and digital public procurement;

xiii. *support* innovation ecosystems by improving access to public-sector data and enabling start-ups and SMEs to participate in digital markets;

xiv. *establish* monitoring and performance-measurement mechanisms to assess implementation progress and policy outcomes;

xv. *strengthen* digital resilience and continuity-of-government systems ensuring uninterrupted public services during crises;

xvi. *adopt* data protection standards and cybersecurity protocols for cross-border cooperation mechanisms;

xvii. *enhance* regional cooperation in cybersecurity through information sharing, joint response mechanisms and closer coordination among national authorities;

xviii. *promote* interoperable, user-friendly and secure digital public service platforms enabling easier access to administrative procedures and cross-border services;

xix. *develop* a common regional roadmap for digital transformation within the BSEC framework while respecting national particularities;

xx. *adopt* legal reforms aimed at facilitating compliance with relevant international and regional digital agreements;

xxi. *strengthen* cooperation with international organisations and actively participate in international initiatives in the fields of digital governance, artificial intelligence and cybersecurity.

10. The Assembly invites the BSEC Council of Ministers of Foreign Affairs to consider this Recommendation.