Ainura Ryspaeva
Associate Professor, PhD
Department of Finance, Analysis and Accounting
I. Razzakov Kyrgyz State Technical University
ainuraryspaeva9@gmail.com

Remi Raher
Associate Professor, PhD
Laboratoire ESPI2R
r.raher@outlook.com

Emilia Milanova
Chief Assistant Doctor
Faculty of Economics and Management
University of Agribusiness and Rural Development
e-milanova@hotmail.com

Anarbubu Sherbekova
Professor, Full Doctor
Department of Finance, Analysis and Accounting
I. Razzakov Kyrgyz State Technical University
a_sherbekova@outlook.com

Lukasz Kozera
Professor, Full Doctor
Institute of Law, Economics and Administration
University of the National Education Commission
lkozera4@hotmail.com

The role of the state administration in ensuring the safety of the digital economy in France, Poland, Bulgaria and Kyrgyzstan

ABSTRACT

The aim of this study was to identify the specifics and differences in approaches to digital security in the public administration systems of France, Poland, Bulgaria and Kyrgyzstan.
The theoretical research was based on a descriptive method, enabling analysis of legal regulation, institutional frameworks and strategic documents.

The study found that France has a structured digital security model based on the Digital Sovereignty Strategy. The Digital Republic Act and Law No. 2004-575, regulate user rights, digital ethics and platform responsibility. The General Data Protection Regulation and Directive on ePrivacy ensure high personal data protection, supported by institutions such as the "Commission nationale de l'informatique et des libertés" and the National Agency for Information Systems Security.
Poland prioritized strengthening cyber defence through the Act on the National Cybersecurity System and the National Cybersecurity Strategy of Poland for 2019-2024. The Cyber Shield program became a tool of direct budget investment in cyber infrastructure.
In Bulgaria, gradual development of digital services was identified under the National Program "Digital Bulgaria 2025" and the Electronic Government Act, though issues with implementation and interagency coordination were noted.
Kyrgyzstan follows a transformation model with strong digital inclusion, implemented via the Concept of Digital Transformation for 2024-2028, the "Tunduk" platform, and activities of the State Institution "Kizmat".
Overall, the results showed that France and Poland prioritize preventive regulation and strategic planning, while Bulgaria and Kyrgyzstan emphasize expanding access to digital services.
The practical significance of the study lies in substantiating the directions of harmonization of digital policy.

KEYWORDS: Cybersecurity – Public Governance – Regulatory Framework – Infrastructure Development – Risk management

1. Introduction

The growing dependence of economies on digital technologies is accompanied by the emergence of new risks: cyberattacks, data leaks, disruptions in the functioning of digital infrastructure. In response to these challenges, public administration is taking on a key role – from developing a regulatory framework to coordinating actions to ensure digital security. Bulgaria, France, Kyrgyzstan and

Poland demonstrate different approaches to protecting the digital environment, which allows us to compare the effectiveness of administrative decisions and identify models that can increase resilience to threats.

The low level of e-government and digital administrative services remains a significant challenge for public administration[1]. This topic was addressed by Kirilova and Naydenov[2], who analysed the state of e-government in Bulgaria compared to other European Union (EU) countries. The study revealed a significant lag in terms of transparency, cross-border availability of services, electronic identification and digital interaction. The low efficiency of electronic administrative services and their low level of use remain a significant challenge for public administration. This was investigated by Yordanova[3], who analysed the regulatory framework, service principles and the state of digital transformation in Bulgaria. The author focused on the implementation of integrated services, electronic identification and a single digital architecture, while noting that only 31.5% of citizens interacted with state bodies online.

In the context of digital transformation, weak interdepartmental coordination and limited implementation of comprehensive cyber security solutions remain obstacles to effective e-governance[4]. Kadyraliev et al.[5] examined the development of a unified digital security system in Kyrgyzstan, focusing on legal regulation, technical barriers, and staffing. The authors noted positive steps in institutional strengthening and support for state digital policy. The ineffectiveness of digital policy coordination at the European Union and

1 N. MUSAYEVA, M. ALIYEVA, L. GASIMOVA, and G. BAYRAMOVA, The Role of Blockchain Technology in Ensuring Transparency, Trust, and Auditing in Financial Markets: Prospects and Challenges. *Operations Research Forum*, 6(4), 2025, 167. https://doi.org/10.1007/s43069-025-00578-y.

2 K. KIRILOVA, and A.T. NAYDENOV, The state of e-government and digital administrative services in the Republic of Bulgaria. *Business Management*, 2, 2021, 5-20.

3 D. YORDANOVA, An overview of administrative services in the state administration in Bulgaria. *TEM Journal*, 14(2), 2025, 1689-1694. https://doi.org/10.18421/TEM142-66.

4 K. KETNERS, A. JAROCKIS, and M. PETERSONE, State budget system improvement for informed decision-making in Latvia. *Scientific Bulletin of Mukachevo State University. Series Economics*, 11(3), 2024, 86–99. https://doi.org/10.52566/msu-econ3.2024.86.

5 A., KADYRALIEV, A. ORUNTAYEVA, T. KAMCHYBEKOV, I. ABYSHOV, and A. BIGALI, The impact of digital technologies on the effectiveness of management in the agricultural sector of the Kyrgyz Republic. *Ekonomika APK*, 31(5), 2024, 35-44. https://doi.org/10.32317/ekon.apk/5.2024.35.

Member State levels makes it difficult to develop a targeted approach to ensuring digital security. Farrand and Carrapico[6] analysed the challenges associated with the coordination of EU digital strategies, drawing attention to the fragmentation of the regulatory framework, the complexity of interaction between national and national structures, and differences in the level of digital readiness of Member States.

While several studies have explored digital security and the transformation of public administrations, few have directly compared EU countries with transitioning economies like Bulgaria and Kyrgyzstan. Notably, Brzozowska-Rup et al.[7] analysed the impact of public administration on the development of the digital economy in Poland, but did not provide a comparative framework with other countries. This paper contributes to the literature by bridging this gap, providing a comparative institutional perspective across countries with different levels of digital infrastructure, legal maturity, and governance capacity.

The European Union's (EU) drive to strengthen digital regulation is facing resistance from individual states, posing challenges to digital sovereignty. Hulkó et al.[8] analysed how current European initiatives – Digital Services Act (DSA)[9], Digital Markets Act (DMA)[10], European Media Freedom Act (EMFA), and Artificial Intelligence (AI)[11] regulation-affect the balance between national self-deter-

6 B. FARRAND, and H. CARRAPICO, Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 2022, 435-453. https://doi.org/10.1080/09662839.2022.2102896.

7 K. BRZOZOWSKA-RUP, M. NOWAKOWSKA, and M. ZDRADZISZ, Cloud computing in the Polish public administration: Current state and development prospects. *Technological Forecasting and Social Change*, 205, 2024, 123500. https://doi.org/10.1016/j.techfore.2024.123500.

8 G. HULKÓ, J. KÁLMÁN, and A. LAPSÁNSZKY, The politics of digital sovereignty and the European Union's legislation: Navigating crises. *Frontiers in Political Science*, 7, 2025, 1548562. https://doi.org/10.3389/fpos.2025.1548562.

9 Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)", 2022. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

10 Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "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. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng.

11 Regulation (EU) No. 2024/1689 of the European Parliament and of the Council "Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial

mination and a single legal field. The authors examined new challenges posed by cyber threats, control over personal data, and the dominance of global technology corporations

The insufficient development of digital competence of civil servants and the absence of comprehensive mechanisms to support digital transformation in the public sector make it difficult to adapt to new challenges. This was analysed by Obelovska et al[12], who studied the impact of digital skills, organizational culture and leadership on the readiness of public administration for digitalization. It was found that the level of digital competences, trust in change and support from management directly affect the effectiveness of digital transformation. The authors also emphasized the importance of continuous learning and improving communication between government bodies.

The insufficient level of ethical and legal regulation of artificial intelligence creates risks for public administration in the digital environment[13]. This was investigated by Turillazzi et al.[14], who analysed the potential and challenges of using AI in the EU public sector. The authors pointed to the low effectiveness of existing regulatory tools, weak regulatory certainty and limited practical experience of public institutions.

Despite the availability of digital transformation strategies and regulatory initiatives, current research lacks comprehensive assessment of their effectiveness, regional disparities, socio-economic impacts, and adaptability to national political contexts – all of which require further in-depth analysis.

The purpose of this study was to determine the specifics of the influence of public authorities on the formation of a secure digital environment in France, Poland, Bulgaria and Kyrgyzstan. Within the framework of achieving this goal,

---

Intelligence Act) (Text with EEA relevance)", 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

12 K. OBELOVSKA, A. ABZIATOV, A. DOROSHENKO, I. DRONYUK, O., LISKEVYCH, and R. LISKEVYCH, Analysis of digital skills and infrastructure in EU countries based on DESI 2024 data. *Future Internet*, 17(6), 2025, 228. https://doi.org/10.3390/fi17060228.

13 K. MAULENOV, S. KUDUBAYEVA, and B. RAZAKHOVA, Modern Problems of Face Recognition Systems and Ways of Solving Them. *Revue d'Intelligence Artificielle*, 37(1), 2023, 209–214. https://doi.org/10.18280/ria.370126.

14 A. TURILLAZZI, M. TADDEO, L. FLORIDI, and F. CASOLARI, The Digital Services Act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), 2023, 83-106. https://doi.org/10.1080/17579961.2023.2184136.

the following tasks were set: to analyse modern approaches to regulating digital risks at the level of public administration in individual European countries; to investigate institutional mechanisms that ensure cybersecurity, personal data protection and the stability of digital infrastructure in the context of the development of the digital economy.

2. Methodology

As part of the theoretical study conducted from May 2024 to May 2025, an analysis of the role of public administration in ensuring digital security was carried out using the examples of France, Poland, Bulgaria and Kyrgyzstan. The choice of these countries is justified by the desire to compare digital policy models of EU countries with a high level of institutional capacity (France and Poland) and states facing the challenges of fragmentation and limited resources (Bulgaria and Kyrgyzstan). Despite Bulgaria's membership in the EU, it demonstrates features of post-socialist digital transformation, which allows comparing its experience with the practices of Kyrgyzstan. This approach made it possible to assess differences in regulatory models and prospects for harmonizing digital security between the EU and countries with economies in transition.

The methodology used is a descriptive comparative analysis of the legal frameworks and institutional mechanisms of the countries studied. Each country was evaluated based on several criteria: (1) cybersecurity regulation, (2) personal data protection, (3) digital infrastructure, and (4) institutional mechanisms for managing digital security.

The study presented the legislative model of France, which covers the strategy of digital sovereignty, the use of cloud technologies in the public sector, as well as institutional responsibility for digital security. The activities of key bodies such as the Autorité de régulation de la communication audiovisuelle et numérique (ARCOM)[15] and the Commission nationale de l'informatique et des libertés(CNIL)[16] are described, as well as the application of pan-European regulatory

15 Audiovisual and Digital Communication Regulatory Authority, Studies, reviews and reports, 2025. https://www.arcom.fr/en/find-out-more/studies-and-data/studies-reviews-and-reports.

16 National Commission on Informatics and Liberty, Media library, 2025. https://www.cnil.fr/fr/mediatheque?field_scald_collection_tid=31.

acts – the General Data Protection Regulation[17] and the Directive No. 2002/58/EC of the European Parliament and of the Council "Concerning the Processing of Personal Data and the Protection of Privacy in the electronic Communications Sector"[18]. The French "Penal Code"[19] was analysed in relation to cybercrime, in particular Article 323, known as the "Godfrey Law", which allowed to outline the legal liability for violations of digital security. The study aimed to determine the balance between national sovereignty policies and the implementation of EU norms.

The study of Poland focuses on the Act on the National Cybersecurity System[20] and the Cybersecurity Strategy of the Republic of Poland for 2019-2024[21], which establish regulatory provisions in the field of cyber security. The government program "Cyber Shield" was also analysed, implemented in response to the growing threat to digital infrastructure.[22] The method of each content analysis will allow to determine the nature of the state response to cyber incidents and to assess the organizational mechanisms of institutional responsibility within the framework of digital policy. The consideration of digital governance in Bulgaria was implemented on the basis of the National Program "Digital Bulgaria 2025"[23], which seeks strategic directions for the digitalization of the public

17 Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

18 Directive No. 2002/58/EC of the European Parliament and of the Council "Concerning the Processing of Personal Data and the Protection of Privacy in the electronic Communications Sector (Directive on Privacy and Electronic Communications)", 2002. https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng.

19 PENAL CODE, 2025. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2025-09-24.

20 Act on the National Cybersecurity System, 2018. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf.

21 MINISTRY OF DIGITAL AFFAIRS, Cybersecurity strategy of the Republic of Poland for 2019-2024, 2019. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf.

22 D. VIALKO, Poland to allocate 3 billion zlotys for cybersecurity after Russian cyberattack. 2024. https://newsukraine.rbc.ua/news/poland-to-allocate-3-billion-zlotys-for-cybersecurity-1717451067.html.

23 M. JĀKOBSONE, Bulgaria – Digital Bulgaria 2025 national programme, 2022. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/bulgaria-digital-bulgaria-2025-national-programme.

sector. Particular attention is paid to regulatory support, in particular the Strategy for the Development of Electronic Government[24] and the Electronic Government Act (2020). The structure of administrative services and the main barriers to digital security are studied, including weak coordination between institutions, insufficient digital training of personnel and a system of risk fragmentation.[25] This analysis was carried out with the aim of clarifying problem areas in ensuring the integrity of the state digital policy.

In the case of Kyrgyzstan, the Concept Digital Transformation of the Kyrgyz Republic for 2024-2028[26] was studied, which fixed the strategic vector of digital reforms. The activities of the State Institution "Kizmat"[27], the single digital platform "Tunduk"[28] and the mobile application that ensures the provision of electronic services to citizens are described. Approaches to digital inclusion in conditions of socio-economic instability were studied, as well as practices of access to services in remote communities.[29,30] This turned out to reveal institutional flexibility in the management of digital processes. The final element was the formation of a comparative assessment of the approaches of France and Poland, as well as Bulgaria and Kyrgyzstan, regarding institutional responsibility, the use of cloud solutions, the regulatory framework and the level of digital readiness. In addition, the study explored the prospects for harmonizing digital security approaches between the analysed countries, with an emphasis on experience transfer, modernization of administrative procedures, and strengthening the resilience of state institutions in the digital environment.

---

24 REPUBLIC OF BULGARIA STATE E-GOVERNMENT AGENCY, Strategic documents – State Agency "Electronic Government", 2025. https://e-gov.bg/wps/portal/agency-en/strategy-policy/startegical-documents#:~:text=Strategy%20for%20the%20development%20of,within%20the%20individual%20administrative%20bodies..

25 Bulgaria 2025 Digital Decade Country Report, 2025. https://digital-strategy.ec.europa.eu/en/factpages/bulgaria-2025-digital-decade-country-report.

26 MINISTRY OF DIGITAL DEVELOPMENT OF THE KYRGYZ REPUBLIC, Concept Digital Transformation of the Kyrgyz Republic for 2024-2028, 2025. https://digital.gov.kg/en/activities/konczkpcziya-czifrovoj-transformaczii-kyrgyzskoj-respubliki-na-2024-2028-gody/.

27 Kyrgyzstan to enhance public services through partnership between MEGA and Kyzmat, 2025. https://www.trend.az/casia/kyrgyzstan/4037876.html.

28 TUNDUK, Information systems operated by the state enterprise "Tunduk", 2025. https://tunduk.gov.kg/en/pages/2-information-systems.

29 United Nations Development Programme, Annual report 2024, 2025a. https://www.undp.org/sites/g/files/zskgke326/files/2025-04/otchet_dlya_pechati.pdf.

30 S. KEMP, Digital 2025: Kyrgyzstan, 2025. https://datareportal.com/reports/digital-2025-kyrgyzstan.

3. The role of public administration in ensuring digital security in France and Poland

Four main dimensions were used to guide the comparative analysis: (1) cybersecurity regulation, (2) personal data protection, (3) digital infrastructure, and (4) institutional coordination mechanisms. The results show that France and Poland adopt a structured, preventive approach to cybersecurity, supported by clear regulations and robust infrastructures. In contrast, Bulgaria and Kyrgyzstan, while less advanced in terms of regulation and infrastructure, focus on digital inclusion and expanding public digital services. These differences have direct implications for each country's ability to manage cyber threats and maintain citizens' trust.

France provides one of the most comprehensive regulatory approaches to digital security in Europe, combining national legislation with European directives and sector-specific acts. The core of this system is the Sécurité et Régulation de l'Espace Numérique (SREN) – Law No. 2024-449 aimed at Securing and Regulating the Digital Space[31], which aims to raise security standards in the digital environment and strengthen digital sovereignty. This law obliges both public institutions and private companies to implement advanced cybersecurity systems, provide ongoing training for staff and implement mandatory moderation mechanisms to remove illegal content – in particular hate speech, terrorist material or fraudulent activities. Particular attention is paid to mandatory age verification to protect minors, the implementation of filters against online fraud and the obligation to report digital incidents. Compliance with these provisions is monitored by the regulatory authorities Audiovisual and Digital Communication Regulatory Authority[32] and National Commission on Informatics and Liberty[33], with significant administrative and financial sanctions for non-compliance.[34]

---

31 Law No. 2024-449 aimed at Securing and Regulating the Digital Space, 2024. https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100.

32 Audiovisual and Digital Communication Regulatory Authority, Studies, reviews and reports, 2025. https://www.arcom.fr/en/find-out-more/studies-and-data/studies-reviews-and-reports.

33 National Commission on Informatics and Liberty, Media library, 2025. https://www.cnil.fr/fr/mediatheque?field_scald_collection_tid=31.

Another key component is the system for protecting personal data. France applies the Law No. 78-17 "On Information Technologies, Data Files and Individual Liberties (as amended up to June 1, 2019), France"[35], which has been harmonized with the requirements of the General Data Protection Regulation (GDPR)[36] and Directive No. 2002/58/EC of the European Parliament and of the Council[37]. The GDPR requires all organizations that handle personal data to implement technical and organizational security measures, conduct a privacy impact assessment, and notify the CNIL and affected individuals in the event of a data breach. Fines for violations can reach EUR 20 million or 4% of a company's annual turnover.[38] In the field of digital platforms, France complies with European regulations, including the DSA and the DMA, which impose obligations on transparency, content moderation, user protection, and the prevention of market monopolization.[39] There is also a Code on the Protection of Consumer Rights in the Digital Environment, which establishes the liability of companies for the electronic services provided. In the field of combating cybercrime, France uses the "Penal Code"[40] (Article 323, known as the Godfrey Law), which provides for criminal liability for unauthorized access to information systems, data

34 S. BETTACH, and A. VUCHOT, France: The SREN Law and its impact on digital platforms, 2024. https://www.twobirds.com/en/insights/2024/france/la-loi-sren-et-son-impact-sur-les-plateformes-numeriques.

35 Law No. 78-17 "On Information Technologies, Data Files and Individual Liberties (as amended up to June 1, 2019), France", 2019. https://www.wipo.int/wipolex/en/legislation/details/18965.

36 Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

37 Directive No. 2002/58/EC of the European Parliament and of the Council "Concerning the Processing of Personal Data and the Protection of Privacy in the electronic Communications Sector (Directive on Privacy and Electronic Communications)", 2002. https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng.

38 National Commission for Information Technology and Civil Liberties. Cybersecurity, GDPR: the best prevention against cyber risks, 2024. https://www.cnil.fr/sites/default/files/2024-05/cnil_cybersecurity_2024_en.pdf.

39 S. BETTACH, and A. VUCHOT, France: The SREN Law and its impact on digital platforms, 2024. https://www.twobirds.com/en/insights/2024/france/la-loi-sren-et-son-impact-sur-les-plateformes-numeriques

40 PENAL CODE, 2025. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2025-09-24.

modification, obstruction of information processing and other IT offenses.

A special role in ensuring the resilience of the state digital infrastructure is played by laws on critical infrastructure facilities, which establish requirements for the cyber resilience of the energy, health, finance, etc. sectors. Control is carried out by the National Agency for Information Systems Security[41], which coordinates incident response measures and formulates requirements for critical infrastructure entities. Additionally, there is the Digital Republic Act[42], which promotes digital inclusion, net neutrality, and transparency in data processing, as well as the Loi pour la Confiance dans l'Économie Numérique (LCEN) – Law No. 2004-575 "On Confidence in the Digital Economy (as amended up to August 8, 2015), France"[43], which obliges digital providers to respond promptly to the detection of illegal content and cooperate with law enforcement agencies.

France is taking an integrated approach to regulating artificial intelligence (AI) and personal data protection, combining European legislation – notably the EU Artificial Intelligence Act[44] and the GDPR – with national legislation and the work of specialized bodies. The National Commission for Informatics and Liberties, which already oversees compliance with the GDPR and is preparing to take on the supervisory role under the AI Act, plays a key role in this process. The legislative implementation of the AI Act began in August 2024, with a phased implementation of the requirements by August 2025.[45] It provides for a differentiated risk system, which prohibits certain practices (such as social scoring), strict requirements for high-risk systems, and general ethical guidelines for systems with minimal risk. To comply with these rules, the CNIL has created a specialized unit to develop recommendations on the compatibility of AI with

41 FRENCH CYBERSECURITY AGENCY, Regulation, 2025. https://cyber.gouv.fr/en/regulation.

42 Law No. 2016-1321 for a Digital Republic, France, 2016. https://www.wipo.int/wipolex/en/legislation/details/16380.

43 Law No. 2004-575 "On Confidence in the Digital Economy (As Amended up to August 8, 2015), France", 2015. https://www.wipo.int/wipolex/en/legislation/details/15802.

44 EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act, 2025. https://artificialintelligenceact.eu/.

45 B. MAY, D. ROCHE, A. KAHLAL, and L. MAILHAC, Artificial Intelligence 2025, 2025. https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2025/france.

the law, and the newly created AI Security Institute INESIA[46] is responsible for the national assessment of models, their reliability and regulatory support, in particular in collaboration with the ANSSI agency. Particular attention is paid to transparency, accountability and compliance with ethical principles, based on the European "Ethical Recommendations for Trustworthy AI"[47] and the Paris Charter for the Development of AI for the Public Interest.[48]

In the field of personal data protection, France follows a strict approach enshrined in the GDPR, which ensures the protection of the rights of data subjects, the lawfulness of processing, the security of storage and the obligation to inform. The Law No. 78-17[49] complements the European regulation and establishes specific requirements, for example, for the processing of biometric, genetic and medical data. The CNIL is empowered to conduct investigations, impose fines and issue injunctions to eliminate violations. In the context of AI, particular attention is paid to the principle of "privacy by design", which involves integrating data protection standards already at the design stage of models. AI systems must adhere to principles such as purpose limitation, data minimization, algorithm transparency and time limits for information storage. Users have the right to know that their data is being used to train AI, and to request access, rectification, erasure or objection to their processing. The CNIL has also clarified the conditions for the reuse of open data for training models, emphasizing the need to exclude irrelevant information and comply with the restrictions of the GDPR.[50] At a practical level, the CNIL is issuing detailed guidance for developers and users of AI systems, which addresses the need to assess the impact on data protection, determine the legal grounds for processing, implement protection by

46 The Government announces the creation of the National Institute for the Evaluation and Security of Artificial Intelligence (INESIA), 2025. https://www.entreprises.gouv.fr/espace-presse/le-gouvernement-annonce-la-creation-de-linstitut-national-pour-levaluation-et-la.

47 Ethics guidelines for trustworthy AI, 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

48 The Paris Charter on Artificial Intelligence in the Public Interest, 2025. https://www.elysee.fr/en/emmanuel-macron/2025/02/11/the-paris-charter-on-artificial-intelligence-in-the-public-interest.

49 Law No. 78-17 "On Information Technologies, Data Files and Individual Liberties (as amended up to June 1, 2019), France", 2019. https://www.wipo.int/wipolex/en/legislation/details/18965.

50 F. SARDAIN, and C. ALLAVENA, Data Protection & Privacy 2025, 2025. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/france.

design in the system architecture and constantly comply with the principles of confidentiality. This approach, which combines supranational initiatives with national law enforcement practices, ensures a high level of responsibility in France when implementing AI technologies, as well as the consistent integration of human rights, digital ethics, and cybersecurity into the system of public governance of the digital economy.[51]

The digital security model in the Polish public administration system is based on a combination of a clear regulatory framework, strategic planning, a developed institutional infrastructure and innovative technological solutions. The basis of the regulatory framework is the Act on the National Cybersecurity System[52], which adapted the provisions of the EU Directive on Security of Network and Information Systems (NIS Directive) to national legislation. This law clearly defines the responsibilities of state bodies, critical service operators and digital providers, requiring them to implement effective cybersecurity measures, regular risk management and mandatory reporting of cyber incidents. The created system provides for the operation of several specialized Cyber Incident Response Teams (CSIRTs), which ensure operational response in three key domains: governmental (CSIRT GOV), civilian (CSIRT NASK) and military (CSIRT MON), thus forming a focused and effective cyber defence model.[53,54]

The strategic development of digital security is regulated by the National Cybersecurity Strategy of Poland for 2019-2024.[55] Its main goal is to strengthen cyber resilience and information protection in all sectors – public, military and private. The strategy provides for the implementation of risk management sy-

---

51 A.-L. VILLEDIEU, and M. HANTIOT, Data protection and cybersecurity laws in France, 2021. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/france.

52 Act on the National Cybersecurity System, 2018. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf.

53 K. ZURKUS, NIS directive met, Polish cybersecurity in effect, 2018. https://www.infosecurity-magazine.com/news/nis-directive-met-polish/.

54 MINISTRY OF DIGITAL AFFAIRS, Cybersecurity strategy of the Republic of Poland for 2019-2024, 2019. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf.

55 MINISTRY OF DIGITAL AFFAIRS, Cybersecurity strategy of the Republic of Poland for 2019-2024, 2019. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf.

stems, the development of information security standards, staff training, infrastructure development, as well as close interagency and international cooperation. From 2025, Poland plans to implement a new 10-year program "Cyber Shield", which provides for large-scale investments in the protection of critical infrastructure and the digitalization of the public sector.[56] The government has already reserved several billion zlotys for the implementation of these initiatives, in particular for the modernization of protection against cyberattacks, the number of which in 2023 increased by 300% compared to the previous year, mainly due to the activities of foreign hacking groups.[57]

From an organizational point of view, the leading role is played by the Ministry of Digital Affairs, in particular the Department of Cybersecurity, which is responsible for regulatory regulation, policy development and coordination of measures. The Government Commissioner for Cybersecurity ensures the implementation of policy decisions, while the National Cybersecurity Council performs an advisory function. In addition, numerous regulations concerning individual sectors and technologies (in particular cloud services) define technical requirements for state institutions and ensure that digital services meet the highest security standards. Technically, the Polish digital security model is based on the transition to cloud computing with a high level of data protection, the implementation of quantum-resistant cryptography, edge computing and artificial intelligence in digital services of the public sector[58]. All state authorities are obliged not only to implement cybersecurity measures, but also to conduct regular audits of the effectiveness of such measures. Particular attention is paid to improving the competences of personnel through training programs, as well as to raising the general level of awareness of citizens about cybersecurity. The Polish model combines prevention, rapid response to incidents, infrastructure development, in-

56 D. VIALKO, Poland to allocate 3 billion zlotys for cybersecurity after Russian cyberattack. 2024. https://newsukraine.rbc.ua/news/poland-to-allocate-3-billion-zlotys-for-cybersecurity-1717451067.html.

57 Poland Unveils Landmark Digital Strategy 2035: A Comprehensive Roadmap for Digital Transformation, 2024. https://decentcybersecurity.eu/poland-unveils-landmark-digital-strategy-2035-a-comprehensive-roadmap-for-digital-transformation/.

58 J. KUBICZEK and M. TUSZKIEWICZ, Intraday Patterns of Liquidity on the Warsaw Stock Exchange before and after the Outbreak of the COVID-19 Pandemic. *International Journal of Financial Studies*, 10(1), 2022, 13. https://doi.org/10.3390/ijfs10010013.

vestment in innovation and coordinated policy, making it one of the most systematic approaches to digital security in the public administration system in Central Europe.[59]

To gain a deeper understanding of approaches to ensuring digital security in public administration systems, it is appropriate to conduct a comparative analysis of the models adopted in France and Poland. Both countries are members of the European Union and thus actively implement EU-wide regulations such as the General Data Protection Regulation (GDPR) and the NIS Directive. At the same time, each country develops its own national initiatives based on the specifics of its administrative structure, technical infrastructure, and strategic priorities. The table 1 presented a comparison of the key elements of digital security in France and Poland, allowing the identification of similarities and differences in their approaches.

Table 1. Comparison of digital security models in public administration: France vs. Poland.

Criterion	France	Poland
Legal framework	Combination of EU acts: GDPR (Regulation (EU) No. 2016/679 of the European Parliament and of the Council…, 2016), DSA (Regulation (EU) No. 2022/2065 of the European Parliament and of the Council "On a Single…, 2022), DMA (Regulation (EU) No. 2022/1925 of the European Parliament and of the Council "On Contestable…, 2022)) with national laws: Law No. 2024-449 (2024), Law No. 2004-575 (2015), Digital Republic Act (Law No. 2016-1321 for…, 2016)	Implementation of the NIS Directive through the National Cybersecurity System Act (Poland: Announced amendment…, 2025); Cybersecurity strategy of the Republic of Poland for 2019-2024 (Ministry of Digital Affairs, 2019)
Key regulators	CNIL (data protection) (National Commission on Informatics and Liberty, 2025), ANSSI (cybersecurity), Audiovisual and Digital Communication Regulatory Authority (2025) (content), INESIA (AI) (The Government announces…, 2025)	Ministry of Digital Affairs, Government Plenipotentiary for Cybersecurity, CSIRT GOV/NASK/MON
AI regulation	Focus on EU AI Act (EU Artificial Intelligence, 2025); establishment of INESIA; CNIL oversight	No specific AI legal framework; integration of AI elements within public sector digital services
Personal data	GDPR combined with Law No. 78-17 (2019); strict CNIL oversight, "privacy	GDPR as the core; mandatory internal auditing mechanisms in

59 EUROPEAN COMMISSION, Digital Public Administration factsheet 2020, 2020. https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Poland_vFINAL.pdf.

protection	by design" principle	public sector institutions
Institutional structure	Multi-level system of regulators with clearly defined responsibilities	Centralized coordination via Ministry of Digital Affairs and CSIRTs; specialization of CSIRTs for public, civil, and defence sectors
Security instruments	Systemic requirements for online platforms, mandatory data impact assessments, content moderation, anti-fraud mechanisms	Incident response via CSIRTs, risk management, system auditing, transition to secure cloud infrastructure
National strategies	Comprehensive digital sovereignty frameworks, ethical AI regulation, combating disinformation	Ongoing Cybersecurity Strategy (2019-2024); implementation of the "Cyber Shield" program from 2025 for critical infrastructure protection
Level of investment in digital security	High, through centralized agencies, GDPR penalty system, and innovation support in AI	Significant public investment, particularly in infrastructure modernization and increasing resilience to cyber threats

[Source: compiled by the authors]

The analysis reveals that France builds its digital security model based on strict regulation, ethical standards, and national technological sovereignty. Poland, on the other hand, emphasizes institutional coordination, strategic planning, and a specialized incident response system. Despite a common EU legal foundation, the two countries have chosen different implementation approaches, highlighting the flexibility of the European system to adapt to national contexts. This study, unlike Sarjito[60] work, focused on the analysis of national approaches to ensuring digital security in France and Poland. Both studies examined the challenges of cyber threats and the significance of the GDPR, but Sarjito provided a general overview, while this study analyzed specific legislative acts, institutions and instruments, including the regulation of artificial intelligence. A. Sarjito's work did not present an in-depth assessment of the institutional structure and financial and technical support, which became key in this study.

A similar thematic focus was observed in Huixia[61], who emphasized the transformative impact of digital technologies on the structure of public administration. Both works recognize the key role of the state and the need to protect

60 A. SARJITO, Data security and privacy in the digital era: Challenges for modern government. *Scientific Journal of Public Administration*, 8(3), 2024, 1-13. https://doi.org/10.56071/jian.v8i3.933.

61 W. HUIXIA, Digitization of public administration in China: From e-government to digital government. *Bulletin of Taras Shevchenko National University of Kyiv. Public Administration*, 20(2), 2024, 56-62. https://doi.org/10.17721/2616-9193.2024/20-9/12.

personal data. However, Huixia mainly considered conceptual shifts, while this study focused on the analysis of national strategies, specific institutions and cybersecurity policies. In the work of Chen and Liu[62], attention was paid to the Chinese model of digital interaction between the state, the market and platforms. The authors showed a complex structure of coordination of digital transformation, but paid less attention to personal data, an aspect that was key in this study. A comparison with European approaches allows us to see the difference in priorities: in China, the emphasis is on centralized control, while in France and Poland, the balance between institutional regulation and user rights.

There is also an interesting parallel with the study by Zhou[63], in which digital governance was also examined through the prism of platform control, liability for data leaks and protection of digital rights. Zhou, however, focused on ethical challenges and information stability in the Chinese context, while this study focused on the legal detail of European instruments and inter-agency coordination. The work of Febiri et al.[64] deserves special attention due to its attempt to build a conceptual model of digital governance for Indonesia. Although both studies recognize the critical role of the state in digital transformation, the approaches differ significantly: while Febiri et al. focuses on strategic data management, this study shows real examples of the functioning of legislative and institutional mechanisms in the EU.

4. Peculiarities of state digital policy in Bulgaria and Kyrgyzstan

Compared to France and Poland, both Bulgaria and Kyrgyzstan face persistent barriers such as institutional fragmentation, limited inter-agency coordination, and resource constraints. The development of e-government and digital services in Bulgaria is taking place within the framework of a holistic state strategy

62 B. CHEN, and Y. LIU, Promotion and advancement of data security governance in China. *Electronics*, 13(10), 2024, 1905. https://doi.org/10.3390/electronics13101905.

63 Y. ZHOU, Data governance strategy guidance: Boost China's digital government construction towards high-quality development. In: *Proceedings of the 2024 8th International Seminar on Education, Management and Social Sciences*. Dordrecht: Atlantis Press, 2024, 1012-1018. https://doi.org/10.2991/978-2-38476-297-2_122.

64 F. FEBIRI, M.I. GARIBA, M. HUB, and R. PROVAZNIKOVA, The synergy between human factors, public digitalization and public administration in the European context. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(4), 2024, 100424. https://doi.org/10.1016/j.joitmc.2024.100424.

based on national programs, legislative acts and organizational structure aimed at ensuring the effective digital transformation of public administration. The central place in this process is occupied by the National Program "Digital Bulgaria 2025"[65], approved by the Council of Ministers in December 2019. It continued the priorities of the previous program of 2015 and is in line with the pan-European goals of digital growth. The main goal of the program is the complete transformation of public administration towards the provision of user-oriented electronic administrative services, with an emphasis on smart, sustainable and inclusive digital growth by 2025. The program covers the modernization of information and communication infrastructure, the development of system interoperability, ensuring a high level of network and information security. Digital Bulgaria 2025 identifies six key areas of action, including supporting shared e-government resources, promoting the use of cloud technologies, big data, artificial intelligence, blockchain solutions, and developing digital skills and cybersecurity. The program is accompanied by a roadmap for 2019-2023, which contains priority measures, responsible institutions and funding mechanisms, including over EUR 1.3 billion from the Recovery and Cohesion Funds.[66]

The previously established concept of digital governance was shaped by the e-Government Development Strategy for 2014-2020. It envisaged the creation of an effective and interconnected digital administration with secure identification, simple "single window" services and access to them 24/7. At the same time, problems with interaction between systems, requirements for the physical presence of users or the submission of original documents, as well as low popularization of services among citizens were recorded.[67] The institutional model for the provision of administrative services is based on the provisions of

65 M. JĀKOBSONE, Bulgaria – Digital Bulgaria 2025 national programme, 2022. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/bulgaria-digital-bulgaria-2025-national-programme.

66 Bulgaria 2025 Digital Decade Country Report, 2025. https://digital-strategy.ec.europa.eu/en/factpages/bulgaria-2025-digital-decade-country-report.

67 A. VODOPYANOV, Z. DZHUSUPOVA, C.V. FLIPOV, I.T. TAUSHANOVA, and D. DOICHINOVA, e-Government in Bulgaria: The journey to 2020 and the future ahead, 2021. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/650881631189254371.

the Strategy for the Development of Electronic Government[68] and the Law on Electronic Government.[69] The effectiveness of the system depends on coordination between numerous agencies to ensure the unification, integration and standardization of digital services. However, development is in many cases fragmented – projects are implemented in isolation, without sustainable centralized management and without a single administrative information system. This complicates integration and increases implementation costs. Efforts are ongoing to unify state registers, increase the interconnection of government systems and create a single e-government portal.[70]

The main barrier to the implementation of digital services remains an insufficient level of digital security. High-profile incidents, including the data leak from the National Revenue Agency, have raised concerns about the cyber resilience of government infrastructure. In this regard, the Digital Bulgaria 2025 program identifies building a secure digital environment as a priority. Among the main problems are insufficient preparedness for cyber threats, a weak authentication system, and the fragmentation of systems without a unified security management. Additional barriers include weak system interoperability, low trust in digital services, and limited digital skills among a segment of the population. Overall, Bulgaria demonstrates consistent implementation of e-government, but to ensure its resilience, it is necessary to strengthen cybersecurity, improve system integration, and increase the digital literacy of the population.[71]

In Kyrgyzstan, public administration plays a leading role in shaping the digital economy, providing institutional support for digital reforms, regulating the digital environment in the context of transformation, and promoting digital inclusion against the backdrop of socio-economic challenges. The priority of digi-

68 REPUBLIC OF BULGARIA STATE E-GOVERNMENT AGENCY, Strategic documents – State Agency "Electronic Government", 2025. https://e-gov.bg/wps/portal/agency-en/strategy-policy/startegical-documents#:~:text=Strategy%20for%20the%20development%20of,within%20the%20individual%20administrative%20bodies..

69 ELECTRONIC GOVERNMENT ACT, 2020. https://census2021.bg/wp-content/uploads/2020/01/Electronic_Government_Act_en.pdf.

70 A. VODOPYANOV, Z. DZHUSUPOVA, C.V. FLIPOV, I.T. TAUSHANOVA, and D. DOICHINOVA, e-Government in Bulgaria: The journey to 2020 and the future ahead, 2021. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/650881631189254371.

71 Bulgaria 2025 Digital Decade Country Report, 2025. https://digital-strategy.ec.europa.eu/en/factpages/bulgaria-2025-digital-decade-country-report.

tal transformation is enshrined at the state level in the Concept Digital Transformation of the Kyrgyz Republic for 2024-2028[72], approved by the President, which defines digital progress as a key criterion for the effectiveness of public administration. According to the document, all government bodies – from ministries to local governments – are obliged to implement digital technologies to optimize processes, reduce bureaucracy, and increase the efficiency of service delivery. Institutional support is implemented through the activities of the Ministry of Digital Development and Innovative Technologies, which coordinates digital initiatives and is responsible for their implementation. The centralized system for providing electronic services is implemented by the State Institution "Kizmat"[73], which provides citizens with access to online services. A single digital platform "Tunduk"[74] and a mobile application have been created, which facilitate interdepartmental data exchange and provide simplified access to services. In parallel, fintech infrastructure is developing – QR payments, bank cards and electronic wallets have become available even in remote regions. State bodies are actively cooperating with international organizations, in particular the United Nations Development Program, to adapt digital policy, increase digital literacy and strengthen partnerships in the field of technology.[75]

At the same time, the government regulates the digital environment, introducing laws and mechanisms that promote innovation. The launch of the digital som – a national digital currency that will affect most sectors of the economy is expected in 2025. Biometric identification of voters has been introduced, as well as an electronic system of interdepartmental interaction to increase transparency and security. Data compatibility between various state structures is ensured, which helps reduce duplication of information and increase management efficiency.

---

72 MINISTRY OF DIGITAL DEVELOPMENT OF THE KYRGYZ REPUBLIC, Concept Digital Transformation of the Kyrgyz Republic for 2024-2028, 2025. https://digital.gov.kg/en/activities/konczkpcziya-czifrovoj-transformaczii-kyrgyzskoj-respubliki-na-2024-2028-gody/.

73 Kyrgyzstan to enhance public services through partnership between MEGA and Kyzmat, 2025. https://www.trend.az/casia/kyrgyzstan/4037876.html.

74 TUNDUK, Information systems operated by the state enterprise "Tunduk", 2025. https://tunduk.gov.kg/en/pages/2-information-systems.

75 Kyrgyzstan is confidently advancing on the path of digital transformation, 2025. https://www.undp.org/kyrgyzstan/press-releases/kyrgyzstan-confidently-advancing-path-digital-transformation.

Cybersecurity is part of the digital readiness agenda, which has become particularly relevant during the COVID-19 pandemic.[76]

In the context of socio-economic instability, Kyrgyzstan pays special attention to digital inclusion. State policy is aimed at ensuring broad access to the Internet (penetration rate is 88.5%) and mobile communications, the number of connections of which exceeds the population. Digital services are developed taking into account the needs of vulnerable groups, and joint programs with the United Nations (UN) include digital skills training and awareness-raising. Cashless payments are actively supported, which contributes to reducing the digital divide, especially in rural regions.[77] Thus, the public administration of Kyrgyzstan plays a key role in shaping the digital economy, combining institutional coordination, regulatory flexibility and social inclusion. This approach, combined with international cooperation and the development of digital infrastructure, creates a favourable basis for the modernization of the economy on the basis of sustainable development.

A comparative analysis of the approaches of Bulgaria and Kyrgyzstan to public administration in the digital environment demonstrates both similar strategic orientations and differences due to institutional maturity, geopolitical context and the presence of international partnerships. Both countries officially declare the digital transformation of public administration as a national priority, enshrined in strategic development programs: Bulgaria – through the Digital Bulgaria 2025 initiative, and Kyrgyzstan – in the Digital Transformation Concept for 2024-2028. In both cases, centralized state platforms have been created: in Bulgaria – a single e-services portal with a system of register interaction, in Kyrgyzstan – the Tunduk platform and the Kizmat application. Structurally, Bulgaria has a developed multi-level system of interacting bodies, while Kyrgyzstan is focused on a centralized model based on the Ministry of Digital Development.

---

76 Advancing digital transformation in Kyrgyzstan: A joint effort for sustainable development, 2023. https://www.undp.org/kyrgyzstan/press-releases/advancing-digital-transformation-kyrgyzstan-joint-effort-sustainable-development.

77 S. KEMP, Digital 2025: Kyrgyzstan, 2025. https://datareportal.com/reports/digital-2025-kyrgyzstan.

International standards play a significant role in shaping the digital environment[78]. Bulgaria, as a member of the EU, is integrated into the framework of the European Union's digital strategies, such as the Digital Agenda, the EU Interoperability Framework, the Digital Economy and Society Index (DESI)[79], and also participates in Organisation for Economic Co-operation and Development (OECD)[80] initiatives. This contributes to standardization, legislative coherence, and the formation of a mature digital culture.[81] Kyrgyzstan, on the other hand, does not have a similar regional integration vector, but actively involves the support of international institutions – primarily United Nations Development Programme (UNDP)[82,83] – in policy development, personnel training, and infrastructure modernization. In particular, the development of a digital currency (electronic som) is an example of the transfer of innovations through cooperation with international financial institutions.

Regarding the security of the digital environment, Bulgaria has a systematic approach, enshrined in the digital strategy, based on compliance with EU standards in the field of data protection (in particular, GDPR), electronic identification, digital signatures, and cybersecurity. However, gaps remain, particularly in regional infrastructure coverage and digital competencies of civil servants. In Kyrgyzstan, digital security is evolving: biometric voter identification systems are being introduced, legislative changes are being made in the areas of fintech, identification, and digital currency. The institutional framework is still being formed, which makes it difficult to ensure comprehensive risk management (Table 2).

---

78 Y. PATASHKOVA, S. NIYAZBEKOVA, S. KERIMKHULLE, M. SERIKOVA, and M. TROYANSKAYA, Dynamics of Bitcoin trading on the Binance cryptocurrency exchange. *Economic Annals-XXI*, 187(1–2), 2021, 177–188. https://doi.org/10.21003/EA.V187-17.

79 The Digital Economy and Society Index (DESI), 2025. https://digital-strategy.ec.europa.eu/en/policies/desi.

80 Organisation for Economic Co-operation and Development, How we work, 2025. https://www.oecd.org/en/about/how-we-work.html.

81 Bulgaria 2025 Digital Decade Country Report, 2025. https://digital-strategy.ec.europa.eu/en/factpages/bulgaria-2025-digital-decade-country-report.

82 United Nations Development Programme, Annual report 2024, 2025a. https://www.undp.org/sites/g/files/zskgke326/files/2025-04/otchet_dlya_pechati.pdf.

83 United Nations Development Programme, UNDP Kyrgyzstan Annual Report 2024, 2025b. https://www.undp.org/kyrgyzstan/publications/undp-kyrgyzstan-annual-report-2024.

Table 2. Comparative approaches of Bulgaria and Kyrgyzstan to digital public administration.

Aspect	Bulgaria	Kyrgyzstan
Institutional maturity	Longstanding, EU-aligned, multiple agencies	Emerging, centralized ministry-led
Digital platforms	Established interoperability frameworks and portals	Unified platforms under rapid development
International standards	Strong EU and OECD engagement	Partnership-driven with UN and development partners
Regulatory framework	Comprehensive legal basis for e-services, privacy	Developing laws including digital currency
Digital security approach	Systemic, aligned with EU standards but with capacity gaps	Growing focus on secure ID and cybersecurity
Digital skills and inclusion	Recognized gaps in skills and rural infrastructure	Emphasis on connectivity and digital literacy efforts

[Source: compiled by the authors based on [84,85,86]]

Thus, both countries demonstrate a focus on the digital transformation of public administration, but Bulgaria relies on deep institutional integration into European structures, while Kyrgyzstan is building its own digital model in cooperation with international donors. Differences in approaches to security, institutional maturity, and regulatory regulation indicate different levels of digital readiness, but the common goal remains the creation of transparent, efficient, and inclusive public services[87,88]. This study opened up the applied dimension of digital transformation, focusing on administrative strategies in Bulgaria and Kyrgyzstan, in particular, the creation of unified platforms, institutional governance and international cooperation. This contrasted sharply with the work of Morató and Soro[89], which conceptualized digital policy in the cultural sphere in Spain, emphasizing the interaction between the central and

84 Bulgaria 2025 Digital Decade Country Report, 2025. https://digital-strategy.ec.europa.eu/en/factpages/bulgaria-2025-digital-decade-country-report.

85 United Nations Development Programme, Annual report 2024, 2025a. https://www.undp.org/sites/g/files/zskgke326/files/2025-04/otchet_dlya_pechati.pdf.

86 United Nations Development Programme, UNDP Kyrgyzstan Annual Report 2024, 2025b. https://www.undp.org/kyrgyzstan/publications/undp-kyrgyzstan-annual-report-2024.

87 O. KOLODIZIEV, M. KRUPKA, N. SHULGA, M. KULCHYTSKYY, and O. LOZYNSKA, The level of digital transformation affecting the competitiveness of banks. *Banks and Bank Systems*, 16(1), 2021, 81–91. https://doi.org/10.21511/bbs.16(1).2021.08.

88 V. KHARCHENKO, Y. PONOCHOVNYI, A.-S.M. QAHTAN, and A. BOYARCHUK, Security and availability models for smart building automation systems. *International Journal of Computing*, 16(4), 2017, 194–202.

89 A.R. MORATÓ, and G.G. SORO, Digital cultural policy in Spain: The game of emulation. In: O.M. Hylland, J. Primorac (Eds.), *Digital Transformation and Cultural Policies in Europe*. London: Routledge, 2023, 64-85. https://doi.org/10.4324/9781003334576-5.

regional levels and the support of creative industries. Both studies recognized the important role of the state in shaping the digital environment, but while in Spain the emphasis was on evolutionary coordination of actions, in Bulgaria and Kyrgyzstan – on centralized administrative models. In the work of Del-Real and Díaz-Fernández[90], the focus was shifted to the local level: the digital maturity of Spanish municipalities was investigated, in particular the impact of managerial competencies and internal culture on the pace of digitalization. This study, by contrast, examined state digital policy in a broader – national – context. They were united by a common thesis about the key role of the state in digital transformations, although the level of analysis and objects of the study differed significantly.

The approach of Mishra et al.[91] was conceptually different: the authors focused on the social consequences of digital transformation in countries of the Global South, analysing transparency, inclusion and risks of inequality. They critically examined the dangers of centralization of power and the digital divide. This study was more interested in technical and organizational tools within the framework of a national strategy. Battisti[92] raised the issues of digital sovereignty, transparency and accountability, emphasizing the risks for democracy in conditions of technological control. In contrast, this study paid attention to specific administrative solutions – e-government, coordination between agencies and technical infrastructure. Although both approaches recognized the importance of digitalization for governance, one explored idea, the other explored practical implementation mechanisms. An interesting contrast was also observed in comparison with the work of Fratini et al.[93]: there the emphasis was

90 C. DEL-REAL, and A.M. DÍAZ-FERNÁNDEZ, Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. *International Cybersecurity Law Review*, 3, 2022, 313-343. https://doi.org/10.1365/s43439-022-00069-4.

91 A. MISHRA, Y.I. ALZOUBI, M.J. ANWAR, and A.Q. GILL, Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, 120, 2022, 102820. https://doi.org/10.1016/j.cose.2022.102820.

92 D. BATTISTI, The digital transformation of Italy's public sector: Government cannot be left behind! *JeDEM – eJournal of eDemocracy and Open Government*, 12(1), 2020, 25-39. https://doi.org/10.29379/jedem.v12i1.591.

93 S. FRATINI, E. HINE, C. NOVELLI, H. ROBERTS, and L. FLORIDI, Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society,* 3(3), 2024. https://doi.org/10.2139/ssrn.4816020.

placed on local digitalization initiatives in Italian communities, with attention to digital competence and population involvement. Instead, this study moved in the opposite direction – from nationwide strategies to centralized platforms, demonstrating the macro-level implementation of digital policy. They were united by the idea of digital inclusion, but the scale and type of institutional action differed.

The work of Falkner et al.[94] raised the issue of the normative balance between national and European legal systems, considering digital transformation in the context of political and legal mechanisms. In this context, this study looked like its exemplary addition, where legal conflicts gave way to managerial practice. That is, the difference was not in the importance of the topic, but in the depth of its consideration: regulatory discourse versus administrative implementation. In the work of Pierucci[95], digital sovereignty was interpreted through the prism of European influence on AI regulation, which allowed the author to consider the state as a subject of strategic autonomy in the global digital agenda. This study did not go beyond the applied dimension: it was about institutional coordination, the development of state platforms and the technical basis of the digital state. The common thesis was the need for state participation in digitalization, but each text represented a different depth and optics of understanding the problem.

Thus, the study of digital policies in Bulgaria and Kyrgyzstan demonstrated different models of public governance of digital transformation, focused on centralized administration, creation of unified electronic platforms and attraction of international assistance. Despite differences in institutional maturity, both countries confirmed the strategic importance of digitalization as a factor in modernizing administrative processes and increasing transparency. Bulgaria relies on regulatory integration into the European framework, while Kyrgyzstan is shaping its own model through partnerships with international organizations. What remains common is the desire to provide efficient, secure and inclusive electronic

94 G. FALKNER, S. HEIDEBRECHT, A. OBENDIEK, and T. SEID, Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy*, 31(8), 2024, 2099-2120. https://doi.org/10.1080/13501763.2024.2358984.

95 F. PIERUCCI, Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. *Digital Society*, 4, 2025, 27. https://doi.org/10.1007/s44206-025-00189-4.

services for citizens.

5. Prospects for harmonizing approaches to digital security in the international context

In the context of growing cyber threats, geopolitical turbulence and accelerated digitalization of state functions, harmonization of approaches to digital security at the international level is becoming not only desirable, but also a necessary condition for ensuring the effective functioning of state institutions. The prospects for such convergence are particularly relevant in the area of cooperation between the European Union and countries with economies in transition, in particular Kyrgyzstan, which, although they have limited resources, demonstrate a high level of institutional readiness for digital transformations. One of the key tools in this process is the transfer of experience and models of digital security management[96,97]. The European Union has developed an effective legal architecture in this area, which includes documents such as the Directive on Security of Network and Information Systems (NIS)2 Directive, the General Data Protection Regulation (GDPR) and National Cybersecurity Strategies, integrated into the pan-European DESI indicator system. This experience can be adapted by countries with economies in transition through the format of technical assistance, joint exercises, digital missions or knowledge platforms (for example, the OECD Digital Government Toolkit). Kyrgyzstan, which already cooperates with United Nations Development Programme[98] and the World Bank[99] in the digital sphere, has the potential to use European practices in the field of cyber incident response, the creation of independent supervisory bodies, digital sovereignty and platform regulation.

---

96 E. DAHAN, I. AVIV, and M. KIPERBERG, Trust Domain Extensions Guest Fuzzing Framework for Security Vulnerability Detection. *Mathematics*, 13(11), 2025, 1879. https://doi.org/10.3390/math13111879.

97 M.M. PETROVA, O. SUSHCHENKO, I. TRUNINA, and N. DEKHTYAR, Big data tools in processing information from open sources. *2018 IEEE 1st International Conference on System Analysis and Intelligent Computing (SAIC 2018)*, 2018, article number 8516800. https://doi.org/10.1109/SAIC.2018.8516800.

98 United Nations Development Programme, UNDP Kyrgyzstan Annual Report 2024, 2025b. https://www.undp.org/kyrgyzstan/publications/undp-kyrgyzstan-annual-report-2024.

99 WORLD BANK, World Bank in the Kyrgyz Republic, 2025. https://www.worldbank.org/en/country/kyrgyzrepublic.

The next direction is the improvement of the regulatory framework and administrative procedures, which involves not only the translation and formal implementation borrowing of legislative acts, but also a deep adaptation of norms to national realities. For example, EU countries prioritize the coding of digital processes in legislation, in particular through digital pilots – tests of the operation of new regulations before their full implementation[100,101]. Such a methodology can be transferred to Bulgaria and Kyrgyzstan as a tool to reduce the risks of unsuccessful implementation. Also promising is the introduction of regulatory sandboxes – zones where innovative technologies, including AI and blockchain, are tested under relaxed conditions under the supervision of regulators[102]. This approach will create a balance between innovation and security, especially in the healthcare, social protection and digital justice sectors. Special attention should be paid to areas of strengthening the digital resilience of state institutions, which should be based on a multi-level approach. The first level is the human resources and educational base[103]. Currently, most of the countries participating in the study have a shortage of cybersecurity specialists in the public sector. France is solving this by implementing specialized programs in École nationale d'administration (ENA) and cooperating with technical universities; Poland – through national competitions and grants for training civil servants in digital technologies. Kyrgyzstan is already implementing pilot educational modules in partnership with international organizations, but needs to institutionalize digital education at the level of the National Civil Service

100 A. TROFYMCHUK, A. STENIN, and I. DROZDOVYCH, Modeling of information systems of service-oriented architecture. *2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo 2019)*, 2019, article number 9165416. https://doi.org/10.1109/UkrMiCo47782.2019.9165416.

101 K. KAVALDZHIEVA, The Impact of Digitalization on the Measurement of Value in the Production and Operation of Industrial Products. *2019 International Conference on High Technology for Sustainable Development (HiTech 2019)*, 2019, article number 9128260. https://doi.org/10.1109/HiTech48507.2019.9128260.

102 K.A. BISENOVNA, S.A. ASHATULY, L.Z. BEIBUTOVNA, K.S. YESILBAYULY, A.A. ZAGIEVNA, M.Z. GALYMBEKOVNA, and O.B. ORALKHANULY, Improving the efficiency of food supplies for a trading company based on an artificial neural network. *International Journal of Electrical and Computer Engineering*, 14(4), 2024, 4407–4417. https://doi.org/10.11591/ijece.v14i4.pp4407-4417.

103 E. GINTERS, M. MEZITIS, and D. AIZSTRAUTA, Sustainability simulation and assessment of bicycle network design and maintenance environment. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC 2018)*, 2018, article number 8601225. https://doi.org/10.1109/ICONIC.2018.8601225.

Agency.

The second level is infrastructural resilience, which involves diversifying data exchange channels, backing up critical information, and the autonomy of state digital systems[104,]. In this context, Bulgaria has already implemented a state data centre project with backup capacity in Plovdiv, while Kyrgyzstan is developing a similar project with the support of Chinese investors. The third level is procedural and scenario-based readiness, which includes regular cyber exercises, updating incident response algorithms, and creating interagency response teams (CERT or CSIRT). International cooperation in these aspects can consist of joint exercises, mutual access to early warning mechanisms, and the exchange of threat indicators. An additional aspect of harmonizing approaches to digital security is the mutual value of sharing experiences between the EU and transition economies, in particular the possibility of borrowing solutions not only in the "west-east" direction, but also in the reverse direction[105]. European Union countries, in particular France and Bulgaria, can use some innovative developments from countries with more flexible administrative structures, such as Kyrgyzstan, to test non-standard digital solutions in the context of less regulation and faster decision-making cycles. For example, the introduction of a digital currency (electronic som) in Kyrgyzstan demonstrates a bold approach to fintech regulation, which can become a test bed for more cautious European countries in innovations.

In addition, Kyrgyzstan is actively integrating mobile applications as a platform for accessing government services even in remote areas with unstable internet, which could be useful for Bulgaria or Poland in their efforts to digital inclusion in rural areas. Poland, in turn, can use the example of Bulgaria in the field of centralized storage of state data with a backup infrastructure, which is especially relevant in the context of increasing cyberattacks on critical facilities. On the other hand, countries with economies in transition, in particular Kyrgyzstan, can

104 V. KHODA, N. LESHCHUK, A. TOPALOV, S. ROBOTKO, O. KLYMENKO, and S. NEKRASOV, Computerized Lathe Control System based on Internet of Things Technology. *Proceedings – International Conference on Advanced Computer Information Technologies (ACIT)*, 2024, 674–677. https://doi.org/10.1109/ACIT62333.2024.10712548.

105 E. SHAHINI and E. SHAHINI, The Economic and Political Legacy of Trump's First Term: Implications for the Second Presidency. *Politics and Policy*, 53(5), 2025, e70066. https://doi.org/10.1111/polp.70066.

borrow a lot from EU countries in areas such as systemic regulation of personal data protection (for example, GDPR), the creation of independent data protection authorities (such as CNIL in France), the introduction of single indicators for measuring digital transformation (DESI) and the unification of procedures for public electronic services. Such elements of the European model provide not only legal certainty, but also increase citizens' trust in the digital state.

In the future, it is the bilateral exchange of tools, institutional solutions and technological models that will ensure the sustainable development of digital security. The European Union, with its regulatory-rich but sometimes cumbersome model, can learn flexibility, local adaptability, and rapid response from smaller and more dynamic governance systems, while non-EU states can institutionalize their own progress based on proven European standards[106,107]. Such a symmetrical exchange of approaches will contribute to the formation of an effective global digital security ecosystem. Thus, harmonization of approaches to digital security has not a declarative, but an applied potential, the implementation of which is possible through flexible copying and adaptation of best practices, gradual updating of regulatory architecture and institutional modernization. Synergy between EU countries and countries with economies in transition can not only strengthen national systems, but also contribute to the formation of a single Eurasian digital space with a guaranteed level of security, trust and inclusiveness.

The study by Metin et al.[108] and this study shared a focus on the role of the state in ensuring cybersecurity. Both emphasized the need for regulatory regulation, institutional support, and technological protection of the digital environment. Metin et al. proposed a universal model for Small and Medium-sized Enterprises (SMEs) and criticized the current standards for being too complex. This study, instead, focused on the analysis of specific government policies in France,

106 S. ABBASOVA, V. İSMAYILOV, and N. TRUSOVA, Problems of financing the state budget deficit. *Scientific Bulletin of Mukachevo State University. Series Economics*, 10(4), 2023, 9–19. https://doi.org/10.52566/msu-econ4.2023.09.

107 A. SHAFA, Historical aspects of economic thought in Azerbaijan. *Voprosy Istorii*, 8(2), 2021, 148–155. https://doi.org/10.31166/VoprosyIstorii202108Statyi41.

108 B. METIN, F.G. OZHAN, and M. WYNN, Digitalisation and cybersecurity: Towards an operational framework. *Electronics*, 13(21), 2024, 4226. https://doi.org/10.3390/electronics13214226.

Poland, Bulgaria, and Kyrgyzstan. While Metin et al. focused on a bottom-up adaptive approach, this study demonstrated examples of centralized government management. The two works complemented each other conceptually and practically. Continuing the topic of strategic approaches to digital threats, it is worth mentioning the study by Radanliev[109], which had a similar vision of the role of the state in strengthening cyber defence. Both works emphasized the need for state intervention, partnership with business, and strengthening trust in digital solutions. However, while this study was based on an analysis of the current legal environment and mechanisms for implementing policies, Radanliev emphasized a proactive approach, including the concept of "resilience-by-design" and management in complex conditions

Further, considering the work of Khanna[110], it was also possible to trace a common understanding of digital security as a complex problem that required not only technical but also regulatory solutions. Both studies emphasized the importance of transparency, trust, and effective risk management. However, while Khanna focused on global challenges – dependence on foreign technologies and supply chain vulnerabilities – this study analysed domestic institutional responses and paths to integrating European norms. Again, both perspectives complemented each other, revealing both external and internal dimensions of digital security. In this context, the work of Rhogust[111] was particularly noteworthy, considering digital security at the corporate level. The author emphasized the importance of implementing International Organization for Standardization (ISO) standards, developing a cyber culture, and adapting security to internal company processes. This was markedly different from the state focus of this study, which focused on regulatory harmonization, institutional coordination, and administrative resilience. At the same time, these approaches were not contradictory – on the contrary, they demonstrated the need for synergy between state regulation

109 P. RADANLIEV, Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology*, 9(1), 2025, 28-78. https://doi.org/10.1080/23742917.2024.2312671.

110 A. KHANNA, Future trends in digital security. In: A. Khanna (Ed.), *Securing an Enterprise: Maximizing Digital Experiences through Enhanced Security Measures*. Berkeley: Apress, 2025, 481-504. https://doi.org/10.1007/979-8-8688-1029-9_22.

111 M. RHOGUST, Legal framework for cybersecurity in the digital economy: Challenges and prospects for Indonesia. *Journal of Law, Social Science and Humanities*, 1(2), 2024, 166-180.

and private initiative.

A study by Adeyeri and Abroshan[112] broadened the discussion by highlighting the importance of digital security in developing country contexts. The authors focused on the issues of digital inequality, institutional weakness and the need for regional cooperation. In contrast, the study on France, Poland, Bulgaria and Kyrgyzstan focused on the modernization of public administration and integration with international standards. This contrast allowed for a better understanding of how digital security varied depending on the institutional capacity of the countries. Equally important was the comparison with the work of Chiara[113], which introduced an ethical and legal dimension to digital security. The author argued for the need to balance data protection and human rights, emphasizing the risks of excessive control. In this study, by contrast, the priority was to increase the resilience of state institutions through increased control and harmonization of norms. As a result, both approaches offered different aspects of the same problem – one from a human rights perspective, the other from a public administration perspective.

Of particular note was the work of Parambil et al.[114], which highlighted the importance of national strategies, coordination between institutions and adaptation to emerging threats in the digital environment. Although the main focus was on the education sector and countries with limited resources, the study demonstrated that cyber resilience required common standards and cooperation across all sectors. In comparison, the four-country study focused on institutional responsibility and regulatory unification within the European policy framework. The work of Almeida[115] added an educational and strategic component to the discussion. The author paid attention to the development of digital culture,

112 A. ADEYERI, and H. ABROSHAN, Geopolitical ramifications of cybersecurity threats: State responses and international cooperations in the digital warfare era. *Information*, 15(11), 2024, 682. https://doi.org/10.3390/info15110682.

113 P.G. CHIARA, Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, 53, 2024, 105961. https://doi.org/10.1016/j.clsr.2024.105961.

114 M.M.A. PARAMBIL, J. RUSTAMOV, S.G. AHMED, Z. RUSTAMOV, A.I. AWAD, N. ZAKI, and F. ALNAJJAR, Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, 7, 2024, 100327. https://doi.org/10.1016/j.caeai.2024.100327.

115 F. ALMEIDA, Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, 151, 2025, 104329. https://doi.org/10.1016/j.cose.2025.104329.

leadership and the integration of cybersecurity into governance systems, particularly in the educational environment. This resonated with the topic of this study, although within a different context. While Almeida called for the transformation of governance practices through education, in this study the main goal was to strengthen the regulatory architecture of states. In conclusion, the work of Zhang et al.[116] brought a global perspective to the relationship between digital trade and security. The authors considered digital security through the prism of geopolitics, interstate rivalry, and artificial intelligence. This differed from the administrative-legal approach of this study, which aimed to adapt national systems to European norms. However, both approaches confirmed that digital security was no longer an isolated technical field – it was becoming a key component of state and international policy.

As a result, harmonization of approaches to digital security turned out to be not only theoretically desirable, but also practically necessary to increase the efficiency of state institutions in the context of digital transformation. The study showed that the exchange of experience between EU countries and countries with economies in transition, in particular Kyrgyzstan, has significant potential for the formation of a resilient digital infrastructure. Analysis of the examples of France, Poland, Bulgaria and Kyrgyzstan demonstrated that symmetric borrowing of solutions – from regulatory adaptation to the implementation of innovative tools – contributes to increasing cyber resilience at the interstate level.

6. Conclusion

In conclusion, the study highlights the critical importance of international cooperation in the field of digital security, particularly between the EU and transitioning economies. It suggests that EU countries could benefit from the more flexible innovations observed in countries like Kyrgyzstan, while also sharing their regulatory models. Future research could focus on assessing the impact of digital security policies in these countries, particularly through case studies on the implementation of the proposed strategies.

116 C. ZHANG, X. CHEN, J. YANG, and X. GAO, Nexus between digital trade and security: Geopolitical implications for global economy in the digital age. *Asian Review of Political Economy*, 3, 2024, 10. https://doi.org/10.1007/s44216-024-00032-6.

A comparative analysis of four countries – France, Poland, Bulgaria and Kyrgyzstan – revealed different models of public policy in the field of digital security, depending on the level of institutional maturity, technical infrastructure, integration into international regulatory systems and administrative approaches to digital transformation. France demonstrated a comprehensive model based on a combination of strict regulation, ethical standards and technological sovereignty. Particular attention was paid to the implementation of European legislation (in particular GDPR, NIS2, AI Act), the development of an institutional structure with separate supervisory authorities (CNIL, ANSSI, ARCOM, INESIA) and the harmonization of national acts with EU requirements. Poland is implementing a centralized approach based on a clear strategic framework, institutional coordination and innovative solutions in the field of cyber defence, including the creation of CSIRT teams, the transition to secure cloud technologies and the implementation of a long-term program "Cyber Shield" for infrastructure modernization.

Bulgaria, integrated into the European digital field, demonstrates consistency in the implementation of digitalization programs (Digital Bulgaria 2025), but faces the problems of low institutional coherence, fragmentation of projects and insufficient cyber resilience. Kyrgyzstan, as a country with a transition economy, is building its own digital model, relying on international partnerships (UNDP, World Bank), a centralized administrative system, the development of mobile services and the implementation of innovative solutions, such as a digital currency or the "Tunduk" platform. Despite their differences, all four countries recognize the strategic importance of digital transformation and strive to create secure, efficient and inclusive public digital services. One of the key results of the study was the identification of the potential for harmonizing approaches to digital security between the European Union and countries with economies in transition. The prospects for bilateral exchange of models, institutional solutions and technological tools were determined: from the transfer of European standards on personal data, cyber incidents and administrative liability to the adaptation of more flexible and innovative solutions tested in Kyrgyzstan. A limitation of this study was that it was based solely on the analysis of regulatory and institutional mechanisms without including empirical data on the effectiveness of policy im-

plementation on the ground. Future research could further investigate the implementation gaps and institutional learning processes between countries through qualitative case studies or longitudinal monitoring.