Mapping Stakeholder Perceptions: Navigating Biometric Data Protection Initiative and Face Recognition Technology Support in Indonesia

Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen *

Posted Date: 8 September 2023

doi: 10.20944/preprints202309.0547.v1

Keywords: stakeholder; perception; biometric data protection; face recognition technology

Article

Mapping Stakeholder Perceptions: Navigating Biometric Data Protection Initiative and Face Recognition Technology Support in Indonesia

Sih Yuliana Wahyuningtyas [1] and Yerik Afrianto Singgalen [2,*]

[1] Faculty of Law, Atma Jaya Catholic University of Indonesia, South of Jakarta, DKI Jakarta, 12930, Indonesia; yuliana.siswartono@atmajaya.ac.id

[2] Faculty of Business Administration and Communication, Atma Jaya Catholic University of Indonesia, South of Jakarta, DKI Jakarta, 12930, Indonesia; yerik.afrianto@atmajaya.ac.id

* Correspondence: yerik.afrianto@atmajaya.ac.id; Tel. : +62-81259599504

Abstract: This research aims to thoroughly understand the delicate interplay between stakeholders' perspectives, biometric data protection policies, and the deployment of face recognition technologies in Indonesia's dynamic digital world. Adopting a qualitative methodology, the study conducts Focus Group Discussions (FGDs) with various stakeholders, including government agencies, technology developers, regulatory agencies, civil society groups, and data subjects as end-users. Face-to-face group discussions facilitate an in-depth exploration of participants' perspectives, yielding rich qualitative data that reveals nuanced insights into the delicate balance between technological innovation, ethical considerations, and socioeconomic repercussions associated with implementing face recognition technology. The research comprehensively explains the difficulties and opportunities associated with responsible technological progress and biometric data security. The findings from the FGDs influence the development of strategies that effectively balance technical advancement with individual rights, privacy, and social well-being within the growing digital landscape of Indonesia. The regulatory function of the government seeks to bridge the gap between public expectations and technological advancements. Collaboration between academic institutions, government agencies, the private sector, and data subjects as end-users emerges as a crucial element, fostering an all-encompassing strategy integrating research, law, technology deployment, and user empowerment. This holistic approach is necessary to ensure that biometric data and facial recognition technology are utilized responsibly, thereby laying the way for Indonesia's technologically sophisticated and ethically aware digital future.

Keywords: stakeholder; perception; biometric data protection; face recognition technology

1. Introduction

Globally, the growth of face recognition technology has spawned transformational improvements in numerous domains. This technology is becoming more prevalent in Indonesia, a rapidly developing digital society, and it has great promise for enhancing security, efficiency, and convenience. Due to the sensitive nature of facial information, face recognition technology needs a stringent focus on biometric data security [1]. This introduction explores the emerging environment of face recognition technology deployment in Indonesia, highlighting the need for adequate biometric data protection to traverse the complex intersection of technical innovation and privacy protection.

The acceptability of facial recognition technology is a complicated phenomenon driven by cognitive, social, and contextual aspects that influence the propensities of individuals to embrace or reject such advancements [2]. This paradigm extends to the knowledge of biometric data hazards, in which individuals' cognitive identification of potential vulnerabilities to the security and privacy of their biometric information plays a crucial part in determining their attitudes and actions toward adopting such technology [3]. The intricate interplay between these characteristics exemplifies the

 doi:10.20944/preprints202309.0547.v1

complex dynamics underlying the adoption and use of face recognition technology, demonstrating the delicate equilibrium between perceived benefits and concerns over biometric data risks [4].

The complexity of the infrastructure requirements to enable facial recognition technology encompasses processing resources, network bandwidth, and hardware capabilities, which combined define the efficiency and scalability of the deployment [5]. This multilayered task necessitates robust computational architectures capable of rapidly processing complex facial patterns and a network infrastructure to accommodate the considerable data transmission demands inherent to real-time recognition operations [6]. In addition, deploying hardware components optimized for facial feature extraction and matching adds to the complexity of this technological obstacle, highlighting the need for a comprehensive and integrated approach to infrastructure development for the seamless integration and operation of face recognition technology [7].

The problem of biometric data protection through face recognition technology is complicated, needing the harmonization of technical, legal, and ethical frameworks in order to eliminate inherent vulnerabilities and secure the privacy of individuals' biometric data [8] [9]. This difficulty is compounded by the complexity of face data, which, once compromised, has irreversible repercussions, demanding sophisticated encryption techniques, secure storage mechanisms, and severe access controls to prevent unauthorized acquisition or manipulation [10]. Moreover, the establishment of comprehensive legal frameworks tailored to the unique complexities of biometric data, as well as the cultivation of ethical guidelines pertaining to consent, transparency, and data sovereignty, serves as a critical imperative for navigating the complex landscape of biometric data protection, thereby bolstering societal trust in the application of face recognition technology [11].

The originality of the research pertaining to the biometric data protection issue and face recognition technology in a developing country context, specifically Indonesia, lies in its exploration of the intricate interplay between nascent technological implementations and the intricate socioeconomic, cultural, and legal dimensions typical of such settings. This study is the first to investigate the unique problems and opportunities within the Indonesian context, offering insight into the intricate dynamics of technology adoption, data privacy issues, and legislative frameworks peculiar to a developing nation. By elucidating these complex interactions, the study contributes to a deeper understanding of the multifaceted landscape surrounding biometric data protection and face recognition technology in developing countries, paving the way for contextually informed strategies that balance technological progress and individual and societal well-being.

The correlation between sustainability, biometric data protection, and face recognition technology constitutes a pivotal nexus wherein ensuring enduring socio-technological progress converges with the necessity to safeguard individual privacy and ethical considerations in an increasingly digitized landscape [12]. The amalgamation of these elements elucidates a multifaceted interrelationship, as the sustainable deployment of face recognition technology necessitates meticulous attention to biometric data protection, thereby engendering a harmonious equilibrium between technological advancement and ethical accountability [13]. This symbiotic relationship underscores the significance of cultivating resilient technological ecosystems that not only propel socio-economic development but also uphold the fundamental rights of individuals, thereby fostering a holistic framework that resonates with sustainable principles while navigating the complexities of emergent biometric technologies.

The significance of stakeholders' perception mapping lies in its capacity to systematically identify, analyze, and comprehend the multifaceted dimensions of sustainability in connection with biometric data protection, which end implies the support of face recognition technology. This process facilitates the holistic evaluation of diverse stakeholders' perspectives, ranging from government bodies, regulatory authorities, and technology developers to civil society groups and data subjects as end-users, illuminating an intricate tapestry of insights into the complex interplay between technological innovation, ethical considerations, and socio-economic implications. By synthesizing these perceptions, this mapping not only aids in pinpointing potential conflicts and synergies within sustainability initiatives but also informs the formulation of contextually appropriate strategies that

 doi:10.20944/preprints202309.0547.v1

promote responsible technological advancement, address privacy concerns, and foster a harmonious socio-technological milieu centered on enduring ethical and societal values.

2. Literature Review

2.1. Face Recognition Technology

Understanding face recognition technology requires a comprehensive awareness of the numerous processes involved in recording, processing, and evaluating facial characteristics for identification and verification purposes [14]. This technique employs sophisticated algorithms to turn unique facial features into mathematical representations, enabling the construction of individual biometric profiles [15]. Facial recognition systems enable the identification of persons or the validation of their claimed identity through feature extraction and comparison [16]–[18]. The understanding of this technology extends beyond its technical complexities to incorporate broader considerations, such as its potential applications across diverse domains, its ethical implications in terms of privacy and data protection, and its societal impacts on security, convenience, and human-computer interaction paradigms [19]–[22]. Thus, a thorough knowledge of face recognition technology entails an appreciation of its technical foundations and ramifications within broader sociocultural and ethical contexts.

The architecture of face recognition technology consists of a structured framework with discrete components that permit the identification and authentication of persons based on their facial traits [23], [24]. Face images are often collected by cameras or sensors, followed by preprocessing operations that include noise reduction, alignment, and normalization to improve image quality and consistency [25], [26]. Subsequently, feature extraction techniques extract relevant facial characteristics and convert them into numerical representations capable of discrimination [27]. Pattern recognition algorithms create similarity scores for identification or verification by comparing these extracted features to a stored template database [28]. Additionally, the design includes decision-making modules that analyze matching results and determine the ultimate identification confirmation [29]. Depending on the system's complexity, additional components such as encryption techniques, database management systems, and user interfaces contribute to the system's overall architecture [30]–[33]. Understanding this architecture is essential to comprehending the complex orchestration of activities that enable the efficient operation of face recognition technology systems [34].

The growth of face recognition technology is hindered by various limitations and obstacles that impede its application across diverse industries [35]–[39]. A significant barrier is the possibility of algorithmic bias, wherein mistakes result from the unequal representation of demographic groups in training data, leading to varied performance across different populations [40]. In addition, worries continue regarding the technology's sensitivity to adversarial attacks, whereby tiny modifications to facial photos might evade identification systems, undermining their dependability and security [41]. Ethical and privacy concerns are equally important since the prevalence of face data collecting raises concerns about inappropriate surveillance, consent, and illegal data use [42]. In addition, the efficacy of the technology can be impaired by poor lighting, occlusions, or fluctuations in facial expressions, making it less reliable in real-world, uncontrolled conditions [43]–[45]. Face recognition's broad capabilities create concerns regarding the possibility of mass monitoring infringing on civil liberties, making it difficult to balance security imperatives and individual rights [46]. In order to advance facial recognition technology while respecting societal norms, privacy, and ethics, it is essential to navigate these complex obstacles.

Within the environment of face recognition technology, a glaring research void appears, necessitating deeper investigation and study. Although substantial progress has been made in refining the technical components of recognition algorithms, little effort has been devoted to comprehending the socio-cultural dimensions underpinning this technology's deployment and impact. Few studies examine the complex interplay between cultural variables, demographic differences, and algorithmic biases, which can lead to differential performance among population

groups. Moreover, the ramifications of facial recognition technology on privacy, data security, and individual rights remain largely unexplored. The flexibility and dependability of the system in real-world contexts typified by dynamic lighting conditions, facial expressions, and occlusions should be the subject of further research. In addition, there needs to be more studies on the long-term societal consequences of broad face recognition adoption, notably its effects on human interaction, civil rights, and potential shifts in social norms. Bridging these gaps is essential for understanding face recognition technology, its ramifications, and its possible compatibility with ethical, legal, and societal frameworks.

2.2. Biometric Data Protection

Understanding biometric data protection regulation, technology, and systems requires a multifaceted examination of the complex framework comprising legal safeguards, technological mechanisms, and operational protocols designed to protect individuals' biometric data's security, privacy, and integrity [47], [48]. This knowledge necessitates an exhaustive investigation of regulatory frameworks developed at the regional, national, and international levels, outlining the allowed processing of biometric data that includes all stages of data processing from the collection, storage, analysis, distribution to the deletion of biometric data [49]. Concurrently, it needs an in-depth investigation of biometric systems' technical underpinnings, including encryption approaches, safe storage solutions, and robust authentication mechanisms [50]. This comprehension extends to the operational complexities of biometric implementation, including informed consent procedures, audit trails, and data breach mitigation techniques [51]. A holistic perspective highlights the essential symbiosis between legal requirements, technological advances, and operational imperatives, which converge to ensure a cohesive and effective biometric data protection ecosystem capable of preserving individual rights and fostering societal trust in an era of increasing digital reliance [52].

Constructing a biometric data protection system involves a comprehensive procedure incorporating advanced technology components and installing stringent security measures to protect the biometric information of persons [53]. This is the coordination of systematic processes for biometric data gathering, which frequently requires specific sensors or equipment to capture unique physiological or behavioral characteristics. Then, complex algorithms extract prominent elements from the gathered data and turn them into different templates [54]. These templates are then encrypted and stored securely to prevent unwanted access and limit future data breaches [55]. In addition, the system incorporates authentication methods to ensure that only authorized users can access and use the stored biometric templates. The development process must also involve extensive testing under various scenarios to evaluate the system's precision, dependability, and resistance to hostile attacks [56]. As biometric data protection continues to evolve, developing these systems requires a dynamic approach that aligns technological advancements with ethical considerations and regulatory compliance, thereby creating a robust ecosystem for protecting sensitive biometric information.

A particular research gap exists in biometric data protection regulation, needing a more in-depth examination of the complex dynamics regulating emerging technology, ethical considerations, and legal frameworks [57]. There exists a noticeable deficit in research that rigorously investigates the alignment of existing legislation with the rapid improvements in biometric technologies, notwithstanding the rising prevalence of biometric data usage across varied industries [58]. The evolution of biometric applications, such as facial recognition and fingerprint scanning, has outpaced the capacity of regulatory structures to address the complex challenges they introduce, resulting in a gap between the potential risks posed by unauthorized access or data breaches and the effectiveness of existing protective measures [59]. In addition, the cross-jurisdictional nature of biometric data transfers and the absence of unified international standards complicate the development of comprehensive legislation [60]. As a result, a research gap exists in identifying the gaps between the expanding scope of biometric technologies and the sufficiency of legal safeguards, necessitating academic endeavors to fill this void and inform the establishment of adaptive, egalitarian, and ethically acceptable regulatory frameworks.

 doi:10.20944/preprints202309.0547.v1

A particular study gap exists in biometric data protection technology studies, highlighting the necessity for thoroughly investigating the growing landscape of data security, privacy preservation, and ethical issues regarding biometric applications [61]. Existing research frequently needs a methodology that spans the whole lifecycle of biometric data, from capture and storage through transmission and processing, leaving possible vulnerabilities and preventive measures at each stage unexplored [62]. Moreover, as biometric technologies grow more prevalent in various fields, a detailed assessment of the socio-cultural, legal, and economic factors that influence biometric systems' design, acceptance, and regulation is required. This research vacuum gives a unique opportunity for academics to explore unknown territory, promoting a comprehensive grasp of the various difficulties and opportunities posed by biometric data protection. By bridging this gap, researchers can contribute to developing holistic frameworks that address the convergence of technological advancements, ethical considerations, and regulatory imperatives, thereby advancing theoretical insights and practical solutions in the dynamic field of biometric data protection technology.

3. Materials and Methods

Focus Group Discussion (FGD) as a methodological approach has substantial scholarly significance in thoroughly examining stakeholders' perceptions and the complex navigation of Indonesia's Biometric Data Protection Initiative and Face Recognition Technology Support. As a qualitative research method, FGDs provide a structured forum for eliciting various nuanced perspectives from stakeholders, including government agencies, technology developers, regulatory authorities, civil society organizations, and data subjects as end-users, representing a penta-helix approach [63]–[65]. By encouraging participatory discussions, FGDs enable the exploration of multidimensional aspects of biometric data protection and face recognition technologies, such as socio-cultural norms, ethical issues, legal frameworks, and technological capabilities. Through the dynamic interchange of ideas and experiences, FGDs not only reveal the complexities of stakeholders' viewpoints but also reveal potential conflicts, consensus, and gaps in the discourse, thereby enhancing the comprehension of the ecosystem in which these technologies are embedded.

In Indonesia, where the adoption and regulatory environment for biometric data protection and face recognition technology are subject to specific dynamics, FGDs are a significant tool for navigating the implementation complexities. They examine how cultural norms and local contexts interface with global technological developments and regulatory frameworks, illuminating the congruence or discordance between stakeholder views and policy directive goals. In addition, FGDs assist in identifying specific issues, obstacles, and opportunities that may arise in promoting proper biometric data protection and face recognition technology support mechanisms in Indonesia. By capitalizing on the interactive nature of FGDs, this research strategy equips scholars and policymakers to navigate the complexities of stakeholder perceptions and the regulatory landscape, fostering a holistic understanding that informs the development of strategies congruent with ethical, legal, and societal imperatives in the Indonesian context.

The FGD themes cover a variety of essential factors necessary for a thorough analysis of stakeholder perspectives and for navigating the complex landscape of the Biometric Data Protection Initiative and Face Recognition Technology Support in Indonesia. The first topic, "Informed Consent for Biometric Data Procedures," explores the ethical and legal implications of acquiring, utilizing, and keeping biometric data and the stakeholders' awareness of informed consent mechanisms and potential obstacles. "Technology Acceptance" investigates the factors influencing stakeholders' propensities to accept or reject biometric technology, delving into their opinions of its efficacy, security, usability, and potential consequences. The issue of "Face Recognition Technology and Support" examines stakeholders' perspectives on the deployment of face recognition technology, including its benefits, challenges, and practicality within the sociocultural context of Indonesia. Regulation for Data Protection explores stakeholders' perspectives regarding the effectiveness, sufficiency, and alignment with global standards of the existing regulatory frameworks controlling biometric data protection. "Digital Transformation and Artificial Intelligence Technology in

 doi:10.20944/preprints202309.0547.v1

Indonesia" examines stakeholders' understanding of the broader digital transformation landscape, including the role of artificial intelligence and its implications for biometric technology integration within Indonesia's transforming socioeconomic fabric. By engaging stakeholders in these varied themes, the FGD technique offers a comprehensive study of views, concerns, and goals, enhancing comprehension of this complex environment.

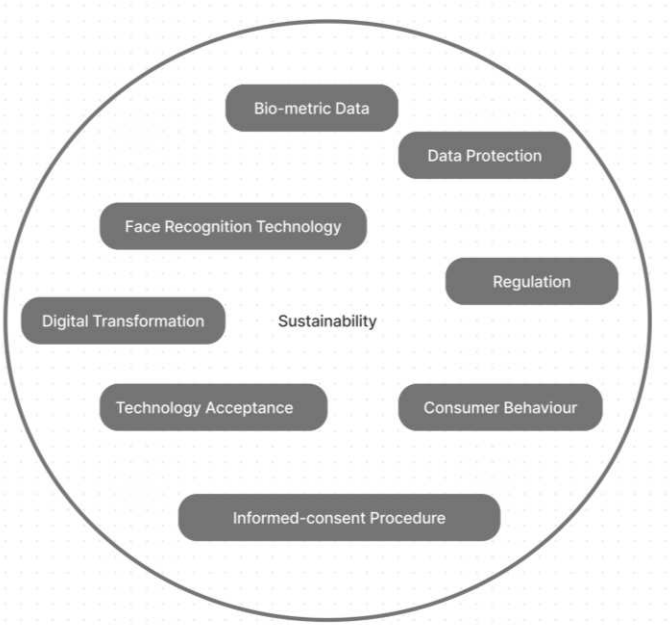

Figure 1. Focus Group Discussion (FGD) Entitled Biometric Data Protection and Face Recognition Technology In Indonesia.

The FGD sessions cover a broad range of issues that collectively address essential aspects of biometric data, data protection, facial recognition technology, regulation, technology acceptability, consumer behavior, informed-consent procedures, and digital transformation in the Indonesian environment. The discussions center on the complex dynamics of biometric data, including stakeholder perceptions of its sensitivity, utility, and potential threats, as well as the methods and systems necessary for solid data protection in the face of developing technology. The debate on face recognition technology engages stakeholders in discussions regarding its virtues, drawbacks, and applicability within the sociocultural context of Indonesia. Existing legal frameworks are reviewed for their sufficiency in protecting biometric data privacy and managing potential hazards, with regulation emerging as a central subject. The propensities of stakeholders toward technological acceptance and consumer behavior are examined to determine the factors that shape stakeholders' preferences and attitudes regarding biometric applications and, hence, influence adoption patterns. Examining informed consent procedures, a pillar of ethical data handling exposes stakeholders' understanding, comprehension, and expectations around collecting and utilizing their biometric data. The discussion concludes with the immense panorama of digital transformation, including the role of emerging technologies, notably artificial intelligence, in shaping the biometric data protection ecosystem and guiding Indonesia's changing digital trajectory. Through these in-depth FGD talks, a nuanced understanding of the perspectives of stakeholders and the multifaceted context around biometric data security and technology deployment in Indonesia is fostered.

Table 1. Institution Representative in Focus Group Discussion (FGD) Entitled Biometric Data Protection and Face Recognition Technology in Indonesia.

Institution	Representation (Initial)	Position/Role

 doi:10.20944/preprints202309.0547.v1

Ministry of Communication and Informatics of the Republic of Indonesia	HSY	Coordinator of Personal Data Protection Governance
Lembaga Studi Advokasi Masyarakat/the Institute for Policy Research and Advocacy (ELSAM)	PP	Researcher
Lembaga Kajian dan Advokasi Independensi Peradilan (LeIP)	SD	Researcher
Situmorang, Raharja, dan Associates (Law Firm)	DG	Lawyer Associate
S. ASEAN International Advocacy & Consultancy	SS	CEO & Founder
Atma Jaya Studies on Aviation, Outer Space, and Cyber Laws (AJAvOC)	IB R S	Law Professor and Head of Research Centre
Kepala Departemen Hukum TIK-KI Universitas Padjajaran	SD	Law Professor and Head of Study Program on ICT
Information System Department	SPS	IT Developer
Faculty of Engineering	EK	End-User/Data Subject
Tourism Department	YAS	Tour and Travel Researcher
Faculty of Law	SYW	Law Researcher

The engagement of stakeholders in exhaustive deliberations and collaborative endeavors is of the utmost importance for addressing critical issues and drafting a substantial white paper that provides the Indonesian government with informed recommendations regarding biometric data protection and the implementation of face recognition technology. A comprehensive spectrum of perspectives is tapped by bringing together representatives from governmental bodies, technology developers, regulatory agencies, civil society groups, and data subjects as end-users, including diverse insights into biometric data's technological, ethical, legal, and societal dimensions. This dialogue enables identifying and analyzing obstacles, opportunities, and potential repercussions of adopting such technologies in the Indonesian environment. As a result of these joint efforts, the subsequent creation of a white paper acts as a formal repository of condensed recommendations that provide balanced views, actionable proposals, and contextualized tactics that fit with the national ethos and regulatory framework. This approach guarantees that the document reflects the combined expertise of stakeholders and serves as a comprehensive guide for the Indonesian government to navigate the complexities of biometric data protection and face recognition technology, fostering a symbiotic relationship between technological innovation and societal welfare.

3. Results

The relationship between the two topics, "Biometric Data Security, Regulation, and Politics in Indonesia as a Challenge in the Digital Transformation Era" and "The Implementation of Face Recognition Technology: Case of PT. Kereta Api Indonesia," demonstrates a profound connection between the broader challenges of biometric data security, regulation, and political dynamics in Indonesia's digital transformation landscape, and a case study illustrating the practical application of face recognition technology. The first topic describes the complex interplay between evolving biometric technologies, regulatory frameworks, and political considerations in safeguarding sensitive biometric data. In contrast, the second topic illustrates how these challenges manifest in implementing face recognition technology for transportation security. This juxtaposition serves as a lens for analyzing how the overarching challenges of biometric data security and regulation manifest in a tangible operational context, shedding light on the complexities faced by organizations like P.T. Kereta Api Indonesia in reconciling technological advancements with ethical, legal, and societal dimensions. Examining the complexities of a specific case within the context of the larger challenge landscape fosters a more comprehensive understanding, thereby facilitating the extrapolation of practical strategies that align technology implementation with regulatory imperatives and ethical considerations in Indonesia's digital transformation era.

3.1. Biometric Data Security, Regulation, and Politics in Indonesia as a Challenge in the Digital Transformation Era

 doi:10.20944/preprints202309.0547.v1

The difficulty of Biometric Data Security, Regulation, and Politics in Indonesia in the Era of Digital Transformation highlights the delicate interplay between growing biometric technologies, legal frameworks, and political dynamics in Indonesia's digitally transforming landscape. As the prevalence of biometric technology across industries increases, the need for adequate data security and privacy protection becomes more pressing. However, implementing biometric data protection methods effectively depends on the interaction of technical protections, regulatory laws, and sociopolitical factors. This difficulty necessitates a comprehensive assessment of how the emerging regulatory framework in Indonesia strikes a delicate balance between supporting technical innovation and protecting individual rights, as well as addressing broader sociopolitical and ethical elements. Investigating this problem provides insights into the complexities of integrating biometric data security measures within the regulatory and political frameworks of a developing nation undergoing digital transformation, thereby informing the formulation of strategies that align technological advances with ethical and legal mandates.

The convoluted terrain of private data protection in Indonesia, particularly concerning biometric data, necessitates collaboration between academic institutions, government agencies, and private sector organizations. In personal data, biometric information possesses unique sensitivity, needing a diversified strategy to meet the numerous security, regulatory, and ethical concerns connected with its use. The collaboration between academia, government, and the private sector has the potential to capitalize synergistically on their respective strengths: academia contributes expertise in research and analysis, providing insights into evolving technological trends and potential vulnerabilities; government agencies provide the regulatory framework necessary for protecting individual rights and preserving public trust; and the private sector contributes practical implementation. This collaborative effort is essential not only for harmonizing the diverse perspectives of stakeholders but also for fostering a comprehensive approach that holistically addresses the complex technical, legal, and ethical dimensions of private data protection, thereby creating a more resilient and trustworthy data ecosystem tailored to Indonesia's socioeconomic and cultural context.

The increased danger of biometric data exploitation due to human mistakes or flaws in database security protocols underscores the importance of preventative measures from an academic approach. Academic debate highlights the urgent need to establish proactive solutions that prevent these hazards and foster a complete understanding of their underlying causes. This involves examining multidisciplinary methods, including human aspects of psychology, cryptography, information systems, and ethical issues, to identify potential failure points in biometric data management. On the other hand, there is an urgent need to address the use of automation technology with the deployment of, for instance, an algorithmic decision-making (ADM) technology for processing biometric data. While ADM might not have human bias, there are risks of algorithmic bias in the deployment of ADM [66], among others, from ethical [67] and legal [68]–[70] points of view as exemplified in cases of discriminatory ADM [68]. From a data protection viewpoint, the use of ADM potentially risks data subjects' autonomy by taking over the ability of data subjects to control and make decisions on their own [71], [72]. Hence, the need for a reliable and justified mechanism to ensure the ability of the data subject to give a freely given, specific, informed, and unambiguous consent is paramount.

In this context, academia can play a crucial role by pioneering research projects to identify possible human and algorithmic errors in data handling processes, expose design faults in security architecture, and develop creative encryption approaches to strengthen database integrity. By fostering collaborations between academia, industry, and regulatory bodies, a comprehensive framework can be expanded to anticipate, prevent, and rectify potential vulnerabilities, thereby establishing a solid foundation for biometric data protection that conforms to ethical standards and regulatory mandates.

According to the government's institutional stance regarding regulating biometric data protection, incorporating a rigorous informed consent method is paramount. This viewpoint emphasizes the need to strike a careful balance between technological progress and individual rights, understanding that collecting, storing, and using biometric data requires individuals' informed and express consent. From a legislative perspective, this comprises the formation of legal frameworks

 doi:10.20944/preprints202309.0547.v1

mandating complete disclosure of data usage goals and potential hazards, as well as implementing methods allowing individuals to exercise control over their data. This viewpoint emphasizes the government's duty to guarantee that informed-consent procedures are robustly implemented and aligned with ethical values, considering the subtleties of biometric data collection and processing. By highlighting the need for informed consent, the government's institutional approach is to develop a coherent legal framework that fosters openness, accountability, and data subject empowerment in the evolving biometric data protection landscape.

This stance aligns with the new Indonesian Data Protection Act (Law No. 22 of 2023 concerning Personal Data Protection, hereafter, the PDPA) [73]. The PDPA was adopted in October 2022 and requires data controllers and other parties relating to the processing of personal data to adjust to the obligations under the new law within two years after the law's adoption until 2024. The enactment of the new PDPA is expected to provide a comprehensive protection of data subject rights and to end the sectoral regulations to protect personal data. The new PDPA lays down a series of obligations for data controllers and data processors for both public and private sectors.

The PDPA sets out two requirements for the processing of biometric data under the protection of specific data (or sensitive data) (PDPA Article 4 par. (2) lit. b). First, with the categorization of the processing of biometric data as high-risk data processing, the PDPA requires data controllers to carry out a personal data impact assessment (hereafter, PDIA) before the processing of biometric data (PDPA Article 34 par. (1), (2) lit. b). Second, the PDPA requires the data controllers to appoint a data protection officer to help ensure the compliance of data processing with the PDPA principles (PDPA Article 53 par. (1) lit. c).

To implement the mandatory DPIA, the PDPA mandates further regulation in the form of a Government Regulation which draft was recently released on 30 August 2023 for a public consultation [74]. Under the current draft, the DPIA shall consist of the following: (1) a systematic description of the personal data processing activities and the purpose of data processing, including the interests of the data controller from such processing; (2) an assessment of needs and proportionality between purposes and activities of processing the personal data; (3) a risk assessment of the protection of data subjects' rights; and (4) measures used by the data controller to protect data subjects from the risks of processing such personal data (Article 128 of the current Draft of the Government Regulation for the Protection of Personal Data, hereafter GR-PDP Draft). Data controllers may consult with an institution functioning as a data protection supervisory authority regarding implementing the DPIA requirement (GR-PDP Draft Article 129).

The perspective of the commercial sector on biometric data use emphasizes business potential and marketing tactics based on identifying client requirements and habits. This viewpoint acknowledges biometric data as a valuable instrument for identifying and forecasting purchase trends, enabling marketing campaigns tailored to individual tastes. Organizations can obtain insights into customer behavior, preferences, and consumption patterns by integrating biometric data. This allows them to refine their product offers, improve the customer experience, and optimize their marketing efforts. This viewpoint emphasizes the private sector's motivation to capitalize on the intrinsic value of biometric data for crafting personalized and targeted marketing campaigns that align with evolving consumer demands while recognizing the ethical imperatives of transparent data usage and consent. In conclusion, the private sector's perspective highlights the synergistic potential of biometric data analysis to promote corporate growth and customer engagement while negotiating the ethical issues inherent to the proper deployment of personal data for commercial advantage.

The data subjects' perspective as end users about untrusted applications requiring personal data highlights the need for transparency and assurance in knowing how private sector firms protect personal data, including biometric data, during digital transactions. Data subjects or end-users desire information regarding the complete processes implemented by private sector entities to ensure data privacy, hence creating trust and confidence in the usage of such applications. In particular, the data subjects' perspective emphasizes the significance of understanding the methods to safeguard biometric data across diverse digital interactions, as these physiological characteristics include intrinsic sensitivity. Users require knowledge of the encryption methods, safe storage techniques,

 doi:10.20944/preprints202309.0547.v1

and authentication practices used by private sector firms to mitigate potential risks and vulnerabilities, enabling them to make informed judgments regarding the applications they employ. This perspective emphasizes the significance of data subjects' rights to transparency and calls for the availability of information that enables individuals to evaluate the dependability of applications and make informed decisions consistent with their data protection preferences.

Academic, government, private sector, and data subject viewpoints are interconnected to establish a dynamic framework encompassing the complex discourse on biometric data protection and facial recognition technology. The academic approach brings rigorous research and multidisciplinary ideas that shed light on technical weaknesses, ethical problems, and societal consequences. This knowledge influences the government's perspective, which builds legislative frameworks to safeguard data security, individual rights, and sociopolitical concord. Motivated by corporate opportunities and consumer demands, the private sector uses modern technologies while conforming to legal and ethical requirements. This interaction influences data subjects as end-users, equipped with transparency and data protection consciousness, make educated decisions about engaging with technologies and entrusting personal data. Therefore, the symbiotic relationship between these perspectives catalyzes a holistic approach that balances innovation, regulation, ethical considerations, and user empowerment, thereby guiding the responsible development and deployment of biometric data protection and face recognition technology.

In Indonesia's digital transformation era, recommendations regarding biometric data protection, regulation, and the intersection of politics should adopt a multifaceted approach considering the country's socio-cultural diversity, regulatory dynamics, and technological evolution. First, informed by robust academic research, comprehensive and adaptable regulatory frameworks should be designed to balance innovation and ethical considerations, supporting data security and individual rights. Second, it is essential to develop collaboration between academia, government, and the corporate sector to solve any legal gaps and ensure that policies match the practical landscape. Thirdly, these frameworks must incorporate political considerations to prevent undue influence, preserve data sovereignty, and encourage public trust. Fourthly, it is crucial to cultivate general knowledge and participation, emphasizing transparent informed-consent procedures and comprehensive education campaigns that equip data subjects as end-users to navigate digital environments. Lastly, these guidelines should be frequently evaluated and revised to align with emerging technical trends, regulatory adjustments, and political factors, ensuring that Indonesia's biometric data protection stays resilient and adaptable throughout its digital transformation journey.

3.1. The Implementation of Face Recognition Technology: Case of P.T. Kereta Api Indonesia

Face Recognition Technology implementation in a developing nation has complexities related to technical acceptance, resource limits, and socioeconomic dynamics. This challenge is especially pertinent in countries like Indonesia, where aligning innovative technology with limited resources requires careful consideration of infrastructure restrictions, digital inclusion, and cultural sensitivities. The technology also poses data subjects risks in light of the right to data protection [75], [76] including various concerns over surveillance [77].

However, this difficulty presents an opportunity to stimulate economic growth. Face Recognition Technology has the ability to boost innovation, improve security, and streamline many industries, thus promoting economic growth by streamlining processes, enhancing service delivery, and attracting investments. Indonesia can leverage the transformative potential of this technology to stimulate economic growth and create the framework for a digitally empowered future by employing prudent implementation tactics that address local challenges. In the tourism industry, Face Recognition Technology offers a valuable instrument to boost the industry by allowing personalization and data-driven services to enhance travelers' experiences such as customized and optimal travel planning, enhancement of safety and security, and seamless financial transactions [78].

The correlation between customer purchase behavior and technology acceptance highlights a crucial relationship in which consumer propensities to embrace and engage with technology are directly influenced by their shopping preferences and habits. In applications such as the KAI (*Kereta*

 doi:10.20944/preprints202309.0547.v1

Api Indonesia) Application, building confidence in data protection acquires a position of preeminence. As customers engage in digital transactions, their desire to embrace technology depends on their assurance that their data, including biometric information, is protected. Ensuring comprehensive data protection methods in application databases is essential for complying with regulatory regulations and fostering an environment that encourages consumer trust. Because of the KAI Application's function in supporting travel services, this mutual reinforcement between technology acceptability and data protection is very pronounced. By prioritizing stringent data protection measures, KAI can increase customer trust, foster positive perceptions, enhance technology acceptance, and promote a symbiotic relationship between purchasing behavior, technology engagement, and data security assurance within its digital ecosystem.

The scholarly viewpoint emphasizes concern about the potential risks associated with accessing insecure databases provided by third-party companies that offer Face Recognition Technology services. This concern arises from the complex relationship between the reliability of data sources, data integrity, and privacy concerns in the context of biometric data consumption. Due to the emphasis on empirical research and analytical rigor in academia, it is vital to critically analyze the security procedures employed by external organizations that supply such technology services. The intricacy of biometric data, its susceptibility to security breaches, and the likelihood of illegal access underscore the importance of paying close attention to the security measures implemented by these third-party vendors. Accurate data sources are vital for ensuring face recognition technology's efficacy and moral application from an academic standpoint. Further, there are concerns for illegitimate processing, including data transfer to unauthorized parties. This perspective emphasizes the importance of collaborative efforts between academia, regulatory bodies, and industry stakeholders to develop stringent standards and protocols that mitigate the risks posed by unsecured databases, thereby ensuring the responsible use of biometric data and bolstering the integrity of emerging technologies in the face of potential vulnerabilities.

The government's perspective centers on increasing engagement with the commercial sector to facilitate the implementation of Face Recognition Technology, which extends beyond companies such as KAI to include other public services such as Transjakarta. This viewpoint is influenced by a larger objective to use technological advances to improve operational efficiency and public service delivery. The government acknowledges that strategic partnerships with private sectors adept in Face Recognition Technology service delivery can speed the adoption of practical and creative solutions. By incorporating biometric technology into public services such as transportation, the government intends to improve operations, reduce bottlenecks, and enhance the customer experience. This viewpoint emphasizes the government's responsibility in arranging a symbiotic partnership that leverages the knowledge of the private sector while adhering to regulatory requirements and guaranteeing responsible data handling methods. This perspective highlights the potential for public-private partnerships to achieve transformational technological adoption, ultimately contributing to improved service quality and operational efficiency in the Indonesian public sector.

The private sector's perspective is optimizing transactional processes for effectiveness and efficiency, emphasizing security through apps that comply with stringent data protection regulations. This perspective coincides with the fundamental goals of organizations to improve the user experience, reduce operational difficulties, and speed up transactions. Recognizing the sensitive nature of biometric data, the private sector acknowledges the need to fully comprehend and adhere to consent protocols, ensuring that data subjects as end-users are educated and empowered participants in data sharing. By prioritizing these factors, the commercial industry intends to foster user trust and confidence in Face Recognition Technology applications. This viewpoint highlights the private sector's role in forging a symbiotic relationship between technological innovation and ethical considerations. It ultimately fosters a digital environment that prioritizes seamless transactions while ensuring stringent data protection measures, advancing its operational objectives while meeting its customers' privacy and security expectations.

The data subject's perspective is defined by its emphasis on data security that transcends transactional efficiency and effectiveness considerations. In addition to faster purchasing and trip

 doi:10.20944/preprints202309.0547.v1

validation, data subjects as end-users place significant stress on the stringent protection of their data, mainly through biometric data. This perspective is motivated by a heightened awareness of the potential risks associated with data breaches and unauthorized access. Data subjects as end-users prioritize a comprehensive understanding of how personal data is collected, stored, and utilized by technologies such as Face Recognition. The need for secure data processing resonates strongly with data subjects as end-users, emphasizing informed consent procedures, transparent data usage, and stringent security. This perspective highlights the significance of aligning technological advancements with individual privacy expectations, ensuring that while enhancing purchasing and travel experiences, the deployment of biometric technology also provides data protection, fostering user trust and maintaining the symbiotic relationship between technological convenience and information security.

4. Discussion

The academic perspective on biometric data and facial recognition technology in Indonesia is multidimensional, incorporating multidisciplinary research, ethical considerations, and a comprehensive analysis of the societal repercussions. Scholars in computer science, law, ethics, and the social sciences contribute to this perspective by exploring the technological complexity of biometric data management, investigating legal and regulatory frameworks, and delving into the sociocultural ramifications of technology adoption. This viewpoint necessitates empirical research to examine the efficacy and limitations of facial recognition systems in the Indonesian context, addressing topics such as accuracy, prejudice, and the potential for misuse. In addition, ethical inquiries consider the moral implications of biometric data usage, highlighting the need to balance technological innovation and individual privacy rights and ensure that such technology's societal impact is consistent with national values and traditions.

In addition, the scholarly viewpoint stresses the importance of bridging the digital divide in Indonesia, where digital literacy and access to technology vary. Scholars emphasize the need to ensure that biometric data and facial recognition technology do not inadvertently exacerbate existing gaps but contribute to inclusive progress. Examining the potential ramifications for marginalized communities and proposing ways to close the gaps caused by unequal access to technology and information are central to this perspective [79]. Academics also dialogue with government bodies and industry stakeholders to inform policy development, recommend regulatory frameworks and advocate for comprehensive data protection mechanisms that balance technological innovation, ethical standards, and societal well-being in Indonesia.

The government's intentions regarding biometric data protection and regulation and implementing face recognition technology in transportation services such as KAI reflect a multifaceted agenda that seeks to balance technological advancement, individual rights, public safety, and regulatory oversight. The government acknowledges the revolutionary potential of biometric data and face recognition technology for enhancing public services and security, particularly in the transportation industry. Consequently, its objective is to build comprehensive legislative frameworks that regulate collecting, storing, analyzing, using, distributing, and deleting biometric data, ensuring compliance with ethical standards, data protection legislation, and privacy concerns. This perspective necessitates collaboration between government authorities, academic institutions, and the private sector to establish standards that balance innovation and protecting individual rights while considering Indonesia's sociocultural context.

In the context of KAI, the government intends to integrate facial recognition technology to maximize operational efficiency and passenger satisfaction. Using biometric information for ticketing, validation, and passenger identification, the government wants to streamline operations, reduce fraud, and enhance public safety. This purpose demands a tight partnership with private-sector technology suppliers to ensure adherence to existing laws and moral principles [80]. The government also emphasizes the significance of open communication with the public, assuring citizens that the technology would be implemented with responsible data management practices and privacy safeguards. By aligning the implementation of face recognition technology with the broader

 doi:10.20944/preprints202309.0547.v1

goals of public service enhancement and safety improvement, the government hopes to foster public confidence, optimize transportation services, and pave the way for the responsible use of biometric data within Indonesia's rapidly evolving technological landscape.

Its strategic focus on developing and marketing face recognition technology solutions to the Indonesian government exemplifies the private sector's desire to expand its commercial operations and capitalize on the opportunities presented by the digital transformation era [81]. This ambition is consistent with the industry's pursuit of innovation, expansion, and market penetration. It is supported by biometric technology's capacity to meet expanding social needs, enhance operational efficiencies, and enhance security. By aggressively pursuing the development and commercialization of facial recognition technology, private sector entities want to satisfy the government's demand for new solutions in line with the nation's digital transformation objectives. This objective encompasses developing robust, adaptive technology that complies with regulatory norms, addresses ethical problems, and serves the greater public interest. By positioning themselves as providers of cutting-edge biometric solutions, the private sector seeks not only to generate revenue but also to contribute to the evolution of Indonesia's technological landscape, fostering a symbiotic relationship that advances both economic growth and national development goals.

The data subject perspective as an end-user, intricately entwined with academic, government, and commercial sector objectives, gives an essential dimension to Indonesia's discourse on biometric data and facial recognition technologies. Data subjects as end-users are concerned not just with technological advancements and legal frameworks but also with the effects of these initiatives on their privacy, data security, and user experiences [82]. As beneficiaries or subjects of these technological breakthroughs, data subjects as end-users require assurances that academic research and analysis will correctly and responsibly handle their data. The data subjects as end-users rely on the government's goals to ensure comprehensive regulation safeguards their rights and maintains public confidence. In addition, they interact with the commercial sector as potential consumers, necessitating user-centric programs that prioritize seamless functionality while handling data privacy concerns transparently [83]. The data subject perspective highlights the need to strike a balance between innovation, regulatory compliance, and individual rights, highlighting the interdependence between academic insights, government policies, private sector initiatives, and data subjects as end-user expectations in shaping the responsible and effective deployment of biometric data and face recognition technology within Indonesia's sociotechnical landscape.

5. Conclusions

The exhaustive research on biometric data protection, legislation, and facial recognition technologies in Indonesia sheds light on a complex ecosystem defined by numerous stakeholder relationships. The academic approach contributes empirical studies and perspectives highlighting the technical challenges, ethical concerns, and societal implications of biometric data utilization. Government objectives include legislative frameworks that balance the rise of technology with individual rights and privacy concerns, producing a balanced approach that fosters innovation while maintaining public confidence. Motivated by economic opportunities and consumer demands, the private sector strives to harness technology for efficiency gains while adhering to ethical and regulatory standards. Similarly, the data subjects' perspective highlights the significance of data protection, transparency, and frictionless transactions in a digital world. The interaction between these perspectives illustrates the complexity of Indonesia's digital transformation phase when the potential of facial recognition technology is coupled with data security, privacy, and inclusivity concerns. The regulatory function of the government seeks to bridge the gap between public expectations and technological advancements. Collaboration between academic institutions, government agencies, the private sector, and data subjects as end-users emerges as a crucial element, fostering an all-encompassing strategy integrating research, law, technology deployment, and user empowerment. This holistic approach is necessary to ensure that biometric data and facial recognition technology are utilized responsibly, thereby laying the way for Indonesia's technologically sophisticated and ethically aware digital future.

Author Contributions: Conceptualization, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; methodology, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; software, Yerik Afrianto Singgalen; validation, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; formal analysis, Yerik Afrianso Singgalen; investigation, Sih Yuliana Wahyuningtyas; resources, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; data curation, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; writing—original draft preparation, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; writing—review and editing, Sih Yuliana Wahyuningtyas and Yerik Afrianto Singgalen; visualization, Yerik Afrianto Singgalen; supervision, Sih Yuliana Wahyuningtyas; project administration, Sih Yuliana Wahyuningtyas; funding acquisition, Sih Yuliana Wahyuningtyas. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded under the first year of a two-year research grant by the Directorate of Research, Technology, and Community Service, Directorate General of Higher Education, Research and Technology, Ministry of Education, Culture, Research and Technology of the Republic of Indonesia of 2023, grant number SP DIPA-023.17.1.690523/2023, 4th revision, on 31 March 2023 and contract between the Higher Education Service Institution Region III and Atma Jaya Catholic University of Indonesia number 1415/LL3/AL.04/2023 on 26 June 2023, and the APC was funded by Atma Jaya Catholic University of Indonesia.

Institutional Review Board Statement: This study was classified as exempt since data collection was performed using a Focus Group Discussion and conducted within an educational setting. It involved typical educational and professional practices that did not potentially negatively impact participants.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Qualitative data are not publicly available due to ethical restrictions since they include confidential information that could compromise the privacy/anonymity of research participants.

Acknowledgments: The authors would like to express their gratitude to all participants involved in this research through FGD, the Directorate of Research, Technology, and Community Service, Directorate General of Higher Education, Research and Technology, Ministry of Education, Culture, Research and Technology of the Republic of Indonesia, LPPM, Faculty of Law, Faculty of Business Administration and Communication, the Atma Jaya Catholic University of Indonesia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. K. Faisal, *Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective*, vol. 28, no. 1. Routledge, 2023. doi: 10.1080/10811680.2023.2180266.
2. M. Rukhiran, S. Wong-In, and P. Netinant, "User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model," *Sustainability*, vol. 15, no. 4, pp. 1–18, 2023, doi: 10.3390/su15043092.
3. A. Fletcher, "Government surveillance and facial recognition in Australia: a human rights analysis of recent developments," *Griffith Law Review*, vol. 32, no. 1, pp. 30–61, 2023, doi: 10.1080/10383441.2023.2170616.
4. A. Mostafavi, "Architecture, biometrics, and virtual environments triangulation: a research review," *Archit Sci Rev*, vol. 65, no. 6, pp. 504–521, 2022, doi: 10.1080/00038628.2021.2008300.
5. L. Yan, Y. Zhang, and Y. Zhang, "A fast face recognition system based on annealing algorithm to optimize operator parameters," *Imaging Science Journal*, vol. 71, no. 4, pp. 323–330, 2023, doi: 10.1080/13682199.2023.2182261.
6. N. Stevens and O. Keyes, "Seeing infrastructure: race, facial recognition and the politics of data," *Cultural Studies*, vol. 35, no. 4–5, pp. 833–853, 2021, doi: 10.1080/09502386.2021.1895252.
7. F. Z. Xu, Y. Zhang, T. Zhang, and J. Wang, "Facial recognition check-in services at hotels," *Journal of Hospitality Marketing and Management*, vol. 30, no. 3, pp. 373–393, 2021, doi: 10.1080/19368623.2020.1813670.
8. E. Ringel and A. Reid, "Regulating Facial Recognition Technology: A Taxonomy of Regulatory Schemata and First Amendment Challenges," *Communication Law and Policy*, vol. 28, no. 1, pp. 3–46, 2023, doi: 10.1080/10811680.2023.2180271.
9. A. Ioannou, I. Tussyadiah, and G. Miller, "That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure," *J Travel Res*, vol. 60, no. 7, 2021, doi: 10.1177/0047287520951642.
10. G. Carswell and G. De Neve, "Transparency, exclusion and mediation: how digital and biometric technologies are transforming social protection in Tamil Nadu, India," *Oxford Development Studies*, vol. 50, no. 2, pp. 126–141, 2022, doi: 10.1080/13600818.2021.1904866.

11. Z. Li, Y. Guo, M. Yarime, and X. Wu, "Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China," *Policy Design and Practice*, vol. 6, no. 1, pp. 27–40, 2023, doi: 10.1080/25741292.2022.2162248.
12. X. Liu, C. Li, J. L. Nicolau, and M. Han, "Face recognition of profile images on accommodation platforms," *Current Issues in Tourism*, vol. 25, no. 21, pp. 3395–3400, 2022, doi: 10.1080/13683500.2022.2107494.
13. R. Wevers, "Denormalising surveillance through curation in Face Value: Surveillance and Identity in the Age of Digital Face Recognition," *Media Practice and Education*, no. May, 2023, doi: 10.1080/25741136.2023.2210425.
14. N. Li *et al.*, "Chinese face dataset for face recognition in an uncontrolled classroom environment," *IEEE Access*, vol. 11, no. August, pp. 86963–86976, 2023, doi: 10.1109/ACCESS.2023.3302919.
15. Z. Huang, J. Zhang, and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark," *IEEE Trans Pattern Anal Mach Intell*, vol. 45, no. 6, pp. 7917–7932, 2023, doi: 10.1109/TPAMI.2022.3217882.
16. C. Fu, X. Wu, Y. Hu, H. Huang, and R. He, "DVG-Face: Dual Variational Generation for Heterogeneous Face Recognition," *IEEE Trans Pattern Anal Mach Intell*, vol. 44, no. 6, pp. 2938–2952, 2022, doi: 10.1109/TPAMI.2021.3052549.
17. R. He, J. Cao, L. Song, Z. Sun, and T. Tan, "Adversarial Cross-Spectral Face Completion for NIR-VIS Face Recognition," *IEEE Trans Pattern Anal Mach Intell*, vol. 42, no. 5, pp. 1025–1037, 2020, doi: 10.1109/TPAMI.2019.2961900.
18. M. Luo, J. Cao, X. Ma, X. Zhang, and R. He, "FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2341–2355, 2021, doi: 10.1109/TIFS.2021.3053460.
19. G. Srivastava and S. Bag, "Modern-day marketing concepts based on face recognition and neuro-marketing: a review and future research directions," *Benchmarking*, 2023, doi: 10.1108/BIJ-09-2022-0588.
20. W. L. Shiau, C. Liu, M. Zhou, and Y. Yuan, "Insights into customers' psychological mechanism in facial recognition payment in offline contactless services: integrating belief–attitude–intention and TOE–I frameworks," *Internet Research*, vol. 33, no. 1, pp. 344–387, 2023, doi: 10.1108/INTR-08-2021-0629.
21. M. A. S. Palash, M. S. Talukder, A. K. M. N. Islam, and Y. Bao, "Positive and negative valences, personal innovativeness and intention to use facial recognition for payments," *Industrial Management and Data Systems*, vol. 122, no. 4, pp. 1081–1108, 2022, doi: 10.1108/IMDS-04-2021-0230.
22. F. Bacchini and L. Lorusso, "Race, again: how face recognition technology reinforces racial discrimination," *Journal of Information, Communication and Ethics in Society*, vol. 17, no. 3, pp. 321–335, 2019, doi: 10.1108/JICES-05-2018-0050.
23. H. C. Boo and B. L. Chua, "An integrative model of facial recognition check-in technology adoption intention: the perspective of hotel guests in Singapore," *International Journal of Contemporary Hospitality Management*, vol. 34, no. 11, pp. 4052–4079, 2022, doi: 10.1108/IJCHM-12-2021-1471.
24. C. T. Lee and L. Y. Pan, "Resistance of facial recognition payment service: a mixed method approach," *Journal of Services Marketing*, vol. 37, no. 3, pp. 392–407, 2023, doi: 10.1108/JSM-01-2022-0035.
25. H. Yang and X. Han, "Face recognition attendance system based on real-time video processing," *IEEE Access*, vol. 8, pp. 159143–159150, 2020, doi: 10.1109/ACCESS.2020.3007205.
26. Z. Zhu *et al.*, "WebFace260M: A Benchmark for Million-Scale Deep Face Recognition," *IEEE Trans Pattern Anal Mach Intell*, vol. 45, no. 2, pp. 2627–2644, 2023, doi: 10.1109/TPAMI.2022.3169734.
27. H. Il Kim, K. Yun, and Y. M. Ro, "Face Shape-Guided Deep Feature Alignment for Face Recognition Robust to Face Misalignment," *IEEE Trans Biom Behav Identity Sci*, vol. 4, no. 4, pp. 556–569, 2022, doi: 10.1109/TBIOM.2022.3213845.
28. P. Terhorst, M. Huber, N. Damer, F. Kirchbuchner, K. Raja, and A. Kuijper, "Pixel-Level Face Image Quality Assessment for Explainable Face Recognition," *IEEE Trans Biom Behav Identity Sci*, vol. 5, no. 2, pp. 288–297, 2023, doi: 10.1109/TBIOM.2023.3263186.
29. W. Li, J. Sun, J. Zhang, and B. Zhang, "Face Recognition Model Optimization Research Based on Embedded Platform," *IEEE Access*, vol. 11, no. June, pp. 58634–58643, 2023, doi: 10.1109/ACCESS.2023.3277495.
30. J. Zhao, S. Yan, and J. Feng, "Towards Age-Invariant Face Recognition," *IEEE Trans Pattern Anal Mach Intell*, vol. 44, no. 1, pp. 474–487, 2022, doi: 10.1109/TPAMI.2020.3011426.

31. Y. F. Liu, J. M. Guo, P. H. Liu, J. Der Lee, and C. C. Yao, "Panoramic Face Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 8, pp. 1864–1874, 2018, doi: 10.1109/TCSVT.2017.2693682.
32. L. Li, X. Mu, S. Li, and H. Peng, "A Review of Face Recognition Technology," *IEEE Access*, vol. 8, pp. 139110–139120, 2020, doi: 10.1109/ACCESS.2020.3011028.
33. L. Best-Rowden and A. K. Jain, "Longitudinal Study of Automatic Face Recognition," *IEEE Trans Pattern Anal Mach Intell*, vol. 40, no. 1, pp. 148–162, 2018, doi: 10.1109/TPAMI.2017.2652466.
34. A. Cavazza, F. Dal Mas, P. Paoloni, and M. Manzo, "Artificial intelligence and new business models in agriculture: a structured literature review and future research agenda," *British Food Journal*, vol. 125, no. 13, pp. 436–461, 2023, doi: 10.1108/BFJ-02-2023-0132.
35. Y. Yağmur, A. Demirel, and G. D. Kılıç, "Top quality hotel managers' perspectives on smart technologies: an exploratory study," *Journal of Hospitality and Tourism Insights*, 2023, doi: 10.1108/JHTI-09-2022-0457.
36. E. Moriuchi, "Bridging social marketing and technology in the disability field: an empirical study on the role of cybernetic avatar and social inclusion," *J Soc Mark*, vol. 13, no. 2, pp. 218–240, 2023, doi: 10.1108/JSOCM-05-2022-0111.
37. N. Samala, B. S. Katkam, R. S. Bellamkonda, and R. V. Rodriguez, "Impact of AI and robotics in the tourism sector: a critical insight," *Journal of Tourism Futures*, vol. 8, no. 1, pp. 73–87, 2022, doi: 10.1108/JTF-07-2019-0065.
38. X. Shan, Z. Zhang, F. Ning, S. Li, and L. Dai, "Application and realization of key technologies in China railway e-ticketing system," *Railway Sciences*, vol. 2, no. 1, pp. 140–156, 2023, doi: 10.1108/rs-01-2023-0005.
39. S. Bharwani and D. Mathews, "Techno-business strategies for enhancing guest experience in luxury hotels: a managerial perspective," *Worldwide Hospitality and Tourism Themes*, vol. 13, no. 2, pp. 168–185, 2021, doi: 10.1108/WHATT-09-2020-0121.
40. H. S. Dunn, "Risking identity: a case study of Jamaica's short-lived national ID system," *Journal of Information, Communication and Ethics in Society*, vol. 18, no. 3, pp. 329–338, 2020, doi: 10.1108/JICES-04-2020-0040.
41. M. Khosravy, K. Nakamura, Y. Hirose, N. Nitta, and N. Babaguchi, "Model Inversion Attack by Integration of Deep Generative Models: Privacy-Sensitive Face Generation from a Face Recognition System," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 357–372, 2022, doi: 10.1109/TIFS.2022.3140687.
42. P. Brey, "Ethical aspects of facial recognition systems in public places," *Journal of Information, Communication and Ethics in Society*, vol. 2, no. 2, pp. 97–109, 2004, doi: 10.1108/14779960480000246.
43. C. N. Fondje, S. Hu, and B. S. Riggan, "Learning Domain and Pose Invariance for Thermal-to-Visible Face Recognition," *IEEE Trans Biom Behav Identity Sci*, vol. 5, no. 1, pp. 15–28, 2023, doi: 10.1109/TBIOM.2022.3223055.
44. P. Majumdar, S. Chhabra, R. Singh, and M. Vatsa, "Recognizing Injured Faces via SCIFI Loss," *IEEE Trans Biom Behav Identity Sci*, vol. 3, no. 1, pp. 112–123, 2021, doi: 10.1109/TBIOM.2020.3047274.
45. S. Ge, C. Li, S. Zhao, and D. Zeng, "Occluded face recognition in the wild by identity-diversity inpainting," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 10, pp. 3387–3397, 2020, doi: 10.1109/TCSVT.2020.2967754.
46. A. L. Cushing and G. Osti, "'So how do we balance all of these needs?': how the concept of AI technology impacts digital archival expertise," *Journal of Documentation*, vol. 79, no. 7, pp. 12–29, 2022, doi: 10.1108/JD-08-2022-0170.
47. S. Li, X. Chen, Z. Wang, Z. Qian, and X. Zhang, "Data Hiding in Iris Image for Privacy Protection," *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, vol. 35, no. sup1, pp. 34–41, 2018, doi: 10.1080/02564602.2018.1520153.
48. P. Singh, "Aadhaar and data privacy: biometric identification and anxieties of recognition in India," *Inf Commun Soc*, vol. 24, no. 7, pp. 978–993, 2021, doi: 10.1080/1369118X.2019.1668459.
49. C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, "The European Union general data protection regulation: What it is and what it means," *Information and Communications Technology Law*, vol. 28, no. 1, pp. 65–98, 2019, doi: 10.1080/13600834.2019.1573501.
50. D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3152–3167, 2020, doi: 10.1109/TIFS.2020.2983250.

51. V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Information and Computer Security*, vol. 28, no. 4, pp. 645–662, 2020, doi: 10.1108/ICS-01-2020-0004.
52. Z. Georgiopoulou, E. L. Makri, and C. Lambrinoudakis, "GDPR compliance: proposed technical and organizational measures for cloud provider," *Information and Computer Security*, vol. 28, no. 5, pp. 665–680, 2020, doi: 10.1108/ICS-01-2020-0009.
53. B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, pp. 135632–135649, 2019, doi: 10.1109/ACCESS.2019.2941575.
54. E. I. Toki, G. Tatsis, V. A. Tatsis, K. Plachouras, J. Pange, and I. G. Tsoulos, "Applying Neural Networks on Biometric Datasets for Screening Speech and Language Deficiencies in Child Communication," *Mathematics*, vol. 11, no. 7, pp. 1–15, 2023, doi: 10.3390/math11071643.
55. H. Tan and I. Chung, "Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019, doi: 10.1109/ACCESS.2019.2948207.
56. G. Sanil, K. Prakash, S. Prabhu, V. Nayak, and S. Sengupta, "2D-3D Facial Image Analysis for Identification of Facial Features Using Machine Learning Algorithms with Hyper-parameter Optimization for Forensics Applications," *IEEE Access*, vol. 11, no. August, pp. 82521–82538, 2023, doi: 10.1109/ACCESS.2023.3298443.
57. K. Turksoy, C. Monforti, M. Park, G. Griffith, L. Quinn, and A. Cinar, "Use of wearable sensors and biometric variables in an artificial pancreas system," *Sensors (Switzerland)*, vol. 17, no. 3, pp. 1–17, 2017, doi: 10.3390/s17030532.
58. K. Gorur, "Fourier Synchrosqueezing Transform-ICA-EMD Framework Based EOG-Biometric Sustainable and Continuous Authentication via Voluntary Eye Blinking Activities," *Biomimetics*, vol. 8, no. 378, pp. 1–29, 2023.
59. N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," *J Imaging*, vol. 9, no. 168, pp. 1–12, 2023.
60. L. Lin, Y. Zhao, J. Meng, and Q. Zhao, "A Federated Attention-Based Multimodal Biometric Recognition Approach in IoT," *Sensors*, vol. 23, no. 13, p. 6006, 2023, doi: 10.3390/s23136006.
61. U. Salama, L. Yao, and H. Y. Paik, "An internet of things based multi-level privacy-preserving access control for smart living," *Informatics*, vol. 5, no. 2, pp. 1–18, 2018, doi: 10.3390/informatics5020023.
62. M. N. S. Jahromi *et al.*, "Privacy-constrained biometric system for non-cooperative users," *Entropy*, vol. 21, no. 11, pp. 1–15, 2019, doi: 10.3390/e21111033.
63. A. Capetillo, A. Abraham Tijerina, R. Ramirez, and J. A. Galvan, "Evolution from triple helix into penta helix: the case of Nuevo Leon 4.0 and the push for industry 4.0," *International Journal on Interactive Design and Manufacturing*, vol. 15, no. 4, 2021, doi: 10.1007/s12008-021-00785-x.
64. M. K. S. Budhi, N. P. N. E. Lestari, and N. N. R. Suasih, "THE RECOVERY OF THE TOURISM INDUSTRY IN BALI PROVINCE THROUGH THE PENTA-HELIX COLLABORATION STRATEGY IN THE NEW NORMAL ERA," *Geojournal of Tourism and Geosites*, vol. 40, no. 1, 2022, doi: 10.30892/GTG.40120-816.
65. K. Sudiana, E. T. Sule, I. Soemaryani, and Y. Yunizar, "The development and validation of the penta helix construct," *Business: Theory and Practice*, vol. 21, no. 1, 2020, doi: 10.3846/btp.2020.11231.
66. G. Adomavicius and M. Yang, "Integrating Behavioral, Economic, and Technical Insights to Understand and Address Algorithmic Bias: A Human-Centric Perspective," *ACM Trans Manag Inf Syst*, vol. 13, no. 3, 2022, doi: 10.1145/3519420.
67. I. Fischer, "Evaluating the ethics of machines assessing humans The case of AQA: An assessment organisation and exam board in England," *Journal of Information Technology Teaching Cases*, 2023, doi: 10.1177/20438869231178844.
68. K. Martin and A. Waldman, "Are Algorithmic Decisions Legitimate? The Effect of Process and Outcomes on Perceptions of Legitimacy of AI Decisions," *Journal of Business Ethics*, vol. 183, no. 3, 2023, doi: 10.1007/s10551-021-05032-7.
69. A. Köchling and M. C. Wehner, "Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development," *Business Research*, vol. 13, no. 3, 2020, doi: 10.1007/s40685-020-00134-w.
70. C. Starke, J. Baleis, B. Keller, and F. Marcinkowski, "Fairness perceptions of algorithmic decision-making: A systematic review of the empirical literature," *Big Data Soc*, vol. 9, no. 2, 2022, doi: 10.1177/20539517221115189.

71. L. Dogruel, D. Facciorusso, and B. Stark, "'I'm still the master of the machine.' Internet users' awareness of algorithmic decision-making and their perception of its effect on their autonomy," *Inf Commun Soc*, vol. 25, no. 9, 2022, doi: 10.1080/1369118X.2020.1863999.
72. J. W. Burton, M. K. Stein, and T. B. Jensen, "A systematic review of algorithm aversion in augmented decision making," *J Behav Decis Mak*, vol. 33, no. 2, 2020, doi: 10.1002/bdm.2155.
73. *Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
74. *Draft Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.
75. V. L. Raposo, "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation," *Information and Communications Technology Law*, vol. 32, no. 1, 2023, doi: 10.1080/13600834.2022.2054076.
76. T. G. Moraes, E. C. Almeida, and J. R. L. de Pereira, "Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces," *AI and Ethics*, vol. 1, no. 2, 2021, doi: 10.1007/s43681-020-00014-3.
77. I. Nesterova, "Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world," *SHS Web of Conferences*, vol. 74, 2020, doi: 10.1051/shsconf/20207403006.
78. S. Gupta, S. Modgil, C. K. Lee, and U. Sivarajah, "The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry," *Information Systems Frontiers*, vol. 25, no. 3, 2023, doi: 10.1007/s10796-022-10271-8.
79. F. Kurniasari, E. D. Lestari, and H. Tannady, "Pursuing Long-Term Business Performance : Investigating the Effects of Financial and Technological Factors on Digital Adoption to Leverage SME Performance and Business Sustainability — Evidence from Indonesian SMEs in the Traditional Market," *Sustainability*, vol. 15, no. 12668, pp. 1–20, 2023.
80. Z. Li and H. Wang, "Exploring Risk Factors Affecting Sustainable Outcomes of Global Public – Private Partnership (PPP) Projects : A Stakeholder Perspective," *building*, vol. 13, no. 2140, pp. 1–31, 2023.
81. S. Danladi and U. M. Modibbo, "Achieving Sustainable Development Goals through Financial Inclusion : Collaborative Approaches to Fin-tech Adoption in Developing Countries," *Sustainability*, vol. 15, no. May, pp. 1–13, 2023.
82. D. Ulybyshev, M. Rogers, V. Kholodilo, and B. Northern, "End-to-End Database Software Security," *Software*, vol. 2, no. 2, pp. 163–176, 2023, doi: 10.3390/software2020007.
83. H. Mihaljevic, C. J. Larsen, S. Meier, W. Nekoto, and F. Morón Zirfas, "Privacy-centred data-driven innovation in the smart city. Exemplary use case of traffic counting," *Urban Plan Transp Res*, vol. 9, no. 1, pp. 425–448, 2021, doi: 10.1080/21650020.2021.1950044.