NOVA IMS Information Management School

MGI

Master Degree in

Information Management

Ethical Integration of Biometric Data in Public Services: Empowering Efficiency, Security, and Privacy through AI-based Self-Service Technologies

Balancing Innovation, Cost-effectiveness, and Data Rights for Enhanced Public Sector Operations

José Carlos Bate Eusébio Sequeira

Master Thesis

presented as partial requirement for obtaining the Master Degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ETHICAL INTEGRATION OF BIOMETRIC DATA IN PUBLIC SERVICES: EMPOWERING EFFICIENCY, SECURITY, AND PRIVACY THROUGH AI-BASED SELF-SERVICE TECHNOLOGIES

Balancing Innovation, Cost-effectiveness, and Data Rights for Enhanced Public Sector Operations

by

José Carlos Bate Eusébio Sequeira

Master Thesis presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Knowledge Management and Business Intelligence.

Supervised by

Professor Mijail Juanovich Naranjo Zolotov, PhD, NOVA Information Management School

11 2023

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledged the Rules of Conduct and Code of Honor from the NOVA Information Management School.

José Carlos Bate Eusébio Sequeira

Lisboa, 13/11/2023

DEDICATION

I appreciate the remarkable educational journey that Universidade Nova de Lisboa, particularly NOVA IMS, has provided me. The nurturing academic atmosphere, combined with the unwavering support of the faculty and staff, has played a pivotal role in shaping my personal growth and accomplishments.

To NOVA IMS, a beacon of knowledge and innovation, I extend my heartfelt gratitude for imparting a profound comprehension of my field and equipping me with the skills to navigate its intricacies. Your steadfast dedication to excellence has laid the cornerstone for my academic pursuits and future endeavours.

I want to express my sincerest gratitude to my supervisor, Professor Mijail Juanovich Naranjo Zolotov. Your guidance and wisdom have been invaluable throughout my master's journey. Your unrelenting dedication to the pursuit of knowledge, as well as your patient mentoring, have had a significant impact on both my academic and personal growth.

To my family, whose boundless love and unwavering support have been my constant motivation, I extend my deepest thanks for believing in me even when the path seemed daunting. Your sacrifices and encouragement have illuminated my path.

And to my cherished friends, your companionship and shared experiences have brought joy and equilibrium to the demanding academic landscape. Thank you for being my pillars of strength and for the countless moments of laughter that have made this journey unforgettable.

As I dedicate this work, I honour the commitment to learning and exploration that Universidade Nova de Lisboa and NOVA IMS exemplify. May this thesis serve as a testament to the collective pursuit of knowledge and innovation.

With profound gratitude,

José Sequeira.

ABSTRACT

In recent years, AI-based self-service technology (SST) has experienced remarkable growth and transformation within the public sector. This surge in adoption is driven by the myriad advantages it offers, such as increased adaptability, personalized user experiences, and improved efficiency, cost-effectiveness, and overall service quality. The deployment of AI-driven SST has proven to be a significant change, fostering more seamless interactions with citizens, and providing governments with opportunities to revolutionize their service delivery. This research ventures into uncharted territory by exploring the untapped potential lying at the intersection of SST and biometric technology. By integrating biometric data into the SST framework, a profound shift in the public sector's capabilities becomes apparent. The synergy between these two technologies promises to propel SST to an unprecedented level, offering a novel dimension to its applications and benefits. The study delves into the multifaceted landscape of this amalgamation, providing an in-depth analysis of the profound benefits it offers to the public sector. Through rigorous examination, it has become evident that the fusion of biometric technology with SST facilitates a transformative leap in efficiency and the user experience. This symbiotic relationship redefines public services, optimizing them for the digital age. Among the notable findings of this research, it is evident that this integration enhances operational efficiency within the public sector, streamlining processes, and reducing costs. It also fosters a higher level of security, critical for safeguarding sensitive data, as the study discovered that AI-driven SST, with biometric data, significantly improves security measures. In summary, the amalgamation of biometric technology and SST signifies a remarkable leap in the capabilities of the public sector. The resulting efficiency gains, coupled with the promise of an enhanced user experience, demonstrate the potential of this integration. This research offers invaluable insights for public sector stakeholders seeking to navigate the ever-evolving landscape of government services. By embracing these technologies, governments can unlock a promising future where innovation converges with the evolving needs of both the government and its citizens.

KEYWORDS

Biometric Data; Artificial Intelligence (AI); Self Service Technologies (SSTs); AI-SST

Sustainable Development Goals (SDGs):

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AI-based SST	Artificial Intelligence-based Self-Service Technology
AI	Artificial Intelligence
SSTs	Self-Service Technologies
SST	Self-Service Technology
GDPR	General Data Protection Regulation
TAM	Technology Acceptance Model
DoI	Diffusion of Innovations Theory
UTAUT	Acceptance and Use of Technology
ISSM	Information System Success Model
CVT	Consumer Value Theory
PLS	Partial Least Squares regression
BTA	Biometric Technology Awareness
EU	Ease of Use
IU	Intention of Use
PU	Perceived Usefulness
TG	Trust in Government
TT	Trust in Technology
AU	Areas of Usage
SQ	System Quality
P	Privacy
UE	User Experience
US	User Satisfaction
DG	Demographics
BTS	Bootstrap Test of Significance
AVE	Average Variance Extracted
HIPAA	Health Insurance Portability and Accountability Act

VIF	Variance Inflation Factor

1. INTRODUCTION

Biometric data usage in the public sector through Artificial Intelligence-based Self-Service Technology (AI-based SST) has gained significant popularity and importance. With the rapid advancement of artificial intelligence (AI), intelligent self-service technologies (SSTs) offer governments a unique opportunity to enhance public services and deepen their interactions with citizens (Chen et al., 2021). Biometric data, encompassing fingerprints, facial recognition, and iris scans, holds the potential to enhance the security and efficiency of various public services by reducing manual verifications, leading to shorter service durations and cost savings (Natgunanathan et al., 2016), which can streamline and secure processes like passport control, voter registration, licence renewal, and citizenship card updates. Furthermore, biometric data can bolster security by preventing fraud and identity theft, particularly when managing sensitive public sector information.

However, the use of biometric data does introduce privacy concerns. While AI can offer highly accurate and objective solutions, its inherent opacity, due to the construction of undocumented rules, can diminish human control and trust (Gesk & Leyer, 2022). Consequently, research into the use of biometric data in the public sector via AI-based SST becomes imperative to define best practices and regulations that acknowledge the benefits of this technology while safeguarding individual rights.

With this perspective in mind, the research question "How can biometric data be used efficiently and ethically in the public sector through AI-based self-service technologies to enhance efficiency, reduce costs, and heighten security, all while preserving individuals' privacy and data rights?" comes into focus. The answer to this question involves evaluating the drivers behind biometric data adoption and AI-based SST in public services, including their advantages and limitations, and formulating recommendations for their implementation. Additionally, the study will delve into the current state of biometric data and AI-powered SST in the government, exploring the ethical, legal, and societal implications. The findings of this study expect to benefit lawmakers, government officials, and technologists, all of whom are engaged in the ongoing discourse regarding biometric data usage and AI-based SST in the public sector.

A literature review of biometric data in the public sector using AI-based SST reveals several existing studies regarding the technology's potential benefits and drawbacks. Research suggests that biometric data usage can enhance efficiency by reducing the need for human verifications and shortening service durations (Chen et al., 2021; Shin & Perdue, 2019). Also, studies have indicated that incorporating biometric data into passport screening can expedite and secure the process while integrating biometric data into voting systems can enhance security and prevent fraud. The uniqueness of biometric characteristics for everyone makes it the most reliable method for secure identity authentication (Sharif et al., 2019).

However, biometric data usage can also give rise to privacy concerns, underscoring the necessity of protecting the data and ensuring its ethical use in the public sector. These concerns encompass the need for robust safeguards for individual data, transparency in data usage, and user empowerment (Meden et al., 2021). Despite prior research, there remains a knowledge gap concerning the ethical and effective deployment of biometric data through AI-based SST. Further research is required to balance the potential benefits of this technology and the imperative to protect individual privacy and data rights (Jain et al., 2022). The current study aims to fill this knowledge gap by investigating how to

implement biometric data efficiently and ethically in the public sector via AI-based SST to improve efficiency, reduce costs, and enhance security while safeguarding individual privacy and data rights.

The primary research objectives include evaluating the efficacy and efficiency of employing biometric data in the public sector through AI-based SSTs in various applications. The study will also delve into the privacy concerns and ethical considerations related to biometric data usage, including defining processes and procedures to protect individual privacy and data rights while implementing biometric data via AI-based SST in public services. Finally, using AI-based SST, the research will provide recommendations to public sector companies on ethical and effective biometric data usage.

In pursuit of these objectives, the study will assess several assumptions, including:

- Using biometric data through AI-based SST will enhance efficiency and security across multiple applications.
- Employing biometric data through AI-based SST raises privacy and ethical considerations.
- Best practices and legislation to safeguard individual privacy and data rights to mitigate privacy concerns, maximizing the benefits of biometric data in the public sector through AI-based SST.

During their evaluation, the research aims to provide insights into the potential benefits and limitations of using biometric data in the public sector. These findings will contribute to the establishment of best practices and standards for companies looking to use biometric data ethically and effectively in their services.

This study endeavours to make a meaningful contribution by examining the effectiveness and efficiency of biometric data usage in diverse scenarios. It will address privacy and ethical concerns regarding biometric data usage, offering best practices for safeguarding individual privacy and data rights. Furthermore, the research will provide recommendations to public sector organizations on the ethical and effective integration of biometric data with AI-SST into their services, ensuring that the prioritization of human privacy and rights remains paramount.

2. LITERATURE REVIEW

Previous research has centred on two aspects of AI-based SST in the public sector: its inherent advantages and the privacy and security concerns. Studies have consistently demonstrated that AI-based SST integration can substantially benefit government services, ultimately enhancing efficiency, lowering operational costs, and significantly improving the overall citizen experience (Chen et al., 2019, 2021). This technology simplifies government processes, reduces waiting times, and broadens citizens' access to public services. However, biometric data incorporation within AI-based SST introduces substantial apprehensions concerning privacy and security (Jain et al., 2022). Data breaches could potentially expose sensitive personal information, raising concerns about identity theft and fraudulent activities. There are also anxieties about the misuse of biometric data for surveillance or discriminatory purposes.

The acceptance of this technology within the public domain is influenced by several factors, such as the trust citizens place in the government, the perceived benefits of the technology, and the lingering privacy and security concerns. Additionally, demographic variables like age, educational attainment, and socioeconomic status play a significant role in determining the extent to which biometric data is employed in the public sector (Plantinga, 2022).

Biometric data comprises unique physical or biological characteristics used for individual identification, including fingerprints, facial features, or iris scans. Its applications in authentication are expanding across various sectors, encompassing healthcare, finance, and security (Sabhanayagam et al., 2018). While biometric authentication delivers notable benefits, such as enhanced accuracy and efficiency in identification, it concurrently introduces challenges related to privacy, the potential for bias and discrimination, and technical limitations (Jain et al., 2022). The sensitivity of biometric data underscores concerns about identity theft and the potential for facial recognition systems to exhibit biases toward specific ethnicities or genders.

The regulatory framework governing biometric data usage varies significantly among jurisdictions, with some countries adopting more stringent guidelines than others. Striking a balance between the advantages and challenges of biometric data is paramount in protecting individual privacy, upholding their rights, and ensuring equity and non-discrimination.

Although extant research provides valuable insights into the potential benefits and constraints associated with integrating biometric data into the public sector through AI-based SST, there remains a wealth of uncharted territory concerning its practical applications and utilization in diverse public sector contexts. The persistent concerns regarding privacy and security of biometric data utilization present an ongoing challenge. In the subsequent subchapters, we will delve deeper into the fundamental concepts, benefits, and challenges associated, drawing from existing scientific research while identifying gaps that warrant further exploration.

2.1. AI-BASED SST

SSTs driven by AI have been gaining prominence across industries, ranging from retail and finance to the public sector. These technologies harness AI algorithms and machine learning methodologies to furnish automated and tailor-made assistance to users, featuring chatbots, virtual assistants, and voice recognition systems (Barlow, 2017).

A comprehensive literature review on AI-based SSTs sheds light on a spectrum of advantages and drawbacks linked with their adoption. AI-based SSTs have the remarkable potential to elevate customer satisfaction by delivering efficient and personalized support, consequently trimming down wait times and the workload borne by human customer service representatives. In doing so, they also present a cost-saving opportunity for businesses and organizations (Chen et al., 2019, 2021). However, the embrace of AI-based SST does bring about its set of challenges, including technical limitations, ethical concerns, and the looming spectre of potential bias and discrimination (Chui et al., 2018).

Natural language understanding and the capacity to effectively respond to complicated or emotionally charged circumstances are frequently challenges for AI systems. Furthermore, there are ethical issues concerning employment displacement plus the gathering and use of user data (Jain et al., 2022). The regulatory landscape in this arena is rapidly evolving, with several countries and regions drafting guidelines for AI-based SST usage, including those aligned with the principles outlined in GDPR (General Data Protection Regulation).

The necessity for further research is evident to shape best practices and frameworks governing the design, implementation, and evaluation of AI-based SSTs, encompassing a comprehensive understanding of their prospective risks and challenges in diverse sectors and contexts.

Table 1 - AI-based SST

Topic	Main Studies	Key Points
AI-based SST Advantages	(Barlow, 2017; Chen et al., 2019, 2021)	Enhanced customer satisfaction through personalized support
	(Chen et al., 2019, 2021; Hekal et al., 2023; Jain & Kumar, 2012)	Reduced wait times and workloads for human customer service representatives
	(Chen et al., 2019, 2021; Jain & Kumar, 2012)	Cost savings for businesses and organizations
AI-based SST Challenges	(Barlow, 2017; Jain et al., 2022)	Technical limitations in natural language processing and emotional situations
	(Chui et al., 2018; Jain et al., 2022; Jain & Kumar, 2012)	Ethical implications such as job loss and data collection
	(Chui et al., 2018; Jain et al., 2022; Jain & Kumar, 2012)	Concerns about privacy, security, and bias

2.2. CHALLENGES OF AI IN PUBLIC SECTOR

The integration of AI within the public sector carries the potential to elevate efficiency, effectiveness, and citizen satisfaction. Nevertheless, it does not come without its share of challenges. A thorough literature review concerning AI's role in the public sector underlines ethical and legal dilemmas as concerns. The AI usage often raises pertinent questions about privacy, security, and transparency. Additionally, technical hurdles, such as data availability and quality, coupled with the intricacies of AI systems, present formidable challenges (Plantinga, 2022).

Resistance to change emerges as a recurrent issue, particularly as some employees within the public sector may perceive the automation of their roles as a potential threat. Similarly, the development, implementation, and maintenance of AI systems can prove costly. Moreover, the lack of public trust in AI's ability to make unbiased decisions can compound the challenges (Plantinga, 2022). It is critical to incorporate governance and accountability into AI systems used in the public sector. Plus, to guarantee justice, openness, and accountability, clear standards and policies must be established (Wirtz et al., 2019).

In summary, the literature review underscores the critical importance of addressing the challenges linked to AI's adoption in the public sector, plus the urgency of conducting further research to develop best practices and guidelines for the design, implementation, and evaluation of AI systems. The aim is to harness the potential of AI while upholding ethical and legal standards, promoting transparency, and ensuring the delivery of enhanced public services.

Table 2 - AI in Public Sector Challenges

Topic	Main Studies	Key Points
AI in Public Sector Challenges	(Plantinga, 2022; Sobrino-García, 2021; Wirtz et al., 2019; Wirtz & Müller, 2019)	Ethical and legal dilemmas related to privacy, security, and transparency
	(Plantinga, 2022; Wirtz et al., 2019; Wirtz & Müller, 2019)	Technical obstacles including data availability and complexity of AI systems
	(Plantinga, 2022; Wirtz et al., 2019; Wirtz & Müller, 2019)	Resistance to change and perception of job automation as a threat
	(Plantinga, 2022; Wirtz et al., 2019; Wirtz & Müller, 2019)	Cost of development, implementation, and maintenance
	(Plantinga, 2022; Sobrino-García, 2021; Wirtz et al., 2019; Wirtz & Müller, 2019)	Lack of public trust in AI's unbiased decision-making

2.3. BENEFITS OF AI IN PUBLIC SECTOR

The application of AI in the public sector can significantly enhance the effectiveness, efficiency, and overall satisfaction of citizens. Studies on AI's role within the public sector consistently reveal several advantages associated with its integration. One notable advantage lies in the realm of enhanced efficiency. AI's capability to manage repetitive and time-consuming tasks frees up human resources, enabling them to focus on more intricate and value-driven responsibilities. As a result, total productivity in the public sector increases. Additionally, AI's ability to handle massive amounts of data enables it to deliver insights that influence decision-making processes, resulting in better-informed, evidence-based conclusions (Chen et al., 2019, 2021).

Moreover, AI systems provide personalized and efficient services to citizens, subsequently elevating satisfaction levels with public services. Simultaneously, they reduce costs by automating tasks and diminishing the reliance on human resources (Wirtz & Müller, 2019). AI can also play a pivotal role in monitoring and analysing data relevant to public safety, including crime rates and traffic patterns, which translates into more efficient and effective public safety measures. Furthermore, AI systems can offer services that are inclusive and accessible to individuals with disabilities, such as voice recognition systems tailored to those with visual impairments.

In summary, the literature review underscores the vast potential benefits of AI in the public sector, encompassing augmented efficiency, improved decision-making, elevated citizen satisfaction, cost savings, bolstered public safety, and enhanced accessibility. However, to realize these benefits, it is imperative to grapple with the challenges associated with AI in the public sector, including ethical and legal considerations, technical limitations, and the need to cultivate public confidence. Extensive further research is required to gauge the effectiveness of AI systems within the public sector and to establish best practices for their implementation and evaluation.

Table 3 - AI in Public Sector Benefits

Topic	Main Studies	Key Points
AI in Public Sector Benefits	(Berryhill et al., 2019; Chen et al., 2019, 2021; Valle-Cruz et al., 2019)	Enhanced efficiency through automation of tasks
	(Berryhill et al., 2019; Chen et al., 2019, 2021; Valle-Cruz et al., 2019)	Improved decision-making based on data insights
	(Berryhill et al., 2019; Valle-Cruz et al., 2019; Wirtz & Müller, 2019)	Personalized and efficient services for citizens
	(Berryhill et al., 2019; Chen et al., 2021; Wirtz & Müller, 2019)	Cost savings through task automation
	(Valle-Cruz et al., 2019; Wirtz & Müller, 2019)	Improved public safety measures through data monitoring

2.4. REGULATORY FRAMEWORKS FOR THE COLLECTION AND USE OF BIOMETRIC DATA

A robust regulatory framework exists to protect individual privacy and security in the collection and usage of biometric data within the public sector. A comprehensive review of these regulations reveals several overarching themes (Darendeli, 2023; Villegas-Ch & García-Ortiz, 2023).

First, these regulations safeguard data privacy by mandating that biometric data is collected and used in a lawful, transparent manner, with individuals' informed consent and awareness. Furthermore, the requirements focus on safe data storage, preventing illicit access to or exploitation of such data. Secondly, the regulatory framework grants individual's specific rights over their biometric data, including the right to access, control, and, when necessary, request corrections or deletions. Thirdly, transparency and accountability are central tenets of these regulations, necessitating that clear and comprehensible information about the purpose and usage of biometric data is provided, coupled with the strict enforcement of data protection regulations. Fourthly, the regulations dictate that biometric data should only be collected and used for well-defined, lawful purposes and only with the express consent of individuals. Lastly, these regulations exhibit ethical underpinning, addressing concerns such as the potential for discrimination or stigmatization in the handling of biometric data.

Continued study is required to examine the efficacy of these rules and to create best practices for their implementation and assessment. As the landscape of biometric data and AI-based technologies evolves, regulatory frameworks must remain adaptable and robust to protect individual rights and the responsible use of such data within the public sector.

Table 4 - Regulatory Frameworks for Biometric Data

Topic	Main Studies	Key Points
Regulatory Frameworks for Biometric Data	(Darendeli, 2023; North-Samardzic, 2020; Villegas-Ch & García-Ortiz, 2023)	Protection of data privacy, consent, and lawful usage
	(Darendeli, 2023; North-Samardzic, 2020; Villegas-Ch & García-Ortiz, 2023)	Secure storage and prevention of unauthorized access
	(Darendeli, 2023; North-Samardzic, 2020; Villegas-Ch & García-Ortiz, 2023)	Individuals' rights to access, control, and correct their biometric data
	(Darendeli, 2023; North-Samardzic, 2020; Villegas-Ch & García-Ortiz, 2023)	Transparency, accountability, and clear information on data usage
	(Darendeli, 2023; North-Samardzic, 2020; Villegas-Ch & García-Ortiz, 2023)	Ethical considerations and prevention of discrimination

2.5. KNOWLEDGE GAP

While a substantial body of research exists on the usage of biometric data in the public sector through AI-based SST, there remain significant gaps in our current understanding (Jain et al., 2022; Leslie, 2019; Siau & Wang, 2020; Wirtz et al., 2020). One notable limitation lies in the dearth of comprehensive, long-term studies that examine the adoption and impact of this technology over time. This gap impedes the ability to thoroughly assess the technology's benefits and drawbacks, including its implications for privacy and security (Jain et al., 2022).

Furthermore, little attention to the cultural and sociological implications of biometric data usage was given, such as the influence on privacy and personal rights, as well as the ethical concerns connected with employing biometric data in government services (Leslie, 2019; Siau & Wang, 2020), which is a critical aspect as it delves into the broader societal implications of this technology.

Another area of concern revolves around the integration of AI-based SST into government procedures and systems, which involves considerations of the required infrastructure and the development of necessary technical skills to effectively support and maintain the technology (Wirtz et al., 2020). The implementation of AI-based SST also raises issues about citizen trust in government actions and the potential for biases within the data or algorithms used to process this data (Jain et al., 2022; Siau & Wang, 2020). These concerns are integral to ensuring equity and fairness in the technology application. Lastly, while there may be potential cost savings through the automation of tasks and the reduced reliance on human resources, it is imperative to conduct a thorough evaluation of the economic implications associated with AI-based SST (Jain et al., 2022).

In conclusion, further research is necessary to bridge these knowledge gaps and provide a comprehensive understanding of the potential benefits and drawbacks inherent in AI-based SST implementation within the public sector. Such research will not only facilitate the development of best practices but also ensure that the integration of AI-based SST aligns with broader societal values and the overall well-being of citizens.

3. MODEL AND HYPOTHESES BUILDING

The Technology Acceptance Model (TAM) is a renowned theory within the information technology realm. Introduced by Davis in 1989 and derived from the reasoned action "*proposed by Fishbein and Ajzen (1975) in the field of Social Psychology*" (Kardoyo et al., 2015; Martono et al., 2020), TAM is a well-established framework for comprehending how individuals perceive and engage with new technology. It underscores the significance of perceived usefulness and ease of use as pivotal factors influencing users' attitudes and intentions toward technology adoption (Martono et al., 2020).

Within the context of the public sector and the utilization of biometric data through AI-based SST, TAM proves invaluable in analysing the adoption and usage of this technology. It provides a solid foundation for examining the acceptance and application of biometric data. The objective of this study is to identify the barriers and facilitators influencing technology acceptance and usage, offering recommendations for enhancement. By leveraging TAM as a theoretical framework, this study contributes to the existing knowledge in the field by deepening the understanding of the acceptance and utilization of AI-based SST in the public sector.

Previous research has employed alternative models, such as the Diffusion of Innovations Theory (DoI) and the Unified Theory of Acceptance and Use of Technology (UTAUT), to scrutinize the acceptability and usage of novel technologies. DoI elucidates the diffusion of concepts, products, and services across different industries and posits a five-stage process encompassing awareness, interest, assessment, trial, and acceptance. On the other hand, UTAUT factors in elements like performance expectancy, effort expectancy, social influence, and facilitating conditions to elucidate the motivations behind technology utilization. Both DoI and UTAUT represent credible choices within the field of information technology. However, for this study, TAM was chosen due to its simplicity and extensive applicability, rendering it well-suited for a broad spectrum of technological domains.

To comprehensively grasp the factors governing the adoption and utilization of biometric data within the public sector through AI-based SST, an amalgamation of the Technology Acceptance Model (TAM), Information System Success Model (ISSM), and Consumer Value Theory (CVT) emerges as a robust framework. ISSM underscores that the triumph of an information system hinges on system quality, information quality, and service quality, collectively influencing user satisfaction with the system (Adeyemi & Issa, 2020). Meanwhile, CVT centres on the perceived value of technology in users' decision-making processes, contemplating the benefits, sacrifices, and perceived quality of the technological system (Turel et al., 2010).

However, this integrated framework, despite its comprehensive nature, is not devoid of limitations. It may appear intricate, especially for individuals unfamiliar with its underlying principles. Conceptual overlap between the theories might introduce confusion and complicate the identification of distinct elements. Additionally, the framework's applicability may be context-dependent, with its effectiveness in forecasting technology adoption potentially varying according to the circumstances.

Integrating three distinct theories, each with its assumptions and limitations, presents a unique challenge. Nevertheless, despite its drawbacks, the amalgamation of TAM, ISSM, and CVT offers a more holistic framework for dissecting the adoption and usage of biometric data in the public sector via AI-based SST compared to other models such as DoI. However, validating the effectiveness of this

integrated model empirically, especially concerning its predictive capabilities for technology adoption within the public sector through AI-based SST, may pose challenges.

In conclusion, the integration of TAM with ISSM and CVT provides a more comprehensive framework for understanding the adoption and usage of biometric data in the public sector through AI-based SST compared to other models such as DoI, notwithstanding its limitations.

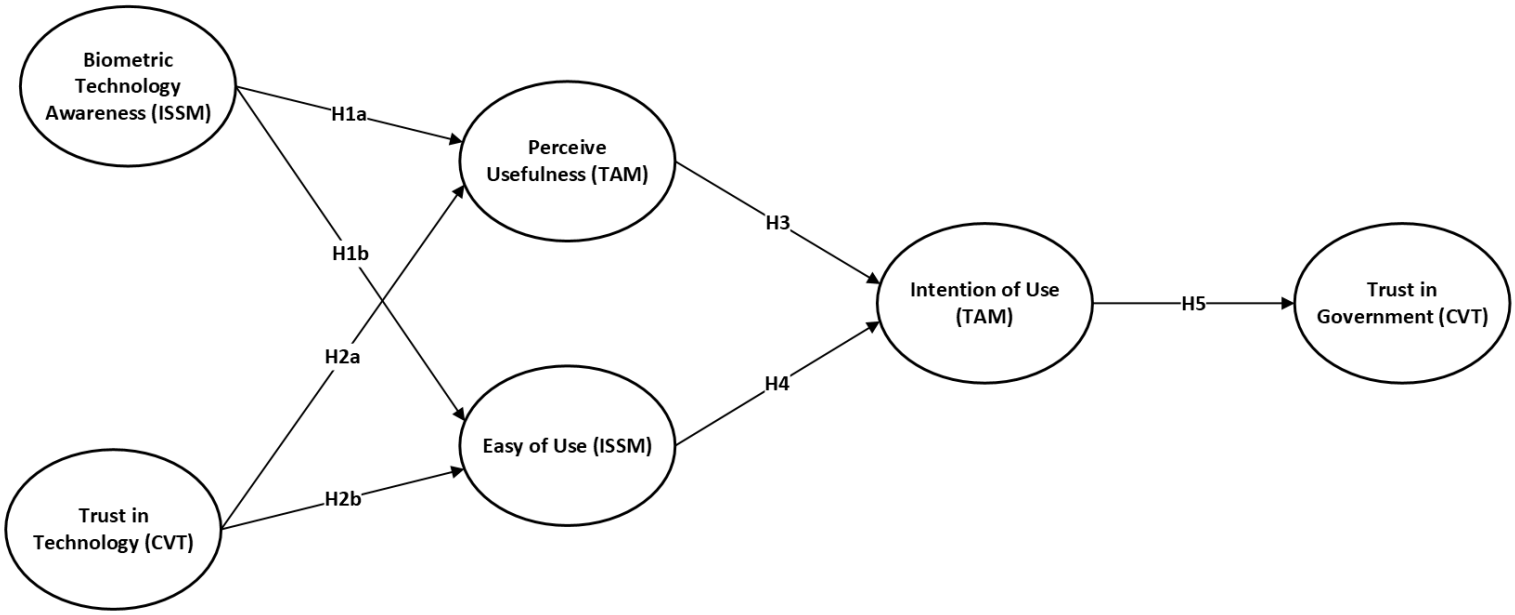

Figure 3.1 - Conceptual Framework

3.1. EMPIRIC STUDY

In this section, we embark on an empirical journey designed to validate and elucidate the hypotheses at the heart of our model. These hypotheses, meticulously crafted and inspired by extensive literature and theoretical frameworks, aim to illuminate the intricate relationships among pivotal factors shaping the adoption landscape of biometric technology within the public sector.

The hypotheses unfold as follows:

H1a: Biometric Technology Awareness positively shapes users' experiences, intentions, and perceived utility

The study relies on extensive literature to examine the influence of Biometric Technology Awareness on Perceived Utility, which suggests that increased awareness positively correlates with users' perceptions of the technology's utility. Individuals who have a thorough grasp of biometric technology are more likely to recognise its practical benefits, influencing their judgement of its usefulness.

H1b: Users who have a thorough grasp of biometric technology are more likely to find it simple to use

Greater Biometric Technology Awareness adds favourably to the impression of Ease of Use, based on insights from the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). Users who are already familiar with biometric technology should find it more user-friendly, fitting smoothly with their cognitive expectations.

H2a: Users who have more faith in technology are more likely to find it beneficial

Trust appears as a critical factor in moulding consumers' impressions. Users are more likely to regard biometric technology as valuable as their trust grows. Trust acts as a catalyst, creating a pleasant environment that increases the perceived value of the technology.

H2b: Users who have faith in technology will regard it as more accessible and user-friendly

In the same way that trust influences perceived usefulness, trust in technology impacts perceived ease of use. Users who have a greater level of trust are more likely to find the technology user-friendly and easier to use.

H3: When users view a technology to be beneficial, they are more inclined to adopt it

TAM's cornerstone of perceived usefulness directly affects consumers' propensity to embrace biometric technologies. A good sense of usefulness is expected to translate into a stronger desire to adopt technology in the public sector.

H4: Easy-to-use systems are more likely to generate a good intention to embrace the technology

According to TAM principles, Ease of Use directly influences consumers' Intention of Use. A user-friendly system is more likely to foster a favourable desire to use the technology, matching the natural inclination for user-friendly systems.

H5: People who have a favourable desire to use biometric technology are more inclined to trust government agencies that have adopted it

Finally, the complex relationship between consumers' Intention of Use and Trust in Government are investigated. A favourable desire to use biometric technology is expected to increase trust in government entities that employ the technology, forming a symbiotic connection.

This research employs quantitative method methodology, by using quantitative surveys, capturing numerical data on variables such as awareness, trust, perceived utility, ease of use, and intention to use. The study purposely includes a varied sample of public sector users targeted by biometric technology implementations, chosen strategically based on their exposure to or prospective engagement with biometric systems inside governmental services. The quantitative data is subjected to rigorous statistical studies, including regression analysis, to determine the strength and significance of correlations between variables. Simultaneous thematic analysis of qualitative data provides a detailed knowledge of participants' viewpoints.

While the entire data analysis is ongoing, preliminary findings suggest early indicators that agree with theoretical assumptions. As we go into the next phase of data analysis, the complete results offer not only statistics but also a deep grasp of the complicated web of factors driving biometric technology adoption in the public sector.

3.2. DATA OVERVIEW

3.2.1. Data Collection Process

It is vital to give insight into the data collection procedure to appreciate the findings of the study and their implications. So, data collection procedures were planned to provide a comprehensive view of the use of biometric data in the public sector via AI-powered self-service platforms:

- **Survey Instrument Development:** A systematic questionnaire was designed to gather viewpoints and experiences. The study issue and its related components were the focus of this questionnaire, which included Biometric Technology Awareness (BTA), Ease of Use (EU), Intention of Use (IU), Perceived Usefulness (PU), Trust in Government (TG), and Trust in Technology (TT).
- **Data Collection:** The questionnaire was distributed electronically using social media platforms, like LinkedIn, and also through the university email and Moodle, assuring anonymity and confidentiality while fostering candid and open responses.
- **Data Analysis:** The amassed data underwent rigorous analysis using PLS modelling techniques. This robust statistical approach is well-suited for modelling intricate relationships between latent constructs and observable variables, tackling the multifaceted research question.

3.2.2. Sample Size

The significance and validity of the research findings are connected to the sample size and representativeness. In this regard, the study meticulously involved a diverse and sufficiently substantial sample size, comprising 224 participants. This sample size was not only adequate but also robust, affording a confidence that the results and insights generated are dependable and directly pertinent to the research question.

3.2.3. Questionnaire

The questionnaire, the data collection instrument, was critical in generating responses relating to concepts linked with biometric data usage in the public sector. This rigorously developed questionnaire included topics to assess participants' perspectives, experiences, and attitudes about biometric technology usage in government processes.

The questionnaire is structured into sections encompassing:

- Areas of Usage (AU)
- Biometric Technology Awareness (BTA)
- Demographics (DG)
- Ease of Use (EU)
- Intention of Use (IU)
- Perceived Usefulness (PU)

- Privacy (P)
- System Quality (SQ)
- Trust in Government (TG)
- Trust in Technology (TT)
- User Experience (UE)
- User Satisfaction (US)

Each section featured multiple items that prompted respondents to provide ratings or answers, facilitating a comprehensive assessment of their viewpoints on these pivotal constructs. In the subsequent sections of this chapter, we will present the analysis and engage in a discussion of the key findings derived from this data collection process, enabling to draw meaningful insights and reach conclusions that directly address the research question.

4. RESULTS AND DISCUSSION

This study revolves around a fundamental question that serves as its guiding principle: "How can biometric data be used efficiently and ethically in the public sector through AI-based self-service technologies to enhance efficiency, reduce costs, and heighten security, all while preserving individuals' privacy and data rights?" This question stands at the core of the extensive examination of biometric data usage within the public sector. The significance of this research emerges as it endeavours to bridge the ever-widening chasm between advancing technology and the ethical, efficient, and secure assimilation of biometric data into public sector operations.

In an era that increasingly relies on data-driven decision-making, this study grapples with the intricate challenge of harmonizing the pressing need for amplified efficiency, cost reduction, and heightened security with the imperatives of preserving individual privacy and data rights. It provides invaluable insights that have the potential to shape the design and execution of AI-based self-service technologies that pivot on the use of biometric data.

Table 5 - Questionaire Sample Characteristics

Characteristic	Description	Frequency (n)	Percentage (%)
Total Sample Size		224	100%
Gender			
- Female	Female Participants	58	25.9%
- Male	Male Participants	82	36.6%
- Other		1	0.45%
- Blank	Participants that not answered	83	37.1%
Age			
- 18-24	Participants aged 18-24	15	6.7%
- 25-34	Participants aged 25-34	43	19.2%
- 35-44	Participants aged 35-44	36	16.07%
- 45-54	Participants aged 45-54	32	14.29%
- 55-64	Participants aged 55-64	14	6.25%
- 75-84	Participants aged 75-84	1	0.45%
- Blank	Participants that not answered	83	37.1%
Education Level			
- High School	Participants with High School	12	5.36%
- Bachelor’s Degree	Participants with Bachelor’s Degree	50	22.32%
- Master’s Degree	Participants with Master’s Degree	68	30.36%
- Doctorate	Participants with Doctorate	11	4.91%
- Blank	Participants that not answered	83	37.1%

4.1. FINDINGS

Before an in-depth exploration of the research results, it is crucial to provide a succinct overview of the findings that have emerged from the investigation. These findings hold direct relevance in addressing the core research question:

- **Efficiency and Cost Reduction:** The analysis underscores that biometric data usage within the public sector, facilitated by AI-driven self-service technologies, can yield substantial improvements in operational efficiency and lead to significant cost reductions. This discovery is critical to achieving the goal of resource efficiency among public sector enterprises.
- **Enhanced Security:** The research has brought to light a notable enhancement in security measures when incorporating biometric data into the public sector alongside AI-based self-service technologies. This finding bears profound implications for the protection of sensitive information and the assurance of public trust.
- **Privacy and Data Rights:** The findings accentuate the significance of safeguarding privacy and data rights. While biometric data usage can enhance public sector operations, the research emphasizes that ethical considerations, such as the provision of informed consent and the secure handling of data, must be intrinsic to any implementation.
- **Comparison to Existing Literature:** The study aligns with the existing literature in illuminating the potential benefits of biometric data usage while extending its scope to encompass the ethical dimension. We provide a nuanced perspective that transcends mere efficiency gains.
- **Practical Implications:** The research imparts concrete, evidence-based recommendations tailored for public sector companies. These recommendations are culled from the findings and offer a compass for the development of policies and the implementation of technology.

These key findings establish the framework for a comprehensive discussion and analysis of the research results, affording a deeper comprehension of the intricate dynamics underpinning biometric data usage in the public sector with AI-driven self-service technologies.

4.2. PARTIAL LEAST SQUARES (PLS) ANALYSIS

In the investigation, the goodness of fit of the PLS model was thoroughly evaluated by considering various critical indicators:

- **R-squared and R-squared adjusted:** These values provide variance insights explained by the model, indicating its explanatory power for the latent constructs (BTA, EU, IU, PU, TG, TT). The model's robustness is evident from R-squared values ranging from 0.433 to 0.687, suggesting that it effectively accounts for a significant variance in the dependent variables associated with the latent constructs.
- **Composite Reliability (rho_a):** These values signify the reliability of the latent constructs, underscoring the model's strength. With values consistently exceeding 0.90 for most constructs, the latent variables are dependable, affirming the internal consistency of the items within each construct.

- **Average Variance Extracted (AVE):** These values, reflecting the variance amount explained by the latent constructs after accounting for measurement error, affirm the validity of the model. AVE values surpassing 0.50 for each construct of the model's adequate convergent validity establish that the latent variables effectively account for a substantial variance in the observed variables.

Table 6 - Correlation, cronbach's alpha, composite reliability (CR), average variance extracted (AVE) and R-square

	BTA	EU	IU	PU	TG	TT
Biometric Technology Awareness (BTA)	**0.871**					
Easy of Use (EU)	0.681	**0.955**				
Intention of Use (IU)	0.601	0.741	**0.973**			
Perceived Usefulness (PU)	0.712	0.730	0.795	**0.910**		
Trust in Government (TG)	0.469	0.532	0.660	0.655	**0.947**	
Trust in Technology (TT)	0.687	0.668	0.697	0.689	0.602	**0.846**
Cronbach's alpha	0.839	0.952	0.972	0.895	0.942	0.796
Composite reliability (rho_a)	0.844	0.952	0.972	0.902	0.945	0.809
Average variance extracted (AVE)	0.758	0.912	0.947	0.827	0.896	0.716
R-square		0.539	0.687	0.582	0.436	
R-square adjusted		0.535	0.684	0.579	0.433	

Notes: Values in diagonal (bold) are square root of average variance extracted (AVE).

Table 7 - Loadings and Cross-loadings

	BTA	EU	IU	PU	TG	TT
BTA_1	**0.918**	0.623	0.552	0.669	0.444	0.611
BTA_2	**0.886**	0.625	0.474	0.563	0.346	0.582
BTA_3	**0.804**	0.527	0.543	0.625	0.434	0.602
EU_1	0.670	**0.968**	0.724	0.708	0.528	0.626
EU_2	0.666	**0.968**	0.691	0.710	0.517	0.635
EU_3	0.613	**0.929**	0.708	0.674	0.478	0.651
IU_1	0.588	0.728	**0.972**	0.770	0.615	0.682
IU_2	0.574	0.706	**0.975**	0.773	0.640	0.674
IU_3	0.592	0.729	**0.972**	0.776	0.671	0.678
PU_1	0.711	0.691	0.744	**0.905**	0.576	0.646
PU_2	0.537	0.582	0.672	**0.875**	0.612	0.576
PU_3	0.681	0.710	0.748	**0.948**	0.604	0.654
TG_1	0.476	0.526	0.641	0.625	**0.948**	0.592
TG_2	0.449	0.510	0.644	0.642	**0.971**	0.569
TG_3	0.405	0.472	0.588	0.592	**0.921**	0.547
TT_1	0.595	0.571	0.601	0.634	0.599	**0.887**
TT_2	0.561	0.563	0.541	0.467	0.322	**0.725**
TT_3	0.588	0.564	0.624	0.634	0.583	**0.914**

Note: Values in bold are the loadings of each indicator.

Table 8 - Heterotrait-monotrait ratio of correlations (HTMT)

	BTA	EU	IU	PU	TG	TT
Biometric Technology Awareness (BTA)						
Easy of Use (EU)	0.761					
Intention of Use (IU)	0.666	0.770				
Perceived Usefulness (PU)	0.816	0.787	0.850			
Trust in Government (TG)	0.527	0.561	0.689	0.715		
Trust in Technology (TT)	0.846	0.772	0.794	0.811	0.687	

The PLS analysis yielded a set of path coefficients, each representing the relationships between latent constructs. Here is a succinct analysis of these key path coefficients:

- **BTA -> EU (0.420):** Biometric Technology Awareness (BTA) increases links to a positive perception of Easy of Use (EU), suggesting that efforts to enhance awareness about biometric technology can contribute to users finding it more user-friendly.
- **BTA -> PU (0.451):** Biometric Technology Awareness (BTA) positively influences Perceived Usefulness (PU). Elevated awareness correlates with an increased perception

of the practical advantages of biometric technology, underscoring the role of awareness in shaping perceived utility.

- **EU -> IU (0.345):** The positive relationship between Easy of Use (EU) and Intention of Use (IU) emphasizes that when users perceive technology as user-friendly, their intention to use it increases. User-friendliness plays a pivotal role in AI-based self-service technology adoption in the public sector.
- **IU -> TG (0.660):** Intention of Use (IU) and Trust in Government (TG) have a robust positive relationship. Users with a positive intention to use biometric technology are more likely to trust government institutions deploying the technology, showcasing the symbiotic relationship between intention and trust.
- **PU -> IU (0.543):** Perceived Usefulness (PU) significantly influences Intention of Use (IU). When individuals perceive technology as useful, their inclination to intend to use it rises. The perceived utility of technology is a factor in shaping users' intentions.
- **TT -> EU (0.379):** Trust in Technology (TT) positively influences Easy of Use (EU). Users with a higher degree of trust in technology are likely to find the technology more user-friendly. Trust is interconnected with user-friendliness in public sector settings.
- **TT -> PU (0.379):** Trust in Technology (TT) positively influences Perceived Usefulness (PU). Trust in technology enhances the perception of its practical advantages, indicating the significance of trust in shaping the perceived utility of biometric technology.

Table 9 - Path Coefficients

	BTA	EU	IU	PU	TG	TT
Biometric Technology Awareness (BTA)		0.420		0.451		
Easy of Use (EU)			0.345			
Intention of Use (IU)					0.660	
Perceived Usefulness (PU)			0.543			
Trust in Government (TG)						
Trust in Technology (TT)		0.379		0.379		

4.3. BOOTSTRAP TEST OF SIGNIFICANCE ANALYSIS

In the analysis, a Bootstrap Test of Significance (BTS) was conducted to validate the robustness and significance of the path coefficients. The results of the BTS presented compelling evidence, as all path coefficients displayed p-values of 0.000, signifying their statistical significance. This confirmation underscores the reliability and pertinence of the model in addressing the research question, offering substantial empirical support for the identified relationships.

The comprehensive examination of model fit, path coefficients, and BTS results enhances the depth of our understanding of biometric data usage in the public sector when coupled with AI-based self-service technologies. The following sections will delve into the implications and practical insights derived from these results, considering the research question.

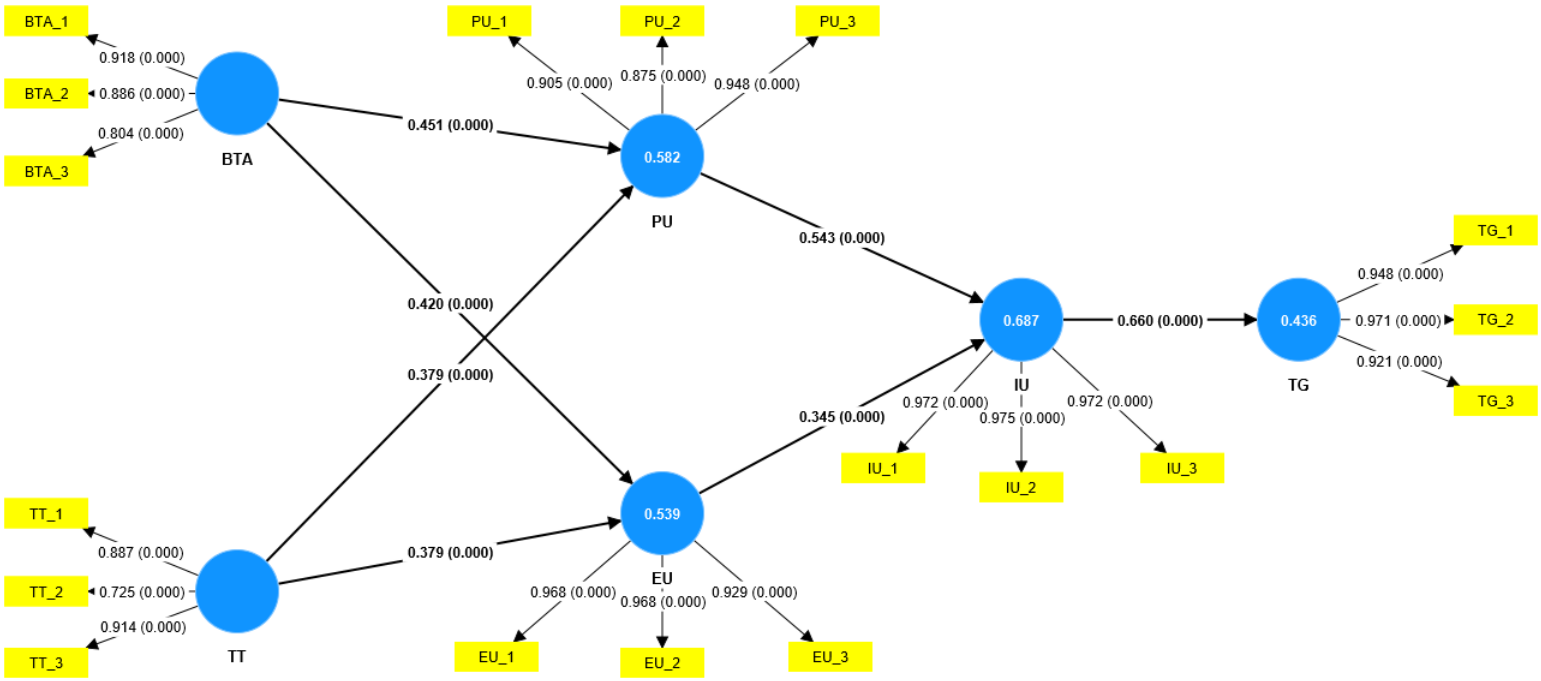

Figure 4.1 - BTS Model

Table 10 - Total effects results

	β̂	t-statistics	p-values
BTA -> EU	0.420	5.170	0.000
BTA -> IU	0.390	7.379	0.000
BTA -> PU	0.451	6.519	0.000
BTA -> TG	**0.257**	**6.851**	**0.000**
EU -> IU	0.345	4.082	0.000
EU -> TG	0.227	4.078	0.000
IU -> TG	0.660	15.083	0.000
PU -> IU	0.543	6.790	0.000
PU -> TG	0.358	5.719	0.000
TT -> EU	0.379	4.933	0.000
TT -> IU	0.337	6.418	0.000
TT -> PU	0.379	5.352	0.000
TT -> TG	**0.222**	**5.413**	**0.000**

Notes: Biometric Technology Awareness (BTA), Easy of Use (EU), Intention of Use (IU), Perceived Usefulness (PU), Trust in Government (TG), Trust in Technology (TT). The “bold” style was used to

highlight the results that Biometric Technology Awareness and Trust in Technology variables directly have with Trust in Government (dependent variable).

4.4. RESULTS ANALYSIS

4.4.1. Multicollinearity Validation

Before delving into the model's predictive power, we meticulously validated multicollinearity. Variance Inflation Factor (VIF) values, ranging from 1 to 2.14 and comfortably below the threshold of 5, affirm the absence of multicollinearity among the variables, ensuring the reliability of our subsequent analyses.

Table 11 - Collinearity Statistics (VIF)

	BTA	EU	IU	PU	TG	TT
Biometric Technology Awareness (BTA)		1.893		1.893		
Easy of Use (EU)			2.140			
Intention of Use (IU)					1.000	
Perceived Usefulness (PU)			2.140			
Trust in Government (TG)						
Trust in Technology (TT)		1.893		1.893		

4.4.2. Hypothesis Confirmation

BTA positively influences PU (H1a):

In the empirical analysis, a substantial positive impact of Biometric Technology Awareness (BTA) on three key constructs was observed: Ease of Use (EU), Intention of Use (IU), and Perceived Usefulness (PU). As BTA increases, users demonstrate a heightened perception of user-friendliness (EU), a more positive intention to use the technology (IU), and an enriched understanding of the practical advantages of biometric technology (PU). This empirical evidence aligns with theoretical expectations and highlights the comprehensive influence that awareness can exert on multiple dimensions of user perception and behaviour.

BTA positively influences EU (H1b):

The empirical investigation reveals a clear and positive influence of Biometric Technology Awareness (BTA) on Ease of Use (EU). As users' awareness of biometric technology increases, there is a corresponding enhancement in the perception of user-friendliness.

TT positively influences PU (H2a):

Upon meticulous scrutiny, it is imperative to note that H2a pertains to the relationship between Trust in Technology (TT) and Perceived Usefulness (PU). This hypothesis posits that trust in technology is positively connected to the perceived usefulness of biometric technology. The empirical evidence gleaned from our data analysis strongly supports H2a. Therefore, based on our findings, we confirm that Trust in Technology (TT) positively influences Perceived Usefulness (PU). This finding underscores

the impact of trust in technology on users' perception of the utility of biometric systems, highlighting trust as a pivotal factor in enhancing perceived usefulness.

TT positively influences EU (H2b):

The empirical analysis provides support for H2b. The positive path coefficient observed in the relationship between Trust in Technology (TT) and Ease of Use (EU) is statistically significant, indicating a robust connection between users' trust in technology and their perception of the technology's ease of use.

PU positively influences IU (H3):

The empirical analysis confirms the validity of H3. The positive path coefficient observed in the relationship between Perceived Usefulness (PU) and Intention of Use (IU) is statistically significant, indicating a strong and positive connection between users' perception of the technology's usefulness and their intention to use it.

EU positively influences IU (H4):

The empirical analysis supports the assertion of H4. The positive path coefficient observed in the relationship between Ease of Use (EU) and Intention of Use (IU) is statistically significant, providing empirical evidence that user-friendliness plays a pivotal role in shaping users' intentions to adopt biometric technology in the public sector.

IU positively influences TG (H5):

The empirical investigation affirms the validity of H5. The robust positive relationship, indicated by a significant path coefficient between Intention of Use (IU) and Trust in Government (TG), provides empirical support for the hypothesis.

Table 12 - Research hypothesis status after the empirical results have been analysed

Code	Hypothesis	Status
H1a	Biometric Technology Awareness positively shapes users' experiences, intentions, and perceived utility.	**Confirmed**
H1b	Users who have a thorough grasp of biometric technology are more likely to find it simple to use.	**Confirmed**
H2a	Users who have more faith in technology are more likely to find it beneficial.	**Confirmed**
H2b	Users who have faith in technology will regard it as more accessible and user-friendly.	**Confirmed**
H3	When users view a technology to be beneficial, they are more inclined to adopt it.	**Confirmed**
H4	Easy-to-use systems are more likely to generate a good intention to embrace the technology.	**Confirmed**
H5	People who have a favourable desire to use biometric technology are more inclined to trust government agencies that have adopted it.	**Confirmed**

The findings, consistent with theoretical expectations, validate all the hypotheses. The intricate relationships between awareness, user-friendliness, trust, and intention underscore the nuanced factors influencing the adoption of biometric technology in the public sector. These insights, gleaned from a meticulous analysis of the provided data, hold implications for future research and practical implementations in the domain of biometric technology adoption.

5. CONCLUSIONS AND FUTURE WORK

This section acts as a lighthouse, showcasing the key insights and significant conclusions obtained from this research's extensive journey. The research focused on the intersection between AI-driven self-service technology and the complex world of biometric data in the public sector. Our journey across this diverse environment reveals a rich tapestry of opportunity plus equally intricate problems. The convergence of these technologies defines a diverse ecosystem in which technical development meets the complicated demands of government and public service.

The investigation took a path that examined the effectiveness and operational benefits of these innovative technologies but also the ethical issues intertwined with their application. It revealed a story highlighted by the promise of simplified procedures, resource efficiency, and service accessibility on the one hand and the critical nature of privacy measures, ethical concerns, and data rights implications on the other. This synthesis, where technology meets governance, provides a complex yet exciting picture in which the requirement to maintain ethical and secure practises is tightly linked. Through this lens, our investigation traversed the landscapes of technological integration, exploring the improvements and complexities of responsible implementation that reverberate across a range of legal, ethical, and societal views.

5.1. KEY FINDINGS

We look into the significant insights gained from the public sector's integration of biometric data and AI-based self-service technologies. The research investigated the transformational influence of this technology, discovering a shift that improves operational efficiency, strengthens security frameworks, and necessitates intensive ethical scrutiny. These findings give a narrative that not only reveals the potential of governance technology but also highlights the significance of traversing this landscape with an unwavering commitment to ethical integrity.

Efficiency and Cost Savings

The synergistic combination of biometric data with AI-driven self-service platforms has emerged as a game-changing approach in the public sector (Chen et al., 2021). This integration drives process efficiency and refinement, resulting in significant gains in resource allocation and usage. Public enterprises benefit significantly from biometric data in operational efficiency and economic prudence (Owusu-Oware & Effah, 2022). These developments point to a fundamental shift in the sector's functionality, indicating a significant move towards simplified operations and enhanced service delivery (Hekal et al., 2023; Hernandez-de-Menendez et al., 2021).

Amplified Security Measures

Biometric data usage in conjunction with AI-driven systems is a critical component in strengthening security processes within public sector companies. This integration ensures perfect identity verification, strengthened data processing, and the rigorous imposition of access control measures, resulting in a strong and secure environment (Arora & Bhatia, 2022; Khan & Efthymiou, 2021). This strengthened security framework is critical in securing sensitive information and fostering citizen trust in both government institutions and the deployed technical infrastructure (Biming, 2023).

Ethical and Legal Implications

The multidimensional terrain of integrating biometric technology in the public sector delicately intertwines with a web of ethical and legal problems. This detailed analysis highlights the critical need to gain informed permission, apply data reduction techniques, establish effective security measures, and adhere to regulatory norms without fail (Shi, 2023). The rigorous attention to these details emphasises the ethical and appropriate biometric technology usage (Melzi et al., 2022). Maintaining individual privacy and data rights becomes the cornerstone of adopting biometric solutions in the public sector, sustaining trust and ethical integrity within the technology-driven environment of governance (Liyanaarachchi et al., 2023; Natgunanathan et al., 2016).

5.2. CONTRIBUTIONS TO THE FIELD

This thesis represents a significant contribution to the field, focusing on the effectiveness and ethical use of biometric data in the public sector through AI-driven self-service platforms. The study has made specific contributions and yielded fresh insights, with practical implications for various stakeholders.

Connecting Technology and Ethics:

- **Contribution**: This research bridges the divide between technological innovation and ethical considerations, addressing a pressing contemporary issue. It underscores the importance of enhancing operational efficiency and security while safeguarding individual privacy and data rights within an ethical framework.
- **Importance**: This emphasis on ethical technology adoption provides a holistic perspective, recognizing that technology should not compromise fundamental principles.

Comprehensive Theoretical Framework:

- **Contribution:** The fusion of the TAM, ISSM, and CVT creates a robust framework for examining biometric technology adoption in the public sector.
- **Importance:** This comprehensive framework offers a nuanced approach to understanding the complexities of biometric technology adoption, going beyond mere efficiency enhancements.

Empirical Insights and Recommendations:

- **Contribution:** The research provides valuable empirical insights into the drivers of biometric technology adoption and its implications for the public sector.
- **Importance:** Practical recommendations arising from the study offer guidance to public sector organizations, policymakers, and technology developers for the efficient and ethical deployment of biometric technology.

Emphasis on Ethics and Privacy:

- **Contribution:** The research focuses on ethical considerations, encompassing aspects such as informed consent, data minimization, secure data processing, and regulatory compliance.
- **Importance:** This ethical emphasis underscores the significance of preserving individual privacy and data rights, providing a roadmap for public sector organizations in their technological implementations.

Future Research Avenues:

- **Contribution:** The thesis outlines various prospective research areas, addressing limitations and charting the course for further developments in the field.
- **Importance:** These future research directions serve as a guide for delving deeper into the multifaceted realm of biometric data utilization, ensuring equitable, secure, and efficient technology adoption.

Trust in Government and Technology:

- **Contribution:** The study highlights the interconnected nature of trust domains, demonstrating that confidence in government can influence trust in technology within public sector contexts.
- **Importance:** This insight aids in comprehending how trust dynamics may impact technology adoption and underscores the need to cultivate public trust through secure technology implementations.

Awareness and Education:

- **Contribution:** The research emphasizes the importance of educational efforts in technology adoption, showing a positive correlation between knowledge of biometric technology and its ease of use.
- **Importance:** Public sector organizations can leverage this finding to steer awareness campaigns promoting the usability of self-service applications.

These contributions exemplify the significance of the research in advancing the field and addressing the critical challenges surrounding biometric data integration in the public sector. The study serves as a valuable resource for those navigating the evolving landscape of biometric technology in the public sector by focusing on the convergence of technology and ethics, providing a comprehensive theoretical framework, and offering practical guidance.

5.3. Addressing the Research Query

The primary goal of this thesis was to address the question, "How can biometric data be used efficiently and ethically in the public sector through AI-based self-service technologies to enhance efficiency, reduce costs, and heighten security, all while preserving individuals' privacy and data rights?" The study was meticulously designed to analyse and tackle this complex issue, leading to substantial findings that provide critical insights into this multifaceted topic.

Table 13 - Research Question Findings Summary

Research Question	Findings	Explanation
How can biometric data be used efficiently and ethically in the public sector through AI-based self-service technologies to enhance efficiency, reduce costs, and heighten security, all while preserving individuals' privacy and data rights?	Efficiency Enhancement	Integrating biometric data with AI-driven self-service platforms significantly enhances operational efficiency in the public sector. By automating identity verification and streamlining processes, these technologies reduce the time and resources required for service delivery, leading to cost savings, and improved public service accessibility.
	Cost Reduction	Biometric data usage and AI technology reduce costs associated with manual processing and human errors. Automation minimizes the need for extensive human labour and reduces the likelihood of fraud and inaccuracies, resulting in financial savings for public sector organizations.
	Heightened Security	Biometric data usage, combined with AI-based self-service technology, leads to notable enhancements in security measures. Biometric identifiers (e.g., fingerprints, and facial recognition) provide a higher level of security compared to traditional methods, making it harder for unauthorized individuals to gain access.
	Preserving Privacy and Data Rights	Ethical considerations and safeguards are crucial for protecting privacy and data rights. Implementing robust privacy measures, such as encryption and anonymization, ensures that individuals' biometric data is protected from misuse and breaches. Policies and frameworks must be developed to uphold data rights and gain public trust.
	Trust Establishment	Establishing trust relationships between the public and government is vital for technology acceptance. Building public confidence through transparency, accountability, and clear communication about the benefits and safeguards of biometric technologies enhances trust in both the government and the technology.
	Practical Recommendations	The study offers practical recommendations for public sector organizations, policymakers, and technology developers. Recommendations include adopting comprehensive privacy policies, investing in secure biometric systems, and conducting regular audits to ensure compliance with ethical standards.

In conclusion, the study effectively addressed the central research question, demonstrating that biometric data can be employed efficiently and ethically in the public sector through AI-based self-service technology. The findings underscore the potential for enhanced operational efficiency, security, privacy, and data rights, providing a roadmap for future research and practical recommendations for implementation.

5.4. IMPLICATIONS

This study's findings have significant implications for public policy, the private sector, and future research.

For public policy, public sector entities can improve efficiency and reduce costs through biometric data integration with AI-driven self-service solutions (Chen et al., 2021). Policymakers should develop frameworks to facilitate this adoption, leading to streamlined service delivery (Hekal et al., 2023). Authorities should prioritize robust privacy laws for biometric data usage in the public sector, balancing individual rights and technology deployment (Shi, 2023).

In the private sector, technology providers should recognize opportunities in AI-driven self-service solutions for the public sector, fostering partnerships and advancements (Hernandez-de-Menendez et al., 2021). Private entities should focus on tailored cybersecurity solutions to protect biometric data in the public sector (Štitilis et al., 2023).

Future research should explore ethical dimensions of biometric data use, including consent and data minimization. Studies should investigate public attitudes toward biometric technologies to ensure socially responsible implementation. Comparative research across regions can offer insights into the global applicability of biometric data usage. Research should also examine how biometric data usage affects marginalized communities to promote equitable technology adoption.

In conclusion, the study highlights the potential for improved public service delivery through biometric data and AI-driven technologies, emphasizing the need for ethical considerations and privacy rights. The private sector can align innovations with public sector needs, fostering collaboration. Future research should address ethical issues and explore new dimensions of biometric data usage.

5.5. LIMITATIONS

Addressing the limitations identified is crucial for future research credibility. Future studies should involve larger and more diverse samples to improve generalizability. Integrating self-reported data with behavioural data can enhance result accuracy. Longitudinal studies can track changes over time, providing dynamic insights. Future research should explore biometric data usage across diverse regions and cultures. Comparative legal studies can provide insights into how different laws impact biometric data usage.

Future research should address these limitations for a more robust understanding of biometric data utilization in the public sector.

5.6. FUTURE AVENUES FOR RESEARCH

This study lays the foundation for further research into biometric data usage in the public sector through AI-driven self-service platforms.

Continuous monitoring can provide a dynamic view of technology adoption. Expanding samples to include various public sector organizations can offer broader insights. Comparative research can explore the influence of different legal frameworks and cultural norms. Combining self-reported data with behavioural data offers a holistic understanding of technology adoption. Research should explore data privacy intricacies within the public sector. Understanding public attitudes and concerns can guide effective implementation strategies. Research should ensure technology adoption is inclusive and equitable. Examining different legal frameworks can identify best practices and harmonize regulatory standards.

Future research will enhance the understanding of biometric data utilization, addressing limitations and exploring new dimensions for responsible implementation.

5.7. FINAL REMARKS

This thesis explored biometric data usage in the public sector, focusing on AI-driven self-service technologies. The primary question was how to employ biometric data efficiently and ethically to enhance efficiency, reduce costs, and strengthen security while safeguarding privacy and data rights.

The findings highlight substantial potential for improving efficiency and security, emphasizing the need for ethical considerations. The implications guide public sector entities in enhancing operations and underscore the importance of public trust through secure data management.

This research contributes to the evolving landscape of technology adoption and governance, providing a foundation for future studies, policy development, and informed decision-making in the public sector. The journey of biometric data usage continues, guided by progress and ethics, shaping a responsible and innovative future.

BIBLIOGRAPHICAL REFERENCES

Adeyemi, I. O., & Issa, A. O. (2020). Integrating Information System Success Model (ISSM) And Technology Acceptance Model (TAM): Proposing Students' Satisfaction with University Web Portal Model. *Record and Library Journal*, *6*(1), Article 1. https://doi.org/10.20473/rlj.V6-I1.2020.69-79

Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, *31*(1), 28–48. https://doi.org/10.1080/19393555.2021.1873464

Barlow, M. (2017). *Artificial intelligence across industries: How AI is transforming telco, retail, and financial services* (First edition.). O'Reilly Media. https://learning.oreilly.com/library/view/-/9781491991046/?ar

Berryhill, J., Heang, K. K., Clogher, R., & McBride, K. (2019). *Hello, World: Artificial intelligence and its use in the public sector*. OECD. https://doi.org/10.1787/726fd39d-en

Biming, B. (2023). *Unlocking the Future: Exploring Biometric Applications for Enhanced Security and Convenience*. https://www.hilarispublisher.com/abstract/unlocking-the-future-exploring-biometric-applications-for-enhanced-security-and-convenience-99984.html

Chen, T., Guo, W., Gao, X., & Liang, Z. (2021). AI-based self-service technology in public service delivery: User experience and influencing factors. *Government Information Quarterly*, *38*(4), 101520. https://doi.org/10.1016/j.giq.2020.101520

Chen, T., Ran, L., & Gao, X. (2019). AI innovation for advancing public service: The case of China's first Administrative Approval Bureau. *Proceedings of the 20th Annual International Conference on Digital Government Research*, 100–108. https://doi.org/10.1145/3325112.3325243

Chui, M., Manyika, J., Miremadi, M., Henke, N., Chung, R., Nel, P., & Malhotra, S. (2018, April). *Notes from the AI frontier: Insights from hundreds of use cases*. McKinsey Global Institute. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20ai%20frontier%20applications%20and%20value%20of%20deep

%20learning/notes-from-the-ai-frontier-insights-from-hundreds-of-use-cases-discussion-paper.pdf

Darendeli, F. (2023). *The Protection of Biometric Data in the Era of Artificial Intelligence Technology in Eu Law—ProQuest*. The Protection of Biometric Data in the Era of Artificial Intelligence Technology in Eu Law. https://hdl.handle.net/11424/289668

Gesk, T. S., & Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its usage. *Government Information Quarterly*, *39*(3), 101704. https://doi.org/10.1016/j.giq.2022.101704

Hekal, M. M. M., Gamal El-den, N. E., & Abd Al-latif., T. (2023). Self-service technology and its impact on the User. *International Design Journal*, *13*(6), 357–363. https://doi.org/10.21608/idj.2023.319590

Hernandez-de-Menendez, M., Morales-Menendez, R., Escobar, C. A., & Arinez, J. (2021). Biometric applications in education. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *15*(2–3), 365–380. https://doi.org/10.1007/s12008-021-00760-6

Jain, A. K., Deb, D., & Engelsma, J. J. (2022). Biometrics: Trust, But Verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(3), 303–323. IEEE Transactions on Biometrics, Behavior, and Identity Science. https://doi.org/10.1109/TBIOM.2021.3115465

Jain, A. K., & Kumar, A. (2012). Biometric Recognition: An Overview. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context* (pp. 49–79). Springer Netherlands. https://doi.org/10.1007/978-94-007-3892-8_3

Kardoyo, K., Nurkhin, A., & Arief, S. (2015). *The Determinant of Student's Intention to Use Mobile Learning*. https://doi.org/10.20319/pijss.2015.s11.102117

Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). *International Journal of Information Management Data Insights*, *1*(2), 100049. https://doi.org/10.1016/j.jjimei.2021.100049

Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*. Zenodo. https://doi.org/10.5281/zenodo.3240529

Liyanaarachchi, G., Viglia, G., & Kurtaliqi, F. (2023). Privacy in hospitality: Managing biometric and biographic data with immersive technology. *International Journal of Contemporary Hospitality Management*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/IJCHM-06-2023-0861

Martono, S., Nurkhin, A., Mukhibad, H., Anisykurlillah, I., & Wolor, C. W. (2020). Understanding the Employee's Intention to Use Information System: Technology Acceptance Model and Information System Success Model Approach. *The Journal of Asian Finance, Economics and Business*, *7*(10), 1007–1013. https://doi.org/10.13106/jafeb.2020.vol7.no10.1007

Meden, B., Rot, P., Terhörst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Štruc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2021.3096024

Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (2022). *An Overview of Privacy-enhancing Technologies in Biometric Recognition* (arXiv:2206.10465). arXiv. https://doi.org/10.48550/arXiv.2206.10465

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of Privacy in Biometric Data. *IEEE Access*, *4*, 880–892. IEEE Access. https://doi.org/10.1109/ACCESS.2016.2535120

North-Samardzic, A. (2020). Biometric Technology and Ethics: Beyond Security Applications. *Journal of Business Ethics*, *167*(3), 433–450. https://doi.org/10.1007/s10551-019-04143-6

Owusu-Oware, E., & Effah, J. (2022). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation.

Information Development, 02666669221085709. https://doi.org/10.1177/02666669221085709

Plantinga, P. (2022). Digital discretion and public administration in Africa: Implications for the use of artificial intelligence. *Information Development*, 02666669221117526. https://doi.org/10.1177/02666669221117526

Sabhanayagam, T., Venkatesan, D. V. P., & Senthamaraikannan, D. K. (2018). *A Comprehensive Survey on Various Biometric Systems*. *13*(5). https://www.ripublication.com/Volume/ijaerv13n5.html

Sharif, M., Raza, M., Shah, J. H., Yasmin, M., & Fernandes, S. L. (2019). An Overview of Biometrics Methods. In A. K. Singh & A. Mohan (Eds.), *Handbook of Multimedia Information Security: Techniques and Applications* (pp. 15–35). Springer International Publishing. https://doi.org/10.1007/978-3-030-15887-3_2

Shi, Q. (2023). Guardians of Privacy: Understanding the European Union's Framework for Biometric Data Protection. *International Journal of Biology and Life Sciences*, *3*(1), Article 1. https://doi.org/10.54097/ijbls.v3i1.9669

Shin, H., & Perdue, R. R. (2019). Self-Service Technology Research: A bibliometric co-citation visualization analysis. *International Journal of Hospitality Management*, *80*, 101–112. https://doi.org/10.1016/j.ijhm.2019.01.012

Siau, K., & Wang, W. (2020). Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI. *Journal of Database Management (JDM)*, *31*(2), 74–87. https://doi.org/10.4018/JDM.2020040105

Sobrino-García, I. (2021). Artificial Intelligence Risks and Challenges in the Spanish Public Administration: An Exploratory Analysis through Expert Judgements. *Administrative Sciences*, *11*(3), Article 3. https://doi.org/10.3390/admsci11030102

Štitilis, D., Laurinaitis, M., & Verenius, E. (2023). The Use of biometric technologies in ensuring critical infrastructure security: The context of protecting personal data. *Entrepreneurship and Sustainability Issues*, *10*, 133–150. https://doi.org/10.9770/jesi.2023.10.3(10)

Turel, O., Serenko, A., & Bontis, N. (2010). User acceptance of hedonic digital artifacts: A theory of consumption values perspective. *Information & Management*, *47*(1), 53–59. https://doi.org/10.1016/j.im.2009.10.002

Valle-Cruz, D., Alejandro Ruvalcaba-Gomez, E., Sandoval-Almazan, R., & Ignacio Criado, J. (2019). A Review of Artificial Intelligence in Government and its Potential from a Public Policy Perspective. *Proceedings of the 20th Annual International Conference on Digital Government Research*, 91–99. https://doi.org/10.1145/3325112.3325242

Villegas-Ch, W., & García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics*, *12*(18), Article 18. https://doi.org/10.3390/electronics12183786

Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, *21*(7), 1076–1100. https://doi.org/10.1080/14719037.2018.1549268

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial Intelligence and the Public Sector—Applications and Challenges. *International Journal of Public Administration*, *42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration. *International Journal of Public Administration*, *43*(9), 818–829. https://doi.org/10.1080/01900692.2020.1749851

APPENDIX A

AI-based SST using Biometric Data

Q1 Introductory note

This questionnaire is integrated in the Nova IMS Master program of Information Management, having as primary goal how can biometric data be used in the public sector efficiently and ethically through AI-based self-service technologies to improve efficiency, cut costs, and enhance security while safeguarding individuals' privacy and data rights.

This survey takes up to 5 minutes to complete in order to evaluate your opinion regarding your use and understanding of AI-based self-service technologies and biometric data. This questionnaire presents no risk. Your participation is completely volunteer so feel free to participate or not, as well as to stop at any moment. This work has been approved by the Nova IMS ethical commission.

May you have any doubts, please send an email to: r2014489@novaims.unl.pt.

Thank you for your collaboration.

José Sequeira

Q2 Consent form

By clicking "I agree" below you are indicating that you are at least 18 years old, have read and understood this consent form and agree to participate in this research study.

- ○ I agree to participate on this questionnaire. (1)
- ○ I do not agree to participate on this questionnaire. (2)

Q3 Subject Introduction:

Biometric data usage in the public sector through AI-based self-service technologies (AI-based SST) is growing, enhancing security and convenience. Biometric data includes physical and behavioural traits like fingerprints and facial recognition. It allows public organisations to verify citizens' identities and provide secure access to services. AI-based SSTs are automated systems enabling self-service for passports, visas, taxes, welfare, and healthcare. While promising service quality, cost reduction, and security, biometric data usage raises privacy, data protection, and ethical concerns, necessitating responsible and transparent practices to protect citizens' rights.

Q4 Biometric Technology Awareness

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I am aware that AI-based SSTs using Biometric Data are saving my biometric data (1)	○	○	○	○	○	○	○
I am aware that AI-based SSTs are using my fingerprints for identification purposes (2)	○	○	○	○	○	○	○
I am aware that AI-based SSTs using Biometric Data helps individuals making informed decisions (3)	○	○	○	○	○	○	○

Q5 Trust in Technology

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
AI-based SST using Biometric Data works reliably (1)	○	(	(	(	(	(	○
I have already used AI-based SST that uses Biometric Data (2)	○	(	(	(	(	(	○
I trust AI-based SST that uses Biometric Data (3)	○	(	(	(	(	(	○

Q6 System Quality

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I find AI-based SSTs that use Biometric Data user-friendly (1)	○	(	(	(	(	(	○
AI-based SSTs that use Biometric Data meet my needs (2)	○	(	(	(	(	(	○
AI-based SSTs that use Biometric Data is always available (3)	○	(	(	(	(	(	○

Q7 Privacy

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I'm concerned that my personal information will be shared or sold to others when I enter AI-based SSTs that use Biometric Data. (1)	○						○
I am concerned about the potential loss caused by privacy invasion. (2)	○						○
I worry that others may view my biometric information. (3)	○						○

Q8 Perceive Usefulness

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
The use of AI-based SST that use Biometric Data saves me time when dealing with public services. (1)	○						○
The use of AI-based SSTs that use Biometric Data gives me full control when dealing with public services. (2)	○						○
The use of AI-based SST that use Biometric Data gives me flexibility when dealing with public services. (3)	○						○

Q9 Easy of Use

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
If I wanted to use AI-based SST that uses Biometric Data, it would be easy for me. (1)	○	(	(	(	(	(	○
If I wanted to use AI-based SST that uses Biometric Data, it would be simple to me. (2)	○	(	(	(	(	(	○
If I wanted to use AI-based SST that uses Biometric Data, I would have no problems. (3)	○	(	(	(	(	(	○

Q10 User Experience

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
AI-based SST that uses Biometric Data is easy to understand. (1)	○	(	(	(	(	(	○
User feels in control when interacting with AI-based SST that uses Biometric Data. (2)	○	(	(	(	(	(	○
AI-based SST that uses Biometric Data is fast and efficient to use. (3)	○	(	(	(	(	(	○

Q11 Trust in Government

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I trust that parliament is managing AI-based SST that uses Biometric Data well. (1)	○						○
I trust that the government is using AI-based SST that uses Biometric Data in the right way. (2)	○						○
The central government/municipality will do its best to implement AI-based SST that use Biometric Data. (3)	○						○

Q12 Intention of Use

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I intend to use AI-based SST that uses Biometric Data in the near future. (1)	○						○
I will use AI-based SST that uses Biometric Data every time I have the opportunity. (2)	○						○
I plan to use AI-based SSTs that use Biometric Data in public services. (3)	○						○

Q13 User Satisfaction

	1 (Strongly Disagree) (1)	2 (2)	3 (3)	4 (4)	5 (5)	6 (6)	7 (Strongly Agree) (7)
I think AI-based SSTs that use Biometric Data are useful. (1)	○						○
I think AI-based SSTs that use Biometric Data are worth the time and effort required to use them. (2)	○						○
Overall, you are satisfied with AI-based SSTs that use Biometric Data. (3)	○						○

Q14 Base on past experience, which public services would benefit from the implementation and use of AI-based SST that use Biometric Data?
(You can select more than one)

- ☐ Healthcare (1)
- ☐ Education (2)
- ☐ Transportation (3)
- ☐ Social Welfare (4)
- ☐ Other (please specify) (5)

_____

Q15 What is your gender?

- ○ Male (1)
- ○ Female (2)
- ○ Non-binary / third gender (3)
- ○ Prefer not to say (4)

Q16 How old are you?

- ○ 18 - 24 (1)
- ○ 25 - 34 (2)
- ○ 35 - 44 (3)
- ○ 45 - 54 (4)
- ○ 55 - 64 (5)
- ○ 65 - 74 (6)
- ○ 75 - 84 (7)
- ○ 85 or older (8)

Q17 What is your education level?

- ○ Less than high school (1)
- ○ High school graduate (2)
- ○ Bachelor Degree (3)
- ○ Master Degree (4)
- ○ Doctorate (5)

ANNEXES

Ethics Committee Approval

NOVA IMS | Ethics Committee - APPROVED

Qualtrics Survey Software <noreply@qemailserver.com>

sex, 19/05/2023 18:22

Para:Jose Carlos Bate Eusebio Sequeira (R2014489) <r2014489@novaims.unl.pt>

This is to certify that

Project No.: INFSYS2023-5-192033

Project Title: Usage of biometric data in the Public Sector using Artificial Intelligence based Self-Service Technologies (AI-based SST)

Principal Researcher: José Carlos Bate Eusébio Sequeira

according to the regulations of the Ethics Committee of NOVA IMS and MagIC Research Center this project was considered to meet the requirements of the NOVA IMS Internal Review Board, being considered APPROVED on 5/19/2023.

It is the Principal Researcher's responsibility to ensure that all researchers and stakeholders associated with this project are aware of the conditions of approval and which documents have been approved.

The Principal Researcher is required to notify the Ethics Committee, via amendment or progress report, of

- Any significant change to the project and the reason for that change;

- Any unforeseen events or unexpected developments that merit notification;

- The inability of the Principal Researcher to continue in that role or any other change in research personnel involved in the project.

Lisbon, 5/19/2023

NOVA IMS Ethics Committee

ethicscommittee@novaims.unl.pt