GG
Green Governance: Exploring Politics, Social Justice, and the Environment
GG 2(2): 122–133
ISSN 3062-8113

One data, one identity: An analysis of the once-only principle in e-governance and its relevance to public service efficiency

Achmad Wafa Muzaki[1], Anisa Cahyani Maulida[1], Putri Revalina Salsabila Khairani[1,*]
[1] *Department of English Literature, Faculty of Humanities, Universitas Jember, Jember, East Java 68121, Indonesia.*
*Correspondence: putrirevalinask@gmail.com

Received Date: May 22, 2025 Revised Date: July 18, 2025 Accepted Date: August 29, 2025

ABSTRACT

Background: This study examines the implementation of the once-only principle in Norway's e-governance system and analyzes its relevance for improving public service efficiency in Indonesia within the broader framework of digital democracy. The Nordic countries are widely recognized for their success in developing integrated data governance systems that support transparency, citizen participation, and bureaucratic effectiveness. In contrast, Indonesia continues to face significant challenges related to institutional fragmentation and lack of interoperability among digital systems across government agencies. **Methods:** This article aims to analyze how the once-only principle is implemented through Norway's digital identity system and to evaluate the potential for its adaptation in the Indonesian context. This research adopts a qualitative approach based on a literature review of policy documents, government reports, and academic studies related to e-governance, data integration, and bureaucratic reform. **Findings:** The analysis reveals that Norway's success is supported by strong institutional coordination, high levels of public trust, and a robust legal framework for data protection, which together enable effective and efficient data reuse across agencies. Meanwhile, Indonesia's institutional fragmentation, sectoral ego, weak interoperability, and low public trust contribute to data duplication and service inefficiencies. The findings also show that the theory of data as public infrastructure is reflected in Norwegian practice, whereas in Indonesia data is still treated primarily as institutional property. **Conclusion:** This study concludes that adapting the once-only principle in Indonesia requires strengthening a central coordinating authority, establishing binding interoperability standards, and developing strategies to build public trust so that efficiency gains do not come at the expense of data protection. **Novelty/Originality of this article:** The novelty of this research lies in integrating the analysis of the once-only principle with issues of digital democracy and public trust, thereby highlighting not only technical aspects but also the political and social dimensions of Indonesia's digital transformation.

KEYWORDS: digital democracy; e-governance; once-only principle.

1. Introduction

Modern democratic states are no longer expected merely to provide channels for citizen participation in political processes. They are also required to deliver governance that is efficient, transparent, accountable, and easily accessible to the public. In the contemporary digital era, these expectations are increasingly met through the integration of information and communication technologies (ICT) into governmental processes (Idowu, 2025). This integration has given rise to concepts such as e-government, e-governance, and, more recently, e-democracy or digital democracy. Digital democracy refers to the use of digital technologies to expand citizen participation, enhance

Cite This Article:
Muzaki, A. W., Maulida, A. C., & Khairani, P. R. S. (2025). One data, one identity: An analysis of the once-only principle in Norway's e-governance system and its relevance for public service efficiency in Indonesia. *Green Governance: Exploring Politics, Social Justice, and the Environment, 2*(2), 122–133. https://doi.org/10.61511/gg.v2i2.2025.2936

transparency, and strengthen the relationship between the state and its citizens (Efthymiou, 2025).

According to Lubis et al. (2022), digital democracy encompasses a wide range of internet-based democratic activities, including online public participation in policymaking, digital political campaigns, electronic consultations, and open access to government information. In this sense, digital democracy is not merely a technical innovation but a political and social transformation (Suherlan, 2023). It reshapes how citizens interact with the state, how decisions are made, and how power is distributed in society. A mature system of digital democracy is closely linked to the quality of e-governance, because open data, transparency, and efficient public services form the foundation of meaningful citizen participation.

Based on the explanation above, it can be seen that e-governance needs an effective system to support e-governance, that is digital identity (Amini & Javidnejad, 2023). It serves as online information equivalent to individuals' physical identity documents, secure and verified for online transactions. Digital identity is the backbone of e-governance in receiving public trust in digital platforms, making it easier to interact with government online services, such as Identification for Development (ID4D) from the World Bank, Digital Government Review from the Organisation for Economic Co-operation and Development (OECD), and electronic Identification, Authentication and trust Services (eIDAS) from the European Commission. Moreover, digital identity emphasizes further to uphold e-governance by promoting security, inclusion, and privacy in digital interaction (Kumar, 2024).

Among the countries that are widely regarded as pioneers in digital governance are the Nordic states, particularly Norway, Sweden, Denmark, Finland, and Iceland. These countries have developed highly integrated digital government systems that are trusted by the public and widely used in everyday life. This approach is often referred to as the Nordic Model of Digital Governance. Skogerbø et al. (2021) argue that the main strengths of this model lie in strong digital infrastructure, transparent data governance, and the existence of national digital identity systems that allow citizens to access a wide range of public services through a single, unified platform.

One of the most significant innovations in Nordic digital governance is the implementation of the once-only principle. This principle means that citizens are required to provide their personal data to public authorities only once (Wimmer et al., 2020). After that, the data can be reused by all authorized government agencies whenever needed, without requiring citizens to submit the same information repeatedly. In practical terms, this eliminates redundant data entry, reduces administrative burdens, and minimizes the risk of errors. It also reflects a deeper shift in the philosophy of public administration, where data is treated as a shared public resource rather than as the exclusive property of individual institutions.

In Norway, the once-only principle is implemented through a comprehensive digital identity (eID) system that is integrated with national service portals such as ID-porten and Altinn (Parmiggiani & Mikalef, 2022). According to the Norwegian Digitalisation Agency (2024), more than 92% of the Norwegian population uses eID to access public services online, including healthcare, education, taxation, and social security. The system is connected to the National Population Register, which serves as a single source of truth for demographic data. This ensures that personal information is updated in real time and shared across government agencies without requiring manual input from citizens.

The success of this system is not solely the result of advanced technology. It is also supported by strong institutional coordination, a high level of public trust, and a robust legal framework for data protection (Hafseld et al., 2022). Norway's Data Protection Act, aligned with the European Union's General Data Protection Regulation (GDPR), provides strict rules on how personal data can be processed, stored, and shared. As a result, citizens have confidence that their data is handled securely and ethically, which in turn encourages widespread adoption of digital services.

In contrast, Indonesia presents a very different picture. Over the past decade, the Indonesian government has made significant efforts to digitalize public services. Various applications and platforms have been introduced, such as Mobile Jaminan Kesehatan Nasional for health services, *PeduliLindungi* during the COVID-19 pandemic, and online tax reporting systems (Yuliastuti & Jawahir, 2024). However, these initiatives tend to be sectoral and fragmented. Each ministry or agency develops its own system, often without adequate coordination with others. As a result, citizens are required to create multiple accounts, repeatedly enter the same data, and navigate different platforms for different services.

This fragmentation is partly due to the decentralized nature of Indonesia's bureaucracy and the strong autonomy of individual ministries and agencies (Alqarni et al., 2026). Data is often treated as an institutional asset rather than as a shared public resource. Interoperability between systems remains weak, and there is no fully binding mechanism that forces agencies to integrate their data. Consequently, data duplication, inefficiency, and inconsistencies are common. These problems reduce the quality of public services and lead to the undermining of public trust in digital government.

Moreover, public trust in Indonesia's digital systems is further weakened by repeated cases of data breaches, such as those involving BPJS Kesehatan, eHAC, and the leakage of national identification numbers (*Nomor Induk Kependudukan*, NIK). These incidents reinforce the perception that government systems are not sufficiently secure and that personal data is vulnerable to misuse. As trust is a key factor in the success of digital governance, this situation poses a serious challenge to Indonesia's digital transformation agenda. Given these contrasting experiences, the Nordic model—particularly Norway's implementation of the once-only principle—offers valuable lessons for Indonesia. Norway demonstrates that it is possible to build an integrated, efficient, and trusted digital governance system, provided that there is strong institutional coordination, clear legal frameworks, and a culture of transparency. For Indonesia, which is currently pursuing initiatives such as One Data Indonesia (*Satu Data Indonesia*) and the Electronic-Based Government System (*Sistem Pemerintahan Berbasis Elektronik*, SPBE), the once-only principle represents a concrete model for overcoming fragmentation and improving public service delivery.

Previous research conducted by Tokovska et al. (2023) comparing e-government in Norway and Slovakia, it reveals that countries with higher levels of digital inclusivity and public trust gain more effective adoption of digital government services, emphasizing the importance of institutional readiness alongside technological advancement. Parmiggiani & Mikalef (2022) highlight Norway's success in digital transformation. It underscores that trust is fundamental for successful digital transformation. Thus, the citizen will willingly share their personal information to be adopted into digital public services. In Indonesia context, Amini & Javidnejad (2023) argue that One Data Indonesia (*Satu Data Indonesia*, SDI) was established to create an integrated, credible, and accountable national data ecosystem to gain public transparency and access to government data. However, there is limited attention to the once-only principle as an e-governance mechanism that integrates digital identity for accessing public services prioritizing efficiency and citizen trust. Thus, the purpose of this research is to examine how Norway's implementation of once-only principle through one identity system, such as ID-porten and Altinn can be implemented as a lesson in addressing Indonesia's persistent challenges of duplicated data, fragmented services, and limited interoperability among government institutions.

This paper, therefore, aims to answer three main questions: How is the once-only principle implemented in Norway's digital identity and e-governance system? What are the impacts of this implementation on administrative efficiency, public trust, and digital democracy? How can Indonesia adapt similar principles to address its own challenges in data fragmentation, bureaucratic inefficiency, and low public trust? By answering these questions, this study seeks to contribute not only to the technical discussion on e-governance but also to broader debates on digital democracy, state legitimacy, and the relationship between citizens and the state in the digital age.

2. Methods

This research is conducted through the lens of an interpretive paradigm (Sprake & Palmer, 2022), which holds that government practices are constructed by institutional, political, and socio-cultural contexts where it is occured. By using this paradigm, it helps to scrutinize how Norway's once-only principle is understood, implemented, and institutionalized in Indonesia through policy documents and scholarly literature analysis. This study employs a qualitative research approach with a comparative case study design to analyze the implementation of the once-only principle in Norway's e-governance system and to examine its relevance for improving public service efficiency in Indonesia. Norway was selected as the primary case because of its internationally recognized success in implementing cross-agency data integration through a national digital identity system. Indonesia, on the other hand, was chosen as a comparative case to explore the challenges of adapting similar principles in a developing country context characterized by complex and fragmented bureaucratic structures (OECD, 2017; Skogerbø et al., 2021).

The data collection technique used in this research is a systematic literature review. The study analyzes a wide range of sources, including government policy documents, official reports, academic journal articles, and publications from international organizations. Key sources include Norway's national digital strategy documents, reports from the Norwegian Digitalisation Agency (*Agensi Digitalisasi Norwegia*, Digdir), legal texts related to data protection and digital governance, as well as Indonesian policies such as One Data Indonesia and SPBE (Digdir, 2019; Ministry of Administrative and Bureaucratic Reform, 2024). In addition, reports from international institutions such as the OECD Trust Survey (2023) and the United Nations E-Government Survey (2022) are used to provide comparative data on public trust and digital government performance.

The data analysis process follows a thematic analysis approach. This involves identifying key themes, patterns, and concepts related to data governance, institutional coordination, interoperability, public trust, and legal frameworks. The themes are then compared across the two cases to highlight similarities, differences, and underlying factors that explain the success or failure of the once-only principle. A comparative analytical framework is used to examine differences in institutional arrangements, governance paradigms, and socio-cultural contexts between Norway and Indonesia.

The theoretical framework of data as public infrastructure is applied to interpret the Norwegian case, where data is treated as a shared resource for the collective benefit of society. In contrast, the concept of data as institutional property is used to analyze the Indonesian context, where data is often controlled by individual agencies and used to reinforce bureaucratic power (OECD, 2017; Umar et al., 2022). By applying these frameworks, the study seeks to go beyond technical explanations and explore the political, cultural, and ethical dimensions of digital governance. This methodological approach allows for a holistic understanding of the once-only principle, not only as a technological solution but also as a socio-political innovation that reshapes the relationship between the state and its citizens. Through this lens, the study aims to provide nuanced insights into why certain digital governance models succeed in some contexts but face resistance or failure in others.

3. Results and Discussion

3.1 Implementation of the once-only principle and data governance in Norway

The analysis shows that the successful implementation of the once-only principle in Norway is not merely the result of advanced digital technology, but rather the outcome of a carefully constructed governance ecosystem that integrates institutional coordination, standardized data architecture, strong legal frameworks, and high public trust. In Norway, digital transformation has been approached as a long-term national project rather than as a series of isolated initiatives. This strategic orientation is evident in the establishment of the Norwegian Digitalisation Agency (*Agensi Digitalisasi Norwegia*, Digdir), which functions as the central coordinating body for digital government across ministries and agencies. Digdir plays a crucial role in setting standards, ensuring interoperability, and aligning digital initiatives with national priorities (Digdir, 2019).

At the core of Norway's once-only implementation is the national digital identity (eID) system, which is integrated with service portals such as ID-porten and Altinn. ID-porten acts as a secure gateway that allows citizens to log in to multiple public services using a single digital identity, while Altinn serves as a platform for communication between citizens, businesses, and government agencies. Through these platforms, more than 2,000 public services can be accessed online, ranging from tax filing and social security to education and healthcare services (Hansteen et al., 2016; European Commission, 2016). This level of integration significantly reduces administrative burdens for both citizens and public servants, as data entered once can be reused across different services.

The National Population Register plays a pivotal role in this system by serving as the authoritative source of personal data. All government agencies rely on this register for up-to-date information on citizens' identities, addresses, family relations, and civil status. When a citizen updates their address or marital status, the change is automatically reflected across all relevant systems. This real-time data sharing eliminates inconsistencies and reduces the need for manual verification. In effect, the National Population Register functions as a backbone infrastructure that supports the once-only principle and ensures data accuracy throughout the public sector.

From an institutional perspective, Norway's success can be attributed to a governance model that prioritizes collaboration over competition among agencies. Ministries and agencies are required to comply with national standards for data exchange and system interoperability. Open standards and shared frameworks are mandatory, which prevents the emergence of incompatible systems and data silos. This is a critical factor, as many countries fail in their digital transformation efforts due to fragmented systems developed independently by different institutions. In Norway, by contrast, digital projects are evaluated not only in terms of their individual benefits but also in terms of their contribution to the overall digital ecosystem.

The legal framework further strengthens this integrated approach. Norway's Data Protection Act, in alignment with the European Union's GDPR, provides clear rules on data processing, consent, data minimization, and purpose limitation. Citizens have the right to know how their data is used, to access their data, and to request corrections. Importantly, data sharing between agencies is regulated and must be justified by a legal basis. This ensures that the once-only principle does not become a pretext for uncontrolled data circulation. Instead, it is implemented within a framework of accountability and respect for individual rights.

Public trust emerges as a central enabling factor in the Norwegian case. The OECD Trust Survey (2023) indicates that approximately 81% of Norwegians express trust in public institutions. This high level of trust is the result of long-standing traditions of transparency, low levels of corruption, and strong welfare state institutions. In such a context, citizens are more willing to share their data with the government because they believe that it will be used responsibly and for legitimate purposes. Skogerbø et al. (2021) note that in the Nordic countries, digital governance is embedded in a broader social contract in which the state is seen as a benevolent actor that works for the collective good.

This trust is reinforced by practical experiences with digital services. When citizens consistently experience efficient, reliable, and user-friendly services, their confidence in the system grows. For example, the ability to complete tax declarations in a few minutes using pre-filled forms, or to access healthcare information online without bureaucratic hurdles, creates a positive feedback loop. Efficiency leads to satisfaction, satisfaction leads to trust, and trust encourages further adoption. In this way, the once-only principle contributes not only to administrative efficiency but also to the legitimacy of the state in the eyes of its citizens.

From a theoretical perspective, Norway's approach reflects the concept of data as public infrastructure. Data is treated as a shared resource that should be managed collectively for the benefit of society. This contrasts sharply with traditional bureaucratic models, where data is often hoarded by individual agencies as a source of power. In Norway, data sharing is institutionalized, and agencies are expected to contribute to and benefit from common data resources. This paradigm shift is fundamental to the success of the once-only principle. Moreover, the Norwegian case illustrates how digital governance can support digital democracy. When data is integrated and services are accessible, citizens are better informed and more capable of engaging with public institutions. They can monitor government actions, participate in consultations, and exercise their rights more effectively. In this sense, the once-only principle is not merely an administrative tool but also a democratic enabler. It reduces barriers to participation and makes the state more responsive to citizens' needs.

3.2 Fragmentation of e-governance and barriers to data integration in Indonesia

In stark contrast to the Norwegian experience, the Indonesian case is characterized by fragmentation, institutional silos, and uneven implementation of digital initiatives. Although Indonesia has made significant progress in digitalizing public services over the past decade, these efforts have largely been driven by individual ministries and agencies rather than by a unified national strategy. As a result, the digital landscape is highly fragmented, with more than 27,000 public service applications operating independently (Ministry of Administrative and Bureaucratic Reform, 2024). This proliferation of applications reflects a lack of coordination and standardization, which undermines the efficiency and coherence of the system.

The policy framework for digital governance in Indonesia includes initiatives such as One Data Indonesia and SPBE. These policies aim to improve data quality, interoperability, and integration across government agencies. In theory, Satu Data Indonesia is intended to establish common data standards, metadata, and reference codes, while SPBE seeks to promote the use of electronic systems in government administration. However, in practice, implementation has been uneven and often superficial. Many agencies continue to develop their own systems without fully complying with national standards.

One of the key obstacles is the strong autonomy of ministries and agencies, which often leads to what is commonly referred to as *ego sektoral* (sectoral ego). Each institution tends to prioritize its own interests and maintain control over its data. Data is seen as a strategic asset that can enhance institutional influence, budget allocations, and political leverage. This mindset is reinforced by bureaucratic traditions and hierarchical structures that reward control rather than collaboration. Consequently, efforts to integrate data across agencies are frequently met with resistance.

This institutional fragmentation has concrete consequences for public service delivery. For example, in social assistance programs, data on potential beneficiaries may be held by different agencies, such as the Ministry of Social Affairs, the Statistics Indonesia (*Badan Pusat Statistik*, BPS), and local governments. Because these datasets are not fully synchronized, discrepancies arise regarding who is eligible for assistance. This can lead to exclusion errors (eligible individuals not receiving benefits) and inclusion errors (ineligible individuals receiving benefits). Such problems not only reduce the effectiveness of social programs but also undermine public trust in government.

The existence of the national identification number *(Nomor Induk Kependudukan*, NIK) as a unique identifier for citizens represents a significant potential advantage for Indonesia. In principle, NIK could serve as the backbone of a once-only system, enabling data integration across services such as healthcare, taxation, education, and social protection. However, in practice, NIK is not yet fully utilized as a single source of truth. Different agencies maintain their own databases and may not always synchronize their data with the population registry. As a result, citizens are often required to provide the same information repeatedly when accessing different services.

Another major barrier is the issue of data security and public trust. Indonesia has experienced several high-profile data breaches in recent years, including leaks involving the national health insurance agency (*Badan Penyelenggara Jaminan Sosial Kesehatan*, BPJS Kesehatan), eHAC (an application used during the COVID-19 pandemic), and large-scale leaks of NIK data. These incidents have been widely reported in the media and have generated public concern about the safety of personal information. Yuliastuti & Jawahir (2023) note that such breaches significantly undermine citizens' willingness to use digital services, as they fear misuse of their data.

The United Nations E-Government Survey (2022) indicates that while Indonesia's E-Government Development Index (EGDI) score has improved, levels of e-participation and user engagement remain relatively low. This suggests that technical progress has not been matched by social acceptance. Digital literacy also varies widely across regions and socio-economic groups, creating a digital divide that limits the inclusiveness of digital governance. In rural areas and among older populations, access to digital services remains limited, further complicating efforts to build a comprehensive digital ecosystem.

From a governance perspective, Indonesia's digital transformation is hampered by the absence of a strong central authority with the power to enforce standards and coordinate across agencies. Although the Ministry of Administrative and Bureaucratic Reform (*Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi*, KemenPANRB) and the Ministry of Communication and Information Technology (*Kementerian Komunikasi dan Informatika* or *Kementerian Komunikasi dan Digital*, Komdigi) play important roles, their authority is often limited by overlapping mandates and political constraints. Without a single, empowered institution to lead digital transformation, policies risk remaining at the level of rhetoric rather than being translated into concrete action.

Culturally, there is also a degree of skepticism toward government initiatives, rooted in historical experiences of corruption, inefficiency, and lack of transparency. While significant reforms have been undertaken since the fall of the New Order regime, public perceptions change slowly. Trust is not built overnight; it requires consistent behavior and tangible improvements in service quality. In this context, digitalization alone is insufficient to generate trust. If digital systems are perceived as unreliable, insecure, or complicated, they may even reinforce negative perceptions. The Indonesian case thus illustrates the limits of technological determinism. Simply introducing digital tools and platforms does not automatically lead to better governance. Without institutional reform, cultural change, and trust-building measures, digital initiatives may fail to deliver their promised benefits. In fact, they may even exacerbate existing problems by adding new layers of complexity to an already convoluted bureaucracy.

3.3 Comparing digital governance paradigms and their implications for Indonesia

A comparative analysis of Norway and Indonesia reveals profound differences in their underlying paradigms of digital governance. These differences go beyond technical capacity and reflect deeper political, institutional, and cultural factors. Norway's approach is rooted in a collaborative, citizen-centric model that treats data as a public good and prioritizes service integration. Indonesia's approach, by contrast, remains largely institution-centric, with data controlled by individual agencies and digital initiatives developed in silos.

The concept of data as public infrastructure is central to understanding Norway's success. In this paradigm, data is seen as a foundational resource that supports multiple functions and services. Just as roads and electricity grids enable economic and social activity, data infrastructure enables efficient governance and citizen participation. This perspective encourages investment in shared platforms, standardization, and interoperability. It also implies a collective responsibility to maintain and improve data quality. In Indonesia, data is more commonly viewed as institutional property. Agencies collect, store, and manage data primarily for their own purposes, and data sharing is often seen as a loss of control. This perspective is reinforced by performance metrics, budgetary incentives, and organizational cultures that reward individual achievements rather than collective outcomes. As Umar et al. (2022) argue, this institutionalization of data ownership creates barriers to integration and undermines the potential benefits of digital transformation.

These contrasting paradigms have important implications for the feasibility of implementing the once-only principle in Indonesia. While the technical prerequisites may exist—such as the NIK system and expanding digital infrastructure—the institutional and cultural conditions are less favorable. Implementing the once-only principle would require a shift in mindset, from viewing data as a source of power to viewing it as a shared resource. It would also require strong political leadership to overcome resistance and align incentives across agencies. Another key difference lies in the relationship between the state and citizens. In Norway, the welfare state model and high levels of social trust create a favorable environment for data sharing. Citizens generally believe that the state acts in their best interests, and they are therefore willing to allow the state to manage their data. In Indonesia, where trust in public institutions is lower, citizens are more cautious. They may fear surveillance, misuse of data, or lack of accountability. This skepticism is understandable given historical experiences and recent data breaches.

Therefore, adapting the once-only principle in Indonesia cannot simply involve copying the Norwegian model. It requires a context-sensitive approach that addresses institutional weaknesses, builds trust, and ensures robust data protection. Three key prerequisites emerge from the analysis. First, there is a need for a strong central coordinating authority for digital transformation. This institution must have clear mandates, sufficient resources, and political backing to enforce standards and coordinate across agencies. Without such leadership, fragmentation will persist. Second, binding interoperability standards must be established and enforced. Agencies should be required to use common data standards, share data through national platforms, and avoid developing isolated systems. This may require changes in regulations, budgeting processes, and performance evaluation criteria. Third, trust-building measures are essential. These include strengthening data protection laws, improving cybersecurity, increasing transparency about data use, and engaging citizens in the design of digital services. Trust is not a by-product of digitalization; it must be actively cultivated.

Importantly, these three elements are interdependent. Institutional reform without trust will lead to resistance. Technical standards without leadership will remain on paper. Trust without effective systems will lead to disappointment. Therefore, a holistic approach is required. The comparison also highlights the broader implications for digital democracy. In Norway, integrated digital systems facilitate participation, accountability, and responsiveness. Citizens can easily access information, communicate with authorities, and engage in democratic processes. In Indonesia, fragmentation and inefficiency limit these possibilities. When citizens struggle to access basic services, their capacity to participate meaningfully in governance is reduced. Thus, improving data integration is not only a matter of efficiency but also a matter of democratic quality.

Ultimately, the once-only principle represents more than a technical solution. It embodies a vision of governance in which the state is organized around the needs of citizens rather than around bureaucratic boundaries. For Indonesia, embracing this vision would require significant change, but the potential benefits—in terms of efficiency, trust, and democratic legitimacy—are substantial.

4. Conclusions

This study demonstrates that Norway's successful implementation of the once-only principle is not merely the result of technological advancement, but of strong institutions, coherent governance structures, legal certainty, and high public trust. By treating data as public infrastructure, Norway has integrated systems such as eID, the National Population Register, ID-porten, and Altinn into a seamless digital ecosystem. This integration reduces administrative burdens, prevents data duplication, and improves the accessibility, accuracy, and reliability of public services. Strong coordination through the Digdir, consistent interoperability standards, and GDPR-aligned data protection further strengthen this system and citizens' confidence in digital governance.

In contrast, Indonesia has made progress through initiatives such as Satu Data Indonesia and SPBE, but their implementation remains constrained by institutional fragmentation, sectoral ego, weak interoperability, and overlapping mandates. Government agencies often operate in silos and develop separate systems, requiring citizens to repeatedly provide the same information. Public trust is also challenged by data breaches and concerns over data security, creating a cycle in which low trust limits digital service adoption and weakens the impact of digital reforms. These differences reflect contrasting governance paradigms: Norway follows a more citizen-centric and collaborative model, while Indonesia remains comparatively institution-centric, with data often controlled by individual agencies.

For Indonesia to adopt the once-only principle effectively, reforms must address both institutional and societal dimensions. First, a central coordinating authority should be strengthened or established with clear mandates and sufficient resources to align digital initiatives and enforce interoperability. Second, binding interoperability standards should be implemented across government agencies rather than treated as optional guidelines. Third, public trust must become a central priority through stronger data protection, improved cybersecurity, greater transparency in data use, and meaningful citizen participation in the development and evaluation of digital services.

Ultimately, the once-only principle should be understood not only as a technical innovation but also as a broader transformation of state–citizen relations. Its implementation can reduce administrative burdens, improve public service efficiency, and strengthen a more responsive, accountable, and citizen-oriented state. For Indonesia, adopting this principle could support stronger democratic legitimacy and a more equitable relationship between citizens and government. However, its success depends on sustained political commitment, institutional cooperation, and a culture of trust. Without these foundations, digital transformation risks remaining fragmented; with them, Indonesia can move toward more integrated and citizen-centered governance in the digital age.

Acknowledgement

The authors would like to express their sincere gratitude to the organizing committee of Scandinavian Day 2025, Universitas Gadjah Mada, for providing an academic forum that facilitated critical discussions on digital democracy and governance models in the Nordic region. This forum served as an important intellectual space for exchanging ideas, refining arguments, and deepening understanding of the comparative perspectives explored in this study. The authors also extend their appreciation to all individuals and institutions who, directly or indirectly, provided support, inspiration, and constructive feedback during the preparation and completion of this research.

Author Contribution

Conceptualization, A.W.M.; Methodology, A.W.M. and A.C.M.; Investigation, A.C.M. and P.R.S.K.; Data Curation, A.C.M.; Formal Analysis, A.C.M. and P.R.S.K.; Writing – Original Draft Preparation, A.W.M., A.C.M., and P.R.S.K.; Writing – Review & Editing, A.W.M. and P.R.S.K.; Supervision, A.W.M. All authors contributed to the critical review and substantive revision of the manuscript and approved the final version submitted for publication.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethical Review Board Statement

This study did not involve human participants, experiments, or the collection of sensitive personal data. All data used in this research were obtained from academic literature, public policy documents, and official reports that are publicly available. Therefore, ethical approval from a research ethics committee was not required.

Informed Consent Statement

Not applicable. This study did not involve human participants, interviews, surveys, or the collection of primary data.

Data Availability Statement

The data used in this study were obtained from secondary sources, including government policy documents, official reports, publications by international organizations, and academic literature that are publicly accessible. All data sources have been cited in the reference list of this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest, either financial or non-financial, that could influence the writing or outcomes of this research.

Declaration of Generative AI Use

In the process of drafting and editing this manuscript, the authors used generative artificial intelligence tools for language assistance, including grammar checking, sentence clarity, and academic structuring. All substantive content, analysis, interpretation of data, and conclusions are the full responsibility of the authors.

Open Access

References

Alqarni, W., Za, S., Muallidin, I., Afrijal, A., & Akhyar, M. N. (2026). The role of institutional quality in shaping digital governance in decentralised Indonesia. *Journal of Contemporary Governance and Public Policy, 7*(1), 83–106. https://doi.org/10.46507/jcgpp.v7i1.793

Amini, M., & Javidnejad, L. (2023). Legal frameworks for digital identity systems in e-governance: Privacy, security, and inclusion. *Legal Studies in Digital Age, 2*(3), 49–63. https://www.jlsda.com/index.php/lsda/article/view/21/24

Agensi Digitalisasi Norwegia (Digdir). (2019). About the Norwegian digitalisation agency. https://www.digdir.no/digdir/about-norwegian-digitalisation-agency/887

Efthymiou, I.-P. (2025). The role of e-government and e-governance in modern societies. In Public Governance Practices in the Age of AI (pp. 45–68). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9286-7.ch003

European Commission. (2016). *eGovernment in Norway*. https://interoperable-europe.ec.europa.eu/sites/default/files/inlinefiles/eGovernment%20in%20Norway%20-%20February%202016%20-%2013_0_v1_00.pdf

Hansteen, K., Ølnes, J., & Alvik, T. (2016). *Nordic digital identification (eID): Survey and recommendations for cross-border cooperation*. https://norden.diva-portal.org/smash/get/diva2:902133/FULLTEXT01.pdf

Hafseld, K. H. J., Hussein, B., & Rauzy, A. R. (2022). Government inter-organizational digital transformation projects: Five key lessons learned from a Norwegian case study. *Procedia Computer Science, 196*, 910–919. https://doi.org/10.1016/j.procs.2021.12.092

Idowu, E. (2025). *The role of ICT in enhancing e-government services*. Preprints.org. https://www.preprints.org/manuscript/202504.1871

Kalsnes, B., Falasca, K., & Kammer, A. (2021). Scandinavian political journalism in a time of fake news and disinformation. In E. Skogerbø, Ø. Ihlen, N. N. Kristensen, & L. Nord (Eds.), *Power, communication, and politics in the Nordic countries* (pp. 283–304). Nordicom. https://doi.org/10.48335/9789188855299-14

Kumar, D. P. (2024). The impact of digital technologies on e-governance: A comprehensive analysis. In S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (Eds.), *Transfer, diffusion and adoption of next-generation digital technologies* (pp. 367–378). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50188-3_32

Lubis, I. A. R., Ramdan, A. T. M., & Wiryany, D. (2022). Politik digital: Manifestasi komunikasi di era digital. *Jurnal Lensa Mutiara Komunikasi, 6*(1), 193–206. https://doi.org/10.51544/jlmk.v6i1.3064

OECD Digital Government Studies. (2017). *Digital government review of Norway: Boosting the digital transformation of the public sector*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/09/digital-government-review-of-norway_g1g7f6ac/9789264279742-en.pdf

Parmiggiani, E., & Mikalef, P. (2022). The case of Norway and digital transformation over the years. In P. Mikalef & E. Parmiggiani (Eds.), *Digital transformation in Norwegian enterprises* (pp. 11–18). Springer International Publishing. https://doi.org/10.1007/978-3-031-05276-7_2

Sinamo, D. R., Gultom, G. M., Sinurat, R., & Lumbantobing, R. (2025). Media dan perubahan sosial studi kasus: Tentang penggunaan media sosial dalam kampanye politik dan dampaknya terhadap partisipasi politik. *Jurnal Penelitian Ilmiah Multidisipliner, 1*(3), 223–230. https://ojs.ruangpublikasi.com/index.php/jpim/article/view/260/65

Skogerbø, E., Kristensen, N. N., Nord, L., & Ihlen, Ø. (2021). Introduction: A Nordic model for political communication? In E. Skogerbø, Ø. Ihlen, N. N. Kristensen, & L. Nord (Eds.), *Power, communication, and politics in the Nordic countries* (pp. 13–27). Nordicom. https://doi.org/10.48335/9789188855299-1

Sprake, A., & Palmer, C. (2022). Understanding the interpretive paradigm: A guide for sports students learning through qualitative research. *Journal of Qualitative Research in Sports Studies, 16*(1), 45–68. https://knowledge.lancashire.ac.uk/id/eprint/48569/

Suherlan, S. (2023). Digital technology transformation in enhancing public participation in democratic processes. *Technology and Society Perspectives (TACIT), 1*(1), 10–17. https://doi.org/10.61100/tacit.v1i1.34

Tokovska, M., Ferreira, V. N., Vallušova, A., & Seberíni, A. (2023). E-government—The inclusive way for the future of digital citizenship. *Societies, 13*(6), 141. https://doi.org/10.3390/soc13060141

Wimmer, M. A., Neuroni, A. C., & Frecè, J. T. (2020). Approaches to good data governance in support of public sector transformation through once-only. In G. Viale Pereira, M. Janssen, H. Lee, I. Lindgren, M. P. Rodríguez Bolívar, H. J. Scholl, & A. Zuiderwijk (Eds.), *Electronic government* (pp. 210–222). Springer International Publishing. https://doi.org/10.1007/978-3-030-57599-1_16

Yuliastuti, H., & Jawahir, Moh. (2023). Analisis efektivitas pemanfaatan aplikasi layanan kesehatan Mobile Jaminan Kesehatan Nasional di Indonesia. *Jurnal Pengabdian*

Kepada Masyarakat (JPKM) Langit Biru, *4*(1), 28–40. https://doi.org/10.54147/jpkm.v4i01.726

Biographies of Authors

Achmad Wafa Muzaki, an undergraduate student in the Department of English Literature, Faculty of Cultural Sciences, University of Jember, Indonesia. He is currently completing his Bachelor's degree with academic interests in political communication, digital democracy, and media studies. He is particularly interested in how digital platforms, online discourse, and e-governance systems influence political participation, citizen engagement, and state–society relations.

- Email: ahmadwafa807@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Anisa Cahyani Maulida, an undergraduate student in the Department of English Literature, Faculty of Cultural Sciences, University of Jember, Indonesia. She is currently pursuing her Bachelor's degree and has a strong academic interest in digital governance, Nordic studies, and comparative public policy. Her areas of interest include e-governance models, digital identity systems, and institutional reform in the context of public sector digitalization.

- Email: anisac304@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Putri Revalina Salsabila Khairani, an undergraduate student in the Department of English Literature, Faculty of Cultural Sciences, University of Jember, Indonesia. She is currently pursuing her Bachelor's degree and is actively engaged in academic writing related to digital governance, public policy, and socio-cultural issues in Indonesia. Her academic interests include digital transformation in the public sector, public trust in government, and the relationship between technology and society in developing countries.

- Email: putrirevalinask@gmail.com
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A