Daiana VESMAȘ (1)
Lucian Blaga University of Sibiu, Romania
Ana MORARI (BAYRAKTAR) (2)
Lucian Blaga University of Sibiu, Romania

THE ETHICS OF E-GOVERNANCE. SAFEGUARDING DATA CONFIDENTIALITY AND HUMAN SECURITY IN PUBLIC ADMINISTRATION

Abstract:	*With the rapid digitalization of government functions, there is an emerging need for strict legal frameworks that will protect the personal data of citizens and guarantee their rights under the GDPR, adapting these provisions into the national legislative system. This legal research discusses how the need for transparency in public administration is weighed against the requirement for the confidentiality of data and how such dynamics impact human security and civil liberties.* *Considering emerging technologies such as blockchain, artificial intelligence, and automated decision-making systems, the legislative measures at present within the European Union need to be reassessed. This reassessment provides the principles of data minimization, and the legal responsibilities of both the data controller and processor in the public sector, emphasizing strongly the principles of accountability and integrity of data. The paper presented tries to provide an integral vision of data protection and human security in the digital transformation of public administration, a combination of legal and ethical considerations.*
Keywords:	**E-governance; data privacy; transparency; algorithmic fairness; digital inclusion**
Contact details of the authors:	E-mail: daiana.vesmas@ulbsibiu.ro (1) ana.morari@ulbsibiu.ro (2)
Institutional affiliation of the authors:	**Faculty of Law, Lucian Blaga University of Sibiu, Romania (1) (2)**
Institutions address:	Calea Dumbrăvii 34, Sibiu, Romania 550324 (1) (2)

Introduction

E-government is a model that manages government affairs based on the usage of local and global information networks to improve efficiency, transparency, and service delivery to citizens, thereby democratizing the processes further with the use of advanced information and communications technologies. This system of e-government information shall be used for gathering, input, searching, processing, storing, and providing information upon demand, according to user specifications, in support of the functions of government, delivery of services to individuals and organizations, and informing the public on the activity of government[1].

This rapid diffusion of e-governance has transformed public administration, allowing governments to reimagine service delivery to meet contemporary digital expectations. By digitizing essential services - such as tax filing, license applications, healthcare access, and social services distribution - governments can streamline once time-consuming and resource-intensive processes. This transformation offers citizens a more convenient,

[1] Evgenyi Romanenko, *E-Governance - A Tool for Democratization of The Public Administration System*, "International Journal of New Economics and Social Sciences", Vol. 2, No. 2, 2015, DOI: 10.5604/01.3001.0010.4772 (26.10.2024)

user-friendly way to interact with government services, reducing the need for in-person visits and long wait times, which previously presented significant barriers to accessibility[1].

Countries like Estonia with its initiative of e-Estonia, Singapore through the program Smart Nation, and India with Digital India have provided comprehensive e-governance frameworks that have set benchmarks as far as efficiency and public participation are concerned[2]. In this respect, such initiatives reflect the potential of e-governance to strengthen democratic processes through higher levels of transparency and easy access to information and services for citizens. This rapid adoption of e-governance brings in its wake malicious consequences in areas of data security, privacy, and digital inclusion. Hence, a balanced approach must be brought in to ensure that an expansion of e-governance protects individual privacy, maintains data security, and fosters equal access to digital public services throughout society[3].

This research will, therefore, be focused on the levels of ethical standards and frameworks that will be required in terms of ensuring data confidentiality and human security in digital public administration. The research will investigate the respective legal frameworks, such as the General Data Protection Regulation within the European Union, for which strict guidelines on data protection have been formulated for their efficacious application within digitalized government settings[4]. It shall further consider the ethical frameworks which may guide the responsible adoption at the core of public sector operations of digital technologies, including artificial intelligence and automated decision-making.

The evolution and digital transformation in governance

E-governance refers to the use of electronic technologies to facilitate interactions between government and citizens, businesses, and within internal government processes. Its aim is to streamline operations, enhance transparency, improve service delivery, and promote democratic engagement. E-governance simplifies administrative functions while supporting more efficient communication between various stakeholders, contributing to better decision-making and governance practices in both public and business sectors. It fosters an accessible, responsive, and more transparent government for the digital age[5].mThe evolution of e-governance began with the adoption of basic technologies to improve administrative efficiency in government operations. Initially, this involved automating internal processes to streamline bureaucratic tasks. As information and communication technology (ICT) advanced, e-governance began incorporating more interactive platforms, enabling public access to government services online and enhancing transparency[6].

By the early 2000s, the focus shifted to more citizen-centered services, fostering engagement through digital means like e-participation and e-voting, encouraging transparency, and improving government accountability. This shift marked a transition from simple automation to facilitating public participation and trust[7].

In recent years, e-governance has embraced complex, integrated solutions. Initiatives in smart cities, data analytics, and AI-driven services now cater to personalized citizen experiences and real-time service

---

[1] Carlos Rodriguez, *Digitalization in Government: Enhancing Public Service Delivery through Technology*, "Social Dynamics Review", Vol. 5, 2022, https://academicpinnacle.com/index.php/SDR/article/view/12/14 (26.10.2024)

[2] Theeraya Mayakul, Prush Sa-Nga-Ngam, Wasin Srisawat, Supaporn Kiattisin, *A Comparison of National Enterprise Architecture and e-Government Perspectives*, in *4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON),* 2019, DOI: https://doi.org/10.1109/TIMES-iCON47539.2019.9024591 (26.10.2024)

[3] Oleksii Mykhalchenko, *E-Governance in The Management Decision-Making Process*, "Economic Analysis", Vol. 32, No. 1, 2022, DOI: https://doi.org/10.35774/econa2022.01.081 (26.10.2024)

[4] Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito, Nicole Monte, *The common EU approach to personal data and cybersecurity regulation*, "International Journal of Law and Information Technology", Vol. 28, No. 4, Winter, 2020, pp. 297–328, https://doi.org/10.1093/ijlit/eaaa021 (28.10.2024)

[5] Phani N. Bindu, Prem C. Sankar, Satheesh K. Kumar, *From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools*, "Government Information Quarterly", Vol. 36, No. 3, July, 2019, pp. 385-399, DOI: https://doi.org/10.1016/j.giq.2019.02.005 (28.10.2024)

[6] Åke Grönlund, Thomas A. Horan*, Introducing e-Gov: History, Definitions, and Issues*, 2004, in *Communications of the Association for Information Systems*, Vol. 15, June, 2005, DOI:10.17705/1CAIS.01539 (28.10.2024)

[7] Dmytro Khutkyy, *Citizen Engagement and Open Government Co-creation: The Cases of Brazil and the Dominican Republic*, in *Proceedings of the 24th Annual International Conference on Digital Government,* July, 2023, pp. 199-204, DOI: https://doi.org/10.1145/3598469.3598491 (28.10.2024)

delivery. Blockchain and encryption technologies address emerging concerns around data confidentiality, integrity, and security within e-governance frameworks[1].

One of the key tools of digital government nowadays is the portals of electronic public services, through which one can remotely obtain certificates, submit applications, pay fees and fines. The effectiveness of such portals is multiplied if the country has established an electronic document flow, which makes it possible to eliminate the need for paper when exchanging documents between agencies and with citizens[2].

Important for the development of digital government are cloud technologies and data storage for scaling IT infrastructure and uninterrupted operation of digital services. The states invest in information security technologies to protect personal data and secure online transactions - encryption, two-factor authentication, etc. The government develop Big Data and artificial intelligence technologies for analytics and data-based decision-making support, and distributed registries to create a trusted environment and fight corruption[3].

Legal aspects of E-governance

Transparency and security in the processing of personal data within digital systems are pursued through a series of legislative and regulatory mechanisms adopted by the international community, aiming at the protection of subjects, accountability in the management of personal data, and the avoidance of misuse or breaches.

General Data Protection Regulation (GDPR)

Ethical standards, guidelines, and frameworks of practice, such as those supported by the *General Data Protection Regulation (GDPR)* in the European Union, stand as the backbone of governance in e-governance systems. This is where it strives to ensure that personal data processing in public administrative systems will fall within the purview of commanding respect for individual privacy, transparency, and accountability. The GDPR stipulates that all personal information maintained by e-governance systems should be processed lawfully, given full consent and permission by the people, and utilized only if necessary. Key ethics linger on **data minimization**, **purpose limitation**, and ensuring data is secure[4].

The GDPR enshrines certain basic rights of data protection and privacy for individuals under Articles 12–23 of the GDPR. These include the right of access to personal data, rectification of inaccurate data, erasure- or better known as the "right to be forgotten"-restriction of processing, and data portability.[5]

For instance, in the case of contact between citizens and digital government services the GDPR encourages the adoption of privacy-preserving techniques, such as anonymization, pseudonymization, encryption, and randomization to guarantee the privacy of the personal information of a data subject undergoing any kind of processing in digital government systems[6].

Ministerial Declaration on eGovernment - the Tallinn Declaration

The Tallinn Declaration on E-Government[7] signed in 2017 by the ministers of the European Union member states, extends the general principles of their commitment to develop digital public services across Europe. Building on the success of the previous e-government initiatives, the citizen-centric, inclusive, and efficient paradigm is put at the heart of digital transformation in public administration.

---

[1] Yang Longzhi, Elisa Noe, Eliot Neil, *Privacy and Security Aspects of E-Government in Smart Cities*, "Smart Cities Cybersecurity and Privacy", 2019, pp. 89-102, DOI: https://doi.org/10.1016/B978-0-12-815032-0.00007-X (28.10.2024)

[2] Shahin Aliyev, *Digital Government: How New Technologies Improve Citizens' Lives*, in *ITCNEWS 2024*, https://ictnews.uz/23/09/2024/egovernment/ (28.10.2024)

[3] *Idem*

[4] European Commission, *Ethics and data protection*, pp. 4-6, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (28.10.2024)

[5] Damian Eke, Bernd Stahl, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, "Digital Society", Vol. 3, No. 11, 2024, DOI: https://doi.org/10.1007/s44206-024-00101-6 (28.10.2024)

[6] Razieh Nokhbeh Zaeem, Suzanne K. Barber, *The Effect of the GDPR on Privacy Policies*, "ACM Transactions on Management Information Systems (TMIS)", Vol. 12, pp. 1-20, 2020, DOI: https://doi.org/10.1145/3389685 (28.10.2024)

[7] European Comission, *Ministerial Declaration on eGovernment - the Tallinn Declaration*, 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration (28.10.2024)

The Tallinn Declaration recognized the key priorities for improvement regarding cross-border public services, user-centricity, and transparency, which ensure security in e-governance systems. Increasing access to digital services for every citizen, irrespective of the place where he/she is located, decreases bureaucratic barriers and increases access to more government services through interoperable systems across the EU. It also calls on member states to take a digital-by-default approach to the delivery of government services, allowing alternatives for those people who cannot access such services.

What is more, the declaration supports data protection and the right to privacy. It declares respect for the GDPR regarding personal data in public administration when proceeding over the e-government platforms. They also pledged to continue the development of cross-border interoperability, "enabling Union citizens and businesses to benefit from full access to digital public services across all EU member states". Therefore, this will foster not only internal mobility within the EU but also a higher degree of integration of the digital single market.

The European Declaration on Digital Rights and Principles

The EU's Declaration on Digital Rights and Principles presents six key principles. These serve as the main directors and influencers of public administration behavior across Europe as it pertains to the implementation of digital services, such as e-governance. Of these principles, the one most relevant to the context is probably "People at the Center of Digital Transformation," which mandates that public administration place citizen's needs and rights in the very center of that digital transformation. The way this principle affects and directs e-governance is not only illuminating; it also highlights the EU's overall approach to digital services[1].

The principle of Solidarity and Inclusion underscores the role of e-governance in achieving digital inclusivity, especially for vulnerable groups. This is exemplified by the Web Accessibility Directive (2016), which states that public websites and mobile applications must be accessible to people with disabilities[2]. This regulation matches the ideal of inclusive e-governance, where digital public services are accessible to all. The declaration also emphasizes the need for Sufficient Safety and Security so that public administrations can confidently engage in cross-border digital service delivery, knowing that their e-government platforms are compliant with the General Data Protection Regulation (GDPR)[3].

Compliance with this regulation is critical in e-governance because it demands that public administrations minimize the amount of personal data they collect, accounting for and protecting the data that is more likely to end up in hazard zones.

Convention for the Protection of Individuals about Automatic Processing of Personal Data

The landmark treaty established by the Council of Europe in 1981, known as the *Convention for the Protection of Individuals about Automatic Processing of Personal Data, or Convention 108*[4] modernized in steps to become Convention 108+ sets out the foundational principles to safeguard personal data and privacy. It has substantial implications for how public administrations can practice e-governance because, as a treaty, it allows signatories to hold public authorities within them accountable for how they handle personal data. As a public administration, we are bound by the principles of transparency, accountability, and proportionality that Convention 108+ embodies. Therefore, gathering and processing essential personal data within the e-governance framework must adhere to some very key tenets that were enshrined in Convention 108 and modernized in Convention 108+[5].

---

[1] European Commission, *European Digital Rights and Principles*, 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles (29.10.2024)

[2] Delia Ferri, Silvia Favalli, *Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion, "*Societies", Vol. 8, No.2, 2018, DOI:https://doi.org/10.3390/SOC8020040 (29.10.2024)

[3] European Commission, *European Digital Rights and Principles*, 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles (29.10.2024)

[4] Council of Europe, *Convention 108 +,* 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (29.10.2024)

[5] Cécile de Terwangne, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, "Computer Law & Security Review, Vol. 40, April, 2021, 105497, DOI: https://doi.org/10.1016/J.CLSR.2020.105497 (30.10.2024)

While most relevant for e-governance in the EU, the focus of the Convention lies in the cross-border flow of data under Article 12[1] establishing an exchange of data between member states with uniform data protection standards that can allow public authorities to provide seamless cross-border digital services with no dent on privacy-appropriately illustrated by systems such as the European e-Justice Portal, which allows access to justice-related services by citizens across borders in the EU, while keeping up with the privacy protections of their data[2].

Ethics of E-governance

Data privacy and confidentiality

Citizens' sensitive information in e-governance is kept private and secure from unauthorized access and misuse by maintaining a robust set of Information Security Policies (ISP). A good ISP promises not just the confidentiality of data but also its integrity and availability--qualities that ensure that data remain accurate, uncorrupted, and accessible despite various types of threats that might be aimed at the government service itself. The act of e-governance, like any other online service, has to ensure not just that the right people can get in and use it (that's user authentication), but also that the wrong people can't get in[3].

In e-governance, ethical responsibilities to protect data privacy and confidentiality are countered by risks like unauthorized access, data breaches, and misuse. Public authorities must safeguard the confidentiality of sensitive information, and integrity to ensure data accuracy, and availability to prevent service disruptions.

Transparency and accountability

To quantify public trust and satisfaction, the *E-Government Transparency Index* measures citizens' perceptions of government websites, assessing factors like thoroughness, accessibility, and timeliness of information[4].

The bond connecting e-governance to transparency and accountability is vital for nurturing public trust and advancing efficient public administration. E-governance, itself an emergent form of public management, can foster this bond through the provision of electronically mediated information. For instance, indices like the *Corruption Perception Index (CPI)* and *Open Budget Index (OBI)* are used to measure transparency levels, revealing that higher transparency correlates with stronger e-governance readiness[5].

Algorithmic fairness and non-discrimination

E-governance relies on AI and automated decision-making in several critical public services, where there is a growing need to put into practice fair algorithms, unbiased and non-discriminatory. Algorithmic fairness stands for developing AI systems that treat all people fairly, without preferential treatment or disadvantage of one group against others, based on gender, ethnicity, or socio-economic background[6]. This is precisely the case with the upcoming EU AI Act, which will establish new rules on the limitation of discrimination in high-risk AI systems, including those that fall in the category of public sector AI applications. This Act will place demands for transparency, frequent auditing, and impact assessments about bias and fairness[7].

---

[1] Gregory W. Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, "International Organisations Research Journal", Vol. 17, No. 1, pp. 56–95, 2020, DOI: https://doi.org/10.17323/1996-7845-2022-01-03, (30.10.2024)

[2] Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context,* "European Journal of International Law", Vol. 21, No. 2, May, 2010, pp. 441-456, https://doi.org/10.1093/ejil/chq025 (30.10.2024)

[3] Shailendra Singh, *E-Governance: Information Security Issues*, in *International Conference on Computer Science and Information Technology (ICCSIT'2011)*, Pattaya Dec. 2011, pp. 120-122, https://www.researchgate.net/publication/266770761_E-Governance_Information_Security_Issues (30.10.2024)

[4] Mysore Ramaswamy, *Improving Transparency Through E-Governance*, "Information Systems", Vol. 15, No. 1, pp. 123-131, 2014, https://iacis.org/iis/2014/23_iis_2014_123-131.pdf (30.10.2024)

[5] Emad A. Abu-Shanab, *The Relationship between Transparency and E-government: An Empirical Support*, "Lecture Notes in Informatics Gesellschaft für Informatik", Bonn, 2012, pp. 85-86, https://subs.emis.de/LNI/Proceedings/Proceedings221/84.pdf (30.10.2024)

[6] Sandra Wachter, Brent Mittelstadt, Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, "Computer Law & Security Review", Vol. 41, 2021, DOI: https://doi.org/10.2139/ssrn.3547922 (30.10.2024)

[7] Matthias Wagner, Markus Borg, Per Runeson, *Navigating the Upcoming European Union AI Act*, "IEEE Software", Vol. 41, No. 1, pp. 19-24, 2024, DOI: https://doi.org/10.1109/ms.2023.3322913 (30.10.2024)

Real-world cases help in underlining that there are challenges in the implementation of fairness: the highly discussed Dutch government welfare fraud detection algorithm was alleged to discriminately point out the immigrant groups more, leading to many being wrongly accused and facing financial adversities[1]. This example underlines the need for audits of algorithms to detect biases and for public disclosure of algorithmic processes to keep transparency.

Digital inclusion and accessibility

Digital inclusion and accessibility in e-government are crucial to ensure a very ethical, fair opportunity for access to public services. It ensures that everyone, regardless of social status, age, or physical ability, will have digital service access and underpins the spirit of the European Accessibility Act 2019, which lays down a requirement that websites and mobile applications of public services must be accessible for persons with disabilities[2].

According to the United Nations E-Government Development Index, countries with more inclusive digital strategies tend to have high rankings in the satisfaction and engagement of the public.[3] Closing the digital divide necessitates that governments address challenges such as internet availability, affordability, and digital literacy, among many others. This is well evidenced in the case of the Smart Nation program in Singapore, which provides training programs for elderly citizens on methods of access and usage of digital public services[4].

Ethical e-government therefore needs policies that public authorities should put into place and technologically guarantee equal access to digital services irrespective of the citizen's status.

Case studies

Danish e-Government initiatives

In the early 2000s, Denmark's public sector began adopting digital communication. As part of the 'eDay 1' launch in 2003, public authorities were urged to email rather than use paper unless restricted due to security. Moving into 'eDay 2' in 2005, secure email was required for the transmission of sensitive data. The number of pieces of physical mail is targeted to be reduced by 40% in late 2005. Civil servants started getting pay statements via a secure 'e-boks' - amid some concerns over digital access[5].

The national eGovernment strategy, led by the Joint Cross-Government Cooperation Committee (STS), the eGovernment Strategy Committee (DSTG), and the Danish Agency for Digitization (DIGST), coordinates digital initiatives to ensure streamlined and secure public services. Public services are delivered across three government levels—central, regional, and municipal—necessitating seamless data flow and secure information sharing, particularly in healthcare[6].

The Danish e-government platform was developed through the important digital portals Borger.dk and Virk.dk, acting as a single entrance point for citizens and businesses, respectively. On the former, Borger.dk, multiple public services were made available, ranging from healthcare and social self-service applications to tax-related applications, including updates of personal records; it would be a one-stop service delivery for citizens. Likewise, Virk.dk, aimed at businesses, provides reporting, registration, and compliance tools. Creating these portals is all part of Denmark's larger interoperability strategy: it allows easy flow of data and one digital entrance at all levels of government. Joint resources, for example NemID-e-identification and the

---

[1] Melissa Heikkilä, *Dutch scandal serves as a warning for Europe over risks of using algorithms*, "Politico", https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/ (30.10.2024)

[2] European Accessibility Act, https://www.inclusion-europe.eu/european-accessibility-act/ (30.10.2024)

[3] UN E-government Knowledgebase, *E-Government Development Index (EGDI)*, https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index (30.10.2024)

[4] Gordon Kuo Siong Tan, *Citizens go digital: A discursive examination of digital payments in Singapore's Smart Nation project*, "Urban Studies", Vol. 59, pp. 2582 –2598, 2021, DOI: https://doi.org/10.1177/00420980211039407 (05.11.2024)

[5] Kim Viborg Andersen, Helle Zinner Henriksen, Eva Born Rasmussen, *Re-organizing government using IT: The Danish model //E-government in Europe*, Routledge, 2006, pp. 139-141

[6] Morten Meyerhoff Nielsen, Mika Yasouka, *An analysis of the Danish approach to eGovernment benefit realization,* "Internet Technologies and Society", 2014, pp. 5-7, https://www.researchgate.net/profile/Morten-Meyerhoff-Nielsen-2/publication/281774408_An_analysis_of_the_Danish_approach_to_eGovernment_benefit_realisation/links/564e050b08aeafc2aab16806/An-analysis-of-the-Danish-approach-to-eGovernment-benefit-realisation.pdf (05.11.2024)

digital postbox, are compulsory to use, which secures a coherent "single voice" experience on government services[1].

One risk of Denmark's e-government strategy is the potential for a digital divide, as some citizens may lack access to digital tools or skills required to fully engage with online services. This could lead to unequal access to essential public services, especially among older adults or low-income groups.

Estonia's Digital Government

Digitalization in Estonia's e-government is a well-organized infrastructure development focused on security, ease of access, and efficiency. At the heart of the operations is the X-Road platform, initiated in 2001, which enables secure data exchange between government databases. It is a decentralized system where agencies, enterprises, and citizens can converge online and support[2].

The Estonians ushered in an obligatory e-ID in 2002, enabling secure digital identification for various services related to health, education, and even voting from any part of the country. Legal-to-use digital signatures in Estonia further facilitate the processes and reduce administrative delays[3].

The Estonian e-Residency Programme, launched in 2014, is a means of providing access to Estonian digital services for non-residents. It is also touted as a painless method for entrepreneurs from anywhere in the world to run a business in a virtual European Union environment. Opening more opportunities in Estonia's digital ecosystem, this initiative supports an international community of digital entrepreneurs[4].

Strong data-privacy policies undergird these Estonian efforts, including the "once-only" principle that enables data sharing across agencies without requiring any submission of repeated inputs. Data integrity in areas such as health is protected by Blockchain. Regular assessment of the services through e-services makes sure that services are constantly improving. Interoperability across sectors saves over 800 years of working time for Estonians yearly, apparently due to increased efficiency[5].

Established in the early 2000s, this kind of infrastructure underpins 99% of the public services online, with 98% of citizens using e-IDs. It is stated that this system contributes to 2% of Estonia's GDP due to digital signatures only. It has also pioneered digital services in agriculture, automating the processes of remote sensing for compliance monitoring by satellite data, and Estonia's digital transformation-investing around 1.1-1.3% of the state budget on digitalization[6].

Singapore - program Smart Nation

Launched in 2014, Smart Nation represents a Singapore laced with digital technologies and data to improve lives, strengthen economic growth, and build a closer community. It focuses on applying Internet of Things devices, data analytics, artificial intelligence, and digital infrastructure across the board-urban mobility, healthcare, digital governance, and cybersecurity[7].

---

[1] Morten Meyerhoff Nielsen, *E-Governance Frameworks for Successful Citizen Use of Online Services: A Danish-Japanese Comparative Analysis*, "JeDEM - eJournal of eDemocracy and Open Government" Vol. 9, No. 2, pp. 68-109, 2017, https://doi.org/10.29379/jedem.v9i2.462 (05.11.2024)

[2] Kristjan Vassil, *Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, world development report*, 2016, pp. 3-4, https://thedocs.worldbank.org/en/doc/165711456838073531-0050022016/original/WDR16BPEstonianeGovecosystemVassil.pdf (05.11.2024)

[3] *Ibidem*, pp. 5-6

[4] Kaspar Korjus, Carlos Ivan Vargas Alvarez del Castillo, Taavi Kotka, *Perspectives for e-Residency strenghts, opportunities, weaknesses and threats*, "2017 Fourth International Conference on eDemocracy&eGovernment (ICEDEG)", pp. 177-181, 2017, DOI: https://doi.org/10.1109/ICEDEG.2017.7962530 (05.11.2024)

[5] Kristjan Vassil, *Op.cit.,* pp. 13-15

[6] OECD, *Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementatio*, "Digital Opportunities for Better Agricultural Policies", OECD Publishing, Paris, 2019, pp. 8-15, DOI: https://doi.org/10.1787/510a82b5-en (05.11.2024)

[7] Sang Keon Lee, Heeseo Rain Kwon, H. Cho, Jong-bok Kim, Donju Lee, *International Case Studies of Smart Cities: Singapore, Republic of Singapore*, in *Inter-American Development Bank (IDB), The Nature Conservancy (TNC)'s Nature Bonds Program,* No. IDB-DP-462, DOI: https://doi.org/10.18235/0000409 (05.11.2024)

Core among these is the NDI, which allows safe access through SingPass Mobile to everything from healthcare and education to financial services[1]. This facility, coupled with digital signatures, enables easy interactions throughout the public and private sectors and ensures secure online transactions[2]. Smart Governance assured better service delivery using data-informed policies. Applications such as OneService allow active citizenry participation in the reporting of issues within public services, providing more direct feedback to agencies on areas needing attention[3].

The Cyber Security Agency provides a multi-layer security model that assures safety for the digital infrastructure in Singapore. The environmental initiatives include but are not limited to intelligent meters, monitoring energy and water for more sustainable regulation[4].

Conclusions

E-governance is the innovative change in public administration, bringing efficiency, transparency, and availability of government services through digital means and networks. Digitizing tax filing, access to healthcare, and license applications smooth many of the most time-consuming tasks for governments while eradicating other problems such as bureaucratic delays. Innovative models at the level of countries like Denmark, Estonia, and Singapore demonstrate different ways in which digital governance can help boost engagement with the public, increase transparency, and promote accountability.

For instance, Denmark's e-government strategy has identified secure communication channels and single windows, such as *Borger.dk* -for citizens and *Virk.dk* -for businesses easy points of entry to public services. The Danish experience also points out the risk of a digital divide, whereby a significant share of citizens elderly, or people from low-income groups do not have the means or skills to participate in online services. Finding responses to these challenges of inclusiveness is an important element of the effort to ensure equity as digital governance develops.

Estonia's digital governance framework, driven by the X-Road network, with mandatory e-ID credentials and e-Residency for foreign participants, demonstrates well the key role of a singular and secure foundation in facilitating nearly all governmental services online.

This has paid dividends in Estonia in extraordinary gains of efficiency, adding about 2% to its economic output due to digital signatures alone and saving residents an immense amount of time every year. Furthermore, Estonia follows a “once-only” principle in commitment to data protection and uses blockchain for integrity; thus, it sets an example with its secure and citizen-oriented e-government.

Singapore's long-term Smart Nation vision connects the Internet of Things with data analytics and insightful artificial intelligence that further enhances urban mobility, healthcare systems, and ways of accessing digital services. It improves living standards and fosters economic development.

The core elements include the National Digital Identity or NDI, inclusive of SingPass Mobile for effortless interaction with the public or private sectors. Safeguarding this advanced framework are cybersecurity strategies crafted by the Cyber Security Agency. In addition, Singapore focuses on sustainability by intelligently metering and overseeing energy projects for the management of eco-friendly resource usage.

Without a solid legal backbone, securing citizens' information against theft or leaks and upholding moral codes remains elusive in implementing digital governance effectively. In Europe, user rights protection leans on pillars of clarity, permission, and the trimming down of data under the General Data Protection Regulation. This ensures that private details are managed with care. Agreements like the Tallinn Declaration along with Convention 108+ bring in seamless compatibility and safety across borders—binding rules

---

[1] Malyun Muhudin Hilowle, William Yeoh, Marthie Grobler, Graeme Pye, Frank Jiang, *Towards Improving the Adoption and Usage of National Digital Identity Systems*, in *ASE 22 Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, No. 223, pp. 1-6 2022, DOI: https://doi.org/10.1145/3551349.3561144 (05.11.2024)

[2] Singapore Ministry of Finance, *Singpass*, 2016, https://www.tech.gov.sg/files/media/media-releases/Annex_A___SingPass_Factsheet.pdf (05.11.2024)

[3] Singapore Ministry of National Development, *One Service Mobile App -- Making It Easier for You to Report Municipal Issues*, 2015, https://www.nas.gov.sg/archivesonline/data/pdfdoc/20150204002/mnd_press_release_(3).pdf (05.11.2024)

[4] Karen Teh, Vivy Suhendra, Soon Chia Lim, Abhik Roychoudhury, *Singapore's cybersecurity ecosystem*, “Communications of the ACM”, Vol. 63, No. 4, pp. 55-57, DOI: https://doi.org/10.1145/3378552 (06.11.2024)

designed to grant access to online services throughout European Union countries while keeping personal privacy intact.

The most topical issues of e-governance include ethics related to data privacy, algorithmic fairness, and inclusivity. Ethical frameworks, such as the EU AI Act, ensure that systems operating with AI algorithms are designed for transparency and auditing processes to prevent algorithmic discrimination, especially in high-risk AI applications applied by governments.

Some cases in real life, such as that of the Dutch welfare fraud algorithm, remind one of the needs for vigilant oversight in order not to allow biased outcomes or to protect vulnerable groups. Ethical e-governance doesn't forget the principle of digital inclusion, considering in this case all groups of citizens, including disabled people, in full accordance with the European Accessibility Act, not excluding digital training initiatives directed to elderly citizens undertaken in Singapore.

These international case studies, if taken as a whole, reveal that e-government, having sound ground on legislation, ethics, and security, raises administration to a great height. However, all of them carry a message for meeting the challenges in this area, the digital divide and data security to ensure that the benefits of digital change are equitably distributed among citizens. Setting standards in terms of accessibility, transparency, and security, these e-governance initiatives serve as models for contemporary public administration and provide guidelines to secure responsive, inclusive, and accountable governments in the digital era.

Bibliography

Book

1. Andersen, Kim, Viborg; Henriksen, Helle, Zinner; Rasmussen, Eva, Born, *Re-organizing government using IT: The Danish mode. E-government in Europe*, Routledge, 2006

Studies and articles

1. Abu-Shanab, Emad, A., *The Relationship between Transparency and E-government: An Empirical Support*, "Lecture Notes in Informatics Gesellschaft für Informatik", Bonn, 2012, https://subs.emis.de/LNI/Proceedings/Proceedings221/84.pdf
2. Aliyev, Shahin, *Digital Government: How New Technologies Improve Citizens' Lives*, "ITCNEWS 2024", https://ictnews.uz/23/09/2024/egovernment/
3. Bindu, Phani, N.; Sankar, Prem, C.; Satheesh, Kumar, K., *From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools*, "Government Information Quarterly", Vol. 36, No. 3, July, 2019, DOI: https://doi.org/10.1016/j.giq.2019.02.005
4. Eke, Damian; Stahl, Bernd, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, "Digital Society", Vol. 3, No.11, 2024, DOI: https://doi.org/10.1007/s44206-024-00101-6
5. Ferri, Delia; Favalli, Silvia; *Web Accessibility for People with Disabilities in the European Union: Paving the Road to Social Inclusion, "*Societies", Vol. 8, No. 2, 2018, DOI:https://doi.org/10.3390/SOC8020040
6. Grönlund, Åke; Horan, Thomas, A., *Introducing e-Gov: History, Definitions, and Issues*, 2004, "Communications of the Association for Information Systems", Vol. 15, June, 2005, DOI:10.17705/1CAIS.01539
7. Hilowle, Malyun, Muhudin; Yeoh, William; Grobler, Marthie; Pye, Graeme; Jiang, Frank; *Towards Improving the Adoption and Usage of National Digital Identity Systems*, in *ASE 22 Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, No. 223, 2022, DOI: https://doi.org/10.1145/3551349.3561144
8. Khutkyy, Dmytro, *Citizen Engagement and Open Government Co-creation: The Cases of Brazil and the Dominican Republic*, in *Proceedings of the 24th Annual International Conference on Digital Government,* July, 2023, DOI: https://doi.org/10.1145/3598469.3598491
9. Kong, Lingjie, *Data Protection and Transborder Data Flow in the European and Global Context,* "European Journal of International Law", Vol. 21, No. 2, May, 2010, https://doi.org/10.1093/ejil/chq025

10. Korjus, Kaspar; Carlos, Ivan, Vargas, Alvarez del Castillo; Kotka, Taavi, *Perspectives for e-Residency strenghts, opportunities, weaknesses and threats*, in *2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG),* 2017, DOI: https://doi.org/10.1109/ICEDEG.2017.7962530
11. Lee, Sang Keon; Kwon, Heeseo, Rain; Cho, H.; Kim, Jong-bok; Lee, Donju, *International Case Studies of Smart Cities: Singapore, Republic of Singapore*, "Inter-American Development Bank (IDB), The Nature Conservancy (TNC)'s Nature Bonds Program" No. IDB-DP-462, DOI: https://doi.org/10.18235/0000409
12. Longzhi, Yang; Noe, Elisa; Neil, Eliot, *Privacy and Security Aspects of E-Government in Smart Cities*, "Smart Cities Cybersecurity and Privacy", 2019, DOI: https://doi.org/10.1016/B978-0-12-815032-0.00007-X
13. Mantelero, Alessandro; Vaciago, Giuseppe; Esposito, Maria, Samantha; Monte, Nicole, *The common EU approach to personal data and cybersecurity regulation*, "International Journal of Law and Information Technology, Vol. 28, No. 4, Winter, 2020, https://doi.org/10.1093/ijlit/eaaa021
14. Mayakul, Theeraya; Sa-Nga-Ngam, Prush; Srisawat, Wasin; Kiattisin, Supaporn; *A Comparison of National Enterprise Architecture and e-Government Perspectives*, in *4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON),* 2019, DOI: https://doi.org/10.1109/TIMES-iCON47539.2019.9024591
15. Mykhalchenko, Oleksii, *E-Governance in The Management Decision-Making Process*, "Economic Analysis", Vol. 32, No. 1, 2022, DOI: https://doi.org/10.35774/econa2022.01.081
16. Nielsen, Morten, Meyerhoff, *E-Governance Frameworks for Successful Citizen Use of Online Services: A Danish-Japanese Comparative Analysis*, "JeDEM - eJournal of eDemocracy and Open Government", Vol. 9, No. 2, 2017, https://doi.org/10.29379/jedem.v9i2.462
17. Nielsen, Morten, Meyerhoff; Yasouka, Mika, *An analysis of the Danish approach to eGovernment benefit realization,* "Internet Technologies and Society", 2014
18. OECD, *Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation*, in *Digital Opportunities for Better Agricultural Policies*, OECD Publishing, Paris, 2019
19. Ramaswamy, Mysore, *Improving Transparency Through E-Governance*, in *Information Systems*, Vol. 15, No.1, 2014, https://iacis.org/iis/2014/23_iis_2014_123-131.pdf
20. Rodriguez, Carlos, *Digitalization in Government: Enhancing Public Service Delivery through Technology*, "Social Dynamics Review", Vol. 5, 2022, https://academicpinnacle.com/index.php/SDR/article/view/12/14
21. Romanenko, Evgeniy, *E-Governance - A Tool For Democratization of the Public Administration System*, "International Journal of New Economics And Social Sciences", Vol. 2, No. 2, 2015, DOI:10.5604/01.3001.0010.4772
22. Singh, Shailendra, *E-Governance: Information Security Issues*, "International Conference on Computer Science and Information Technology (ICCSIT'2011)", Pattaya Dec. 2011
23. Siong, Tan; Gordon, Kuo, *Citizens go digital: A discursive examination of digital payments in Singapore's Smart Nation project*, "Urban Studies", Vol. 59, 2021, DOI: https://doi.org/10.1177/00420980211039407
24. Terwangne, Cécile de, *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, "Computer Law&Security Review", Vol. 40, April, 2021, 105497, DOI:https://doi.org/10.1016/J.CLSR.2020.105497
25. Teh, Karen; Suhendra, Vivy; Lim, Soon, Chia; Roychoudhury, Abhik, *Singapore's cybersecurity ecosystem*, "Communications of the ACM", Vol. 63, No. 4, DOI: https://doi.org/10.1145/3378552
26. Vassil, Kristjan, *Estonian e-Government Ecosystem: Foundation, Applications, Outcomes, World Development Report*, 2016
27. Voss, Gregory, W., *Cross-Border Data Flows, the GDPR, and Data Governance*, "International Organisations Research Journal", Vol. 17, No. 1, 2020, DOI: https://doi.org/10.17323/1996-7845-2022-01-03
28. Wachter, Sandra; Mittelstadt, Brent; Russell, Chris, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, "Computer Law&Security Review", Vol. 41, 2021, DOI: https://doi.org/10.2139/ssrn.3547922

29. Wagner, Matthias; Borg, Markus; Runeson, Per, *Navigating the Upcoming European Union AI Act*, ”IEEE Software”, Vol. 41, No. 1, 2024, DOI: https://doi.org/10.1109/ms.2023.3322913
30. Zaeem, Razieh, Nokhbeh; Barber, Suzanne, K., *The Effect of the GDPR on Privacy Policies*, “ACM Transactions on Management Information Systems (TMIS)”, Vol. 12, 2020, DOI: https://doi.org/10.1145/3389685

Documents

1. Council of Europe, *Convention108+*, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
2. European Commission, *Ethics and data protection*, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf
3. European Commission, *European Digital Rights and Principles,* 2024, https://digital-strategy.ec.europa.eu/en/policies/digital-principles
4. European Commission, *Ministerial Declaration on eGovernment - the Tallinn Declaration*, 2017, https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration
5. Inclusion Europe, *European Accessibility Act*, https://www.inclusion-europe.eu/european-accessibility-act/
6. Ministry of National Development, *One Service Mobile App -- Making It Easier for You to Report Municipal Issues*, 2015, https://www.nas.gov.sg/archivesonline/data/pdfdoc/20150204002/mnd_press_release_(3).pdf
7. Singapore Ministry of Finance*, Singpass*, 2016, https://www.tech.gov.sg/files/media/media-releases/Annex_A___SingPass_Factsheet.pdf
8. UN E-government Knowledgebase, *E-Government Development Index (EGDI),* https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

Websites

1. https://academicpinnacle.com/
2. https://digital-strategy.ec.europa.eu/
3. https://ec.europa.eu/
4. https://iacis.org/
5. https://ictnews.uz/
6. https://publicadministration.un.org/
7. https://subs.emis.de/
8. https://www.europarl.europa.eu/
9. https://www.inclusion-europe.eu/
10. https://www.nas.gov.sg/
11. https://www.tech.gov.sg/