

Governance, data security and public service delivery in Romania: a policy oriented approach

Elena-Mihaela SFRIJAN

*Alexandru Ioan Cuza University of Iasi, Romania
Iasi, Romania
elena.sfrijan@student.uaic.ro*

Ana-Maria BERCU

*Alexandru Ioan Cuza University of Iasi, Romania
Iasi, Romania
bercu@uaic.ro*

Abstract

The digital transformation of public administration is one of the most significant modernization processes in the public sector in recent years. In addition to the benefits it brings, digitization entails a significant responsibility regarding the collection, processing, and storage of an ever-increasing volume of data. The main aim of our paper is to analyze the current state of data security in Romania's public administration, given the complexity of threats to institutional data security and to identify challenges regarding information security, data protection, and cyber risk management. The theoretical foundation of this paper is based on the analysis of several relevant studies from the period 2020 – 2025 that compare the level of cybersecurity at the European level. The research methodology used is empirical, analyzing the harmonization of EU legislation on digitization and data security with Romanian legislation. The results show a sharp increase in cyberattacks. Romania currently has a relatively comprehensive legislative framework regarding digitization, cybersecurity, and data protection, but faces a significant gap between formal legislative compliance and the actual operational capacity for data protection and incident response. The main contribution of this paper lies in providing an updated synthesis of the policy measures adopted, the realities on the ground, and the proposal of recommendations specific to the current Romanian context. Data security in public administration is the first and foremost a matter of political will.

Keywords: public administration, digitization, legislation, cybersecurity, Romania

JEL Classification: H83, O33, L86, M15

1. Introduction

The digital transformation of public administration is one of Romania's strategic priorities within the European agenda for the Digital Decade 2030, as outlined in the National Action Plan for the Digital Decade [1] and the milestones set out in the National Recovery and Resilience Plan (PNRR) [2]. The acceleration of digitization, driven by the COVID-19 health crisis, has expanded the state's cyberattack surface, creating a much wider gap between the pace of digital transformation and the capacity of institutions to protect their infrastructure and managed data [3,4].

The extent of this gap is evident from data provided by the National Cyber Security Directorate (DNSC). In 2024, approximately 27.08 millions relevant cybersecurity incidents were detected and processed; cyber fraud increased by 40.2% compared to 2023; malware incidents rose by 286.8%; and 20 public institutions fell victim to ransomware

attacks [5]. These figures place Romania among the EU member states with the highest cyber risk profile, despite recent legislative progress.

The paradox of the current situation lies in the coexistence of a relatively robust European regulatory framework (the GDPR transposed by Law No. 190/2018, NIS2 implemented by Government Emergency Ordinance No. 155/2024 and Law No. 124/2025, the Cyber Security Law No. 58/2023) alongside an operational implementation capacity that remains below European standards [6]. Studies on digital innovation at the local community level in Romania show that local authorities are increasingly operating through digital technologies. However, this openness is not accompanied by adequate institutional security measures [7]. The gap between technology adoption and cybersecurity maturity constitutes the fundamental structural vulnerability of Romanian e-governance at this stage.

2. The theoretical framework

The analysis of data security in public administration lies at the intersection of several theories, including public administration theory, digital governance, risk management, and information security. From the perspective of public administration theory, digitization is defined by the concept of Digital-Era Governance (DEG). Patrick Dunleavy and his collaborators [4] explain that authentic digital transformation involves more than simply computerizing existing procedures. It involves a profound reorganization of institutional structures, the integration of public services, the intensive use of information technologies, and the redefinition of the relationship between the state and the citizens.

Within DEG, technology is not viewed as an auxiliary tool, but as a central element of administrative processes. Consequently, the efficiency and security of digital infrastructures become essential components of administrative capacity. Cyber vulnerabilities, security breaches, or data protection incidents should not be interpreted exclusively as technical problems caused by software errors or external attacks. They equally reflect shortcomings in strategic planning, institutional coordination, resource allocation, and risk management.

Institutions that implement digital services without simultaneously developing robust security mechanisms, incident response procedures, and clear information protection policies create systemic vulnerabilities. Thus, the security level of a public organization is influenced not only by the technical characteristics of the IT infrastructure, but also by the quality of decision-making processes, organizational culture, and managerial capacity to anticipate and manage risks.

DEG also highlights the need to integrate databases and information systems across different public institutions. Although this integration can generate significant benefits in terms of administrative efficiency and citizens' access to services, it amplifies the risks associated with information security. The interconnection of systems creates complex dependencies, such that a vulnerability existing in a single institution can affect the entire administrative ecosystem. Consequently, data protection can no longer be addressed exclusively at the organizational level but requires coordination and standardization mechanisms at the governmental level.

Furthermore, the DEG approach suggests that citizens' trust in digital government is closely linked to the state's ability to ensure data confidentiality, integrity, and availability. A major security incident can undermine the legitimacy of digital transformation projects and reduce the uptake of electronic services. Thus, cybersecurity becomes not only a technological issue but also one of institutional legitimacy and the strengthening of the relationship between government and society.

From the perspective of the economics of information security, Anderson and Moore [8] argue that security failures are driven by the structure of organizational incentives and the existence of information asymmetries, rather than a lack of technical expertise. According to this approach, institutional actors make security decisions based on perceived costs and benefits, which can lead to low levels of investment in preventive measures. Applied to the context of public administration in Romania, the theory offers an explanation for the tendency of underfunded institutions with insufficient accountability mechanisms to adopt reactive security strategies focused on managing the consequences of incidents, to the detriment of proactive and preventive approaches promoted by international standards in the field [9].

This economic interpretation is complemented by the political perspective on cybersecurity developed by Cavelty [7], which highlights the fact that information protection in the public sector goes beyond the technological sphere and falls within the broader framework of democratic governance. The author argues that the cybersecurity of public institutions is marked by a structural tension between two fundamental objectives: administrative transparency, necessary to ensure public accountability and citizen trust, and the need to protect sensitive information and critical digital infrastructure. Thus, decisions regarding data security involve a continuous process of balancing informational openness with the requirements of confidentiality, integrity, and availability of information.

Consequently, cyber vulnerabilities in public administration can be interpreted not only as the result of technical deficiencies, but also as manifestations of economic, organizational, and political constraints that influence the ability of institutions to implement effective data security policies [7,8,9].

Cigu Rusu, Hyams-Ssekasi, Onofrei, Vătămanu, and Bercu highlight the fact that digitization and innovation processes contribute significantly to transforming the relationship between local authorities and citizens. These processes facilitate the development of governance models characterized by a higher degree of transparency, accessibility, and responsiveness to community needs. The use of digital technologies enables the optimization of public service delivery, the improvement of institutional communication, and the strengthening of citizen participation in local decision-making processes [10]. It should be noted that this rapid shift toward digitalization increases the attack surface for cyberattacks.

Agheorghiesei and Bercu argue that the ethical behavior of organizations is fundamentally influenced by the institutional culture in which they operate. The authors emphasize that

adherence to compliance norms and standards is truly effective only when ethical values are embraced and integrated into organizational practices, not merely formally observed. This perspective is also relevant to the field of data security. An institution that treats organizational ethics as a mere administrative obligation will tend to approach data protection in a formal manner, focused on minimal compliance with legal requirements. Conversely, when accountability and integrity are part of the institutional culture, information security becomes an accepted organizational value, reflected in employees' daily behaviors and work processes. Thus, the actual level of data protection depends not only on the existence of appropriate rules and technologies, but also on the organizational culture that supports their consistent application [11,12].

Mergel, Edelmann, and Haug [13] update the DEG perspective, arguing that authentic digitization involves not only digitizing existing processes but also fundamentally restructuring them. Meijer and Bolivar [14] introduce the concept of data-driven government, placing the exploitation of big data at the center of the analysis of administrative efficiency, with direct implications for the protection of privacy and the security of citizens' data.

3. Cyber threats in Romania (2020-2024)

3.1. Volume and typology of incidents

The DNSC 2024 Annual Report, approved by the Supreme Council for National Defense (CSAT) in June 2025 [16], provides a detailed overview of the state of cybersecurity at the national level and the main threats targeting Romania's digital infrastructure. The data presented highlights the scale of the challenges faced by public institutions and actors in critical sectors, in a context marked by an intensification of hostile cyber activities.

According to the report, approximately 27.08 million cybersecurity events were processed in 2024 through the DNSC's detection sensors and the National Platform for Reporting Cybersecurity Incidents (PNRISC), which became operational at the beginning of that year. This significant volume of data indicates not only the high frequency of threats but also the increased institutional capacity for monitoring and reporting incidents.

Analysis of these events reveals a cyber landscape characterized by an ever-increasing diversity of attack types and the use of increasingly sophisticated techniques by malicious actors. In this context, the development of mechanisms for early detection, reporting, and response to incidents becomes an essential component of strengthening the cyber resilience of public administration and critical infrastructure in Romania.

Table 1. Main cybersecurity indicators in Romania, 2023-2024

Nr. Crt.	Indicator	Variation 2023–2024
1	Reported cyber fraud	+40,2%
2	Malware attacks detected	+286,8%
3	Brute force attempts	+30,3%
4	Compromised accounts	+21,0%
5	Ransomware attacks managed by DNSC	101 incidente
6	DDoS attacks	-38,5%

Nr. Crt.	Indicator	Variation 2023–2024
7	Website defacement	-45,8%
8	Infected IPs identified	-27,8%
9	Phishing attacks	-21,0%
10	Compromised applications	+125,0%

Source: DNSC, Annual Activity Report 2024 [15]

The data highlights (Table 1) a significant shift in the cyber threat landscape in 2024 compared to 2023 [17, 18]. The sharpest increases were recorded in malware attacks (+286.8%), software compromise (+125%), and cyber fraud (+40.2%). We are witnessing a progressive sophistication of the tactics used by malicious actors and an increasingly pronounced focus on exploiting technical and financial vulnerabilities. At the same time, the increase in brute-force attempts (+30.3%) and the number of compromised accounts (+21%) suggests the persistence of issues related to digital identity management and the insufficient use of advanced authentication mechanisms.

On the other hand, the decrease in DDoS incidents (-38.5%), defacement cases (-45.8%), and the number of infected IP addresses (-27.8%) may indicate improved monitoring and protection measures implemented in both the public and private sectors. At the same time, the 21% decrease in phishing attacks suggests the positive effects of awareness campaigns and modern mechanisms for filtering and authenticating electronic communications.

A particularly telling indicator is the 101 ransomware incidents handled by the DNSC in 2024, some of which affected public institutions and critical infrastructure, confirming that ransomware continues to pose one of the most serious threats to operational continuity and data security in Romania's public administration.

The regional geopolitical context is a key factor in the evolution of the cyber threats facing Romania. According to statements by DNSC Director General, the conflict initiated by the Russian Federation against Ukraine has contributed to an intensification of hostile cyber activities targeting Romania's digital institutions and infrastructure. Romania's strategic position as a member of NATO and the European Union, as well as its support for Ukraine, have heightened malicious actors' interest in national IT systems. These actions aim to disrupt the functioning of digital services, as well as to convey political and propaganda messages.

At the same time, the academic literature and security reports highlight the fact that the line between hacktivism and state-sponsored Advanced Persistent Threat (APT) operations is becoming increasingly blurred [5]. Although hacktivist groups present their activities as ideologically motivated independent initiatives, in many cases they employ tactics, techniques, and procedures similar to those associated with state actors. This convergence complicates the attribution of attacks and increases the level of uncertainty regarding the origin and true objectives of cyber operations.

Consequently, the cybersecurity of public administration can no longer be analyzed exclusively through the lens of internal technical risks but must also be understood within

the context of contemporary geopolitical competition. The increasing frequency of politically motivated attacks demonstrates that government digital infrastructures have become components of the strategic arena, and strengthening cyber resilience is an essential condition for protecting national interests and the continuity of public services.

3.2. Representative cases of ransomware incidents

One of the most serious cybersecurity incidents recorded in Romania in 2024 was the attack on Romanian Soft Company (RSC), the developer of the Hipocrate platform. This platform is used by numerous medical facilities to manage clinical and administrative activities. The attack, classified as a supply chain attack, demonstrated how the compromise of a single software service provider can trigger a chain reaction affecting a large number of organizations dependent on its infrastructure.

According to data reported by the DNSC, the incident directly affected 26 hospitals, which faced major difficulties in carrying out their day-to-day operations for approximately one week. During this period, medical staff were forced to resort to alternative procedures and manual record-keeping to ensure the continuity of medical services. The impact of the attack highlighted the high degree of dependence of public institutions on IT systems and the significant effects that their unavailability can have on services critical to citizens.

From an analytical perspective, the incident reveals vulnerabilities that go beyond the strictly technical aspects of cybersecurity. It highlights the importance of digital supply chain risk management. For this reason, it is necessary to periodically assess the security posture of external software vendors. At the same time, the case suggests the existence of deficiencies in business continuity planning. Many medical facilities did not have sufficiently robust mechanisms in place to maintain operations in the event of the main system's unavailability.

Consequently, the attack on Romanian Soft Company can be interpreted as a relevant example of how a third-party vendor's vulnerabilities can become a systemic risk for the public sector. The incident underscores the need to strengthen supplier audit procedures, contractual requirements regarding cybersecurity, and business continuity mechanisms, particularly in critical sectors such as healthcare, where the disruption of digital services can directly affect the delivery of services to the public.

A second key incident for the analysis of cybersecurity in public administration was the attack targeting Timișoara City Hall and its subordinate institutions, including the Tax Department and the General Directorate of Local Police. The incident affected approximately 112 IT systems, causing significant disruptions to administrative services and temporarily limiting citizens' access to a range of essential public services. The impact of the attack highlighted local government's growing dependence on digital infrastructure and the vulnerability of public services when such infrastructure is compromised.

Beyond the immediate operational consequences, the case demonstrates that cyberattacks on public administration can have direct effects on the relationship between institutions and citizens by disrupting access to services, delaying administrative processes, and

undermining public trust in the institutions' ability to securely manage digital information. At the same time, the scale of the incident suggests the need to strengthen network segmentation measures, backup and recovery procedures, as well as incident response mechanisms.

The attack on the Timișoara administration was not an isolated incident. Between 2023 and 2024, other major public institutions were affected by similar incidents, including the Bucharest Sector 5 City Hall, the National Disability Management System administered by the National Authority for the Protection of the Rights of Persons with Disabilities (ANPDPD), and the Bistrița City Hall. The frequency of these incidents indicates that local and central public administration continues to be an attractive target for malicious actors. They are drawn to the large volume of data managed and the varying levels of maturity of the security measures implemented.

Taken together, these incidents highlight the existence of structural vulnerabilities within public administration and confirm the need for an integrated approach to cybersecurity. This must include technological investments, as well as the development of institutional capabilities for preventing, detecting, and managing incidents. Thus, the continuity of digital public services becomes an essential component of administrative resilience in a context characterized by the increasing complexity of cyber threats.

All of these cases share the common feature that the attackers exploited known vulnerabilities in outdated software or used phishing and social engineering techniques. The average time to detect the breach significantly exceeded recommended international standards, suggesting serious shortcomings in continuous monitoring capabilities.

4. Structural vulnerabilities of data security in public administration

4.1. Aging IT infrastructure

One of the most serious structural vulnerabilities is the widespread use of outdated IT infrastructure. A significant proportion of public institutions, particularly at the local and county levels, operate operating systems without active technical support, applications with known and unpatched vulnerabilities (CVE - Common Vulnerabilities and Exposures), and monolithic architectures incompatible with the principles of security and privacy by design enshrined in the GDPR and NIS2 [19,20].

This situation can be explained structurally by severe budgetary constraints: public sector IT spending as a percentage of GDP is among the lowest in the EU, and budget planning mechanisms do not systematically include IT infrastructure renewal cycles. Projects funded through the PNRR, particularly the Government Cloud and the National Interoperability Platform, are designed to address some of the structural vulnerabilities of public administration in the areas of digitalization and information security. However, progress in implementation is hampered by significant delays relative to the initially set deadlines, which postpones the realization of the expected benefits at the institutional level.

4.2. The shortage of specialized human resources

The second vulnerability is the severe shortage of cybersecurity specialists. Romania faces an estimated shortage of over 15,000 specialists in this field [21], and competition with the private sector for human resources is skewed against the public sector, which cannot offer comparable compensation packages. The direct consequence is that many public institutions (mayors' offices, county directorates, decentralized institutions) do not have any in-house cybersecurity specialists.

The DNSC 2024 report confirms that the human factor remains the primary vulnerability in the vast majority of managed security incidents: a lack of awareness of cyber risks, negligent behavior, and exposure to phishing techniques account for a large proportion of security breaches in the public sector. Ciucă's [19] empirical research, based on questionnaires administered to public servants, confirms that the level of practical training is significantly below the level required for effective defense.

4.3. Institutional fragmentation

The third major vulnerability is the fragmentation of the institutional architecture responsible for managing cyber risks and incidents. Currently, responsibilities are distributed among several institutions, including the National Cyber Security Directorate (DNSC), the National Supervisory Authority for Personal Data Processing (ANSPDCP), the Authority for the Digitalization of Romania (ADR), the Ministry of Research, Innovation and Digitalization (MCID), the Romanian Intelligence Service (SRI), and the Special Telecommunications Service (STS), each with specific competencies in the areas of information security, data protection, digital governance, or critical infrastructure protection [21]. Although this distribution is justified by the need for functional specialization, it can lead to coordination difficulties and overlapping responsibilities in situations requiring a rapid and unified response.

In practice, the existence of multiple institutional actors involved in cybersecurity management can lead to areas of responsibility that are insufficiently clarified, particularly in the case of complex incidents that simultaneously affect multiple areas of competence [22]. In such situations, the effectiveness of the response depends not only on the individual capabilities of the institutions, but also on the level of cooperation, information sharing, and inter-institutional coordination.

Another significant limitation is the absence of a fully functional government-run Security Operations Center (SOC) capable of providing centralized monitoring, detection, and response services to public institutions that lack their own technical and human resources. Given that many local authorities and smaller institutions lack the capacity to operate specialized cybersecurity structures, the absence of such a centralized mechanism reduces the ability to rapidly identify threats and mount a coordinated response at the government level.

Compared to the models promoted in several European countries, where government SOCs ensure continuous monitoring of public infrastructure and provide operational support to institutions with low levels of cybersecurity maturity, the situation in Romania highlights

the existence of a significant institutional gap. Consequently, strengthening coordination among the involved actors and developing centralized monitoring and response capabilities are essential conditions for increasing the cyber resilience of public administration and for reducing the vulnerabilities caused by the fragmentation of the current cybersecurity governance system.

4.4. Poor organizational security culture

The fourth vulnerability, and likely the most difficult to address, is the insufficient development of an organizational security culture. In many public institutions, compliance with GDPR and NIS2 requirements is approached primarily in a formal manner and focused on procedural compliance, being reduced to the fulfillment of administrative obligations, without significant effects on organizational practices [19]. Agheorghiesei and Bercu highlight the interdependence between ethical culture and compliance culture, showing that institutions characterized by a low level of ethical responsibility tend to treat data protection as a mere formality. Consequently, data protection impact assessments (DPIAs) are often carried out merely as a formality, without actually influencing the design and security of IT systems [11,12].

5. Legislative and institutional framework

5.1. National legislative framework

Romania currently has a relatively comprehensive legislative framework on cybersecurity and data protection that is aligned with the requirements of European law. The central pillar of personal data protection is Regulation (EU) 2016/679 (GDPR), which is directly applicable and supplemented by Law No. 190/2018 [23]. The transposition of the NIS2 Directive (2022/2555/EU) was carried out through Government Emergency Ordinance No. 155/2024, consolidated by Law No. 124/2025, which establishes the framework for the security of the networks and information systems of essential and important entities, a category that explicitly includes central and local public administration authorities [24].

The main obligations established by this regulatory framework concern the registration of entities with the DNSC, the appointment of a Chief Information Security Officer (CISO), the implementation of risk management measures, and the reporting of incidents within strict deadlines: 24 hours for the initial notification, 72 hours for the interim report, and one month for the final report. Law No. 58/2023 on Romania's cybersecurity and defense regulates the national cybersecurity architecture and the cooperation mechanisms between the DNSC, the SRI, and the STS [25].

The legislative framework is supplemented by Law No. 362/2018 on ensuring a high common level of security of network and information systems, a legislative act that transposed the first NIS Directive (Directive (EU) 2016/1148) and served as the foundation for the development of the national cyber incident management system prior to the adoption of the new regulations inspired by NIS2 [26]. Furthermore, Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, successively amended to harmonize with European legislation, establishes additional obligations regarding the confidentiality of electronic communications and the security of communications services [27].

Government Decision No. 1321/2021 on the approval of Romania's Cybersecurity Strategy for the period 2022–2027 also plays an important role, defining the national strategic objectives in this field and the directions for developing capabilities for the prevention, detection, and response to cyber incidents [28]. The strategy is accompanied by an action plan aimed at strengthening the resilience of public institutions, developing digital skills, and intensifying cooperation between the public and private sectors.

At the same time, in the context of the accelerated digitization of public administration, the provisions of Law No. 242/2022 on data exchange between IT systems and the creation of the National Interoperability Platform are also relevant; this law establishes rules for the secure exchange of data between public authorities and mandates protective measures for information transferred between systems [29]. This regulation has direct implications for cybersecurity, as the expansion of interoperability increases both administrative efficiency and the need to implement robust mechanisms for access control and data protection.

At the European level, the national regulatory framework is also influenced by recent legislative acts currently being implemented, such as the Digital Operational Resilience Act (DORA), applicable particularly to the financial sector, and the Cyber Resilience Act, which introduces security requirements for products with digital components throughout their entire lifecycle. Although these regulations do not exclusively target public administration, they contribute to strengthening the national cybersecurity ecosystem and influence the security standards applicable to public institutions and their suppliers.

Overall, Romania's regulatory framework for cybersecurity has undergone significant development in recent years, but its effectiveness depends not only on the existence of regulations, but also on the ability of public institutions to effectively implement them through adequate resources, specialized personnel, and functional monitoring and control mechanisms [24,25,28].

5.2. GDPR enforcement: between formal compliance and effective resilience

The National Supervisory Authority for Personal Data Processing (ANSPDCP) completed 488 investigations in 2025, a slight increase from the 476 investigations conducted in 2024, indicating an intensification of oversight and verification activities at the national level [16]. The main causes leading to the imposition of sanctions were the failure to implement adequate technical and organizational measures, insufficient periodic security testing, as well as incidents of unauthorized access to personal data, all of which highlight recurring deficiencies in the application of GDPR requirements at the institutional level.

In this context, the ANSPDCP's 2023 activity report indicates 4,772 complaints, reports, and notifications regarding security incidents, as well as the imposition of 73 fines totaling 2,348,265 lei [17]. These figures suggest constant pressure on the supervisory authority, driven by the high volume of reported incidents and the still insufficient maturity of the data protection culture among controllers, including public institutions.

A comparative analysis of Romania’s penalty regime relative to other European Union member states indicates a relatively lower level of fines imposed, a factor that may reflect both the lower financial capacity of the sanctioned entities and a less strict approach in the practical application of Regulation (EU) 2016/679 compared to countries such as Germany, France, or the Netherlands. In this context, the specialized literature introduces the concept of *GDPR fatigue*, described by Kuner [23], which highlights the phenomenon of institutional overload generated by the complexity of compliance requirements, which can lead to procedural formalism and the superficial implementation of data protection obligations.

This trend is also observable in the Romanian public sector, where compliance with GDPR requirements is sometimes treated primarily as an administrative exercise in the formal fulfillment of legal obligations, rather than as a continuous process of strengthening data security and effectively reducing operational risks.

6. Positioning Romania in the European context

The European Commission’s 2023 Digital Economy and Society Index (DESI) ranks Romania near the bottom of the European digital maturity rankings, with an overall score significantly below the European Union average, particularly in terms of digital human capital and the quality of digital public services [21]. These results indicate the existence of structural deficits regarding the population’s digital skills and the public administration’s capacity to provide high-performing and accessible e-services.

Table 2. Romania's positions in the DESI / Digital Decade 2023 ranking compared to the EU-27 average

Nr. Crt.	Indicator	Romania (2023)	UE-27 Avarage	Target 2030	Position UE-27
1	Basic digital skills (% pop. 16-74 ani)	27,8%	55,6%	80%	27/27
2	ICT specialists (% of employed population)	2,8%	4,8%	~10%	24/27
3	FTTP (fiber to the home) coverage	95,6%	64,0%	99%	2/27
4	5G network coverage (% populated areas)	26,8%	89,3%	100%	26/27
5	SMEs with basic level of digital intensity	22,2%	57,7%	90%	27/27
6	Cloud adoption by enterprises	11,3%	38,9%	75%	27/27
7	Artificial intelligence (AI) adoption - enterprises	1,4%	8,0%	75%	26/27
8	Digital public services for citizens (score)	sub media UE	73% (scor UE)	100%	26/27

Source: European Commission, Romania 2024 Digital Decade Country Report [21]

Romania ranks 27th out of 27 (last) on four key indicators: basic digital skills, digital intensity of SMEs, cloud adoption, and digital public services. The only notable exception is fiber-optic infrastructure (FTTP), where Romania ranks 2nd out of 27 in the EU, a

structurally significant contradiction: connectivity is excellent, but its usage and security rank at the bottom of the list.

Similarly, studies on innovation and digital transformation in local communities confirm that the digitization process is unevenly distributed across the country [10]. While major urban centers are making faster progress in adopting digital solutions, most local public administration authorities have carried out the digitization process in a largely formal manner, without ensuring the corresponding strengthening of cybersecurity mechanisms in parallel. This discrepancy creates additional vulnerabilities, particularly in institutions with limited resources and reduced capacity for managing digital risks [30,31].

Table 3. Urban-rural gaps regarding digitalization in Romania (2023)

Nr. Crt.	Indicator (2023)	Urban (%)	Rural (%)	Difference (p.p.)
1	Households with internet access	90,8	81,4	9,4
2	Regular internet use (last 3 months)	89,0	72,0	17,0
3	People with at least basic digital skills	38,0	17,0	21,0
4	Use of e-government services	24,0	10,0	14,0
5	Use of the internet for submitting forms to authorities	18,0	7,0	11,0
6	People making online payments	41,0	19,0	22,0
7	People using internet banking	32,0	11,0	21,0

Source: own compilation

The Estonian model is a benchmark in the field of e-governance. It is based on a digital architecture built around the principles of security by design, national digital identity, and interoperability through the X-Road platform, which has enabled the achievement of a high level of maturity in digital public services [26,27]. The difference compared to Romania is not determined solely by access to technology, but by sustained investment in institutional capacity, the coherence of the long-term strategic vision, and the existence of an administrative culture oriented toward innovation, efficiency, and accountability.

At the European level, the ENISA report for 2023 highlights a 138% increase in cyberattacks on public entities between 2020 and 2023, confirming the intensifying pressure on the public sector amid the expansion of digitalization [2]. In this context, public administration has become the second most targeted category of cyberattacks, after the financial and banking sector, underscoring the importance of strengthening cyber resilience at the institutional level.

With regard to the transposition of the NIS2 Directive, a comparative analysis across Member States reveals significant differences in implementation. Countries such as Sweden and the Netherlands stand out for their proactive approach and transpositions that exceed the directive’s minimum requirements, while other countries maintain a predominantly reactive approach, focused more on responding to incidents than on preventing them.

In this context, Romania's situation can be summarized along three main dimensions. From a legislative perspective, the regulatory framework is relatively robust, thanks to the transposition of the GDPR and NIS2, the operation of the ANSPDCP, and the DNSC's activities in the field of cybersecurity oversight and coordination. From an infrastructure perspective, however, significant deficiencies persist, characterized by outdated IT systems in numerous public institutions, insufficient investment in security, and delays in the implementation of the Government Cloud funded through the PNRR. From a cultural and organizational perspective, the challenges are even more pronounced, marked by a lack of ongoing staff training in cybersecurity and a low level of maturity in security culture, particularly in small and medium-sized public institutions, where the approach to risks often remains fragmented and reactive.

Overall, these three dimensions highlight the fact that Romania's digital gap relative to the European average is not determined exclusively by technological factors, but rather by institutional capacity, the consistency of public policy implementation, and the extent to which a culture of cybersecurity has been internalized within the public administration.

6. Conclusions and recommendations

The overall picture of data security in Romania's public administration is characterized by a fundamental structural contradiction: the existence of a relatively robust European legislative framework that applies also in Romania coexists with an operational capacity that is insufficient to cope with the volume and sophistication of current cyber threats. This contradiction is not accidental but systemic, reflecting the gaps in administrative capacity, public investment, and organizational security culture that separate Romania from Member States with high digital maturity. Data security in public administration is not, ultimately, a technical problem: it is a matter of political will, institutional governance, and organizational culture.

Research on ethical behavior and compliance culture in public organizations shows that isolated technical solutions cannot compensate for deficits in institutional leadership or the perverse incentives generated by bureaucratic structures. Following this logic, reform recommendations must be structured across three timeframes.

In the short term (0 – 12 months) urgent priorities include mandatory implementation of multi-factor authentication (MFA) for all IT systems handling personal data, mandatory activation of backup systems and business continuity plans for all entities covered by NIS2, the launch of a national cybersecurity training program for civil servants, coordinated by the DNSC and the National Institute of Administration (INA), with modules tailored to different levels of responsibility.

In the medium term (1-3 years), the necessary structural interventions include completing the Government Cloud with the mandatory integration of security-by-design requirements, creating a centralized government SOC for continuous monitoring, and reforming inter-institutional coordination mechanisms for managing major cyber incidents. Studies on digital transformation in local communities also recommend a systematic transfer of best practices from authorities with high digital maturity to those with limited capacity.

In the long term (3-7 years), the strategic objective is to achieve a level of digital maturity and cyber resilience comparable to the European average, by incorporating the principles of security by design and privacy by design into all IT projects and by building an organizational security culture that integrates data protection as an institutional value, not merely as a compliance obligation. The successful models of Estonia and the Netherlands demonstrate that these objectives are achievable with consistent political commitment and sustained long-term investment.

References

- [1] Ministerul Cercetării, Inovării și Digitalizării (MCID), Planul Național de Acțiune privind Deceniul Digital pentru România 2030. București: MCID, 2024. [Online]. Available at: <https://www.mcid.gov.ro/wp-content/uploads/2024/04/Plan-national-de-actiune-roadmap-pentru-publicare.pdf> [Accessed: 22.04.2026].
- [2] Planul Național de Redresare și Reziliență (PNRR). Available at: <https://mfe.gov.ro/pnrr/> [Accessed: 22.04.2026].
- [3] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023. Luxembourg: Publications Office of the EU, 2023. Available at: <https://doi.org/10.2824/782573> [Accessed: 22.04.2026].
- [4] P. Dunleavy, H. Margetts, S. Bastow și J. Tinkler, "New public management is dead — long live digital-era governance," *Journal of Public Administration Research and Theory*, vol. 16, nr. 3, pp. 467–494, 2006. Available at: <https://doi.org/10.1093/jopart/mui057> [Accessed: 22.04.2026].
- [5] Directoratul Național de Securitate Cibernetică (DNSC), Raport Anual de Activitate 2024. București: DNSC, aug. 2025. [Online]. Available at: <https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024> [Accessed: 22.04.2026].
- [6] J. E. Fountain, *Building the Virtual State: Information Technology and Institutional Change*. Washington D.C.: Brookings Institution Press, 2001.
- [7] M. D. Cavelti, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," *Science and Engineering Ethics*, vol. 20, nr. 3, pp. 701–715, 2014. Available at: <https://doi.org/10.1007/s11948-014-9551-y> [Accessed: 22.04.2026].
- [8] R. Anderson și T. Moore, "The economics of information security," *Science*, vol. 314, nr. 5799, pp. 610–613, 2006. Available at: <https://doi.org/10.1126/science.1130992> [Accessed: 22.04.2026].
- [9] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. Gaithersburg, MD: NIST, 2018. Available at: <https://doi.org/10.6028/NIST.CSWP.04162018> [Accessed: 22.04.2026].
- [10] E. Cigu Rusu, D. Hyams-Ssekasi, M. Onofrei, A. F. Vătămanu și A.-M. Bercu, "Innovation and Digital Transformation in Local Communities," *European Journal of Public Administration Research*, nr. 1, pp. 53–61, iun. 2023. Available at: https://www.researchgate.net/publication/375813760_INNOVATION_AND_DIGITAL_TRANSFORMATION_IN_LOCAL_COMMUNITIES [Accessed: 22.04.2026]
- [11] M. Agheorghiesei și A.-M. Bercu, "Ethical Behaviour in HEIs. An Exploratory Study From Students Perspective," *Applied Research in Administrative Sciences*, vol. 3, nr. 2, pp. 5–18, 2022. Available at: <https://doi.org/10.24818/ARAS/2022/3/2.01> [Accessed: 22.04.2026]
- [12] D.-M. Agheorghiesei și A.-M. Bercu, "Ethics of the Financial Services — Relationship Between Health Stakeholders," în *European Financial Resilience and Regulation 25 Years United under Euro (EUFIRE-RE 2024)*, M. Tofan, I. Bilan, E. Cigu (eds.), UAIC Publisher, ISSN: 3044-8689, pp. 10–19, 2024.
- [13] I. Mergel, N. Edelmann și N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, nr. 4, p. 101385, 2019. Available at: <https://doi.org/10.1016/j.giq.2019.06.002> [Accessed: 22.04.2026]
- [14] A. Meijer și M. P. R. Bolivar, "Governing the smart city: A review of the literature on smart urban governance," *International Review of Administrative Sciences*, vol. 82, nr. 2, pp. 392–408, 2016. Available at: <https://doi.org/10.1177/0020852314564308> [Accessed: 22.04.2026]

- [15] DNSC, raport înspăimântător: fraude informatice +40,2%, malware +286,8% în România. Available at: https://www.dcbusiness.ro/dnsc-raport-inspaimantator-fraude-informactice-40-2prc-malware-286-8prc-in-romania_678714.html [Accessed: 22.04.2026]
- [16] ANSPDCP, Retrospectiva activității de supraveghere 2024–2025. București: ANSPDCP, 2025. [Online]. Available at: <https://www.dataprotection.ro> [Accessed: 22.04.2026]
- [17] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Raport de activitate 2023. București: ANSPDCP, 2024. [Online]. Available at: https://www.dataprotection.ro/?page=Comunicat_Presa_09_12_2024&lang=ro [Accessed: 22.04.2026]
- [18] DNSC, Buletin de indicatori, statistici și tendințe de securitate cibernetică H1 2025 [TLP:CLEAR]. București: DNSC, 2025. [Online]. Available at: <https://www.dnsc.ro/vezi/document/buletin-de-indicatori-statistici-si-tendinte-de-securitate-cibernetica-h1-2025> [Accessed: 22.04.2026]
- [19] M. T. Ciucă, "Securitatea cibernetică în administrația publică din România: Provocări și măsuri de protecție în contextul digitalizării," Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository, vol. 2, nr. 1, 2025. Available at: <https://scrd.eu/index.php/spr/article/download/659/644/1480> [Accessed: 22.04.2026]
- [20] S.-A. Ene, "Securitatea informației în administrația publică. Studiu de caz," SPoSC&EGOV Repository, vol. 2, nr. 1, 2024. Available at: <https://scrd.eu/index.php/spr/article/view/526> [Accessed: 22.04.2026]
- [21] Comisia Europeană, Digital Economy and Society Index (DESI) 2023 — Romania Country Profile. Luxemburg: Publications Office of the EU, 2023. [Online]. Available at: <https://digital-decade.ec.europa.eu> [Accessed: 22.04.2026]
- [22] C. Stanciu, "Protecția datelor cu caracter personal în administrația publică în contextul siguranței naționale," SPoSC&EGOV Repository, vol. 2, nr. 1, 2025. Available at: <https://scrd.eu/index.php/spr/article/view/538> [Accessed: 22.04.2026]
- [23] C. Kuner, L. A. Bygrave, C. Docksey și L. Drechsler (Eds.), The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020. Available at: <https://doi.org/10.1093/oso/9780198826491.001.0001> [Accessed: 22.04.2026]
- [24] Guvernul României, Ordonanța de Urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil. Monitorul Oficial al României, 2024. Available at: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121> [Accessed: 22.04.2026]
- [25] Parlamentul României, Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României. Monitorul Oficial al României, 2023. Available at: <https://legislatie.just.ro/Public/DetaliiDocumentAfis/265677> [Accessed: 22.04.2026]
- [26] K. Vassil, "Estonian e-Government ecosystem: Foundation, applications, outcomes," Background Paper: World Development Report 2016: Digital Dividends. Washington D.C.: World Bank Group, 2016.
- [27] R. Kattel și I. Mergel, "Estonia's digital transformation: Mission mystique and the hiding hand," în Great Policy Successes, A. Comín și L. Fuentes (eds.). Oxford: Oxford University Press, 2019, pp. 143–160. Available at: <https://doi.org/10.1093/oso/9780198843719.003.0008> [Accessed: 22.04.2026]
- [28] European Parliamentary Research Service, NIS2 Directive: Transposition and Implementation Across EU Member States. Luxemburg: Publications Office of the EU, 2023. Available at: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-luxembourg> [Accessed: 22.04.2026]
- [29] Parlamentul European și Consiliul UE, Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (GDPR). Jurnalul Oficial al UE, L 119/1, 2016. Available at: <https://eur-lex.europa.eu/legal-content/RO/TEXT/?uri=celex:32016R0679> [Accessed: 22.04.2026]
- [30] C. Vrabie, (2024). Smart-optimism: Uncovering the resilience of Romanian city halls in online service delivery. In Proceedings of the Central and Eastern European eDem and eGov Days 2024 (pp. 51–60). Association for Computing Machinery. Available at: <https://doi.org/10.1145/3670243.3670260> [Accessed: 22.04.2026]
- [31] C. Vrabie. (2025). From presence to performance: Mapping the digital maturity of Romanian municipalities. Administrative Sciences, 15(4), Article 147. Available at: <https://doi.org/10.3390/admsci15040147> [Accessed: 22.04.2026]