DATA SECURITY CONCERNS: MISUSE AND FRAUD IN COLLECTION AND CIRCULATION OF CITIZENS' DATA

Anmol Nahar, LL.M. Data Science and Data Protection Law (2024-2026)

This document contains confidential research findings and analysis on data security vulnerabilities, privacy concerns, and fraudulent practices related to citizen data management. All contents are subject to academic review and validation.

INTRODUCTION

In the digital age, personal data has emerged as a critical resource that fuels technological innovation while simultaneously creating unprecedented privacy and security challenges. The mass collection, storage, processing, and circulation of citizens' data by both governmental and private entities has raised significant concerns about potential misuse, fraud, and exploitation. As digital footprints expand and data collection becomes more sophisticated, citizens face growing vulnerability to data breaches, identity theft, financial fraud, and other forms of data misuse. The evolving landscape of data protection is characterized by regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which attempt to establish standards for responsible data handling. However, questions persist regarding the practical effectiveness of these regulations in preventing fraud and misuse, the adequacy of data handling practices across sectors, the emergent challenges posed by artificial intelligence and advanced analytics, and the real-world impacts of data misuse on individual citizens. This research paper presents findings from an empirical study examining citizens' perceptions, experiences, and concerns regarding data security across multiple dimensions. By analysing survey responses from diverse professional backgrounds, the study aims to provide insights into the gap between regulatory intent and practical implementation, illuminate specific vulnerabilities in current data protection ecosystems, and identify potential pathways toward more effective safeguarding of citizens' data.

CONCEPTUALISATION

Data Protection Laws are legal frameworks designed to regulate the collection, processing,

storage, and sharing of personal data, including provisions for individual rights, organizational responsibilities, and enforcement mechanisms. Data Misuse refers to utilization of personal data in ways that exceed stated purposes, violate privacy expectations, or contravene legal requirements, including unauthorized access, processing, or sharing. Data Fraud encompasses deceptive practices involving personal data that result in financial, reputational, or other forms of harm to individuals, including identity theft, financial fraud, and social engineering. Data Security consists of technical and organizational measures implemented to protect personal data against unauthorized access, accidental loss, or deliberate exploitation. Transparency refers to the extent to which data collection and usage practices are clearly disclosed and comprehensible to individuals whose data is being processed. Artificial Intelligence in Data Processing involves the application of machine learning, natural language processing, and other AI technologies to analyse, categorize, predict, or otherwise process personal data at scale.

This study approaches data security concerns through a multi-dimensional framework that examines several interconnected aspects. Regulatory Effectiveness addresses the gap between theoretical protections offered by data protection laws and their practical implementation and enforcement. Institutional Data Governance focuses on the practices, policies, and infrastructure employed by government and private entities to safeguard data they collect and process. Technological Factors explore the impact of emerging technologies, particularly AI, on data vulnerability and security risks. Individual Experience and Response investigates how citizens experience data misuse and adapt their behaviours to protect their personal information. These dimensions are interconnected, with regulatory frameworks shaping institutional practices, technological developments influencing both regulation and governance, and individual experiences providing feedback that may drive further regulatory and institutional evolution.

RESEARCH QUESTIONS AND OBJECTIVES

This study is guided by four primary research questions that align with the central dimensions of data security concerns identified in our conceptual framework:

i. How effective do respondents perceive data protection laws to be, given that only 24.7% have exercised their rights under these laws and 66.3% report seeing only slight improvements in data privacy since their implementation?

This research question examines the perceived efficacy of regulatory frameworks from the citizen perspective, exploring the gap between theoretical protections and practical implementation. It investigates awareness levels, rights exercise patterns, perceptions of improvement, and views on accountability mechanisms to provide a comprehensive assessment of regulatory effectiveness.

ii. What are respondents' main concerns regarding data handling practices, considering that 58.4% believe their data is only somewhat securely stored and 73% feel there isn't enough transparency about how their data is used?

This research question focuses on institutional practices and governance approaches, examining perceptions of security, transparency, consent mechanisms, and organizational responsibilities. It seeks to identify specific trust deficits and priority concerns that might inform improved institutional approaches to data handling.

iii. How does AI impact data security concerns, considering that 88.8% of respondents believe AI has increased risks of data misuse and identify social media and financial services as the sectors facing highest risk?

This research question addresses technological dimensions of data security, particularly the emergent challenges posed by artificial intelligence applications. It explores understanding of AI technologies, risk perceptions across sectors, identified regulatory gaps, and preferred policy measures to manage AI-specific security concerns.

iv. What types of data misuse do respondents experience most frequently, and how do these experiences influence their protective behaviours, given that 40.4% report being victims of data misuse and financial fraud is considered to have the greatest impact?

This research question examines individual experiences with data misuse, including victimization patterns, breach attribution, resolution experiences, and resulting protective behaviours. It aims to connect abstract security concerns with concrete personal impacts to understand how experiences shape attitudes and practices.

Building on these research questions, the study pursues four specific objectives. First, to evaluate the perceived effectiveness of data protection laws in preventing fraud and misuse by

examining awareness, rights exercise, and observed improvements in data privacy practices. Second, to identify key concerns regarding data handling practices by government and private entities by assessing perceptions of security, transparency, consent mechanisms, and priorities for improvement. Third, to analyse the perceived impact of artificial intelligence on data security concerns by examining risk perceptions, sector vulnerabilities, regulatory gaps, and policy preferences related to AI-driven data processing. Fourth, to document common types and impacts of personal data misuse and fraud by identifying prevalence patterns, resolution experiences, perceived impacts, and resulting protective behaviours. Through these objectives, the research seeks to provide evidence-based insights that can inform policy development, organizational practices, and individual decision-making regarding data security.

SUMMARY OF RELEVANT LITERATURE

The literature on data protection regulation reveals an evolving landscape shaped by competing principles and implementation challenges. Hoofnagle et al. (2019) examined the GDPR's first year of implementation, noting significant gaps between regulatory aspiration and practical compliance. Their research identified enforcement limitations, complex compliance requirements, and varying interpretations across EU member states as key challenges. Similarly, Solove and Schwartz (2019) compared the GDPR with the CCPA, highlighting how the latter's more limited scope and opt-out (rather than opt-in) consent model potentially reduces its effectiveness. They noted that while both frameworks establish individual rights, their practical exercise remains cumbersome for most citizens. Bamberger and Mulligan (2015) explored the organizational response to privacy regulation, finding that many companies adopt "compliance-oriented" rather than "protection-oriented" approaches, focusing on minimal legal compliance rather than substantive data protection. This compliance-oriented approach often results in complex privacy policies and consent mechanisms that technically satisfy legal requirements while failing to provide meaningful transparency or control.

Research on institutional data handling practices has identified significant variations in security approaches and transparency. Martin and Murphy (2017) examined consumer responses to data practices, finding that perceived transparency significantly influenced trust. Their research suggested that organizations frequently underestimate the importance of clear explanations about data usage. Acquisti et al. (2016) demonstrated through experimental

studies that even privacy-conscious individuals often make decisions that compromise their data due to cognitive biases, information asymmetries, and immediate gratification effects. This "privacy paradox" helps explain why protective behaviours often lag behind stated privacy concerns. Technical research by Zimmeck et al. (2019) found widespread inconsistencies between stated privacy policies and actual data collection practices across mobile applications and websites, suggesting significant transparency deficits in real-world implementations. Their automated analysis of privacy policies revealed frequent ambiguity, incompleteness, and contradictions.

The integration of AI technologies into data processing systems presents novel challenges documented in recent literature. Barocas and Selbst (2016) analysed how machine learning techniques can circumvent traditional privacy protections through inference and re-identification techniques, potentially compromising anonymized data. Papernot et al. (2018) explored the vulnerability of AI systems to adversarial attacks that can manipulate outcomes or extract protected information, highlighting new security challenges in AI-driven data systems. Their work demonstrated how conventional security measures may be insufficient against these specialized threats. Taddeo et al. (2019) examined ethical and governance frameworks for AI, noting significant regulatory gaps particularly regarding automated decision-making, algorithmic transparency, and accountability mechanisms. They advocated for "ethics by design" approaches that incorporate protective measures at the development stage rather than as after-the-fact considerations.

The literature on personal experiences with data misuse reveals widespread impacts across multiple dimensions. Solove (2006) developed a taxonomy of privacy harms that extends beyond financial loss to include psychological, social, and relational impacts of privacy violations. Empirical work by Ponemon Institute (2020) documented the rising costs of data breaches to both organizations and individuals, including direct financial losses, remediation costs, and long-term reputational damage. Their longitudinal studies show increasing breach severity and complexity of resolution. Calo (2014) conceptualized "privacy harm" as both objective (actual damages) and subjective (perception of vulnerability), arguing that both dimensions require legal recognition. This dual conception helps explain why individuals may experience significant distress even when financial or material harm is limited. Research by Keith et al. (2017) on protective behaviours demonstrated that individuals tend to adopt simple security measures (like password management) more readily than comprehensive approaches

to privacy protection. Their work showed significant gaps between technical best practices and typical user behaviours.

Research Gap

While existing literature provides valuable insights into particular aspects of data security, significant gaps remain in understanding the interrelationships between regulatory frameworks, institutional practices, technological evolution, and individual experiences. In particular, empirical research linking citizens' perceptions of data protection effectiveness to their experiences with data misuse remains limited. This study addresses this gap by examining these dimensions comprehensively through empirical data collection, specifically investigating how perceptions of data protection laws correlate with experiences of misuse, concerns about institutional data handling, and attitudes toward emerging technologies like AI.

OBJECTIVES OF THE STUDY

The primary aim of this research is to assess citizens' perceptions and experiences regarding data security concerns, with particular focus on the collection and circulation of personal data by various entities. The study pursues four specific objectives. First, to evaluate the perceived effectiveness of data protection laws in preventing fraud and misuse by examining awareness, rights exercise, and observed improvements in data privacy practices. Second, to identify key concerns regarding data handling practices by government and private entities by assessing perceptions of security, transparency, consent mechanisms, and priorities for improvement. Third, to analyse the perceived impact of artificial intelligence on data security concerns by examining risk perceptions, sector vulnerabilities, regulatory gaps, and policy preferences related to AI-driven data processing. Fourth, to document common types and impacts of personal data misuse and fraud by identifying prevalence patterns, resolution experiences, perceived impacts, and resulting protective behaviours. Through these objectives, the research seeks to provide evidence-based insights that can inform policy development, organizational practices, and individual decision-making regarding data security.

METHODOLOGY

This study employed a quantitative research design utilizing a structured survey instrument to

collect empirical data. The design was selected to enable systematic measurement of perceptions, experiences, and behaviours across a diverse sample, allowing for identification of patterns and relationships between variables. The research was conducted online, allowing for geographical diversity among respondents. While specific geographic information was not collected to preserve anonymity, the survey was designed to capture perspectives from individuals subject to various data protection regimes. The target population comprised adults from diverse professional backgrounds who interact with digital systems that collect and process personal data. The study aimed to capture perspectives from individuals with varying levels of technical knowledge and professional exposure to data handling practices. A non-probability convenience sampling method was employed, with the survey distributed through professional networks and online platforms. While this approach limits generalizability, it allowed access to respondents with diverse professional perspectives on data security issues. The final sample consisted of 89 respondents representing multiple professional categories, including legal professionals (lawyers, advocates), technology professionals (software engineers, IT consultants), educators (teachers, professors), healthcare professionals (doctors, psychologists), financial sector workers (bankers, analysts), students and others. Demographic diversity was reflected in the sample's age distribution with 18-25 at 28.1%, 26-35 at 42.7%, 36-45 at 19.1%, 46-55 at 7.9%, and 56+ at 2.2%. The sample included gender diversity, with representation across gender identifications.

Data was collected through a structured online questionnaire consisting of 28 questions across several categories including demographic information (age, gender, occupation), knowledge and awareness of data protection concepts, perceptions of data protection laws and their effectiveness, concerns about data handling practices, attitudes toward AI and cybersecurity, and personal experiences with data misuse and protective behaviours. The questionnaire included multiple-choice questions, Likert-scale items, and select-all-that-apply options to capture nuanced responses across topics. The survey was conducted anonymously to encourage candid responses about potentially sensitive experiences with data misuse. Quantitative analysis was conducted on the survey responses, examining frequency distributions across response categories and identifying patterns in perceptions and experiences. The analysis focused particularly on relationships between awareness of data protection laws and exercise of associated rights, perceptions of data security and transparency concerns, AI risk perceptions and policy preferences, and personal experiences with data

misuse and resulting protective behaviours. Findings were organized according to the four research objectives to provide structured insights into each dimension of data security concern.

FINDINGS OF THE STUDY

Effectiveness of Data Protection Laws in Preventing Fraud & Misuse

The study found that awareness of data fraud concepts is widespread but not comprehensive. Research reveals that 59.6% of respondents reported being "somewhat familiar" with the concept of data fraud, while 34.8% described themselves as "very familiar" with data fraud concepts. Only a small minority of 5.6% reported being "not familiar" with data fraud as a concept. This finding suggests a general awareness of data fraud as a phenomenon, providing context for evaluating perceptions of protective measures. Knowledge of specific data protection laws showed more variation among respondents. The survey found that 42.7% reported being "somewhat familiar" with data protection laws such as GDPR or CCPA, and 33.7% were "very familiar" with these legal frameworks. However, nearly a quarter (23.6%) were "not familiar" with data protection laws. This distribution indicates moderate awareness of legal frameworks, though a substantial minority lacks familiarity, potentially limiting their ability to exercise associated rights. Despite moderate awareness of legal frameworks, actual exercise of data protection rights was limited among survey respondents. Only 24.7% of respondents had ever exercised their rights under data protection laws, while the vast majority (75.3%) had never done so. Among those who had exercised their rights, the most frequently cited domains were requesting data deletion, accessing stored information, addressing unnecessary data storage, and managing privacy settings. This significant gap between awareness and action suggests potential barriers to the practical exercise of data protection rights. Respondents expressed limited confidence in improvements resulting from data protection laws. The majority (66.3%) reported seeing only "slight improvement" in data privacy and security since the implementation of these laws. A substantial portion (30.3%) observed "no improvement" whatsoever, while only a small minority (3.4%) perceived "significant improvement." This finding suggests widespread scepticism about the practical impact of data protection regulations, despite their theoretical protections. Regarding organizational accountability for data breaches under existing laws, the research found that the majority of respondents indicated that organizations are only "occasionally" held accountable for data security failures. Few respondents reported seeing consistent accountability in

practice, while a considerable portion perceived rare or non-existent accountability for data breaches. This perception of limited accountability may contribute to scepticism about regulatory effectiveness and warrants attention in enforcement strategies.

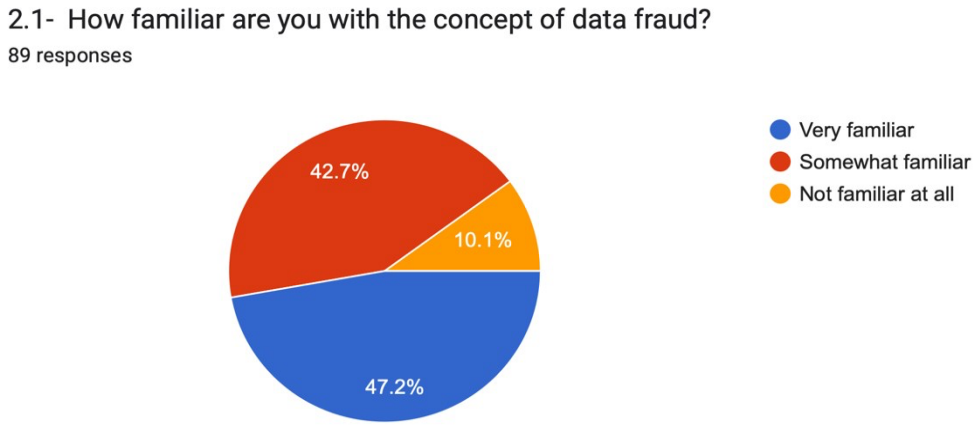

Fig.1

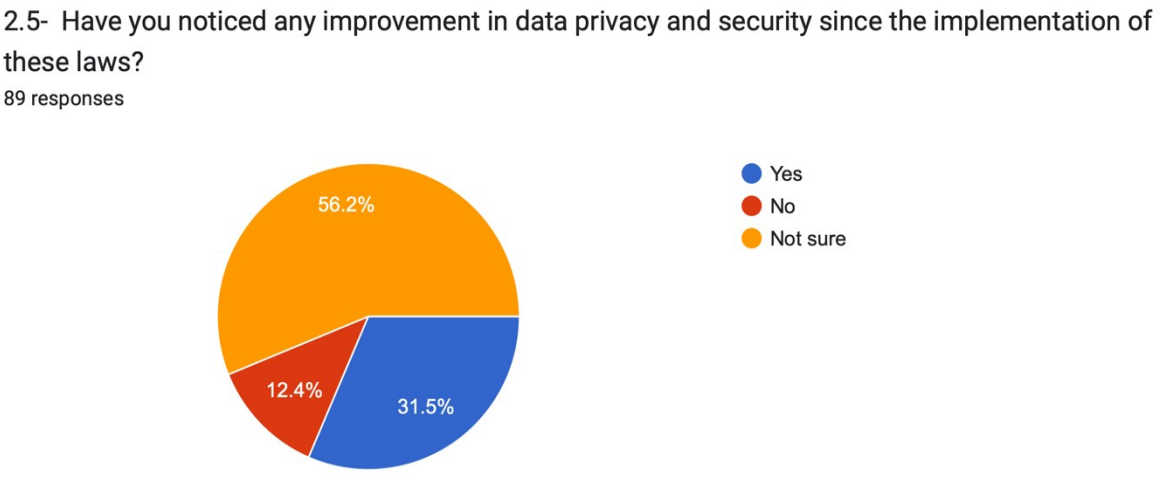

Fig.2

Fig.3

Data Handling by Government and Private Entities

Respondents demonstrated awareness of extensive data collection practices, with particular concern about various types of personal information. The most concerning categories included contact information (88.8%), financial data (87.6%), browsing history (85.4%), personal preferences (78.7%), location data (77.5%), and biometric information (51.7%). This finding indicates recognition of broad data collection practices spanning multiple categories of personal information, with highest concern for immediately identifiable personal and financial details. The survey revealed significant concerns about secure data storage practices across both government and private entities. A majority of respondents (58.4%) believed these entities store their data only "somewhat securely," while a substantial minority (31.5%) believed their data is "not stored securely at all." Only a small percentage (10.1%) expressed confidence that their data is stored "very securely." This distribution indicates a substantial trust deficit regarding data security practices, with particularly low confidence in comprehensive security measures. Concerns about transparency were even more pronounced than security concerns among respondents. Nearly three-quarters (73%) of respondents believed there is not enough transparency about how their data is stored and used by organizations, while only 27% perceived sufficient transparency in current practices. This finding suggests that transparency deficits may be a more significant concern than security vulnerabilities, highlighting the importance of clear communication about data practices.

The survey revealed overwhelming support for permission-based data sharing among respondents. An overwhelming majority (94.4%) believed companies and governments should be legally required to ask for permission before sharing data with third parties, while only a small minority (5.6%) did not support such requirements. This near-consensus indicates strong public support for consent-based approaches to data governance and suggests significant alignment between public opinion and consent-oriented regulatory frameworks. Similarly, there was strong support for data deletion rights among survey respondents. A substantial majority (78.7%) supported the "right to be forgotten" concept without qualification, while an additional 20.2% supported it with some limitations. Only a negligible percentage (1.1%) opposed this right entirely. This finding indicates strong public support for comprehensive data deletion rights, exceeding even the strong support for permission requirements and suggesting broad public alignment with this aspect of modern data protection frameworks.

When identifying their biggest concerns about large-scale data collection, respondents prioritized several key issues. Unauthorized access to sensitive information was the top concern (74.4%), followed by commercial exploitation without consent (59.3%), potential for identity theft (57%), manipulation through targeted content (37.2%), and government surveillance (26.7%). These priorities indicate that security and consent concerns outweigh surveillance concerns for most respondents, suggesting that data protection efforts should prioritize security measures and consent mechanisms. When asked about willingness to pay for enhanced privacy protection, respondents showed mixed attitudes. The largest group (40.4%) would "maybe" pay for services guaranteeing complete data privacy, while smaller proportions would definitely pay (30.3%) or would not pay (29.2%). This distribution suggests moderate market potential for privacy-enhancing services, though price sensitivity and perceived value would be important factors in the actual uptake of such services.

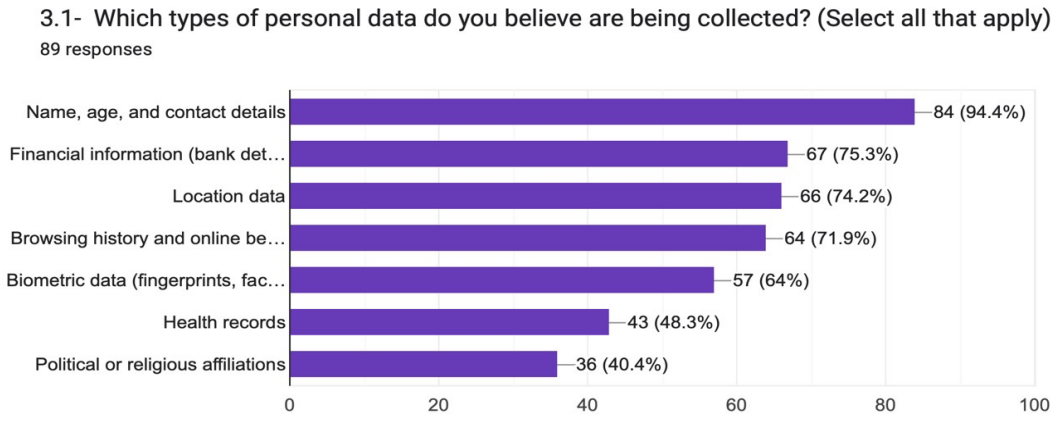

Fig.4

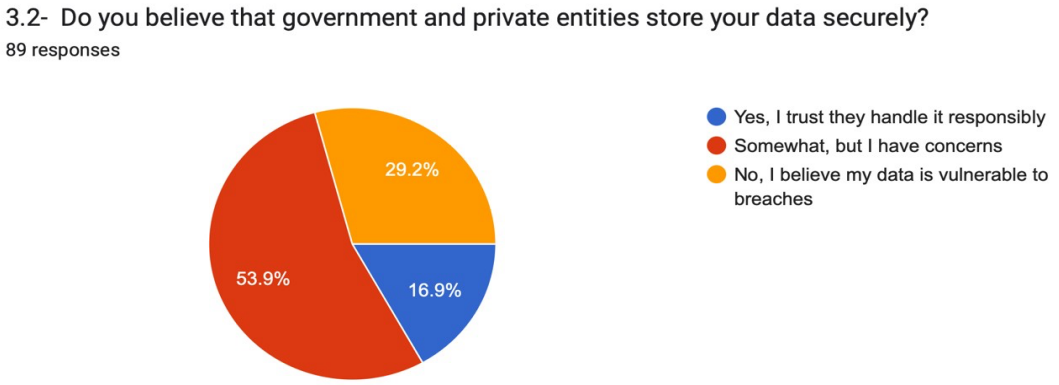

Fig.5

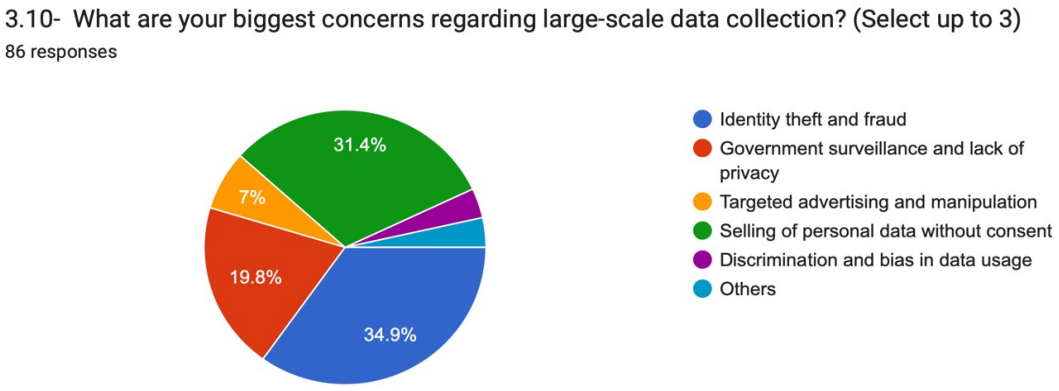

Fig.6

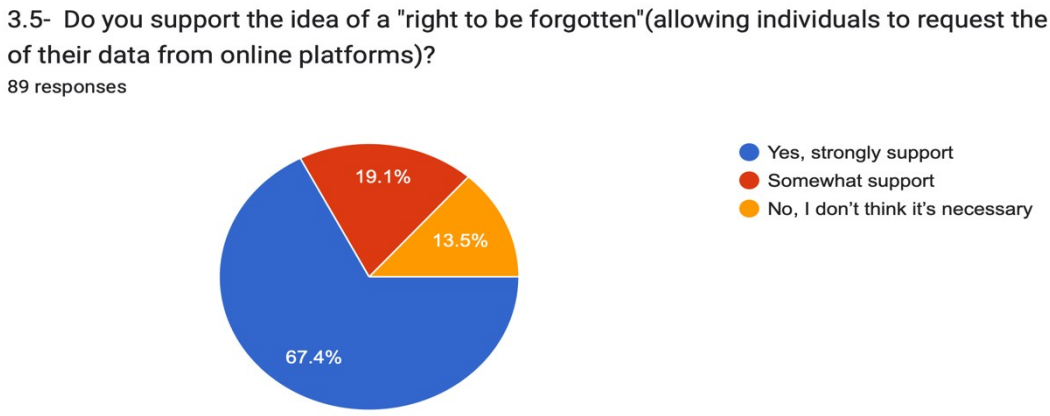

Fig.7

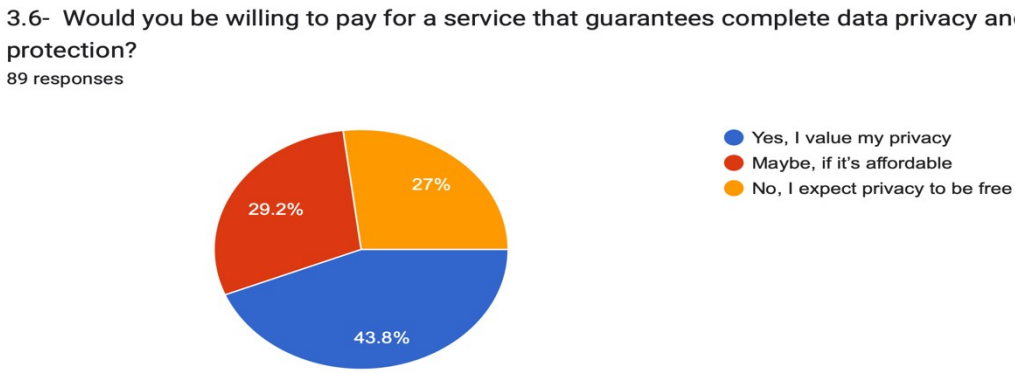

Fig.8

Cybersecurity and AI

Respondents demonstrated varied conceptions of artificial intelligence technologies. The largest portion (40.4%) viewed AI as "technology that can learn and make decisions," while others understood it as "automation of human-like intelligence" (24.7%), "advanced algorithms that process data" (23.6%), or "robots and machine intelligence" (11.2%). This diversity of understanding provides context for interpreting AI-related security concerns and suggests that perceptions may be shaped by different conceptualizations of what AI entails. Despite varied understanding of AI technologies, respondents expressed overwhelming concern about AI's impact on data security. An overwhelming majority (88.8%) believed AI has increased the risks of data misuse and fraud, while only a small minority (11.2%) did not

perceive increased risk. This near-consensus suggests widespread concern about AI's potential to amplify existing data security vulnerabilities, regardless of specific understanding of AI technologies. When identifying sectors at highest risk from AI-driven data misuse, respondents showed varied concerns across different domains. Social media was identified as highest risk by 30.3% of respondents, followed by financial services (28.1%), government (16.9%), healthcare (15.7%), and education (9%). This distribution highlights particular concern about social media and financial applications of AI, potentially reflecting greater public awareness of these applications or perception of greater potential harm in these sectors.

Respondents identified several regulatory gaps in AI-driven cybersecurity that require attention. The most frequently cited gaps were lack of clear guidelines and technical standards (67.4%), insufficient penalties for non-compliance (55.1%), limited specialist knowledge among regulators (52.8%), and inadequate international coordination (47.2%). These findings suggest the need for more comprehensive, technically-informed, and internationally coordinated regulatory approaches to AI security, with particular attention to technical standards and enforcement mechanisms. Despite concerns, respondents expressed cautious optimism about AI's compatibility with cybersecurity. A majority (67.4%) believed AI and cybersecurity can "possibly" coexist effectively, while 27% were definitely confident in their coexistence. Only a small minority (5.6%) believed effective coexistence is impossible. This suggests openness to solutions that mitigate AI risks rather than rejection of AI technologies altogether, indicating potential support for balanced regulatory approaches that enable beneficial AI applications while managing security risks. The most supported measures were regular security audits and compliance checks (74.2%), explicit user consent requirements (70.8%), mandatory data protection impact assessments (61.8%), clear data minimization standards (57.3%), and international regulatory coordination (41.6%). These preferences indicate support for comprehensive oversight combining technical verification, user control, and impact assessment, with particular emphasis on ongoing verification of security measures and explicit consent requirements.

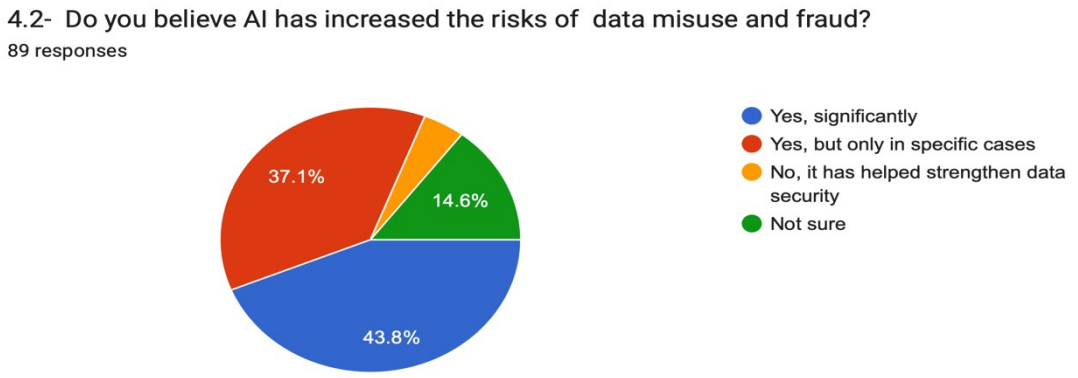

Fig.9

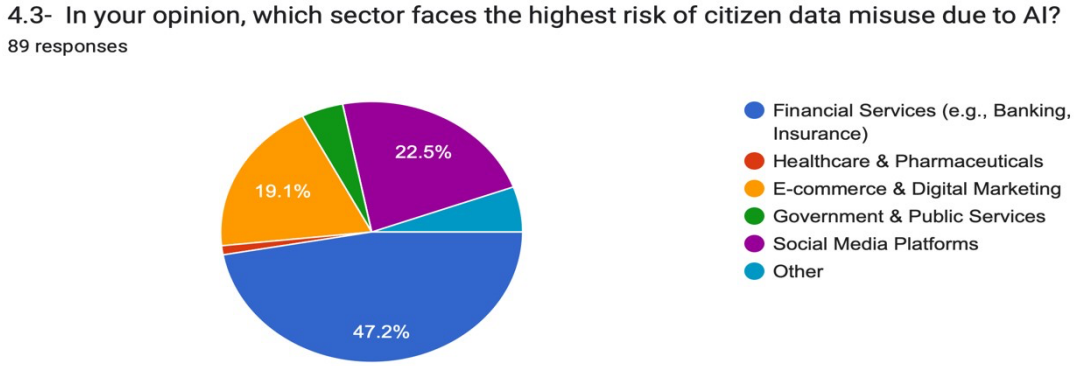

Fig.10

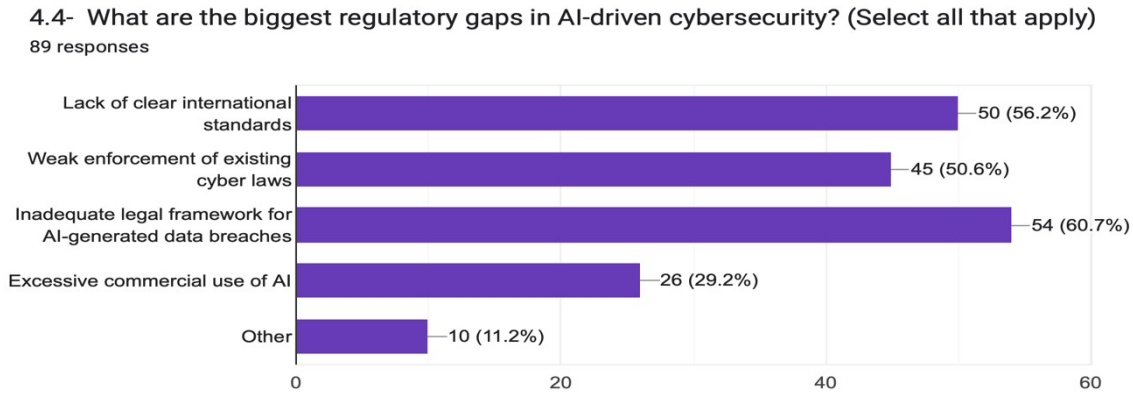

Fig.11

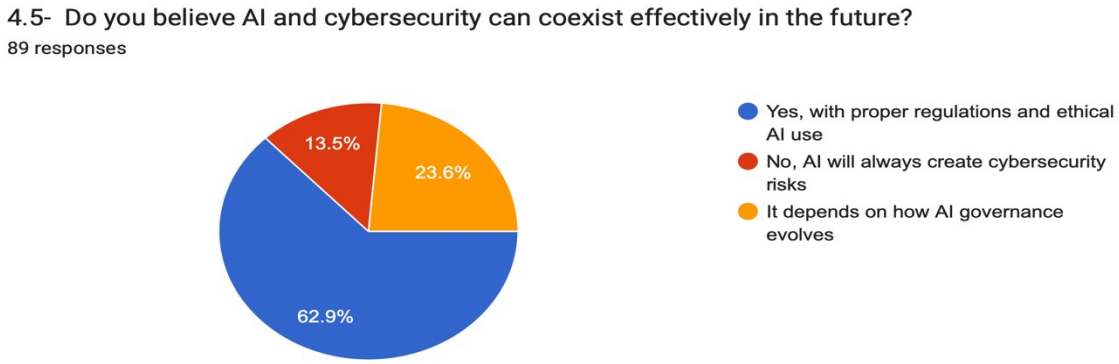

Fig.12

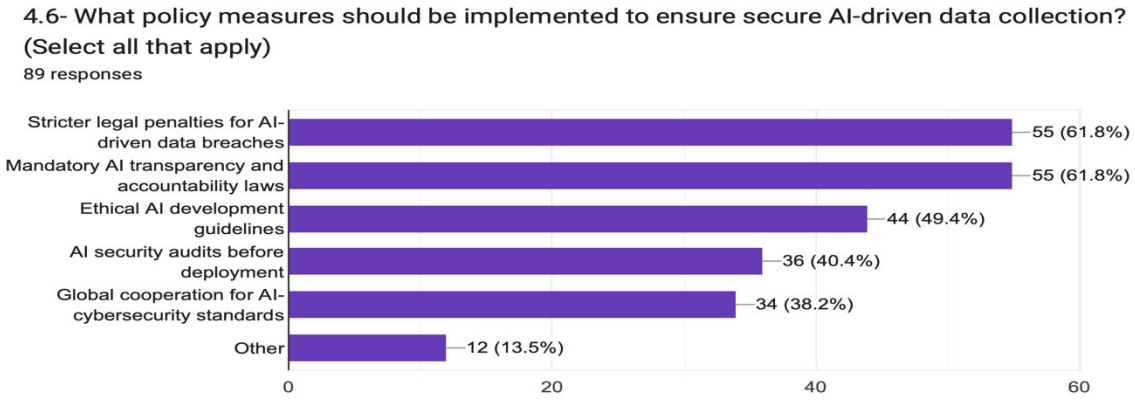

Fig.13

Common Types & Impacts of Personal Data Misuse and Fraud

The survey revealed significant personal experience with data misuse among respondents. A substantial portion (40.4%) reported being victims of personal data misuse or fraud, while 59.6% had not experienced such victimization. This high rate of reported victimization underscores the practical significance of data security concerns beyond theoretical risks and suggests that data misuse is a common experience rather than a rare occurrence. Respondents attributed data breaches to various sources, with clear patterns in perceived vulnerability. Social media platforms were most frequently identified as breach sources (43.8%), followed by e-commerce websites (23.6%), financial institutions (15.7%), government databases (9%), and healthcare systems (7.9%). This attribution pattern aligns with concerns about social

media identified in AI risk assessments, suggesting consistency in sector-specific risk perceptions and highlighting areas that may require particular attention in security measures.

Regarding formal notification of data breaches, respondents reported mixed experiences. A significant minority (39.3%) had received notifications about data breaches involving their information, while a majority (60.7%) had not received such notifications. The substantial proportion receiving notifications indicates that formal breach disclosure mechanisms are functioning to some extent, though potentially not capturing all breaches or not always resulting in notifications to affected individuals. Among those who experienced data breaches, resolution experiences varied considerably. Some respondents (29.4%) resolved issues through self-action, while a smaller proportion (11.8%) achieved resolution through company assistance. Many experienced partial resolution (26.5%) or reported "no adequate resolution" (32.4%). This distribution suggests inadequate institutional response mechanisms, with self-help and incomplete resolutions being more common than comprehensive organizational remediation, pointing to potential gaps in organizational breach response capabilities. Regarding impacts of different types of fraud, respondents identified clear priorities. Financial fraud was considered to have the greatest impact (55.1%), followed by identity theft (28.1%). Other impacts including privacy violations (7.9%), reputational damage (5.6%), and emotional distress (3.4%) were considered less significant. This prioritization of financial impacts may reflect greater measurability of financial harm compared to psychological or reputational impacts, though it may also indicate genuine prioritization of financial security in respondents' values.

When asked about privacy policy reading behaviour, respondents showed limited engagement. A large proportion (44.9%) reported reading policies and avoiding services based on privacy concerns "rarely" or "never," while 36% did so "sometimes." Only a small minority (19.1%) did so "often" or "always." This finding reveals a significant gap between stated privacy concerns and practical information-seeking behaviour, suggesting that privacy policies may not be serving their intended purpose of enabling informed decision-making about services. Respondents reported adopting various protective measures to safeguard their personal data. The most common measures included using strong, unique passwords (77.5%), being selective about sharing personal information (64%), using two-factor authentication (44.9%), and regularly reviewing privacy settings (41.6%). Less common measures included reading privacy policies (23.6%) and using encryption tools (19.1%). This pattern suggests preference

for simple, direct protective measures over more complex or time-consuming approaches, with particular emphasis on password management and information disclosure control.

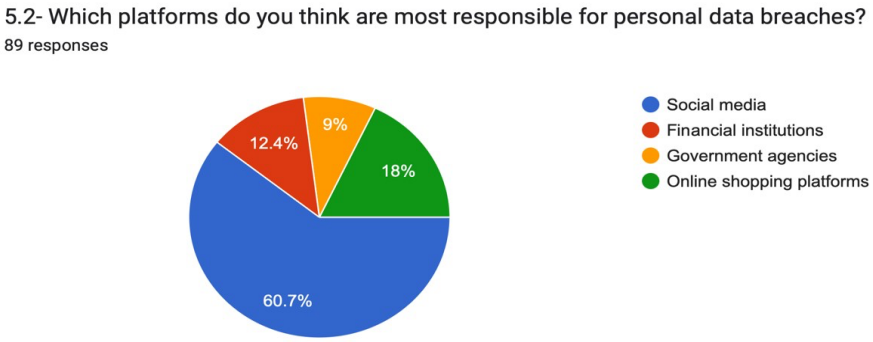

Fig.14

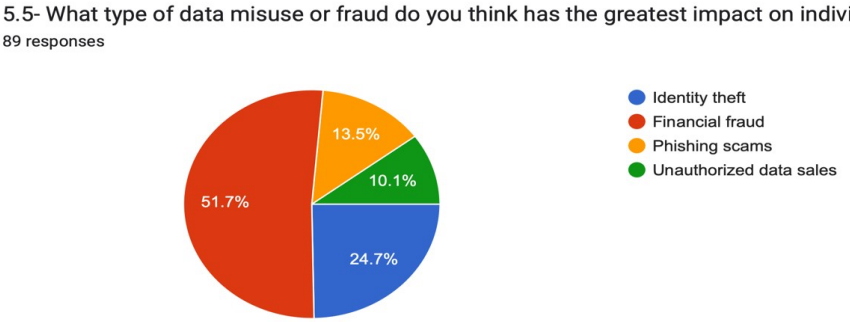

Fig.15

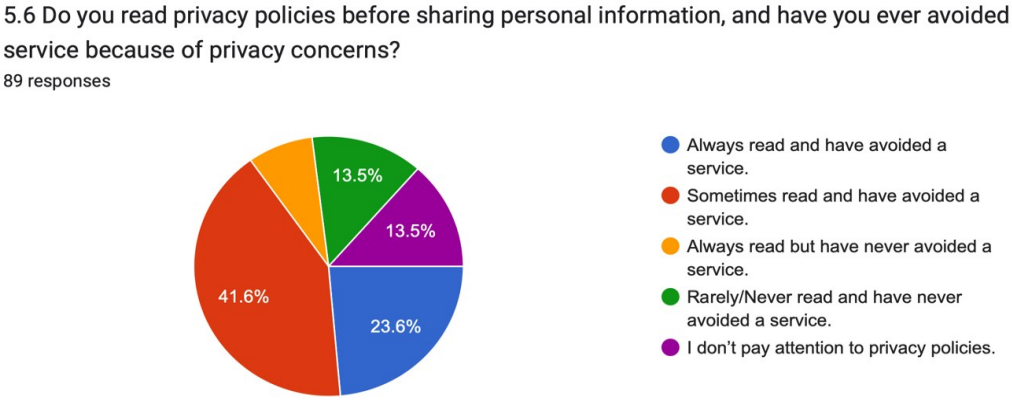

Fig.16

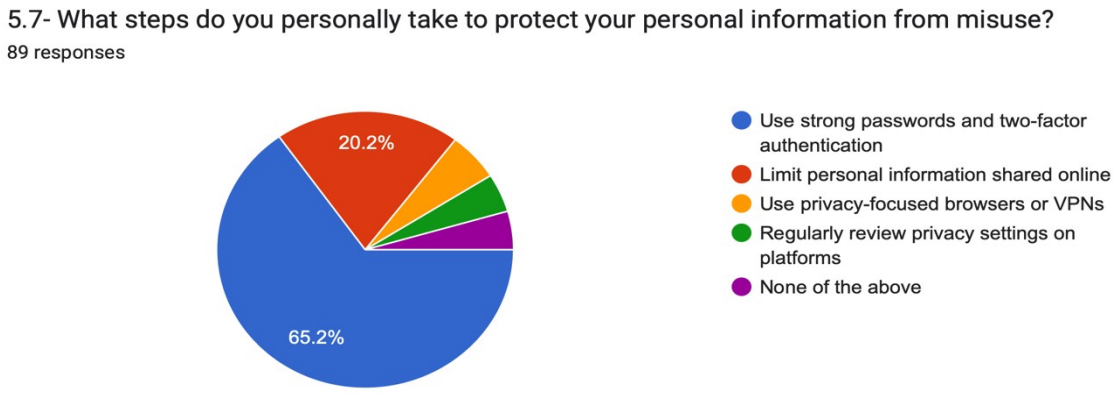

Fig.17

SUMMARY OF FINDINGS

The empirical research reveals several key insights into citizens' perceptions and experiences regarding data security. Regarding regulatory effectiveness, the study demonstrates a significant gap between data protection laws' theoretical protections and their practical implementation. While awareness of data protection concepts is relatively high (42.7% somewhat familiar with laws), practical exercise of rights is limited (24.7%), and perceived improvements are modest (66.3% seeing only slight improvement). This suggests that current regulatory frameworks may be insufficient to achieve meaningful protection in practice, whether due to enforcement limitations, complexity of rights exercise, or other implementation challenges. Citizens express substantial concerns about institutional data handling practices, with limited trust in security measures (58.4% believing data is only somewhat securely stored) and widespread perceptions of inadequate transparency (73%). There is near-unanimous support for consent requirements (94.4%) and data deletion rights (78.7% supporting without qualification), suggesting strong public demand for greater control over personal information. Unauthorized access to sensitive information (74.4%) and commercial exploitation without consent (59.3%) emerge as primary concerns regarding large-scale data collection. The research identifies overwhelming concern about AI's impact on data security (88.8% perceiving increased risk), particularly in social media (30.3%) and financial services (28.1%) sectors. Regulatory gaps include lack of clear guidelines (67.4%), insufficient penalties (55.1%), and limited regulatory expertise (52.8%). Despite these concerns, most respondents express cautious optimism about AI-cybersecurity coexistence (67.4% believing it possibly can coexist effectively) and support comprehensive oversight mechanisms

including security audits (74.2%) and explicit consent requirements (70.8%). The study reveals substantial personal experience with data misuse (40.4% reporting victimization) and limited satisfaction with resolution processes (32.4% reporting no adequate resolution). Social media platforms (43.8%) and e-commerce websites (23.6%) are perceived as primary sources of data breaches, while financial fraud (55.1%) and identity theft (28.1%) are considered most impactful. Protective behaviours focus primarily on password management (77.5%) and selective information sharing (64%), with limited engagement with privacy policies (44.9% rarely or never reading them).

The findings suggest significant interconnections between these dimensions. Perceived regulatory ineffectiveness may contribute to limited trust in institutional data handling, while personal experiences with inadequate breach resolution may reinforce scepticism about accountability mechanisms. Similarly, AI concerns appear to align with sector-specific breach attributions, suggesting consistency in risk perception across technological contexts. Collectively, these findings point to a data protection ecosystem characterized by theoretical rights that face practical implementation challenges, widespread concern about institutional data practices, emerging technological challenges that amplify existing vulnerabilities, and significant personal impacts that shape protective behaviours. This complex landscape suggests the need for multifaceted approaches that address regulatory, institutional, technological, and individual dimensions of data security.

LIMITATIONS OF THE STUDY

Several limitations should be considered when interpreting the findings of this study. Regarding sampling limitations, the use of non-probability convenience sampling limits the generalizability of findings to broader populations. The sample size (n=89) is relatively modest and may not capture the full diversity of perspectives on data security issues. Additionally, the sampling approach likely overrepresents individuals with internet access and digital literacy, potentially excluding perspectives from digitally marginalized populations who may face different data security challenges. The reliance on self-reported perceptions and experiences introduces potential reporting biases. Respondents may have different understanding of technical concepts like "data fraud" or "AI," affecting the consistency of responses. Self-reporting of victimization experiences may be influenced by awareness limitations, as individuals might have experienced data misuse without knowing it, potentially

underestimating actual prevalence. The cross-sectional design captures perceptions at a single point in time, limiting ability to assess changes in attitudes or experiences over time. This is particularly relevant for evolving domains like AI, where risk perceptions may change rapidly as technologies develop and receive public attention. The structured survey format limited collection of contextual information that might explain the reasoning behind specific perceptions or behaviours. Without qualitative elaboration, some nuances in respondent thinking may be missed, particularly regarding complex topics like AI risk assessment or privacy trade-offs. The absence of specific geographic information limits ability to analyse how different regulatory regimes might influence perceptions and experiences. Attitudes toward data protection may vary significantly based on local regulatory frameworks, enforcement practices, and cultural attitudes toward privacy. While the study identifies correlations between perceptions and experiences, it cannot establish causal relationships between variables. For example, while there appears to be a relationship between breach experiences and protective behaviours, the direction of influence cannot be definitively established from the available data. Despite these limitations, the study provides valuable insights into patterns of perception and experience that can inform more targeted research and policy development regarding data security concerns.

CONCLUSION

This empirical investigation into data security concerns reveals a landscape characterized by significant gaps between regulatory intent and practical implementation, widespread distrust of institutional data handling practices, emerging concerns about AI-driven security risks, and substantial personal experience with data misuse and its consequences. Several critical implications emerge from the research findings. First, the limited exercise of data protection rights (24.7%) despite moderate awareness suggests that rights-based frameworks alone may be insufficient to ensure data security. The gap between knowledge and action indicates that practical barriers—whether complexity, time constraints, or perceived futility—may undermine the effectiveness of regulatory approaches that rely primarily on individual initiative to exercise rights. Second, the trust deficit regarding data handling practices (73% perceiving insufficient transparency) suggests that current organizational approaches to communication and security assurance are failing to meet public expectations. The near-unanimous support for consent requirements (94.4%) and data deletion rights (78.7%) indicates strong public demand for control-enhancing mechanisms that many current data

practices may not adequately provide. Third, the overwhelming concern about AI's impact on data security (88.8%) highlights the need for specialized regulatory approaches that can address emerging technological challenges. The identified regulatory gaps—particularly lack of clear guidelines (67.4%) and limited regulatory expertise (52.8%)—suggest that current governance frameworks may be ill-equipped to manage AI-specific risks. Fourth, the substantial prevalence of data misuse victimization (40.4%) and limited satisfaction with resolution processes (32.4% reporting no adequate resolution) indicates that current remedial approaches are insufficient. The focus on reactive rather than preventive measures may leave many citizens without effective recourse when breaches occur.

10.1. Recommendations

Based on these implications, several recommendations can be advanced for improving data security. Simplified Rights Exercise addresses how regulatory frameworks should prioritize practical usability of rights, potentially through standardized exercise mechanisms, automated tools, and clearer organizational responsibilities for facilitating rights exercise. Enhanced Transparency suggests organizations should develop more accessible, comprehensible explanations of data practices that provide meaningful insight into collection, processing, sharing, and security measures beyond technical compliance with disclosure requirements. AI-Specific Governance recommends regulatory approaches should incorporate specialized provisions for AI applications, including technical standards, ethical guidelines, and impact assessment requirements that address the unique risks of automated processing and decision-making. Preventive Security Requirements suggests greater emphasis should be placed on preventive measures rather than post-breach remedies, including mandatory security standards, regular auditing requirements, and potential liability for inadequate preventive measures. Education and Empowerment proposes public education initiatives should move beyond awareness-raising to provide practical skills for personal data protection, including evaluating privacy policies, implementing comprehensive security measures, and effectively responding to potential breaches.

10.2. Future Directions

This study's findings suggest several promising directions for future research. Longitudinal Studies could track changes in perceptions and experiences over time to provide insight into how regulatory interventions, technological developments, and personal experiences shape

data security attitudes. Experimental Research could test different approaches to rights communication, transparency mechanisms, and consent interfaces to identify more effective ways to bridge the gap between regulatory intent and practical implementation. Sector-Specific Analysis would enable more detailed examination of sector-specific data practices and concerns, particularly in high-risk domains like social media and financial services, to inform targeted regulatory approaches. AI Impact Assessment would facilitate deeper investigation of specific AI applications and their security implications to help develop more nuanced governance approaches that address particular risk vectors rather than treating AI as a monolithic phenomenon. Resolution Process Analysis could examine breach resolution experiences to identify best practices and systematic deficiencies in organizational response mechanisms, informing more effective remedial approaches.

The empirical findings presented in this research underscore the complex, multifaceted nature of data security challenges in contemporary digital society. Effective responses will require coordinated efforts across regulatory, organizational, technological, and individual domains to bridge the significant gaps between theoretical protection and practical security. As data collection and processing capabilities continue to expand and new technologies like AI amplify both potential benefits and risks, addressing citizens' well-founded concerns about misuse and fraud becomes increasingly urgent. By identifying specific vulnerability points and potential intervention opportunities, this research aims to contribute to the development of more effective data security frameworks and practices.

REFERENCES

▪ Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2016). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. ACM Computing Surveys, 50(3), 1-41.

▪ Bamberger, K. A., & Mulligan, D. K. (2015). Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. MIT Press.

▪ Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671-732.

▪ Calo, R. (2014). The Boundaries of Privacy Harm. Indiana Law Journal, 86(3), 1131-1162.

▪ Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. Information & Communications Technology Law, 28(1), 65-98.

▪ Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior. International Journal of Human-Computer Studies, 71(12), 1163-1173.

▪ Martin, K. D., & Murphy, P. E. (2017). The Role of Data Privacy in Marketing. Journal of the Academy of Marketing Science, 45(2), 135-155.

▪ Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. (2018). SoK: Towards the Science of Security and Privacy in Machine Learning. IEEE European Symposium on Security and Privacy (EuroS&P), 3(1), 399-414.

▪ Ponemon Institute. (2020). Cost of a Data Breach Report. IBM Security.

▪ Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3), 477-564.

▪ Solove, D. J., & Schwartz, P. M. (2019). Privacy Law Fundamentals. International Association of Privacy Professionals.

▪ Taddeo, M., Floridi, L., & Wachter, S. (2019). Artificial Intelligence, Ethics and the Regulation of AI. Philosophy & Technology, 32(4), 571-574.

▪ Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russell, N. C., & Sadeh, N. (2019). MAPS: Scaling Privacy Compliance Analysis to a Million Apps.

▪ Proceedings on Privacy Enhancing Technologies, 2019(3), 66-86.