An assessment of advanced digital government readiness and related ethical concerns in Romania in the EU digital decade. From missed opportunities to silver linings

Elena DINU,
Faculty of Management, SNSPA, Bucharest, Romania
elena.dinu@facultateademanagement.ro

Cristian-Mihai VIDU,
Faculty of Management, SNSPA, Bucharest, Romania
cristian.vidu@facultateademanagement.ro

Abstract
Objectives This paper attempts to take stock of the realities of digital government in Romania, its ethical considerations in the context of the EU Digital Decade and identify possible remedies..**Prior work** The current investigation builds on the premises of the unified theory of acceptance and use of technology and links the theoretical and empirical research in the field with the contemporary developments of public management. **Approach** The paper bridges the theoretical and empirical research in the field of e-government with a comparative analysis of successful e-government services to reveal the best avenues for e-government development in Romania. **Results** This study presents theoretical and practical insights supporting the implementation of valuable and appropriate e-government solutions in Romania. **Implications** Given the objectives of the inquiry, its implications will primarily concern public management practice and **Value** This exploration provides a novel perspective on the existing challenges and solutions in digital government based on an overarching scientific analysis of up-to-date information and data.

Keywords: E-Government, Romanian case study, digital governance ethics, cybersecurity, comparative analysis.

1. Introduction

The first e-government application in Romania was launched in 2003 with the aim of implementing UN SDG 11 on sustainable cities and communities and SDG 9 on industry innovation and infrastructure [1]. However, 20 years later, digital governance development is still lagging behind, though some online services provided by public organisations are available to some extent. In addition, digital literacy remains subpar, while e-government service use is related to the level of education [2]. Civic participation on cities' websites has decreased after the COVID-19 pandemic [3], and recent studies suggest that public digital services should consider not only citizens' needs but also their skills [4]. Citizens' use of e-government solutions depends on service quality (system quality, reliability, security, accessibility, information quality, service capability, interactivity, and responsiveness) and perceived service value, which determine user satisfaction. [5] Apart from user-related aspects, civic behaviour regarding the use of e-government opportunities is contingent on performance and effort expectancy, social influence and facilitation, but also trust, as proved by Hooda et al. [6]in an extended framework of the unified theory of acceptance and use of technology (UTAUT).

The digital transformation of public administration is a continuous process, unlike traditional projects with specific end dates [7]. As it unfolds, the process leads to profound changes in attitudes, relationships and culture, producing a new paradigm for the public service. Digital transformation aims to connect people, devices, and physical objects remotely and instantly, empowering clients and disrupting traditional thinking paradigms [8]. New studies explore artificial intelligence's benefits to digital government, from service quality, efficiency and performance, risk management, decision-making, societal value, economic growth, sustainability, and user engagement. Potential challenges have also been highlighted, such as ethical problems and legitimacy, data quality, skills, change management, transparency, job displacement, bias and discrimination, etc. [9]. Intelligent e-government 3.0 solutions could mitigate certain aspects concerning the delivery of public e-services [10] [11], whose main benefits following Moore’s 1995 view on public value resides in services, outcomes, and trust [12]. Ultimately, e-government should render better social value and well-being [13].

2. Background

The Authority for the Digitalization of Romania (ADR) was created in 2020 as a public entity under the Ministry of Research, Innovation, and Digitalization (MCID) but does not seem to have a clear leadership position, while the country lacks a digital government strategy [14]. Romania needs further investments in public infrastructure and institutional cooperation to provide open government data access and to build inclusive, transparent, client-centric digital services. At the same time, the socio-economic and generational digital divide and the split between large urban areas and rural ones should be mitigated [15].

According to Eurostat 2023 data, Romania ranks last in the EU when it comes to citizen engagement with public authorities’ websites or apps. At 23%, this is less than half of the figures for Germany and far behind Denmark and other Nordic countries (close to 100%), which are the best EU performers. Denmark is the top world performer in the e-government area according to the UN E-Government Knowledgebase [16]. The types of activities residents could benefit from on e-government platforms involve obtaining information about services and laws, downloading official forms, making appointments and receiving communications, submitting tax declarations, accessing public databases, requesting official documents, making complaints, etc.

Despite being a laggard at the EU level in this respect, Romania appears to be slowly moving ahead based on information available from various sources. For example, data from Statista [17] shows that the number of Romanian e-government users has grown by 9% at the end of the Covid-19 pandemic (2022). The UN Egovkb [16]also shows an improvement in Romania’s performance, with the country being ranked 72 out of 193 in 2024, climbing 15 positions since 2022 in the E-Government Development Index. At the same time, the E-Participation Index reflects an increase in citizen engagement, albeit lower, with a rank of 58 out of 193, representing a four-position improvement.

The International Institute for Management Development’s [18] scoring places Romania in position 48 out of 64 countries on digital competitiveness, which is viewed as an average of three dimensions: knowledge (talent, training/education, and scientific concentration), technology (regulatory and technological frameworks – best scores, and capital), and future readiness (adaptive attitudes, business agility, and IT integration) [18]. Paradoxically, Romania scores good ranks in certain respects: 11 in the number of graduates in sciences, 4 in Internet bandwidth speed, and 14 in government cybersecurity capacity. Nevertheless, the number of mobile broadband subscribers is 56 (among the last in the cluster). The biggest weaknesses IMD identified are low public-private partnerships, scoring 58; public education spending, 56; and achievement, 55. Other significant impeding factors are banking and financial development 57, investment in telecommunications and management of cities 54, total expenditure on R&D 50, and tech development and application 46.

Advanced digital societies have long started employing AI and smart technologies to improve citizens' lives and tackle problems concerning transportation, education, community development, and sustainability, and technology is a driver of innovation [19]. Studies by Ibanescu et al. and Vrabie [20], [21] analysed smart city activities in Romania and showed that, while the first initiatives appeared in 2010, they gained momentum after the launch of various forms of association and the biggest Romanian cities (Bucharest, Iasi, Cluj-Napoca, Timisoara, Craiova) benefitted from more projects. Nevertheless, as the authors noted, most applications focused on the technology-based improvement of living and mobility rather than on communities seen as social networks. In the IMD Smart Cities Index 2024 [22], Bucharest ranks 100th out of 142 with an overall B factor rating, moving up from a CCC factor in group 3 in the previous year. Nevertheless, the city got less than average survey assessments regarding governance-related issues, such as transparency and access to official information, citizen involvement in local decision-making, and online services. As a consequence, trust in authorities is relatively low compared to the best-performing countries (53,3%), and transparency and corruption are perceived as a high priority (50,4%), together with air pollution (65,3%) and road congestion (58,5%).

3. The way forward

A full-scale societal digital transformation could mitigate some of the identified issues by facilitating citizen's access to official information and data based on digital IDs for public self-services while favouring transparency [23] and inclusiveness. Moreover, trustworthy, secure, and user-friendly smart applications could provide residents with useful and dependable tools to participate in decision-making concerning their communities. Furthermore, such instruments could augment the visibility and accountability of public organisations' activity, allowing interested parties to check on the actions of their representatives and provide input for priority policies and procedures. Consequently, transparency would reduce uncertainty, and citizens' trust would increase [24] while opportunities for unscrupulous use of public money or discrimination could be averted, as suggested by empirical studies. [25], [26]

However, at the same time, the progress towards the full-scale digital transformation of society increases the attack surface of the government's infrastructure and the cyber security risks to which citizens' data and private information are subjected. Confidentiality, Integrity and Availability are core cyber security principles that require careful consideration and balancing to achieve the best result. However, prioritisation of one may come at the detriment of another. Moreover, and especially in the context of government data on its citizens, the handling and access of this sensitive and private information, even for authorised parties, requires the design and implementation of solutions that enable the data owner, the private citizen, to gain visibility on who and when has accessed their data, thereby facilitating accountability and transparency.

Threats to data are coming today from multiple adversaries, ranging from young but skilled individuals who were able to challenge global organisations such as Microsoft, Nvidia and others [27] to organised crime groups taking down entire governments [28] [29], all the way up to nation-state and nation-state affiliated actors strategically placing themselves in positions to take down civilian critical infrastructure as a deterrent [30] or actually "turning off the lights for hundreds of thousands of civilians" during war [31]. Not to forget the threats from those authorised to view the information but might misuse their access or get corrupted, such as insiders leveraging their access to sell private citizen information to the highest bidder, as exemplified by Greenberg (2024) in the case of Chinese government clerks, or government agencies leaning on the mass information available to them to spy on their own citizens, which we might extrapolate by bringing the old East-German Ministry for State Security (Stasi) into the current day [32].

While some new technologies, such as blockchain, with an underlying decentralisation principle, can increase some of the core cyber security principles by enhancing resilience, improving availability and ensuring integrity through the elimination of single points of failure and the elimination of centralised management [33] , [34]], they might not be able to also address, at the same time, the challenges of confidentiality or privacy [35].

Considering the concerns about digitalisation and the growing threat landscape posed by cyber-attacks, the EU has put forward the Network and Information Security (NIS) Directive [36], now at its second iteration (NIS2), with the aim of achieving a high level of cybersecurity across the Member States. Similar to GDPR, which was designed to ensure the privacy of EU citizen data, through the NIS directives, the EU is making a bold attempt to create a unified framework for all member states, where national cybersecurity authorities have the mandate, within their respective countries, to ensure that cybersecurity measures are taken by organisations across seven critical sectors (energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure) and to assist and handle incidents at national level through national Computer Security Incident Response Teams (CSIRTs). Furthermore, the NIS directives require organisations to report any significant cyber incidents causing severe operational disruption, financial damage or material loss, which can improve overall security by preventing similar attacks against other organisations through a sharing mechanism. A distinctive feature of the NIS2 directive is the introduction of mandatory training for managers and management bodies of entities subject to the NIS2 directive, equipping them with the necessary knowledge and understanding to approve the implementation of cyber security risk measures [36].

Successful, encompassing, harmonised e-government frameworks must fully consider data reliability, security and usability, interoperability, privacy, inclusiveness, accountability and transparency. As an EU Member State, Romania has to comply with the EU strategies and policies and develop its digital government solutions along the lines of the EU Digital Decade framework (see Decision EU 2022/2481 of the European Parliament and of the

Council) by empowering citizens and businesses while integrating green, advanced digital technologies and AI [37].

4. Methodological approach

In the EU Digital Decade framework, the European Commission monitors the progress in implementing digital public services through the eGovernment Benchmark [37]. The focus is on the 27 EU Member States, the countries associated with the European Free Trade Agreement, and candidate countries (EU27+). The underlying legal framework is comprised of the Declaration on Digital Rights and Principles [38], the Single Digital Gateway, the Web Accessibility Directive [39], the eIDAS regulation [40], the Interoperable Europe Act [39]and the Once Only Technical System (OOTS). Starting from these grounding standards, citizens and businesses are expected to get cross-border online access to all "life events." This term is understood as a bundle of public services reflecting key points in individuals' and enterprises' lives. A user's journey may include informational or transactional services that can be accessed from a unique portal. Four pillars support the users' seamless experience: user centricity, transparency, key enablers, and cross-border access. Electronic identity (eID), eDocuments, Pre-filled forms, and Digital Post are key enablers. Other important indicators are strong cybersecurity safeguards against threats (only 1% of the assessed countries passed the test), digital sovereignty, resilience, interoperability, and data sovereignty. The employment of AI in public services is a new indicator introduced in 2022 (eGovernment Benchmark).

On average, the EU indicator for public services for businesses stands at 85 points, which is higher than for citizens (79). The lowest scoring indicator is the transparency of service delivery, design, and personal data, with an average of 67, raising some concerns about compliance with legal and ethical standards, as citizens do not have a clear view of the personal data held by governmental organisations and by whom that data is accessed. The overall performance of the EU27+ eGovernment reached 76 points, and, unexpectedly, Malta led the appraisal with 97 points, followed by Estonia (92). Romania ranks 48 points and takes the last position in the EU. The only dimension Romania has improved on recently is cross-border services (+ 14 points). One major disparity that draws attention at the EU level is the difference between online services offered at the central and local levels. For this investigation, we chose a comparative analysis method to reveal the top players' standards and best practices in digital government services and analyse how Romania currently compares. Even though the expected differences are high, the examination can still help detect underlying issues preventing successful digitalisation and possible solutions to accelerate the process. Based on the international assessment (e.g. UN and EU indexes), we decided to look at Denmark, Estonia, Singapore and Norway. The first three countries comprise the best formers in the UN Egovkb index and the constant top EU member countries in digitalising governmental services. As underlined in the UN report, the EU area ranks first in the world in this field. Norway is another country in Northern Europe but outside the EU with a confirmed good record in this respect, and data availability in English was a deciding factor when making the selection. Finally, Singapore is the most digitalised country in the world outside of Europe.

5. Results

In this section, each of the countries selected for the comparative analysis is assessed in terms of the degree of digitalisation, the underlying principles and values, and the practical benefits for individuals and businesses.

Denmark

While various impediments to the digitalisation of public services are often invoked, such as a lack of money, resources, or manpower, the investment in adequate digital solutions is justified by offering long-term results, i.e., cost reduction, resource optimisation, and efficient use of public servants. Nevertheless, a government needs political and societal support to achieve this transformation. Moreover, the future users of digital services must have or acquire enough skills to benefit from the new public service paradigm. To this end, an encompassing legal framework must be adopted, creating a new digital model for establishing identity, authenticity of documents, and consent in transactions without duplicating extant bureaucratic models. Digitalisation offers opportunities for innovation and simplification of administrative procedures. From an institutional perspective, a certain degree of de-centralization of administrative services (i.e., central vs local) must be achieved. Furthermore, technical know-how, integration, cooperation, and harmonisation between various public institutions are required. To obtain public support, the digitalisation of essential and cumbersome services must be prioritised (e.g., tax return forms, e-prescriptions, electronic signatures, safety and security services, etc.), support to (first-time) users must be ensured, the focus of administrative interactions should be shifted on the user, and citizen engagement should be enhanced. Given all the above considerations, governments must rely on public-private partnerships to secure technical expertise and manpower for infrastructure development and program management and provide support to and train the users where necessary. Reliable and sustainable digital services are built with cybersecurity, data quality, and ethical values as grounding principles. Trust, community, and low corruption are the fundamental values at the basis of Danish digitised society. In Denmark, for example, public trust in digital solutions reached 78% in 2023, while almost a quarter of all citizens needed some support utilising digital services (Statistics Denmark, 2023). Finland and Norway rank first in digital skills, slightly over 80%, and Romania comes last with almost half of that percentage [41].

Interestingly, the digital strategies of top performers in digital government (e.g., Denmark, Estonia, Norway) state their country’s global positioning as digitalisation leaders, assuming a long-term digital innovation strategy. While all the mentioned programs share common principles, the Danish one includes a distinctive principle regarding ethics and responsibility underlying digitalisation. Moreover, Denmark has a national strategy dedicated to AI development and utilisation for individual and business purposes, where the ethical foundations are highlighted from the start. For example, it is stressed that AI cannot replace human decision-making and that algorithms must ensure fairness, equality, inclusiveness, and transparency. For this purpose, Denmark set a common ethical and human-centred basis for artificial intelligence adoption and development, both in the public and private sectors, to offer better and more customised services. Most Danish companies have introduced policies for data ethics [42]. New education programs on AI are being developed, and a strong research culture is built to allow for competent collaboration opportunities within the EU research and innovation framework. However, even the world's top performer in this area faces challenges. Denmark recognised the need for a comprehensive ethical framework to guarantee human rights and due process, more technical skills for development, further investment, and more and better data for AI, according to the 2019 National Strategy for AI. The country prioritises the usage of AI in healthcare, energy and utilities, agriculture, and transportation.

Acknowledging the risks posed by the increase in digitalisation, Denmark has moved information security from a point in the previous digital strategies to an entirely new and separate 2021 National Strategy for Cyber and Information Security, focusing on four key strategic objectives: robust protection of vital societal functions, improving and prioritising levels of skills and management, strengthening the cooperation between the public and private sectors and active participation in the international fight against cyber threats. However, they also admit that "many agencies lack basic technical security measures", and there is a need to strengthen cross-sector and international collaboration and promote an overall increase of cyber and information security skills within the general population.

Estonia

Praised by various international organisations (such as the UN) and top media and technology outlets as the role model for human-centric digitalisation and the most digitally advanced society, Estonia boasts a 99% availability of all public services online (https://www.eesti.ee/eraisik/en/avaleht) and even offers free lessons on digitalisation on its e-gov communication landing page (https://e-estonia.com/). Starting digitalisation way ahead of others through IT infrastructure development with the Tiger Leap Initiative in 1996, Estonia has developed its own technological solutions, whose codes are often open-source. The e-ID ecosystem comprises an ID card, a Mobile ID, a Smart-ID app, and an e-Residency for foreigners not located in the country. This digital identity, which benefits from advanced solutions (such as SplitKey technology), ensures access to numerous public and private services (e.g., healthcare, paying bills, signing contracts, online voting, etc.). The KSI blockchain is another technology developed locally to ensure data integrity and protection against insider threats, while data transfer is achieved through X-Road, a scalable solution for harmonisation, data exchange and cross-searches between a multitude of public and private IT systems. The Unified eXchange Platform (UXP), a solution employed in Japan, the USA, and NATO, allows secure peer-to-peer data exchange through encrypted and mutually authenticated channels (https://e-estonia.com/solutions/). Estonia employs AI technology for advanced smart mobility services, weather monitoring, etc.

Cybersecurity has become a top priority since the cyber-attacks in 2007, which served to highlight the vulnerability of online services even to low-skill attacks against the availability of these services [43]. As a result of the attacks, Estonia has pioneered the idea of data embassies as a way to persist and continue providing digital services beyond Estonia's borders, thus safeguarding the nation's digital sovereignty even if it were to be occupied [44], [45]. This higher focus on resilience and redundancy, instead of the more classical proactive and protective measures which aim to prevent, neutralise or deter the threats before they have a material impact, is a result of the fact that smaller nations, such as Estonia, lack the resources that larger nations can bring to bear and enable them to achieve the deterrence factor [46].

Norway

Norway provides clear, step-by-step information on one portal to individuals (e.g., certificates, permits, administrative forms (including complaints and remedies) for asset registration, work, healthcare, welfare, pensions, taxes, parenting, education, justice, culture, etc.) and businesses (planning, starting and running a business; governmental support opportunities; bookkeeping and tax requirements; certifications and permits; work legislation essentials; intellectual property rights; export and import conditions; ecolabelling; bankruptcy, closure and deregistration, etc.) (https://www.altinn.no/). Links to the corresponding public institutions' websites are included for each topic, documentation requirements and samples, legal remedies, and even practical advice for beginners. Essential information is available in English. The platform incorporates a communication solution with petitioners, who can securely access the digital mailbox with a registered ID. Norway has had a national AI strategy since 2020 and has established digital innovation hubs for SMEs. Businesses benefit from research support and tax deductions for R&D activities.

Norway was one of the first countries to recognise the importance of cyber security when implementing a digital society and introduced its first cybersecurity strategy in 2003, continuing to update and revise it in 2007, 2012 and 2019 [47]. The current strategy emphasises that companies should continue to digitalise securely, protect themselves against cyber incidents, and increase cybersecurity competence and society's ability to detect and handle cyber attacks.

Singapore

According to the UN Index, after Denmark and Estonia, Singapore is the third-top country in terms of digital government. It is also one of the countries with the lowest corruption levels, ranking 5 on the Corruption Index [48]. Smart Nation Singapore was launched in 2014 to improve citizens' lives with technology. The digital identity for individuals, SingPass, and e-payment networks were first introduced. The HealthHub allows access to the medical file, healthcare services, and medical information. LifeSG is designed to provide services to citizens throughout their life journey. Businesses can get access to government services through CorpPass. By now, 97% of citizens are registered for digital services, 95% of small and medium-sized businesses are digitalised, and 99% of transactions (close to three thousand services) between citizens and the government take place online, with a satisfaction rate of 83% (https://www.smartnation.gov.sg/). Smart Nation 2.0 [49] looks further by leveraging advanced technologies to improve the optimisation and customisation of services and highlights AI as a strategic national priority [50]. Sectoral AI centres of excellence are launched, and investments in AI for research are allocated. In 2020, Singapore started a new National Digital Literacy program focusing on providing pupils with personal learning devices and applied learning programmes on advanced technologies.

AI-backed traffic monitoring optimises public transportation, while passport-less immigration and iris biometric and facial recognition technology make for a swift cross-border clearing for citizens. The Punggol Digital District (PDD) was established in Singapore, integrating smart technologies that automatically interact and adjust various facilities depending on human traffic in commercial and industrial buildings (e.g., light and air conditioning) for sustainable management. AI and smart robots have made their way into healthcare, education, and culture to enhance user experience. Various applications encourage community involvement in supporting members with special needs. The Personal Alert Button installed in elders' homes can signal distress, while the Healthy365 App provides access to resources for a healthier lifestyle. One Service App allows citizens to engage with municipalities, and CrowdTask SG is a crowdsourcing solution for government agencies. Giving.sg is a platform for donations, volunteering and fundraising for NGOs. Challenges related to using smart technologies (e.g., fraud, cyberbullying, disinformation, mental health disorders, job disruption fear, etc.) need to be addressed through specific measures (strengthening of cybersecurity, updated legal frameworks, victim support, empowerment through training).

Singapore's emphasis on rapid technological development and quick adoption of disruptive technologies overlapped with a complex geopolitical setting and a good understanding that an increase in digitalisation has a direct increase in the exposed attack surface area, which makes it even more important to have a secure foundational layer. The Singapore Cybersecurity Strategy of 2021, an update of the first strategy released in 2016, relies on two foundational layers: a vibrant cybersecurity ecosystem and the development and growth of a robust cyber talent pipeline [51]. The strategy's three interconnected pillars, resilient infrastructure, safer cyberspace and enhanced international cooperation, underscore the need for a balanced approach that combines individual resilience with collaborative efforts to address the growing number of threats, ultimately aiming for a secure and stable cyberspace.

Romania

The Romanian National Action Plan for the Digital Decade was finally approved in October 2024 [52]. The document shows that only a quarter of Romanian citizens use digital public services, less than a third have digital skills, and the availability of services is low. The main identified problems from users' perspective include lack of integration, user support and experience (on mobile devices), and pre-filled documents. The legal framework for digital government is being built (see Law 242/2022), and the National Platform for interoperability has been established. Several principles have been laid down for prioritising the digitalisation of public services: infrastructure upgrade, digital identity, interoperability, data-driven solutions, user-driven, proactivity, transparency, open data access, cybersecurity, technological neutrality, and compliance with EU standards. With EU financing under the Recovery and Resilience Plan, Romania is moving forward with the creation of the Government Cloud. Further measures regard the introduction of the national digital ID cards and the ROeID for the single access point to digital services. Since 2022, targeted financing for IT infrastructure, equipment, and improving digital literacy was provided, and regional consortiums were established. Other projects concern the adoption of the National Strategy for AI and the establishment of the Romanian National Center for Artificial Intelligence.

The open data portal of the Romanian Government (https://data.gov.ro/) provides access to some data sets in the fields of Justice and Public Safety, Finance and Economy, Agriculture, and a few national registers for experts. The national courts portal (https://portal.just.ro/SitePages/acasa.aspx) allows for retrieving information about the status of court files and decisions and information about the courts. The National Agency for Cadastre issues fast online certificates on real estate (https://epay.ancpi.ro/epay/Welcome.action). The National Agency for Fiscal Administration offers the Private virtual space function (https://www.anaf.ro/anaf/internet/ANAF/servicii_online/inreg_inrol_pf_pj_spv), where natural and legal persons can register, manage some electronic services, and receive official mail. Also, VAT-related services are available at https://www.anaf.ro/anaf/internet/ANAF/servicii_online/one_stop_shop. The National System for electronic invoicing can be accessed at https://mfinante.gov.ro/web/efactura. On the National System for Online Payments' website (https://www.ghiseul.ro/ghiseul/public/#), citizens can pay taxes and fines to the accounts of enrolled institutions. However, some local administration institutions have developed their own applications for this purpose. The Romanian Agency for Digitalisation launched in 2023 a mobile ROeID app, which has since been used with mixed reviews by citizens. Similarly, ROeIDAS was made available to foreign citizens in EU states. The Ministry of Internal Affairs provides a portal for several online services (https://hub.mai.gov.ro/), such as obtaining certificates (e.g., criminal records) and administrative authorisations or making appointments to services provided in person. An electronic service for the public procurement system is available at https://www.e-licitatie.ro/pub. The single entry point for integrating e-government services was launched on https://edirect.e-guvernare.ro/SitePages/landingpage.aspx, providing information to individuals and businesses about the available services at central and local levels, template documents for requests, petitions, claims, etc., from professional, personal, administrative, educational, and cultural sectors.

One area where efforts are being focused to recover from failed digitalisation attempts is healthcare. The projects for the Integrated Information System, the e-prescription system, the digital national health insurance card, and the electronic patient file have all gone awry. A strategic, unified approach is required to achieve the envisaged goals of providing advanced, patient-centric services in an integrated manner based on quality data and surmounting the inequities concerning access to health, with great differences generated by the income level, the regional development status, and also the urban vs. rural location [53].

Romania published its first cybersecurity strategy in 2013, focusing, similar to other countries, on a safe virtual environment and a high degree of resiliency and trust to serve as a support for national security and good governance. In this first strategy, one of the principles enumerated was the separation of networks, with the aim of reducing the probability of attacks through the use of networks that are not connected to the Internet [54]. However, while this type of separation does provide an increase in the confidentiality and integrity of the data, it also poses a challenge for an increase in the digitalisation of public services. Therefore, in its second revision, from 2021, the principles have been changed and updated to reflect a new vision, removing this previous principle. The updated objectives are safe and resilient information networks, a consolidated legislative approach, public-private partnerships, resilience through a proactive approach and deterrence and an ambitious commitment to making Romania a relevant actor in the international cooperation architecture [55]. In order to fulfil these objectives, Romania has established a new civilian institution, the National Directorate for Cyber Security (DNSC). This newly established institution, which has taken over the responsibilities previously assigned to CERT-RO, is now responsible for ensuring the cyber security and resiliency of the civilian cyberspace, creating the public-private-academia cooperation framework and for the development of the cybersecurity workforce. While DNSC is a new institution, traditionally, Romania has already been considered a leader in this area [56], [57], which represents a strong point and allows DNSC to "hit the ground running" and be in a good position to fulfil the ambitious objectives set forth in the National Cybersecurity Strategy.

6. Discussion and conclusions

The literature review and comparative analysis have revealed an encompassing framework for the successful digitalisation of governmental services that is compliant with the legal, technical, and ethical principles enacted by the European Union in its Digital Decade Programme 2030. In addition, best practices from the most advanced governmental services should be considered. The underlying goals of the EU agenda are the digitalisation of public services, secure and sustainable digital infrastructures, digital transformation of businesses, and digital skills development. Throughout digitalisation, fundamental EU values must be observed, placing people at the core and ensuring freedom of choice, safety and security, solidarity and inclusion, participation, and sustainability.

Tables 1, 2 and 3 show an overview of the research outcome.

Table 1. Synthesis of the comparative analysis of best practices in e-government from a strategic management perspective

Factor	Country/Link	Features
Leadership	Denmark https://en.digst.dk/	Danish National Agency for Digital Government
	Estonia https://www.eesti.ee/eraisik/en/avaleht; https://e-estonia.com/	Estonian Government
	Norway https://www.altinn.no/; https://www.regjeringen.no/en/id4/	Norwegian Digitalisation Agency; Norwegian Government
	Singapore https://www.smartnation.gov.sg/	Digital Government Office
	Romania https://www.mcid.gov.ro/; https://www.adr.gov.ro/	Ministry for Research, Innovation and Digitalisation; Romanian Agency for Digitalisation
Digital strategy	Denmark	Digital Strategy; AI Strategy; National Strategy for Cyber and Information Security
	Estonia	Tiger Leap Initiative; AI Strategy; Cybersecurity Strategy
	Norway	Digital Norway Strategy; AI Strategy; Cybersecurity Strategy
	S.Singapore	Smart Nation Singapore 2.0; AI Strategy; Cybersecurity Strategy

	Romania	National Action Plan for the Digital Decade; Cybersecurity Strategy
Legal digital framework	Denmark	Extensive; digitalisation leader
	Estonia	Extensive; digitalisation leader
	Norway	Extensive
	Singapore	Extesive; digitalisation leader
	Romania	Under development; Law 242/2022

Table 2. Synthesis of the comparative analysis of best practices in e-government from a technological perspective

Cybersecurity	Denmark	Robust, prioritising levels of skills and management, strengthening the cooperation between the public and private sectors and active participation in the international fight against cyber threats; increase in cybersecurity for institutions.
	Estonia	Top priority after the 2007 attacks; data embassy; advanced in-house solutions employed by international partners; resilience and redundancy.
	Norway	High priority; early promoter of cybersecurity in digitalisation; emphasising competencies and detection capabilities.
	Singapore	Highlighting a cybersecurity ecosystem and the development and growth of a robust cyber talent.
	Romania	Updated objectives: safe and resilient information networks, consolidated legislative approach, public-private partnerships, resilience through proactive approach and deterrence, and commitment to making Romania a relevant actor in the international cooperation architecture.
Interoperability	Denmark	High;adjustment between central and local government envisaged.
	Estonia	High.
	Norway	High.
	Singapore	High.
	Romania	Low. The National Platform for interoperability has been established; Infrastructure upgrade; creation of Government Cloud.
Data protection	Denmark	High.
	Estonia	High.
	Norway	High.
	Singapore	High.
	Romania	Good.

Digital inclusion	Denmark	Digital skills development, single access point, equal treatment, user assistance, plain communication, safety training.
	Estonia	Extensive. Programmes for digital skill development in schools.
	Norway	Extensive. User support and resources, plain communication in administration.
	Singapore	Extensive. National Digital Literacy Program; apps for communities; crowdsourcing; advanced services for elders.
	Romania	Low. Reduced digital literacy, limited access and user support, and lack of pre-filled documents.
Common registries	Denmark	Extensive.
	Estonia	Extensive.
	Norway	Extensive.
	Singapore	Extensive.
	Romania	Under development.
E-Identity	Denmark	eID and eIDAS Implemented.
	Estonia	eID and eIDAS Implemented. Multichannel/platform; e-Residency.
	Norway	Implemented. Digital nomad program.
	Singapore	Implemented.
	Romania	Under development.
Transparency	Denmark	High. Human-centred, comprehensive ethical framework, community focus.
	Estonia	High. Role model for human-centred digitalisation.
	Norway	High. Human-centred.
	Singapore	High. Human-centred. High user satisfaction.
	Romania	Low. Bureaucratic, institution-centred services.
Sustainability	Denmark	High. Integration of AI in sustainable services.
	Estonia	High. Advanced integration of AI in sustainable services.
	Norway	High.
	Singapore	High. Advanced integration of AI in sustainable services.
	Romania	Low integration of digital services in sustainability.

Table 3. Synthesis of the comparative analysis of best practices in e-government by sector

E-Health	Denmark	Extensive, integrated healthcare prioritised.
	Estonia	Extensive, integrated services. AI in healthcare prioritised.
	Norway	Extensive, integrated services. AI in healthcare prioritised.
	Singapore	Extensive, integrated services. AI in healthcare prioritised. HealthHub, apps for wellbeing and healthy lifestyle.
	Romania	Under development. Socio-economic divide. Urban vs rural divide.
E-Justice & public safety	Denmark	Extensive services.
	Estonia	Extensive services.
	Norway	Extensive services.
	Singapore	Extensive services.
	Romania	Under development. National courts portal; limited online services provided by the Ministry of Internal Affairs.
E-Education&research	Denmark	Extensive services. Strong research culture. Open access governmental data.
	Estonia	Extensive services. AI in education and culture. Open access governmental data.
	Norway	Extensive services. Innovation hubs.
	Singapore	Extensive services. Advanced programs for applied digital technologies in secondary education. AI Centers of Excellence.
	Romania	Low spending on education and research; lack of equipment and digital resources; weak public-private partnerships and institutional cooperation;limited open data availability.
E-Business	Denmark	Extensive services. Public-private partnerships.
	Estonia	Extensive services. Public-private partnerships.
	Norway	Extensive services. Public-private partnerships.
	Singapore	Extensive services. Public-private partnerships.
	Romania	Limited services in fiscal and commercial matters; e-procurement.
Smart cities	Denmark	Developed. Prioritises the usage of AI in energy and utilities, and transportation.
	Estonia	Developed. Advanced smart mobility solutions, weather monitoring, etc.
	Norway	Developed.
	Singapore	Developed. Extensive AI use in transportation, healthcare, cross-border management, and sustainability management.
	Romania	Limited development. Inequality between big cities and other areas. Regional inequalities.

Source: Authors

At the strategic level, Romania has to create a well-defined vision and context for digital transformation by establishing leadership, reaching political agreement and support for the digital future to ensure programme continuity, and developing its legal framework to ground the digital principles across the socio-economic foundations and ingrain institutional cooperation, coordination, and compliance. Legal predictability without gaps, ambiguity and frequent alterations will support programme stability. On the other hand, digitalisation can reinforce legality by providing digital proof and justification in transactions, deadline observance, and sustainability (less paperwork). In line with programme leadership and management principles, successful projects require an accurate understanding of the scope, a good structure, clear objectives, and well-planned activities grounded on appropriate capabilities and resources. A valuable lesson can be learned from others: the need for strategic application development and deployment. The case of Indonesia's government app proliferation serves as a cautionary tale, highlighting the risks of unchecked application creation. With over 27,000 apps developed and an annual maintenance cost of $386 million, it underscores the importance of effective governance and the adoption of a strategic approach to application development [58].

Programme leadership is paramount to ensure strategic direction, stakeholder management, coordination, resource management, decision-making and problem-solving, communication and oversight. The relevant stakeholders must be involved, and they should be assigned justified tasks and responsibilities with realistic deadlines. A certain degree of flexibility is required to accommodate unforeseen events, but an enforceable risk management plan is essential. Competent oversight and feedback are necessary at all stages, and corrective actions must be taken swiftly to avoid failures. As governmental digitalisation is a complex programme, some components must be delegated to reliable stakeholders, depending on the responsibilities involved. Such a major transformation must leverage all national capabilities and create social synergies. A partnership between public institutions, the private sector and academia, should be enacted to tap into available skills and expertise.

The scope of the digital transformation has to be well-thought, and the vision must be bold, looking into the future, since this is a long-term project which needs adjustments to changing social and technological realities. Digital services should be developed with users and their life journeys in mind. Various user categories have various needs and problems that require resolution. Moreover, citizens and residents must be included and engaged in the relationship with the authorities. All legitimate interests must be represented. It is fundamental to design new services beginning from a paradigm shift. Digital services should not mirror the current paper-based ones but replace bureaucratic procedures and burdening interactions between individuals, businesses, and the state. Competent public communication is required to garner public support and build trust.

Privacy is considered an important aspect of today’s digital environment. The digital footprint of each citizen enables significant power for those who store and can access that information. At the same time, lessons from the past, be that past distant or more recent [59], remind us of the importance for citizens to be able to understand who is accessing the information available on them. Governments should create a framework which enables auditing of all access and provides each citizen with the ability to view the entities accessing their data.

Considering Romania’s communist history, the delivery of governmental services should be proactive, and users should be empowered, thus breaking away from the prevalent bureaucratic culture. Moreover, the service design should embed usability, transparency, accountability and compliance, to preempt favouritism and, thus, inequality between users or illicit behaviours. As previously mentioned, empirical literature corroborated with Eurostat data shows that, in general, people from former communist countries tend to be more reluctant to utilise digital government services as their level of trust and reliance on authorities is, by default, lower. To boost the use, people could be incentivised by reductions in fees, as some suggested [60], which is supported by the service cost cuts following digitalisation.

The social divide between the urban and rural areas should be properly addressed in collaboration with the local administration, and solutions for community engagement should be devised to overcome resource limitations. The digital divide should be mitigated by planning and implementing programmes for digital skill development and user support while the digitalisation programme is ongoing and not at the end. This will allow people to access and benefit from available services, and interact with public institutions. This relationship is negatively influenced by income inequality, low levels of education, and unemployment [61]. By directly engaging with public organisations, people in disadvantaged categories may perceive less social distance, more transparency, and a better understanding of what is done to address their needs.

Empirical research confirms that education and digital skills positively influence interaction with e-government services and development. Moreover, higher government efficiency boosts population trust and reinforces a pattern, sustaining further growth. Consequently, one strategic priority for the government should be increasing the level of digital skills in adults, who are the first users of the system, and youth, who will utilise digital government services in the future. This is also an opportunity to educate and train the next generations of professionals for sustainable e-government development. As confirmed by empirical research, digital competencies and an intrapreneurial attitude significantly affect readiness for the future of work in public administration staff [62]. New solutions can leverage crowdsourcing, take advantage of user insights in the test phase, and increase popular support for the end products. Digital interactions with public authorities significantly affect people’s trust in institutions.

The adoption of AI and Industry 4.0 and 5.0 technologies, switching from automation to human-machine collaboration, can offer flexible and innovative solutions to help mitigate some of the socio-economic challenges and tackle the most stringent problems, e.g., traffic, air pollution, natural resources and weather monitoring, issuing alerts and managing disasters, intake of foreign workforce, ageing population, etc. However, it is crucial to recognise that AI itself poses significant risks, with Generative AI being a prime example. As AI systems become increasingly complex, they often produce results that are opaque and difficult to interpret. This makes it challenging to understand the underlying reasoning behind their decisions. Furthermore, the use of large or partially unknown datasets during training can introduce biases and ethical concerns, which can resurface in the final results.

Understanding that cybersecurity represents a foundational component of any digitalisation effort is one of the first steps required to achieve a successful digital transformation. Increasing digitalisation without proportional attention to the security of the data (from all perspectives: confidentiality, integrity, availability, accountability) is a risk in itself, as recognised by Singapore in its 2021 Cybersecurity Strategy [51]Grasping this perspective, Romania has established itself as a regional leader with strong ambitions and a successful public track record in cybersecurity. However, threats evolve quickly, and maintaining a leadership position requires continuous attention. A few common themes emerge across the countries studied: cooperation, be it public-private or international; talent, manifested through the increase in cybersecurity skills within the country; and resilience, manifested through the ability to maintain the availability of online, digital services even in adverse circumstances. In an attempt to match threats, technology is also evolving at a fast pace. Access to new technology is an important enabler for cybersecurity, and this is partially addressed through the public-private-academia partnerships, which Romania has set as an objective in its National Cybersecurity Strategy. Even more important is the development of the cybersecurity talent. Acquiring and retaining cyber talent is a difficult task even for larger commercial organisations and is even harder for public administration entities or smaller critical information infrastructure entities [63]. Generative AI can help partially address this skills gap but also introduces new risks.

Romania can move forward by overcoming lingering historical, cultural, and socioeconomic legacies and creating new, future-oriented paradigms in all sectors. As a fundamental pillar of the paradigm shift, public administration should focus on people’s needs instead of institutional constraints. In the end, everybody’s lives would be better. Despite still being in the early stages of transitioning to fully-fledged and reliable digital public services, Romania has a great opportunity to achieve a state-of-the-art smart government ecosystem by incorporating the best features deriving from the lessons learnt by the world's top performers in this area, avoiding errors, and mitigating foreseeable risks.

References

[1] World Summit Awards, “Romanian e-Government Gateway,” [Online]. Available: https://wsa-global.org/winner/romanian-e-government-gateway/. [Accessed 2 December 2024].

[2] A. L. Horobeț, I. Mnohoghitnei, E. M. Zlatea and A. Smedoiu-Popoviciu, “Determinants of E-Government Use in the European Union: An Empirical Analysis,” *Societies,* vol. vol. 13, no. 6, Jun 2023.

[3] N. Gavriluță, V. Stoica and G. I. Fârte, “The Official Website as an Essential E-Governance Tool: A Comparative Analysis of the Romanian Cities,” *Sustainability,* vol. 14, no. 11, Jan 2022.

[4] M. D. Lytras and A. C. Șerban, “E-Government Insights to Smart Cities Research: European Union (EU) Study and the Role of Regulations,” *IEEE Access,* vol. 8, p. 65313–65326, 2020.

[5] Y. Li and H. Shang, “Service quality, perceived value, and citizens’ continuous-use intention regarding e-government: Empirical evidence from China,” *Inf. Manage,* vol. 57, no. 3, p. 103197, 2020.

[6] A. Hooda,, P. Gupta, A. Jeyaraj, M. Giannakis, and Y. K. Dwivedi, “The effects of trust on behavioral intention and use behavior within e-government contexts,” *Int. J. Inf. Manag,* vol. 67 , p. 102553, 2022.

[7] I. Mergel, N. Edelmann and N. Haug, “Defining digital transformation: Results from expert interviews,” *Gov. Inf. Q,* vol. 36, no. 4, p. 101385, 2019.

[8] J. Bughin, T. Catlin, M. Hirt and P. Willmott, ““Why digital strategies fail,”,” *McKinsey Q., vol. 1, no. 1, pp. 14–25, 2018..*

[9] A. Zuiderwijk, Y. C. Chen and F. Salem, “Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda,” *Gov. Inf. Q,* vol. 38, no. 3, p. 101577, 2021.

[10] C. Vrabie, “E-Government 3.0: An AI Model to Use for Enhanced Local Democracies,” *Sustainability,* vol. 15, no. 12, 2023.

[11] C. Schachtner, “Smart government in local adoption –Authorities in strategic change through AI,” *Smart Cities Reg. Dev. SCRD J,* vol. 5, no. 3, pp. 53-62, 2021.

[12] C. Wang, T. S. H. Teo and M. Janssen, “Public and private value creation using artificial intelligence: An empirical study of AI voice robot users in Chinese public sector,” *Int. J. Inf. Manag,* vol. 61, p. 102401, 2021.

[13] J. D. Twizeyimana and A. Andersson, “The public value of E-Government – A literature review,,” *Gov. Inf. Q., vol. 36, no. 2, pp. 167–178,,* 2019.

[14] OECD, “Digital Government Review of Romania: Towards a Digitally Mature Government. Paris: Organisation for Economic Co-operation and Development,” 2023. [Online]. Available: https://www.oecd-ilibrary.org/governance/digital-government-review-of-romania_68361e0d-en.

[15] European Commission, “The Digital Economy and Society Index (DESI) | Shaping Europe’s digital future,” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/desi.

[16] UN, “E-Government Knowledgebase,” 2024. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/140-Romania.

[17] Statista, “Romania: share of e-Government users 2019-2022,” [Online]. Available: https://www.statista.com/statistics/1129356/romania-share-of-e-government-users/.

[18] International Institute for Management Development, “World Digital Competitiveness Ranking 2024 - IMD business school for management and leadership courses,” 2024. [Online]. Available: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/.

[19] M. Romanelli, “Cities Rethinking Innovation by Technology,” *Social Science Research Network,* 2019.

[20] B. C. Ibănescu, G. C. Pascariu, A. Bănică and I. Bajenaru, “Smart city: A critical assessment of the concept and its implementation in Romanian urban strategies,” *J. Urban Manag,* vol. 11, no. 2, p. 246–255, 2022.

[21] C. Vrabie, “Analiza orizontală a Web site-urilor primăriilor municipiilor din România,” *Impact Stud. E-Gov. Smart Cities ISEGOV,* 2024.

[22] International Institute for Management Development, “Smart City Observatory 2024,” 2024. [Online]. Available: https://www.imd.org/smart-city-observatory/home/.

[23] M. Cucciniello, G. A. Porumbescu and S. Grimmelikhuijsen, “25 Years of Transparency Research: Evidence and Future Directions,” *Public Adm. Rev,* vol. 77, no. 1, pp. 32-44, 2017.

[24] V. Venkatesh, J. Y. L. Thong, F. K. Y. Chan and P. J. H. Hu, “Managing Citizens’ Uncertainty in E-Government Services: The Mediating and Moderating Roles of Transparency and Trust,” *Inf. Syst. Res,* vol. 27, no. 1, p. 87–111, 2016.

[25] R. Pripoaie, G. C. Schin and A. E. Matic, “Post-Pandemic Exploratory Analysis of the Romanian Public Administration Digitalization Level in Comparison to the Most Digitally Developed States of the European Union,” *Sustainability,* vol. 16, no. 11, 2024.

[26] A. Androniceanu, I. Georgescu and J. Kinnunen, “Public Administration Digitalization and Corruption in the EU Member States. A Comparative and Correlative Research Analysis,” *Transylv Rev. Adm. Sci,* vol. 18, no. 65, pp. 5-22, 2022.

[27] BBC, “Lapsus$: Two UK teenagers charged with hacking for gang,”, https://www.bbc.com/news/technology-60953527, Apr. 01, 2022. Accessed: Nov. 29, 2024. .

[28] Costa Rica ransomware attack,, NATO Cooperative Cyber Defence Centre of Excellence: Cyber Law Toolkit., https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022), May 01, 2024. .

[29] J. Córdoba, “Ransomware gang threatens to overthrow Costa Rica government,”, https://apnews.com/article/technology-government-and-politics-caribbean-gangs-381efc2320abb5356dee7f356e5, May 16, 2022..

[30] C. Bing, “FBI says Chinese hackers preparing to attack US infrastructure,”, : https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastruct, Apr. 18, 2024..

[31] A. Greenberg, Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike,”, Nov. 09, 2023. Accessed: Nov. 29, 2024..

[32] “Lessons from the Stasi – A cautionary tale on mass surveillance,”, Nov. 29, 2024. .

[33] N. Elisa, L. Yang, F. Chao and Y. Cao, “A framework of blockchain-based secure and privacy-preserving E-government system,” *Wirel. Netw.*, vol. 29, no. 3, p. 1005–1015, Apr. 2023.

[34] G. Soos., ““Smart decentralization? The radical anti-establishment worldview of blockchain initiatives,”,” *Smart Cities Reg. Dev. J., vol. 2, no. 2,*, Jun. 2018.

[35] R. Blackman, “Why Blockchain’s Ethical Stakes Are So High,” Harvard Business Review, May 10, 2022..

[36] EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Dir.

[37] European Commission,, “Digital Decade Strategy.” Accessed: Dec. 02, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies.

[38] European Commission, “European Declaration on Digital Rights and Principles.” Accessed: Dec. 02, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

[39] European Union, “Directive - 2016/2102 - EN - EUR-Lex.” Accessed: Dec. 02, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/2102/oj.

[40] European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, vol. 257..

[41] European Commission, “Digitalisation in Europe,” 2023. [Online]. Available: https://data.europa.eu/doi/10.2785/442069. [Accessed 25 May 2024].

[42] “Danish National Agency for Digital Government.” Accessed: Dec. 02, 2024. [Online]. Available: https://en.digst.dk/.

[43] R. Ottis, “Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective,” in Proceedings of the 7th European Conference on Information Warfare, Academic Publishing Limited Reading, MA, 2008, p. 163..

[44] A. Hardy, “Digital innovation and shelter theory: exploring Estonia’s e-Residency, Data Embassy, and cross-border e-governance initiatives,” J. Balt. Stud., vol. 55, no. 4, pp. 793–810, Oct. 2024, doi: 10.1080/01629778.2023.2288118..

[45] Harvard Ash Center, “E-stonia: One Small Country’s Digital Government Is Having a Big Impact,” Innovations in Government. Accessed: Nov. 29, 2024. [Online]. Available: https://medium.com/innovations-in-government/e-stonia-one-small-countrys-digital-g.

[46] L. Kello, “Cyber Defence,” in The Handbook of European Defence Policies and Armed Forces, H. Meijer and M. Wyss, Eds., Oxford University Press, 2018, p. 0. doi: 10.1093/oso/9780198790501.003.0039..

[47] #Ministry of Justice and Public Security, “National Cyber Security Strategy for Norway,” Government.no. Accessed: Nov. 30, 2024. [Online]. Available: https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/.

[48] Transparency International, “2023 Corruption Perceptions Index,” Transparency.org. Accessed: Dec. 02, 2024. [Online]. Available: https://www.transparency.org/en/cpi/2023.

[49] Minister for Digital Development and Information - Singapore, “Smart Nation 2.0 A Thriving Digital Future for All,” 2024. [Online]. Available: https://file.go.gov.sg/smartnation2-report.pdf.

[50] Government of Singapore, “AI for the Public Good For Singapore and the World.” Accessed: Dec. 02, 2024. [Online]. Available: https://file.go.gov.sg/nais2023.pdf.

[51] Cyber Security Agency of Singapore., “The Singapore Cybersecurity Strategy 2021,” Default. Accessed: Nov. 30, 2024. [Online]. Available: https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021.

[52] Ministry of Research, Innovation and Digitalisation, “Romanian National Action Plan for Digital Decade.” 2024. [Online]. Available: https://www.mcid.gov.ro/wp-content/uploads/2024/05/Plan-national-de-actiune-roadm-ap-pentru-publicare_corectat.pdf.

[53] E. DINU, “Exploring the Relationship between National Intellectual Capital Management in the Romanian Healthcare Sector and Technological Innovation,” in Proceedings of Strategica 2021, 9th Ed., Shaping the Future of Business and Economy, Bucharest:.

[54] Guvernul Romaniei, “HG 271 15/05/2013.” Accessed: Nov. 30, 2024. [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/148324.

[55] Guvernul Romaniei, “Strategie de securitate cibernetică a României, pentru perioada 2022-2027.” Accessed: Nov. 30, 2024. [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.

[56] L. Cerulus, “5 reasons why Bucharest won the EU cyber center race,” POLITICO. Accessed: Dec. 01, 2024. [Online]. Available: https://www.politico.eu/article/5-reasons-why-bucharest-won-the-eu-cyber-competence-center-race/.

[57] D. Munteanu, “Romania’s cybersecurity leadership: How a Black Sea nation may become a strategic ally of the U.S.,” Tech Diplomacy. Accessed: Dec. 01, 2024. [Online]. Available: https://techdiplomacy.org/news/romanias-cybersecurity-leadership-how-a-bl.

[58] L. Dobberstein, “Indonesia’s president orders government app development halt,” [Online]. Available: https://www.theregister.com/2024/05/28/indonesia_app_sprawl/. [Accessed 1 December 2024].

[59] A. Greenberg, “China’s Surveillance State Is Selling Citizen Data as a Side Hustle | WIRED,” Wired. Accessed: Dec. 02, 2024. [Online]. Available: https://www.wired.com/story/chineses-surveillance-state-is-selling-citizens-data-as-a-side-hustle/.

[60] T. Szopiński and M. W. Staniewski, “Manifestations of e-government usage in post-communist European countries,” Internet Res., vol. 27, no. 2, pp. 199–210, Apr. 2017, doi: 10.1108/IntR-01-2015-0011..

[61] F. Palmisano and A. Sacchi, “Trust in public institutions, inequality, and digital interaction: Empirical evidence from European Union countries,” J. Macroecon., vol. 79, p. 103582, 2024, doi: https://doi.org/10.1016/j.jmacro.2023.103582..

[62] S. David, D. Zinica, N. Bărbuță-Mișu, L. Savga, and F.-O. Virlanuta, “Public administration managers’ and employees’ perceptions of adaptability to change under ‘the future of work’ paradigm,” Technol. Forecast. Soc. Change, vol. 199, p. 123088, 2024.

[63] ISC2, “2024 ISC2 Cybersecurity Workforce Study.” Accessed: Dec. 01, 2024. [Online]. Available: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study.