Open Access Indonesia Journal of Social Sciences

Journal Homepage: https://journalsocialsciences.com/index.php/OAIJSS

Data Governance and Privacy in Sulu, Philippines: Building Trust and Ensuring Accountability in Digital Public Service Delivery

Datu Ansaruddin K. Kiram[1]*, Mharcelyn M. Kiram[1], Jul-Asri A. Hadjibun[1], Merhana Taraji[1]

[1]Department of Public Administration, College of Public Affairs, Mindanao State University Sulu, Sulu, Philippines

ARTICLE INFO

Keywords:

Data governance

Digital public service delivery

E-government

Privacy

Trust

***Corresponding author:**

Datu Ansaruddin K. Kiram

E-mail address:

datuansaruddin.kiram@msusulu.edu.ph

All authors have reviewed and approved the final version of the manuscript.

https://doi.org/10.37275/oaijss.v8i1.283

ABSTRACT

The province of Sulu in the Philippines faces unique challenges in implementing digital governance initiatives due to its geographical remoteness, socio-economic disparities, and security concerns. This study examines the critical issue of data governance and privacy in Sulu's digital public service delivery, focusing on building trust and ensuring accountability. This research employed a mixed-methods approach. Quantitative data was collected through a survey of 300 residents of Sulu involved in accessing digital public services. Qualitative data was gathered through semi-structured interviews with 20 key informants, including local government officials, civil society representatives, and technology experts. The study analyzed existing policies and frameworks related to data governance and privacy in the Philippines and compared them with international best practices. The findings revealed a significant gap between policy aspirations and the reality on the ground. While national policies emphasize data privacy and security, awareness and implementation at the local level in Sulu remain limited. The study identified challenges such as lack of digital literacy, inadequate infrastructure, and concerns about data misuse. However, it also highlighted opportunities for leveraging digital technologies to improve transparency, accountability, and citizen participation in public service delivery. In conclusion, this study provides valuable insights for policymakers and practitioners working on digital governance in Sulu and other similar contexts. It emphasizes the need for context-specific strategies that prioritize community engagement, capacity building, and robust oversight mechanisms to ensure responsible and ethical data governance.

1. Introduction

The advent of the digital age has ushered in a transformative wave across the globe, with governments at the forefront of harnessing technology to revolutionize public service delivery. This paradigm shift, known as digital governance, promises to enhance efficiency, transparency, and citizen engagement, marking a significant leap toward a more accessible and responsive public sector. However, the path to realizing the full potential of digital governance is not without its challenges. One of the most critical challenges in the digital governance landscape is ensuring the ethical and responsible management of citizen data. As governments increasingly rely on digital platforms to deliver services, they inevitably collect, process, and store vast amounts of personal information. This raises concerns about data governance and privacy, particularly in regions grappling with socio-economic disparities, limited digital literacy, and security concerns (Karyda, 2019; Morris, 2018; Stoll, 2019).

Data governance, in its essence, is the framework that guides the management of data assets, ensuring data quality, security, and ethical use. It is the compass that directs how data is collected, stored, processed, and shared, ensuring that it remains accurate, confidential, and protected from unauthorized access or misuse. Privacy, on the other hand, is the fundamental right of individuals to control their personal information and safeguard it from unwarranted intrusion. It is the shield that protects citizens from the potential harms of data misuse, ensuring that their personal information is handled with respect and responsibility. In the realm of digital governance, data governance, and privacy are two sides of the same coin. Robust data governance frameworks are essential to ensure that privacy is upheld, while privacy considerations must be at the heart of any data governance strategy. The delicate balance between these two elements is crucial to fostering trust between governments and citizens, paving the way for the successful implementation of digital governance initiatives (Al-Abdullah, 2020; Mavriki, 2022; McCarthy, 2020).

This research delves into the critical issue of data governance and privacy in the context of Sulu, a province in the Philippines facing unique challenges in its pursuit of digital governance. Sulu, an archipelago in the southwestern Philippines, is part of the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM), a region with a history of conflict and underdevelopment. The province is characterized by its geographical remoteness, fragmented island structure, and a predominantly Muslim population with diverse ethnic groups and cultural traditions. Sulu's socio-economic landscape presents significant hurdles in its journey toward digital inclusion. Low levels of literacy, high poverty rates, and limited access to basic services, coupled with the province's history of conflict and instability, have created a complex environment for implementing digital governance initiatives. While efforts have been made to improve digital connectivity in Sulu, challenges remain in ensuring equitable access and affordability, particularly in remote and underserved communities. The unique context of Sulu makes the issue of data governance and privacy particularly salient. The province's history of conflict and security concerns necessitates careful handling of sensitive information, while the limited digital literacy among the population makes them vulnerable to data breaches and online exploitation. Furthermore, the lack of robust oversight mechanisms raises concerns about potential data misuse by government agencies or private entities (Carter, 2022; Schneider, 2022; Thillaivasan, 2022). This study aims to shed light on the current state of data governance and privacy in Sulu's digital public service delivery.

2. Methods

This study employed a mixed-methods approach, combining quantitative and qualitative data collection and analysis techniques to investigate the current state of data governance and privacy in Sulu's digital public service delivery. This approach allowed for a comprehensive understanding of the complex issues surrounding data governance and privacy in Sulu by integrating the strengths of both quantitative and qualitative research methods. The quantitative strand provided a broad overview of the situation through a survey of residents, while the qualitative strand delved deeper into the nuances of individual experiences and perceptions through interviews with key informants.

The quantitative data collection involved a survey of 300 residents of Sulu who had accessed digital public services in the past year. The sample size was determined based on the population of Sulu and the desired level of confidence, ensuring that the sample was representative of the population. To further enhance the representativeness of the sample, a stratified sampling technique was employed. This involved dividing the population into subgroups based on age, gender, and location (urban/rural), and then randomly selecting participants from each subgroup in proportion to their representation in the population. This ensured that the sample reflected the diversity of Sulu's population, allowing for a more accurate generalization of the findings to the broader population. The survey instrument was meticulously developed, drawing upon existing literature and adapting it to the local context of Sulu. This involved reviewing relevant studies on data governance and privacy, as well as considering the unique cultural and socio-economic characteristics of Sulu. The survey included a range of questions designed to assess various aspects of data governance and privacy, including; Awareness of data governance and privacy concepts: This section aimed to gauge residents' understanding of data governance and privacy, including their familiarity with relevant terminology and their knowledge of data protection laws; Perceptions of data security and trust in government institutions: This section explored residents' trust in government institutions to handle their personal data responsibly, as well as their perceptions of the security measures in place to protect their data; Experiences with digital public services and any concerns related to data privacy: This section sought to gather information on residents' experiences with digital public services, including any problems they encountered and their concerns about the security of their personal data when using these services; Willingness to share personal data for different purposes: This section investigated residents' willingness to share their personal data for various purposes, such as accessing healthcare services, receiving government assistance, or commercial purposes. The survey was administered through face-to-face interviews conducted by trained enumerators. This approach was chosen to ensure that the survey was accessible to all residents, regardless of their literacy levels or access to technology. The enumerators were carefully selected and underwent rigorous training to ensure that they understood the survey instrument and could administer it effectively. They were also trained on ethical considerations, such as obtaining informed consent and maintaining the confidentiality of participants' responses. The data collected through the survey was carefully entered into a statistical software package, ensuring accuracy and completeness. The data was then analyzed using descriptive statistics to provide an overview of the responses and inferential tests to identify any significant relationships between variables.

The qualitative data collection involved semi-structured interviews with 20 key informants selected purposively to represent diverse perspectives on data governance and privacy in Sulu. The informants were carefully chosen based on their knowledge, expertise, and involvement in digital governance initiatives. The selection process aimed to ensure that the informants represented a range of stakeholders, including; Local government officials responsible for digital governance initiatives: These individuals provided insights into the challenges and opportunities of implementing data governance and privacy frameworks from the government's perspective; Civil society representatives working on issues related to technology and human rights: These individuals offered perspectives on the potential impact of digital technologies on human rights, particularly the right to privacy; Technology experts and academics with expertise in data governance and privacy: These individuals provided expert opinions on the technical aspects of data governance and privacy, as well as the latest developments in the field. The interviews were designed to explore a range of themes related to data governance and privacy, including; Challenges and opportunities in implementing data governance and privacy frameworks in Sulu: This theme aimed to identify the specific challenges and opportunities that exist in Sulu, considering the province's unique context; Perceptions of the role of digital technologies in promoting transparency and accountability: This theme explored how digital technologies can be used to enhance transparency and accountability in public service delivery, while also considering the potential risks to privacy; Recommendations for strengthening data governance and privacy in public service delivery: This theme sought to gather practical recommendations from the key informants on how to improve data governance and privacy in Sulu. The interviews were conducted in a private and comfortable setting to encourage the informants to speak freely and openly. Each interview was audio-recorded with the informed consent of the informant, ensuring that all relevant information was captured. The audio recordings were then transcribed verbatim, providing a rich source of qualitative data. The transcribed interviews were analyzed using thematic analysis, a qualitative data analysis technique that involves identifying patterns and themes within the data. This process involved multiple readings of the transcripts, coding the data, and grouping codes into themes. The themes were then interpreted in relation to the research questions, providing a deeper understanding of the data.

In addition to the quantitative and qualitative data collection, this study also included a policy analysis component. This involved a thorough review of relevant policies and frameworks related to data governance and privacy in the Philippines, including; The Data Privacy Act of 2012 (Republic Act No. 10173): This Act provides a comprehensive framework for the protection of personal data in the Philippines; The e-Government Master Plan 2022: This plan outlines the Philippine government's strategy for promoting digital governance and improving public service delivery through the use of ICT; The Bangsamoro Autonomy Act of 2018 (Republic Act No. 11054): This Act grants greater autonomy to the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM), including in the area of digital governance. The policy analysis focused on identifying the key provisions related to data governance and privacy in each of these policies, assessing their alignment with international best practices, and identifying any gaps or inconsistencies. This analysis provided a broader context for understanding the data governance and privacy landscape in the Philippines, as well as the specific challenges and opportunities in Sulu.

Throughout this study, ethical considerations were paramount. Informed consent was obtained from all participants prior to data collection, ensuring that they understood the purpose of the study, the procedures involved, and their rights as participants. Confidentiality and anonymity were maintained throughout the research process, with all data collected being stored securely and any identifying information removed. The study was conducted in accordance with the ethical guidelines of the researchers' institution, ensuring that the research was conducted in a responsible and ethical manner.

3. Results and Discussion

Table 1 provides a breakdown of the characteristics of the participants involved in both the quantitative and qualitative phases of the research. This allows us to understand the composition of the individuals whose perspectives and experiences informed this study; Quantitative Sample (N=300): The largest age group represented was 25-34 (30%), followed closely by 18-24 (26.7%). This indicates a strong focus on the perspectives of younger adults within the Sulu population. The smaller representation of older age groups (only 10% aged 55+) might indicate a lower level of digital engagement among this demographic, potentially due to factors like lower digital literacy or access. The gender distribution was relatively balanced, with slightly more males (53.3%) than females (46.7%) participating. This suggests a fairly equal representation of perspectives across genders in the quantitative data. A majority of the participants resided in urban areas (60%), which could indicate that urban residents have greater access to or engagement with digital public services compared to those in rural areas. A significant portion of the participants had attained a high school education (40%), followed by college or higher (33.3%). This suggests a relatively good level of education among those engaged with digital public services. However, a notable portion (26.7%) had only elementary education or no formal education, highlighting the importance of considering literacy levels in digital service design and implementation. The most common occupations among participants were farming/fishing (20%) and being unemployed (23.3%), reflecting the socio-economic context of Sulu. A smaller but significant number were employed in the public sector (10%), which could provide valuable insights into the government's perspective on digital service delivery; Qualitative Sample (N=20): The age distribution in the qualitative sample was more evenly spread across the age ranges compared to the quantitative sample, with the 35-44 age group being slightly more represented (30%). This broader age range in the qualitative sample allows for a wider range of perspectives on digital governance and privacy. Similar to the quantitative sample, there was a slightly higher proportion of males (60%) than females (40%) in the qualitative sample. A majority of the key informants were from urban areas (70%), mirroring the trend observed in the quantitative sample. This might suggest that urban areas are leading the way in digital governance initiatives or that individuals in urban areas are more likely to be involved in discussions around these issues. The vast majority of key informants (90%) had received college or higher education, indicating a high level of expertise and knowledge among this group. This is expected, as key informants are often selected based on their knowledge and experience in the field of study. The qualitative sample included a diverse range of key informants, with representation from the public sector (40%), civil society organizations (25%), technology experts (25%), and academia (10%). This diversity ensures a comprehensive understanding of the issues from various perspectives.

Table 2 presents the findings from the quantitative survey of 300 Sulu residents, offering insights into their awareness, perceptions, and experiences related to data governance and privacy in the context of digital public service delivery; Awareness of Data Governance & Privacy: While a moderate percentage (42%) were familiar with the term "data privacy," only 28% could explain its meaning. This suggests a limited understanding of data privacy concepts among Sulu residents. Over half (55%) were aware of laws protecting personal data in the Philippines, indicating some level of awareness about data protection rights; Trust in Government Institutions: A relatively low percentage (35%) trusted the government to handle their data responsibly. This indicates a significant level of distrust towards government institutions regarding data management. Similarly, only 40% believed government agencies had adequate security measures to protect their data. This reinforces the perceived lack of security and trustworthiness of government data handling practices. A large majority (78%) expressed concerns about potential data misuse by government agencies. This highlights a significant fear of data breaches or misuse, contributing to the lack of trust; Willingness to Share Personal Data: Residents showed a high willingness (85%) to share data for healthcare services and a moderate willingness (72%) for receiving government assistance. This suggests a pragmatic approach to data sharing when perceived benefits are clear. However, there was a strong reluctance (15%) to share data for commercial purposes and discomfort (22%) with private companies collecting their data. This indicates a clear distinction in how personal data is valued and trusted in different contexts; Experience with Digital Public Services: A majority (65%) had used digital platforms to access government services, suggesting a reasonable level of digital engagement among the surveyed population. While 58% found digital public services convenient, 45% experienced problems such as technical difficulties or lack of information. This highlights the need for improvements in the usability and accessibility of digital services. A significant majority (70%) were concerned about data security when using digital public services. This underscores the persistent anxiety around data protection in the digital realm.

Table 3 presents the key themes that emerged from the qualitative interviews with key informants in Sulu. These themes provide rich insights into the challenges, concerns, and opportunities related to data governance and privacy in the context of digital public service delivery in the province; Limited Digital Literacy: This theme highlights the challenge of limited digital literacy among Sulu residents. Many interviewees expressed a lack of awareness and understanding of data privacy, with some struggling to comprehend privacy policies and others falling victim to online scams. This underscores the need for educational initiatives to improve digital literacy and empower residents to protect their personal information online; Inadequate Infrastructure: This theme emphasizes the infrastructural challenges hindering digital service delivery in Sulu. Interviewees pointed to limited internet connectivity, particularly in rural areas, and a lack of access to devices such as smartphones and computers. This digital divide between urban and rural areas needs to be addressed to ensure equitable access to digital public services; Lack of Capacity: This theme focuses on the capacity challenges faced by government agencies in implementing data governance frameworks. Interviewees highlighted limited training on data governance and privacy, a lack of resources for data security, and the need for more technical support. Building capacity within government institutions is crucial for ensuring responsible and effective data management; Security Concerns: This theme captures the anxieties and concerns surrounding data security. Interviewees expressed fears of data breaches, concerns about surveillance and misuse of data by the government, and the impact of conflict on data security. These concerns underscore the need for robust data protection measures and transparent data handling practices to build trust and confidence among citizens; Opportunities for Transparency and Accountability: This theme highlights the potential of digital technologies to enhance transparency and accountability in public service delivery. Interviewees emphasized the potential for improved service delivery, increased citizen participation, and enhanced transparency through open data initiatives. These opportunities should be leveraged to foster a more open and accountable government.

Table 4 provides a useful overview of the policy landscape concerning data governance and privacy in the Philippines, specifically analyzing three key policy instruments and their alignment with international best practices; Data Privacy Act of 2012 (RA 10173): This Act provides a comprehensive framework for data protection, defining key concepts like personal and sensitive data, outlining data processing principles, and establishing rights for data subjects. It also created the National Privacy Commission (NPC) as a regulatory body. It generally aligns with international standards like the EU's General Data Protection Regulation (GDPR). The analysis reveals gaps in terms of limited enforcement capacity of the NPC, especially in remote areas like Sulu. There's also a lack of specific guidance on crucial aspects like data sharing between agencies and interoperability. The Act needs updating to address emerging technologies like AI and big data, which pose new challenges to data privacy; e-Government Master Plan 2022: This plan promotes the use of ICT for better public service delivery and emphasizes data security and privacy in digital services. It encourages open data initiatives and aligns with international trends in digital government. It lacks concrete implementation plans and timelines for data governance initiatives. There's a limited focus on crucial aspects like digital literacy and capacity building, which are essential for successful digital governance. It also needs stronger monitoring and evaluation mechanisms to ensure effective implementation; Bangsamoro Autonomy Act of 2018 (RA 11054): This Act grants greater autonomy to the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM), including in governance areas, and recognizes the importance of digital governance for regional development. It promotes digital infrastructure and e-government in the region. It lacks specific provisions on data governance and privacy within the unique context of the BARMM. Further elaboration is needed on how data governance will be coordinated between the BARMM and the national government, especially given the region's autonomy.

Table 1. Participant characteristics.

Characteristic	Quantitative (N=300)	Qualitative (N=20)
Age		
18-24	80 (26.7%)	4 (20%)
25-34	90 (30%)	5 (25%)
35-44	60 (20%)	6 (30%)
45-54	40 (13.3%)	3 (15%)
55+	30 (10%)	2 (10%)
Gender		
Male	160 (53.3%)	12 (60%)
Female	140 (46.7%)	8 (40%)
Location		
Urban	180 (60%)	14 (70%)
Rural	120 (40%)	6 (30%)
Education level		
No formal education	20 (6.7%)	-
Elementary	60 (20%)	-
High school	120 (40%)	2 (10%)
College or higher	100 (33.3%)	18 (90%)
Occupation		
Farming/Fishing	60 (20%)	-
Small business owner	40 (13.3%)	-
Employed in the public sector	30 (10%)	8 (40%)
Employed in the private sector	50 (16.7%)	2 (10%)
Unemployed	70 (23.3%)	-
Student	50 (16.7%)	-
Civil society	-	
Representative of NGO	-	5 (25%)
Community leader	-	3 (15%)
Technology expert	-	
Academic	-	5 (25%)
IT professional	-	2 (10%)

Table 2. Quantitative findings.

Construct/variable	Survey item	Mean (SD)	Percentage agree/ strongly agree
Awareness of data governance & privacy	I am familiar with the term "data privacy."	2.8 (1.2)	42%
	I can explain what data privacy means.	2.1 (1.0)	28%
	I know that there are laws in the Philippines that protect my personal data.	3.2 (1.3)	55%
Trust in government institutions	I trust the government to handle my personal data responsibly.	2.5 (1.1)	35%
	I believe that government agencies have adequate security measures in place to protect my data.	2.7 (1.2)	40%
	I am concerned that my personal data might be misused by government agencies.	3.8 (1.0)	78%
Willingness to share personal data	I am willing to share my personal data to access healthcare services.	4.5 (0.8)	85%
	I am willing to share my personal data to receive government assistance.	4.2 (0.9)	72%
	I am willing to share my personal data for commercial purposes (e.g., marketing, advertising).	1.8 (0.9)	15%
	I am comfortable with private companies collecting my personal data.	2.1 (1.0)	22%
Experience with digital public services	I have used digital platforms to access government services (e.g., online applications, e-payments).	3.5 (1.4)	65%
	I find digital public services convenient and easy to use.	3.2 (1.3)	58%
	I have experienced problems with digital public services (e.g., technical difficulties, lack of information).	2.9 (1.2)	45%
	I am concerned about the security of my personal data when using digital public services.	3.6 (1.1)	70%

Table 3. Qualitative findings - key themes and quotes.

Theme	Sub-theme	Quote	Participant type
Limited digital literacy	Lack of awareness of data privacy	"I don't really know what data privacy means. I just use Facebook and YouTube."	Resident, Urban
	Difficulty understanding privacy policies	"Those privacy policies are so long and complicated. I don't have time to read them."	Resident, Rural
	Vulnerability to online scams and misinformation	"I received a message saying I won a prize, but I had to give my bank details. I almost fell for it."	Resident, Urban
Inadequate infrastructure	Limited internet connectivity	"The internet here is very slow and unreliable. It's hard to access online services."	Resident, Rural
	Lack of access to devices	"I don't have a smartphone or computer. I have to go to the internet café to use the internet."	Resident, Rural
	Digital divide between urban and rural areas	"The internet is much better in the town center, but in the villages, it's almost non-existent."	Local Government Official
Lack of capacity	Limited training on data governance	"We need more training on how to implement the Data Privacy Act. We don't have the expertise."	Local Government Official
	Lack of resources for data security	"Our budget for IT is very limited. We can't afford to buy the latest security software."	Local Government Official
	Need for technical support	"We need more technical support from the DICT. We don't have enough IT staff."	Civil Society Representative
Security concerns	Fear of data breaches	"I'm worried that my personal information might be stolen by hackers."	Resident, Urban
	Concerns about surveillance and misuse of data	"I don't want the government to track my every move or use my data against me."	Civil Society Representative
	Impact of conflict on data security	"The security situation makes it difficult to ensure the safety of data centers and online systems."	Technology Expert
Opportunities for transparency and accountability	Potential for improved service delivery	"Digital platforms can make it easier for people to access government services and information."	Local Government Official
	Increased citizen participation	"Online platforms can be used to gather feedback from citizens and improve government responsiveness."	Civil Society Representative
	Enhanced transparency and accountability	"Open data initiatives can promote transparency and help citizens hold the government accountable."	Technology Expert

Table 4. Policy analysis findings.

Policy/Framework	Key Provisions Related to Data Governance & Privacy	Alignment with International Best Practices	Gaps/Inconsistencies
Data Privacy Act of 2012 (RA 10173)	• Defines personal data and sensitive personal information. • Set out principles for data processing (transparency, legitimate purpose, proportionality). • Establishes rights of data subjects (access, correction, deletion). • Requires data controllers to implement security measures. • Creates the National Privacy Commission (NPC) as the regulatory body.	Generally aligned with international standards, such as the EU General Data Protection Regulation (GDPR).	• Limited enforcement capacity of the NPC, especially in remote areas. • Lack of specific guidance on data sharing and interoperability between government agencies. • Needs updating to address emerging technologies and challenges (e.g., AI, big data).
e-Government Master Plan 2022	• Promotes the use of ICT to improve public service delivery. • Emphasizes data security and privacy in digital services. • Encourages open data initiatives and data sharing.	Aligned with international trends in digital government and open data.	• Lack of concrete implementation plans and timelines for data governance initiatives. • Limited focus on digital literacy and capacity building. • Needs stronger mechanisms for monitoring and evaluation.
Bangsamoro Autonomy Act of 2018 (RA 11054)	• Grants the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM) greater autonomy in governance. • Includes provisions on promoting digital infrastructure and e-government in the region.	Recognizes the importance of digital governance in regional development.	• Lacks specific provisions on data governance and privacy within the BARMM context. • Needs further elaboration on how data governance will be coordinated between the BARMM and the national government.

The study reveals a concerning lack of awareness and understanding regarding data privacy among Sulu residents. This is not merely a matter of unfamiliarity with technical terms but reflects a deeper lack of comprehension regarding the implications of sharing personal data in the digital age. Many residents struggle to grasp the concept of data privacy and its significance in the context of online interactions and digital public services. This lack of awareness creates significant vulnerabilities. Residents who do not fully understand data privacy are more susceptible to data breaches, online scams, and the spread of misinformation. They may unknowingly share sensitive information with malicious actors or fall prey to phishing attempts and other online scams designed to exploit their lack of knowledge. The qualitative data provides compelling evidence of this challenge. One resident admitted, "I don't really know what data privacy means. I just use Facebook and YouTube." This statement reflects a common sentiment among many residents who engage with online platforms without fully comprehending the potential risks to their personal data. Another resident expressed difficulty understanding privacy policies, stating, "Those privacy policies are so long and complicated. I don't have time to read them." This highlights the challenge of presenting complex data privacy information in an accessible and understandable format, particularly for individuals with limited digital literacy. This finding aligns with existing literature on digital governance in developing countries, which consistently highlights the challenges posed by low levels of digital literacy. In such contexts, individuals may have limited exposure to technology and digital concepts, hindering their ability to fully comprehend the implications of sharing personal data online or the potential risks involved. The study's findings underscore the urgent need for targeted interventions to improve digital literacy and empower individuals to make informed decisions about their data. Increasing awareness of data privacy concepts and the importance of protecting personal information online. Presenting data privacy information in clear, concise, and accessible language, avoiding technical jargon and complex legal terms. Encouraging individuals to critically evaluate online information and be cautious about sharing personal data with unknown sources. Equipping individuals with practical skills to manage their online privacy, such as creating strong passwords, recognizing phishing attempts, and adjusting privacy settings on social media platforms (Gersing et al., 2024; Veil, 2023).

Sulu's unique geographical characteristics pose significant challenges for infrastructure development and connectivity. As an archipelago province, Sulu comprises numerous islands, making it difficult and expensive to establish and maintain reliable internet infrastructure. This geographical remoteness, combined with the fragmented island structure, results in limited internet connectivity, particularly in rural areas. The study found that many residents, especially those in rural areas, lack access to reliable internet and digital devices. This digital divide between urban and rural areas exacerbates existing inequalities and hinders the effective implementation of digital governance initiatives. The qualitative data provides further evidence of these infrastructure challenges. One resident explained, "The internet here is very slow and unreliable. It's hard to access online services." This statement highlights the difficulties faced by many residents in accessing and utilizing digital public services due to poor internet connectivity. Another resident described the lack of access to digital devices, stating, "I don't have a smartphone or computer. I have to go to the internet café to use the internet." This illustrates the additional barrier faced by those who lack the necessary devices to access the internet, further limiting their ability to participate in the digital realm. In addition to infrastructure challenges, the study also revealed capacity constraints within government agencies responsible for implementing data governance frameworks. Limited training on data governance and privacy, coupled with a lack of resources for data security, hinders their ability to effectively manage and protect citizen data. The qualitative data sheds light on these capacity constraints. One local government official admitted, "We need more training on how to implement the Data Privacy Act. We don't have the expertise." This statement reflects the need for capacity building within government institutions to ensure they have the necessary knowledge and skills to implement data governance frameworks effectively.

Another official highlighted the lack of resources for data security, stating, "Our budget for IT is very limited. We can't afford to buy the latest security software." This underscores the resource constraints faced by government agencies, particularly in developing countries, which can limit their ability to invest in essential data security measures. These findings resonate with studies highlighting the challenges of implementing digital governance in resource-constrained environments. The lack of adequate infrastructure and capacity can undermine the effectiveness of data governance initiatives and exacerbate existing inequalities. Expanding internet connectivity, particularly in rural and underserved areas, through initiatives such as laying fiber optic cables, establishing community internet centers, and subsidizing internet access for low-income households. Promoting affordable access to digital devices, such as smartphones and computers, through initiatives such as government subsidies, partnerships with technology companies, and digital literacy programs that incorporate device distribution. Investing in capacity building programs for government officials, providing training on data governance, privacy, and data security best practices. Increasing resource allocation for data security, enabling government agencies to invest in essential security software, hardware, and personnel. Providing technical support to government agencies, particularly those in remote areas, through initiatives such as establishing help desks, online resources, and partnerships with technology experts (Delacroix, 2019; Mutemaringa, 2024; Ni Loideain, 2017).

The study reveals a significant level of security concerns and a trust deficit between the government and citizens regarding the handling of personal data. Sulu's history of conflict and security concerns has created a context where anxieties about data misuse are heightened. Many residents expressed concerns about various data security threats, including data breaches, surveillance, and the government's ability to adequately protect their data. The qualitative data provides valuable insights into these security concerns. One civil society representative expressed a strong concern about government surveillance, stating, "I don't want the government to track my every move or use my data against me." This statement reflects a broader concern among many residents about the potential for data to be used for purposes beyond its original intent. Another interviewee highlighted the fear of data breaches, stating, "I'm worried that my personal information might be stolen by hackers." This concern is particularly relevant in the context of Sulu, where the capacity for data protection may be limited, increasing the risk of data breaches. The trust deficit is further compounded by the lack of robust oversight mechanisms and limited enforcement of data protection laws. While the Philippines has a national Data Privacy Act, the study found that its implementation at the local level in Sulu remains limited. This lack of effective oversight and enforcement can undermine trust in the government's ability to protect citizen data. These findings are consistent with research highlighting the critical role of trust in digital governance. Citizens are more likely to engage with digital services and share personal data if they trust that their data will be handled responsibly and securely. Building and maintaining this trust is essential for the successful implementation of digital governance initiatives. Implementing strong data protection measures, such as encryption, access controls, and regular security audits, to safeguard citizen data. Being transparent about data collection practices, including the purpose of data collection, how data is used, and with whom it is shared. Establishing clear accountability mechanisms for data handling, ensuring that those who misuse data are held responsible. Implementing robust oversight mechanisms to monitor data handling practices and enforce data protection laws. Providing accessible redressal mechanisms for citizens to report data breaches or misuse and seek remedies (Mourby, 2019;

Yakovleva, 2020).

Despite the challenges identified in the study, the key informants also highlighted significant opportunities for leveraging digital technologies to improve governance in Sulu. Digital platforms have the potential to enhance service delivery, particularly for those in remote areas with limited access to traditional government services. By providing online access to government services, such as permit applications, license renewals, and information dissemination, Sulu can overcome geographical barriers and ensure that all citizens have equal opportunities to engage with the government. Digital technologies can also be used to increase citizen participation in government decision-making processes. Online platforms can facilitate citizen feedback, enabling residents to share their opinions, concerns, and suggestions with government officials. This increased citizen participation can lead to more responsive and accountable governance, as government officials can better understand the needs and priorities of the communities they serve. Furthermore, digital technologies can promote transparency and accountability in government operations. Open data initiatives, which involve making government data publicly available in accessible formats, can empower citizens to hold the government accountable for its actions. By providing access to government data, such as budget information, spending reports, and performance metrics, Sulu can promote transparency and build public trust. The qualitative data provides further evidence of these opportunities. One local government official highlighted the potential for digital platforms to improve service delivery, stating, "Digital platforms can make it easier for people to access government services and information." Another interviewee emphasized the importance of increased citizen participation, stating, "Online platforms can be used to gather feedback from citizens and improve government responsiveness." A technology expert highlighted the potential of open data initiatives, stating, "Open data initiatives can promote transparency and help citizens hold the government accountable." These findings underscore the transformative potential of digital technologies for governance. By embracing a citizen-centric approach and prioritizing data governance and privacy, Sulu can harness the power of digital technologies to improve public service delivery and promote good governance. Expand internet connectivity and access to digital devices, particularly in rural areas, to ensure that all citizens can participate in the digital realm. Design online government services that are accessible, user-friendly, and tailored to the needs of diverse communities. Implement digital literacy programs to empower citizens with the knowledge and skills to navigate digital platforms and engage with online government services. Establish online platforms and mechanisms for gathering citizen feedback, ensuring that residents have a voice in government decision-making processes. Make government data publicly available in accessible formats, promoting transparency and empowering citizens to hold the government accountable (Alanoca, 2021; Bloemendal, 2021; Wennäkoski, 2022).

4. Conclusion

This study underscores the imperative of nuanced data governance and privacy strategies within the unique socio-political landscape of Sulu, Philippines. The findings highlight a complex interplay of factors influencing trust and accountability in digital public service delivery. It is evident that a mere replication of national policies is inadequate, instead, context-specific approaches are critical, taking into account the multifaceted challenges and opportunities revealed in the research. The relatively low levels of digital literacy and the pervasive concerns about data security necessitate focused educational initiatives and capacity-building programs. Empowering citizens with the knowledge and skills to navigate the digital realm safely and effectively is paramount. Simultaneously, government agencies require support in implementing robust data protection measures and ensuring transparent data handling practices. Addressing the infrastructural deficits, particularly in remote areas, is crucial for ensuring equitable access to digital public services. Bridging the digital divide demands a concerted effort to expand internet connectivity and promote the availability of digital devices. The study's findings also call for strengthening oversight mechanisms and fostering a culture of accountability within government institutions. Despite the challenges, the identified opportunities emphasize the transformative potential of digital technologies for Sulu. By prioritizing community engagement, capacity building, and robust oversight mechanisms, Sulu can harness the power of digital technologies to enhance public service delivery, promote transparency, and foster trust between the government and its citizens. The insights generated by this study have implications beyond Sulu, offering valuable lessons for policymakers and practitioners in regions grappling with similar challenges. The study underscores the importance of context-specific strategies that prioritize ethical and responsible data governance, ensuring that the benefits of digital technologies are accessible to all.

5. References

Al-Abdullah M, Alsmadi I, AlAbdullah R, Farkas B. 2020. Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. Digital Policy, Regulation and Governance. 22(5/6): 389–411.

Alanoca S, Guetta-Jeanrenaud N, Ferrari I, Weinberg N, Çetin RB, Miailhe N. 2021. Digital contact tracing against COVID-19: a governance framework to build trust. International Data Privacy Law. 11(1): 3–17.

Bloemendal MT. 2021. On the advent of environmental, social and governance reporting and its intersection with privacy. Journal of Data Protection & Privacy. 5(1): 39.

Carter SE. 2022. A value-centered exploration of data privacy and personalized privacy assistants. Digital Society. 1(3):27.

Delacroix S, Lawrence ND. 2019. Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law.

Gersing K, Michael S, Prior F, Saltz J, Moffitt R, Rogovin S, et al. 2024. Implementing data governance with multi-modal privacy-preserving record linkages between restricted and public open enclaves. International Journal Population Data Science. 9(5).

Karyda M, Mavriki PV. 2019. Big data in political communication: Implications for group privacy. International Journal of Electronic Government 11(3): 1.

Mavriki PV, Karyda M. 2022. Big data analytics in e-government and e-democracy applications: privacy threats, implications and mitigation. International Journal of Electronic Governance. 14(1/2): 1.

McCarthy N, Fourniol F. 2020. The role of technology in governance: The example of Privacy Enhancing Technologies. Data Policy. 2(e8).

Morris C, Grey A. 2018. NHS Scotland Public Benefit and Privacy Panel (PBPP) – does a proportionate governance review work? International Journal Population Data Science. 3(4).

Mourby M, Gowans H, Aidinlis S, Smith H, Kaye J. 2019. Governance of academic research data under the GDPR—lessons from the UK. International Data Privacy Law. 9(3): 192–206.

Mutemaringa T, Boulle A, Tiffin N. 2024. Data governance for ethical usage of linked routine health data in South Africa: balancing privacy and data sharing. International Journal Population Data Science. 9(5).

Ni Loideain N. 2017. Cape Town as a smart and safe city: implications for governance and data privacy. International Data Privacy Law. 7(4): 314–34.

Schneider D. 2022. Ensuring privacy and confidentiality in social work through intentional omissions of information in client information systems: a qualitative study of available and non-available data. Digital Society. 1(3): 26.

Stoll M. A data privacy governance model. International Journal of IT/Business Alignment and Governance. 2019; 10(1): 74–93.

Thillaivasan D, Wickramasinghe CN. 2022. Reassessing privacy, fairness and governance in the age of algorithms and the impact on society and institutions. International Journal Data Science. 7(2): 121.

Veil W. 2023. Der Data Governance Act und sein Verhältnis zum Datenschutzrecht – Teil I. PinG. (1).

Wennäkoski AA. 2022. New directions for data governance in health data? Examining the role of anonymisation and pseudonymisation. Journal of Data Protection & Privacy. 5(2): 138.

Yakovleva S, Irion K. 2020. Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. International Data Privacy Law. 10(3): 201–21.