Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India

Rina Arum Prastyanti [a]*, Ridhima Sharma [b]

[a] Faculty of Business and Law, Universitas Duta Bangsa Surakarta, Indonesia.
[b] Vivekananda Institute of Professional Studies, New Delhi, India.

*Corresponding author: rina_arum@udb.ac.id

ARTICLE INFO

Article history
Received: November 15, 2023
Revised: February 25, 2024
Accepted: May 20, 2024

Keywords
Consumers;
Data Protection Law;
Trust;

ABSTRACT

Data protection laws play a crucial role in enhancing consumer trust in the digital economy, especially with the rise of online cybersecurity threats due to firm expansion. Despite advances, personal data protection laws remain controversial globally, with challenges in implementation hindering progress in some regions. This research examines the competitive advantage of building consumer trust through the Personal Data Protection Law. This research uses juridical-normative research with a legislative approach and comparison with other countries. A comparison was made with India, one of the countries with higher awareness of the importance of personal data protection laws than other countries. The results show that Consumer trust in a company is measured by the extent to which they believe the company will protect their data. Public privacy policies and government regulations that enforce data security measures and increase transparency positively impact trust by reducing concerns about privacy risks. Although data protection laws have been introduced, obstacles such as lack of legal assistance and overlapping sectoral regulations still exist, hindering the smooth implementation of these laws. Nevertheless, implementing data protection laws, such as Indonesia's Private Data Protection Law No. 27 of 2022 and India's Digital Personal Data Protection Act of 2023, is crucial for boosting consumer confidence and regulating data processing. Data security is critical in establishing and maintaining consumer trust in companies as online cybersecurity threats increase with business expansion.

1. Introduction

The expansion of the internet matches the accelerated pace of technological progress. Globalization has become considerably more convenient for us since the inception of the internet. The information and technology age has entirely transformed consumer behavior, both positively and negatively. One aspect to consider is that the expeditious advancement of media has resulted in a state of near-equivalent knowledge between sellers and consumers. Information technology, communication, and marketing have all undergone substantial development. Consumer comfort is not without its risks. At present, data security

and privacy represent a considerable challenge. Insufficient data protection measures in Indonesia jeopardize the privacy of numerous consumers.

Constantly evolving in importance within the digital economy is safeguarding consumer data. By enabling businesses to collect, transmit, and utilize consumer data for various purposes, from targeted advertising and price differentiation to creating custom products, digital technologies and the Internet have created new revenue streams for businesses.[1] Neglecting consumer protection can result in severe repercussions. Social trust declines without consumer protection, a significant determinant of transaction and social costs. As a result of the prevalence of information brokers and big data, consumers have limited access to information and have not improved their capacity to make logical and sensible decisions. Additionally, service and product providers can deceive and exploit the interests of consumers. The competitive market order is significantly jeopardized due to the anticompetitive practices that big data brokers and corporations employ.[2]

Trust for consumers is essential as a basis for deciding to buy something. The Basis for selecting to purchase something. Trust in business actors is an advantage for the company because it is beneficial for the survival of the company. Survival of the company. Especially in online shopping, the basis of trust is more critical than conventional trade.[3] Belief-based trust is the capacity to become attuned to the actions of a trusted third party. Research has demonstrated the significant influence of trust on individual behavior. Establishing customer trust in the services and products offered should be a fundamental component of the e-payment system. Consumers will invariably only utilize e-commerce and e-payment functionalities in online transactions with such confidence.

The correlation between privacy and personal data protection is a legal matter that significantly affects social progress and civil rights and engenders substantial disputes.[4] The Industrial Revolution 4.0's extremely rapid technological advancements have led to digitalizing all aspects of government and private sector performance, necessitating a balance between stringent regulations and an extensive data management system to prevent data breaches. Without the

[1] Yongmin Chen, Xinyu Hua, and Keith E. Maskus, 'International Protection of Consumer Data', *Journal of International Economics*, 132 (2021), 103517 https://doi.org/10.1016/j.jinteco.2021.103517

[2] Yaseen S. Alhaj-Yaseen, John T. Barkoulas, and Arav Ouandlous, 'Liberalization and Asymmetric Information Flow Dynamics in the Chinese Equity Markets', *The Journal of Economic Asymmetries*, 21 (2020), e00151 https://doi.org/10.1016/j.jeca.2019.e00151

[3] Jianxiong Zhang and others, 'Manufacturer Encroachment with Quality Decision under Asymmetric Demand Information', *European Journal of Operational Research*, 273.1 (2019), 217–36 https://doi.org/10.1016/j.ejor.2018.08.002

[4] Zhilong Guo, Jie Hao, and Lewis Kennedy, 'Protection Path of Personal Data and Privacy in China: Moving from Monism to Dualism in Civil Law and Then in Criminal Law', *Computer Law & Security Review*, 52 (2024), 105928 https://doi.org/10.1016/j.clsr.2023.105928

implementation of specialized legislation governing the safeguarding of personal data, applying big data will not harm; consequently, violations of this nature will persist.[5] Indonesia's Personal Data Protection Law takes effect on 17 October 2022. The Personal Data law also defines a personal data subject as an "individual," any person, public body, or international organization that acts. Legal issues relating to consumer law protection concerning the rights of consumers in conducting e-commerce transactions within one country or in different countries. In buying and selling via the Internet, these legal issues include, among others, the existence of business actors, the goods purchased, the price of goods, payment by consumers, and the protection of personal data. Today, privacy is more than just a compliance issue; it is a critical opportunity for differentiation. This is especially true for new technology platforms and applications that rely on user trust to grow.

Personal leaks stem from consumers having to provide personal information when shopping online. When using e-commerce, nearly all respondents (97.8%) provided personal information.[6] More than half of those polled frequently provide general personal information such as phone numbers, home addresses, and email addresses. ID card photos (37%), selfies with ID cards (32.4%), Citizen numbers (27.5%), account/credit card numbers (20.4%), and birth mother's name (12.3%) are also provided by consumers. Consumers are willing to provide personal data because they believe it will provide benefits such as more complete features (66.4%), ongoing transaction requirements (56.2%), discounts (37.7%), use of paylater/e-wallet (34.6%), and exclusive information (32.7%). These findings suggest that consumers are willing to provide personal information if there is reciprocity. The e-commerce application Shopee is an online shopping platform. Despite being the most popular app, Shopee does not guarantee the security of its users' personal information.[7]

As more businesses conduct their operations, cybersecurity breaches have increased online. As a result, companies must be cautious of errors that could lead to data theft. An example of a case of personal data is the theft of personal data in the Neopats database. Hackers gained access to Neopets' database and stole up to 69 million users (current and former) personal information and 460 MB of source code. The hackers accessed this database from January 3, 2022, to July 19, 2022.[8]

[5] Moh Hamzah Hisbulloh, 'Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi', *Jurnal Hukum*, 37.2 (2021), 119 https://doi.org/10.26532/jh.v37i2.16272

[6] Ayesha Arora and Tarun Jain, 'Data Sharing between Platform and Seller: An Analysis of Contracts, Privacy, and Regulation', *European Journal of Operational Research*, 313.3 (2024), 1105–18 https://doi.org/10.1016/j.ejor.2023.09.035

[7] Shichen Zhang, Liqun Wei, and Jianxiong Zhang, 'Demand Forecast Sharing for a Dominant Retailer with Supplier Encroachment and Quality Decisions', *European Journal of Operational Research*, 301.1 (2022), 39–50 https://doi.org/10.1016/j.ejor.2021.09.024

[8] Abiodun Esther Omolara and others, 'HoneyDetails: A Prototype for Ensuring Patient's Information Privacy and Thwarting Electronic Health Record Threats Based on Decoys', *Health Informatics Journal*, 26.3 (2020), 2083–2104 https://doi.org/10.1177/1460458219894479

The attackers attempted to sell this information for four bitcoins, alerting Neopets to the breach.[9] Names, usernames, email addresses, IP addresses, gender, date of birth, Neopets PIN, hashed in addition to 460 MB of supply code. Attackers stole the non-public facts of 21 million SuperVPN, GeckoVPN, and other customers in May 2022.[10] Optus is a telecommunications commercial enterprise business enterprise based in Australia. It disclosed a considerable breach in September 2022, doubtlessly exposing the information of 9.8 million clients.

Apart from the cases above, there were thirty-five cases of personal data theft between January and June. This figure exceeds the number of data leakage cases that have occurred each year between 2019 and 2021. The following is a list of data leakage incidents in Indonesia. The data from Indonesian SIM cards sold at the time was claimed to be the work of the Bjorka hacker in 2022. There are 1.3 billion SIM card applicant records, according to reports. The 87 GB of leaked data included NIK, provider phone numbers, and registration dates. The cost of this data is IDR 743.5 million. Meanwhile, there was a data leak case involving Bank Syariah Indonesia (BSI) customers in 2023. There were reports of transaction service disruptions on May 8, 2023, before the data was leaked. Lockbit claims the BSI attack stole 1.5 TB of personal data in this data theft case. Lockbit is one of Russia's ransomware groups. Lockbit had negotiated a ransom of IDR 296 billion with BSI. Lockbit distributed the data on the black market on May 16, 2023, because it was never redeemed. Another data leak occurred in 2023. This time, 34 million passport numbers were exposed. This data leak was carried out once more by the hacker Bjorka. On July 5, 2023, the data was uploaded. It is aware of the public's apprehension due to the prevalence of personal information breaches. These breaches can compromise the privacy and security of individual's personal information and adversely affect consumers engaged in electronic commerce. Personal data leaks have severe consequences for those whose information is widely disseminated. Infringement upon privacy and the risk of falling prey to cybercrimes such as extortion, doxing, or fraud involve unauthorized parties disseminating and revealing targets. When viewed from a nation-state perspective, data breaches can potentially disrupt national stability, as the disclosure of population data facilitates computational propaganda operations by any party in the world.

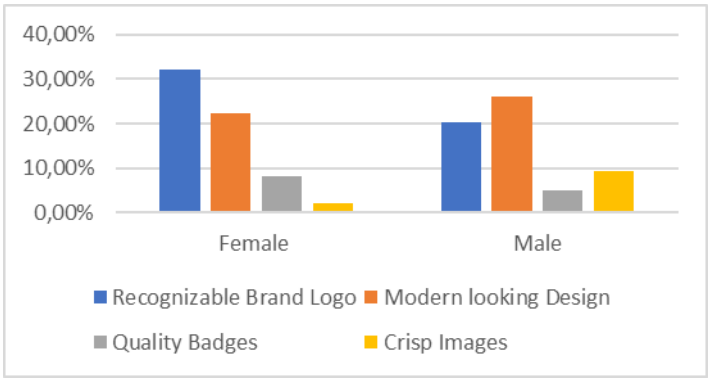
Behind the many cases of data leaks, the electability of e-commerce still influences consumer confidence. The electability of well-known and respected e-commerce attracts consumer interest and transaction confidence. Here's what

[9] 'Strengthening the Security and Privacy of National Identity Numbers (NINs) in Smart Contract Mechanisms through AES Encryption', *Journal of Logistics, Informatics and Service Science*, 10.4 (2023) https://doi.org/10.33168/JLISS.2023.0412

[10] Gaurav Bansal and Fiona Fui-Hoon Nah, 'Internet Privacy Concerns Revisited: Oversight from Surveillance and Right To Be Forgotten as New Dimensions', *Information & Management*, 59.3 (2022), 103618 https://doi.org/10.1016/j.im.2022.103618

people said about the most and least trustworthy online stores.[11] Several factors influence consumer trust in the credibility of a web store.

Figure 1. Factor Positively influence a web store's credibility



Data Source: Kazimierz Rajnerowicz, 2023

The table above shows consumers do not feel worried or think about the risks that will be obtained. In addition, consumers do not know the dangers of a data leak in detail. The records show how the perceived level of belief differs between male and female versions of the internet sites with crisp, high-decision images that became honest with the aid of nine—three more male respondents than the only with low-quality pictures. Several attitudes that influence trust in online purchase intent have been tested.[12] Perceived ease-of-use; consider in an offline save; perceived benefits and net friendly; relative benefit and perceived internet site photograph; quality, consciousness, and institutions of a web shop; performance, privateness, and client service; convenience and entertainment; information safety; and website overall performance are the diagnosed attitudes positively affecting on-line purchase goal.[13]

Consumer attrition after a data breach is a critical corporate and policy issue:[14] Are consumers closing their financial accounts or shopping elsewhere after learning of a data breach? There are numerous reasons why a person would cut

[11] Lin Chen and others, 'Manufacturer's Online Selling Strategies under Spillovers from Online to Offline Sales', *Journal of the Operational Research Society*, 74.1 (2023), 157–80 https://doi.org/10.1080/01605682.2022.2032426

[12] Julia G. Stapels and others, 'Never Trust Anything That Can Think for Itself, If You Can't Control Its Privacy Settings: The Influence of a Robot's Privacy Settings on Users' Attitudes and Willingness to Self-Disclose', *International Journal of Social Robotics*, 15.9–10 (2023), 1487–1505 https://doi.org/10.1007/s12369-023-01043-8

[13] Musaib Ashraf and Jayanthi Sunder, 'Can Shareholders Benefit from Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws', *The Accounting Review*, 98.4 (2023), 1–32 https://doi.org/10.2308/TAR-2020-0787

[14] Anup Anurag Soren and Shibashish Chakraborty, 'Adoption, Satisfaction, Trust, and Commitment of over-the-Top Platforms: An Integrated Approach', *Journal of Retailing and Consumer Services*, 76 (2024), 103574 https://doi.org/10.1016/j.jretconser.2023.103574

ties with a company after receiving a Personal data breach notification.[15] An essential component of sound governance is safeguarding the privacy of customer data, which falls under the domain of customer human rights and contributes to the organization's long-term viability. As this may have repercussions for the company, investors will be especially vigilant if the standard of consumer data protection deteriorates.[16] Data security must be prioritized in supply chain applications that entail the exchange of sensitive and confidential data. Efforts focused on ongoing initiatives demonstrate the imperative to streamline and fortify data logistics. Implementing measures to protect data exchanged within the supply chain ensures data confidentiality, availability, and authenticity. We must emphasize that to reach this objective; solutions are necessary to ensure the survival of the data ecosystem, maintain consumer confidence in remote network security enforcement, and ensure trusted traceability. Because small and medium-sized businesses, among other things, frequently constitute a significant portion of the supply chain, it is also necessary to consider the sovereign participation of both consumers and businesses.[17]

Consumers' personal information protection has a significant impact on customer satisfaction. Security and privacy services significantly influence consumers' online purchasing decisions by ensuring integrity, confidentiality, authentication and preventing potentially harmful transaction recording. Naturally, the security of personal data is of the utmost importance for e-commerce users, given that such information is inherently sensitive. As a result, users can protect their data while utilizing e-commerce by avoiding suspicious activities and remaining vigilant. Establishing a legal connection between personal data security and consumers as e-commerce users is critical for guaranteeing the protection of consumers' personal information and instilling confidence in online purchasing transactions. The global impact of privacy policies on maintaining privacy in various countries is increasing.

The expected level of government intervention to tackle the issues above is substantial. The passage of the Personal Data Protection Bill will provide some reassurance to consumers who have faced negative consequences due to personal data leakage. The fundamental intention behind the Personal Data Protection Law is to ensure compliance with the right to privacy principle. Implementing the

[15] Crispin Niebel, 'The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy', *Computer Law & Security Review*, 40 (2021), 105523 https://doi.org/10.1016/j.clsr.2020.105523

[16] Ninditya Nareswari, Małgorzata Tarczyńska-Łuniewska, and Rizqi Umar Al Hashfi, 'Analysis of Environmental, Social, and Governance Performance in Indonesia: Role of ESG on Corporate Performance', *Procedia Computer Science*, 225 (2023), 1748–56 https://doi.org/10.1016/j.procs.2023.10.164

[17] Johannes Lohmöller and others, 'The Unresolved Need for Dependable Guarantees on Security, Sovereignty, and Trust in Data Ecosystems', *Data & Knowledge Engineering*, 151 (2024), 102301 https://doi.org/10.1016/j.datak.2024.102301

Personal Data Protection Law has redirected focus towards all-encompassing criteria for safeguarding personal data, irrespective of the mode of processing (electronic or non-electronic, in its entirety or part). Each industry has unique characteristics that influence the implementation of personal data protection. The Personal Data Regulation's primary goals are as follows: to protect and ensure individuals' fundamental rights to privacy; to ensure that services offered by governments, companies, public entities, and international organizations are accessible to the general public; to foster the growth of the information and communication technology sector and the digital economy; and to assist in enhancing domestic industry's competitiveness. Perceptions of the safety and security of personal data significantly impact consumer trust. Consumer trust will dramatically increase if e-commerce properly maintains website data information.

The data protection regulations, organizations showcase their commitment to global benchmarks, a critical factor in establishing reliable and robust business associations with international clients and partners. Strong data protection measures can also bolster consumer confidence and the business climate. Consumers are more likely to place trust in and conduct business with organizations that effectively safeguard their personal information.[18] This can foster the expansion of companies and investments while also contributing positively to the overall progress of the national economy. Consequently, regulations on the protection personal information on e-commerce platforms affects the protection and security of consumers and the interests of business actors. Businesses can foster robust international business relationships, attain a competitive edge, and stimulate economic expansion by upholding data protection regulations and ensuring the privacy of business information.[19]

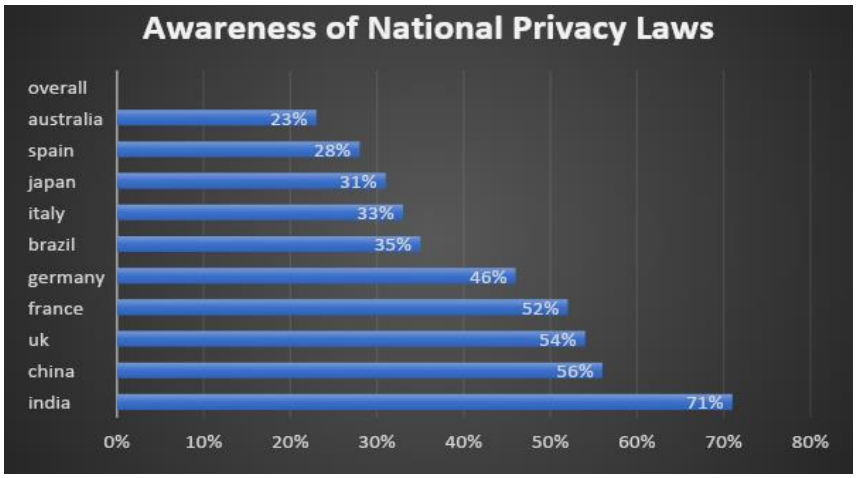
The global impact of privacy policies on maintaining privacy in various countries is increasing. One country with a higher awareness of the importance of privacy laws than other countries is India. The understanding and implementation of privacy in India are contingent upon the region's social structure and the individual. Even in some areas of India, gender influences the perception of privacy. In contrast to Western nations, Indians appear to be more aware of privacy concerns; however, they struggle to accord these matters precedence. As a result, they become more concerned with minor privacy violations. In India, Government agencies that use online transactions follow standard privacy and security guidelines to ensure customers feel safe using this electronic platform. Due to cross-border data transfers, data protection has risen to the top priority list.

[18] Zihao Wu and others, 'Does Effective Corporate Governance Mitigate the Negative Effect of ESG Controversies on Firm Value?', *Economic Analysis and Policy*, 80 (2023), 1772–93 https://doi.org/10.1016/j.eap.2023.11.018

[19] Hassan H. H. Aldboush and Marah Ferdous, 'Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust', *International Journal of Financial Studies*, 11.3 (2023), 90 https://doi.org/10.3390/ijfs11030090

On average, clients outside India expect a higher level of data security. Companies are urging India to strengthen its information security policy so that they can safely outsource work to the country, which has numerous advantages over other countries. According to research, After being notified of a breach, 11% of respondents chose not to interact with the affected organization, leaving 89 percent to do so. While the majority (65%) said the data breach did not impact the amount of business they gave the organization, 23% said they gave them less business than before. They had previously. Surprisingly, 1% said they gave the organization more business due to the data breach.

Figure 2 Awareness of National Privacy Laws



Source: Cisco 2022 Consumer Privacy Survey

Despite progress in other areas, global public awareness of personal data protection laws remains low. Overall, only 43% of respondents in countries with national privacy laws (the same as last year) were aware of their country's laws.[20] The GDPR has been in effect for over three years, but awareness ranges from 28% in Spain to 54% in the United Kingdom.[21] One notable exception is India, where 71% of respondents know the draught PDPB Bill, which has been widely publicized, but adoption remains stalled.[22]

Due to rapid technological changes, law enforcement is also a significant challenge, including difficulties tracing cross-border data breaches. The ever-increasing risk of cyberattacks and data leaks requires a dynamic, transparent, and proactive security approach. Another challenge is finding a balance between

[20] Arezoo Fakhimi, Tony Garry, and Sergio Biggemann, 'The Effects of Anthropomorphised Virtual Conversational Assistants on Consumer Engagement and Trust During Service Encounters', *Australasian Marketing Journal*, 31.4 (2023), 314–24 https://doi.org/10.1177/14413582231181140

[21] Alyssa Jean L. Tan and others, 'Leadership Experiences of Bicultural Business Leaders: An Interpretative Phenomenological Analysis', *Asian Journal of Social Psychology*, 26.4 (2023), 547–59 https://doi.org/10.1111/ajsp.12576

[22] J. Strycharz, J. Ausloos, and N. Helberger, 'Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR', *European Data Protection Law Review*, 6.3 (2020), 407–21 https://doi.org/10.21552/edpl/2020/3/10

innovation and consumer data privacy. Finally, changes in data protection regulations at the global level, such as GDPR, require companies to adapt continuously. To overcome this challenge, intersectoral cooperation involving government, industry, and civil society is needed to develop a solid legal framework, increase awareness, and ensure a reliable technological infrastructure. Safe. A robust, transparent, and explicit legislative framework is needed to protect consumers' personal data privacy. Laws relating to protecting personal data in e-commerce transactions are designed to protect customers from data exploitation, unauthorized disclosure of personal information, and privacy violations. These rules cover several areas of data security, user consent, obligations of electronic system providers, and legal penalties for personal data protection breaches.

Previous research by Georgios Georgiadis show that although Big Data Analytics has generated numerous opportunities and enhanced operational efficiency, it has concurrently heightened the vulnerability to breaches and compromises of personal data. Data Protection Impact Assessment (DPIA) is a requirement of the General Data Protection Regulation (GDPR) to identify suitable controls to mitigate risks associated with personal data protection.[23] Then, Simon Loertscher's research show that as privacy declines, the digital monopoly's profit and social surplus invariably increase. However, regarding privacy, consumer surplus is not monotonous. The match value is flawless without privacy, but the digital monopoly entirely extracts it. Conversely, as privacy increases indefinitely, social surplus and match values decrease to zero. Without privacy protection, consumer surplus is maximized when prices are regulated.[24] Nuria Rodríguez-Priego's research show that the organization's digital transformation is a chance to examine how the company provides customer service by demonstrating appropriate conduct. The primary objective of this study is to explore specific facets of service management, specifically the correlation between customer service and privacy-related conduct. When consumers perceive that the organization genuinely values them, they are more likely to feel empowered about their personal information.[25] Previous research by Mindaugas Degutis et.al show that Consumers' trust in the e-commerce store influences their propensity to disclose personal information. Additionally, the perceived reciprocity of the e-commerce provider surpasses the perceived benefit consumers receive from

[23] Georgios Georgiadis and Geert Poels, 'Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review', *Computer Law & Security Review*, 44 (2022), 105640 https://doi.org/10.1016/j.clsr.2021.105640

[24] Simon Loertscher and Leslie M. Marx, 'Digital Monopolies: Privacy Protection or Price Regulation?', *International Journal of Industrial Organization*, 71 (2020), 102623 https://doi.org/10.1016/j.ijindorg.2020.102623

[25] Nuria Rodríguez-Priego and others, 'Perceived Customer Care and Privacy Protection Behavior: The Mediating Role of Trust in Self-Disclosure', *Journal of Retailing and Consumer Services*, 72 (2023), 103284 https://doi.org/10.1016/j.jretconser.2023.103284

disclosing their data. These findings indicate the presence of symbolic social exchange rather than purely instrumental exchange.[26] Previous research by Artur Strzelecki and Mariia Rizun show that Consumers' trust in the e-commerce store influences their propensity to disclose personal information. Additionally, the perceived reciprocity of the e-commerce provider surpasses the perceived benefit consumers receive from disclosing their data. These findings indicate the presence of symbolic social exchange rather than purely instrumental exchange.[27]

The current gap in the literature is more than just a mere absence of research; it is a significant void that needs to be filled. It stems from the need for more research conducted on the influence of personal data protection regulations on consumer trust. After a few years of personal data protection regulations, little research has examined consumers' reactions to these developments. Although many studies have examined firm behavior, responses, and costs in the aftermath of data breaches, few have examined the consumer perspective. Therefore, the main focus of this research is not just to fill the gap but to potentially influence the competitive advantage of personal data protection regulations on the level of consumer trust (through a comparative study of Indonesia and India). This research is used to conclude changes in consumer trust and regulatory effectiveness after introducing the personal data protection regulations.

2. Research Method

This research is juridical-normative, that is, legal studies that examine relevant prison provisions and what takes place in fact in society or research performed on the actual situation that occurs in society to locate statistics that can be used as research records relating to non-public records protection to increase consumer confidence in enterprise.[28] This study method uses a statutory technique related to a review of all associated legal guidelines and policies. This form of research is also known as descriptive analytical studies because the results of this study are offered descriptively analytically, so this form of study is selected as a method. This study uses two categories of information: primary and secondary data from written resources, including authority files, guidebooks, published research results in news, and diaries. This study, like legal studies in general, often focuses on secondary evidence, primarily written documents about the law: a) primary

[26] Mindaugas Degutis and others, 'Consumers' Willingness to Disclose Their Personal Data in e-Commerce: A Reciprocity-Based Social Exchange Perspective', *Journal of Retailing and Consumer Services*, 74 (2023), 103385 https://doi.org/10.1016/j.jretconser.2023.103385

[27] Artur Strzelecki and Mariia Rizun, 'Consumers' Security and Trust for Online Shopping after GDPR: Examples from Poland and Ukraine', *Digital Policy, Regulation and Governance*, 22.4 (2020), 289–305 https://doi.org/10.1108/DPRG-06-2019-0044

[28] Abdul Kadir Jaelani, Reza Octavia Kusumaningtyas, and Asron Orsantinutsakul, 'The Model of Mining Environment Restoration Regulation Based on Sustainable Development Goals', *Legality : Jurnal Ilmiah Hukum*, 30.1 (2022), 131–46 https://doi.org/10.22219/ljih.v30i1.20764

resources of law, including legal guidelines and relevant criminal regulations, which include statutes, guidelines, and obstacles of the rule.[29]

3. Results and Discussion

Implications of Personal Data Protection Regulation for Consumer Trust

The commerce sector has witnessed rapid expansion within the context of economic development. This results from modifications to the system; transactions previously conducted directly online can now be conducted electronically, via e-commerce, or through a marketplace. E-commerce is a business mode in which transactions are completed using electronic devices and processes. The evaluation of the literature on two elements of e-commerce is extensive for this to look at non-public statistics breaches and consumers' trust in online buying intentions. An intensive examination of personal facts breaches and consumers' acceptance as accurate within the online buy motive will assist in clarifying the individual facts breach phenomenon and reveal consumers' acceptance as accurate with protection. A non-public data breach occurs when touchy, personal, or blanketed facts are accessed and disclosed with an unauthorized celebration. An unauthorized party has accessed and disclosed exclusive or blanketed data. Individual health statistics, identifiable facts, exchange secrets, or intellectual belongings can all be compromised in a facts breach. The unauthorized transmission of information to every other person or entity is known as facts leakage. Data leakage isn't continually the result of deliberate moves. Action. Inside the literature, there may be no specific definition. Some researchers use the terms facts breach and records leakage interchangeably. Other terms for it include identity theft and facts loss.[30]

Given that consumer demand for a product is contingent upon how the firm handles its personal information, the firm may (partially) address consumers' concerns regarding data protection by obtaining consumers' consent for data collection and usage and investing in data security. Digital platforms typically derive revenue from the processing of personally identifiable information. Their services are personalized, and the creation of user profiles is determined by analyzing user behavior data gathered from the internet and their services.[31] As a

[29] Ariefulloh Ariefulloh and others, 'Restorative Justice-Based Criminal Case Resolution in Salatiga, Indonesia: Islamic Law Perspective and Legal Objectives', *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan*, 23.1 (2023), 19–36 https://doi.org/10.18326/ijtihad.v23i1.19-36

[30] Van Dinh and others, 'Determinants Affecting Digital Financial Consumer Protection: Evidence from 135 Countries', *The Journal of Economic Asymmetries*, 27 (2023), e00301 https://doi.org/10.1016/j.jeca.2023.e00301

[31] Viktoria H.S.E. Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data', *SSRN Electronic Journal*, 2019 https://doi.org/10.2139/ssrn.3408971

result, internet security becomes more susceptible to compromise and misuse by malicious actors; consequently, little is said about this case of data leakage.[32]

Current cybercriminals are more curious about obtaining valuable records about their victims than about taking down websites, users, or systems themselves. Statistics leakage is not constrained to online shops or websites but also through cell gadgets. Applications. In keeping with one take a look at, clients had extra belief in online shops that had by no means been breached. But, in response to statistics breaches, members did not create more complicated passwords or display multiplied problems for internet site safety.[33] Most internet customers accept that it's miles the duty of online shops, now not their customers, to shield online facts and mitigate the outcomes of a data breach. Groups that skilled an information breach and well-known responsibility for the consequences obtained excessive scores for three belief components: honesty, benevolence, and competence. Collection of data for engineering Contemporary targeting practices contribute to the phenomenon known as "dataveillance reality," which refers to the automatic, continuous, and non-specific gathering, retention, and analysis of digital traces conducted online by state and corporate actors.[34]

The consumer goods companies and retailers create comprehensive customer profiles based on vast data sources in today's age of big data and digital marketing, even a single security breach can seriously harm consumer confidence. Fifty-nine percent of consumers say they are less likely to buy from a company that has had a data breach. Furthermore, only 51% of consumers say they would be "forgiving" of a company that suffered a data breach as long as the problem was resolved quickly.[35] The widespread coverage of these incidents, 83% of respondents reported being very or somewhat aware of current retail breaches. Furthermore, 83% of the same customers believe that it is critical or essential for consumer product companies to protect the confidentiality of their data when it is

[32] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, 'Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)', *Borneo Law Review*, 5.1 (2021), 46–68 https://doi.org/10.35334/bolrev.v5i1.2014

[33] Ali Masyhar and Silaas Oghenemaro Emovwodo, 'Techno-Prevention in Counterterrorism: Between Countering Crime and Human Rights Protection', *Journal of Human Rights, Culture and Legal System*, 3.3 (2023), 625–55 https://doi.org/10.53955/jhcls.v3i3.176

[34] Moritz Büchi, Noemi Festic, and Michael Latzer, 'The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda', *Big Data & Society*, 9.1 (2022), 205395172110653 https://doi.org/10.1177/20539517211065368

[35] Yanting Huang and Yuqing Liang, 'Influence of Corporate Social Responsibility Considering Dual-Channel Recycling Competition and Privacy Information Protection', *Journal of Cleaner Production*, 373 (2022), 133850 https://doi.org/10.1016/j.jclepro.2022.133850

stored electronically. Regulators are beginning to recognize the privacy threats big data poses, similar to how customers are becoming more aware.[36]

Consumer trust in a company is measured by the degree to which they have faith that the organization will safeguard their private data. Additionally, trust encompasses the assurance that consumers have in the dependability and honesty of an organization or company, along with the protection of information shared with them. The trade-off between sellers and consumers in electronic commerce extends beyond the mere exchange of products.[37] The organization's objective in this scenario is to acquire confidential customer data to make projections regarding forthcoming purchases. Consequently, personal information is transferred from the customer to the organization. Consumer trust in these transactions is contingent upon the seller's ensuing utilization of their personal information. The consumer may anticipate that the vendor will utilize this personal information to suggest products that might interest him or expedite the transaction (e.g., by disclosing payment information, the customary address, etc.).[38] Therefore, any information that customers divulge will be subject to the company's control, with the customer having a secondary influence. In this instance, the organization has authority over the collection and utilization of data, whether for its purposes or to transfer to other businesses. At this time, it is evident that an increase in consumers' perceptions of control can positively influence their level of trust.[39]

In a data-dominated society, data acquisition and processing are essential for operating current technologies and developing new ones. Data protection legislation shields individuals from the dangers of processing "personal data."[40] Regulations about personal data protection are growing in importance within the context of the digital economy. The primary objective is to prevent the improper utilization of personal data, particularly when such data possesses substantial economic worth and is employed in business operations. Law No. 27 of 2022,

---

[36] Joanna Strycharz, Eunah Kim, and Claire M. Segijn, 'Why People Would (Not) Change Their Media Use in Response to Perceived Corporate Surveillance', *Telematics and Informatics*, 71 (2022), 101838 https://doi.org/10.1016/j.tele.2022.101838

[37] Shouzheng Tao, Yezheng Liu, and Chunhua Sun, 'Understanding Information Sensitivity Perceptions and Its Impact on Information Privacy Concerns in E-Commerce Services: Insights from China', *Computers & Security*, 138 (2024), 103646 https://doi.org/10.1016/j.cose.2023.103646

[38] Panchapawn Chatsuwan and others, 'Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs', *Heliyon*, 9.10 (2023), e20648 https://doi.org/10.1016/j.heliyon.2023.e20648

[39] Nuria Rodríguez-Priego, Lucia Porcu, and Philip J. Kitchen, 'Sharing but Caring: Location Based Mobile Applications (LBMA) and Privacy Protection Motivation', *Journal of Business Research*, 140 (2022), 546–55 https://doi.org/10.1016/j.jbusres.2021.11.022

[40] Valentin Rupp and Max von Grafenstein, 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection', *Computer Law & Security Review*, 52 (2024), 105932 https://doi.org/10.1016/j.clsr.2023.105932

which provides comprehensive protection for personal data, will undoubtedly yield favorable outcomes, including heightened public confidence in digital business entities and investors experiencing a sense of security, particularly regarding data storage, when allocating investments in Indonesia. Consequently, it is the government's responsibility to ensure that the provisions of Law No. 27 of 2022 are operational to safeguard individuals' privacy and personal information and foster a business-friendly environment.[41]

Establishing consumer confidence in the Data Protection Law (PDP Law) is critical to maintaining a solid framework for consumer protection. The PDP Law is instrumental in bolstering consumer confidence by protecting personal information and responsibly managing data, both of which are critical for the success of health information exchanges on a national scale.[42] An adequate further reason why consumer confidence and trust in the enforcement framework are at stake is the effective enforcement of consumer protection laws, such as the PDP Law. Establishing pupils' confidence in data management is a prerequisite for developing a reliable nationwide exchange network.[43] By rectifying challenges related to inadequate financial resources and increasing consumer knowledge regarding their entitlements, the PDP Law has the potential to fortify consumer confidence in the enforcement structure.[44]

Numerous nations have enacted legislation about the protection of personal data to bolster consumer confidence. For example, Singapore, Brazil, the European Union, and Japan have all passed comprehensive legislation about data protection. The primary objective of these laws is to protect personal information and foster confidence in the relationship between organizations and individuals. The European Union's data protection laws have positively impacted American consumers by imposing economic, social, and political pressures on American data collectors to adopt comparable methodologies. On the other hand, Singapore's Personal Data Protection Act promotes a culture of privacy and trust by encouraging organizations to exhibit trustworthy conduct towards individuals impacted by data breaches.[45] These examples demonstrate how productive data

[41] Ahmad H. Juma'h and Yazan Alnsour, 'The Effect of Data Breaches on Company Performance', *International Journal of Accounting & Information Management*, 28.2 (2020), 275–301 https://doi.org/10.1108/IJAIM-01-2019-0006

[42] Monika Namysłowska and Agnieszka Jabłonowska, 'Enforcement and Effectiveness of Consumer Law in Poland', 2018, pp. 433–55 https://doi.org/10.1007/978-3-319-78431-1_18

[43] RACHEL M. HAYES, FENG JIANG, and YIHUI PAN, 'Voice of the Customers: Local Trust Culture and Consumer Complaints to the CFPB', *Journal of Accounting Research*, 59.3 (2021), 1077–1121 https://doi.org/10.1111/1475-679X.12364

[44] Putri Hawa Alkatiri, Asep Muhamad Ramdan, and Faizal Mulia Z, 'Analysis of Advertising Effectiveness Free Shipping and Consumer Trust to Increase Purchase Decisions', *Almana : Jurnal Manajemen Dan Bisnis*, 6.2 (2022), 209–20 https://doi.org/10.36555/almana.v6i2.1633

[45] Krittiya Kantachote, 'Micromanagement of Foreign Domestic Workers in Singapore: The Influence of State Regulations and Laws', *Heliyon*, 9.7 (2023), e17679 https://doi.org/10.1016/j.heliyon.2023.e17679

protection legislation can be in fostering consumer confidence by ensuring the confidentiality and security of personal information.[46]

As the EU's overarching data protection regulation, GDPR is applicable throughout the entirety of Europe. The General Data Protection Regulation (GDPR), which primarily codifies European data protection law, requires the processing of "personal data," defined as "any information relating to an identified or identifiable natural person." Determining whether someone processes personal data or only other (non-personal) information is critical because it determines whether the processing parties, controllers, and processors must comply with the GDPR's legal requirements.[47] However, due to the ambiguous concept of protection, it is now impossible to accurately and reliably determine a person's identity. This scenario is rapidly worsening as the scope of data protection regulation extends in tandem with our society's rising digitization. More and more social interaction is dependent on data processing and, thus, potentially personal data. As a result, there needs to be more clarity about when data protection law applies to data processing (and hence the need for a legal basis, information requirements, data subjects' rights, etc.). This implies, on the one hand, disproportionate legal requirements for developing and implementing data-driven technology. On the other hand, people often perceive data protection as ineffective or useless. The obligations and principles established by European data protection law, such as purpose limitation, data minimization, privacy by design and default, and IT security, among others, constitute a rational framework for regulating the overall processing of data. Ultimately, these principles ensure a just, secure, and conscientious management of small and large data sets; therefore, they are fundamental to a society emphasizing individual liberties and rights.

May 2018 marks the implementation of the General Data Protection Regulation (GDPR) within the European Union (EU), which aims to standardize data protection throughout the EU and address contemporary challenges in protecting personal data. While companies anticipate benefits from the GDPR, such as consistent data protection activities and liabilities across EU member states and the facilitation of more integrated data protection policies across the EU, the regulation also poses new challenges. They must prepare for the upcoming changes and may be ignorant of the GDPR's forthcoming obligations and coercive measures. The successful execution of the GDPR mandates necessitates significant financial and human investments and employee training; therefore, organizations require direction to assist them throughout this transition.

---

[46] Danny S. Guamán and others, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications', *Computers & Security*, 130 (2023), 103262 https://doi.org/10.1016/j.cose.2023.103262

[47] Tanja Kammersgaard Christensen, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective', *Computer Law & Security Review*, 53 (2024), 105980 https://doi.org/10.1016/j.clsr.2024.105980

The consequences of data processing may affect data subjects' fundamental rights in various social contexts. As the reason for using legal protection, data protection law is linked to the term "processing" of personal data, which can mean "automated processing" or "systematic and permanent storage" of personal data (depending on the legal system in place). This is done to stop this kind of possible abuse of information power. The General Data Protection Regulation (GDPR) aims to tackle current challenges in protecting personal data, bolstering online privacy rights, and promoting the digital economy in Europe. Its primary goal is to provide individuals with enhanced capabilities to manage and control their data, thereby bolstering data subjects' confidence in organizations that collect such information. The free movement of data under the new data protection framework could be an additional benefit for individual service consumers, provided that it expands businesses offering enhanced and personalized services. A significant obstacle to the GDPR's implementation is a need for more awareness and comprehension among businesses about the forthcoming changes and requirements imposed by the GDPR's new rules. To comply with the GDPR, such requirements necessitate reviewing and revising existing data privacy practices and technological data protection measures and possibly developing new ones.[48]

Western nations, including the United States and Europe, formulated legislation about personal data privacy during that period. The United States government established the Fair Information Practices (FIPs) in 1973, the Swedish federal state of Hessen passed the Data Protection Act in 1970, and the Swedish Data Protection Act in 1973 were the initial measures to safeguard data privacy. Since then, several additional privacy regulation initiatives have emerged. The Organization for Economic Co-operation and Development (OECD) guidelines, DIR95, and now the ones listed above have all implemented and built on FIPs by adding the Privacy by Design (PbD) and Privacy by Default (FDP) principles. Distinct regulatory frameworks and approaches account for global personal data protection laws variations. As a result of current legislation's inability to adapt to technological developments such as artificial intelligence, there are discrepancies in how jurisdictions manage and safeguard personal information. Difficulties in regulating online data processing, striking a balance between legal and self-regulatory approaches, and implementing regulations internationally call into question the efficacy and enforcement of these laws. Organizations implement many models to manage transborder data flows, including organization-to-organization, jurisdiction-to-jurisdiction, and data localization approaches. These models contribute to the intricacy of global data protection initiatives. The international community has witnessed a surge in the implementation or

[48] Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies', *Computer Law & Security Review*, 34.1 (2018), 134–53 https://doi.org/10.1016/j.clsr.2017.05.015

modification of data privacy legislation. This trend reflects the increasing significance that organizations around the globe attribute to data privacy.[49]

The General Data Protection Regulation (GDPR) and other personal data protection regulations are pivotal in establishing and maintaining consumer confidence. These regulations aim to grant individuals authority over their data, safeguarding their rights to such information as explicit consent, erasure, and portability.[50] Public privacy policies and governmental regulations that enforce data security measures and increase transparency positively affect confidence by mitigating concerns about privacy risks. Regardless of the enforcement of these regulations, establishing consumer confidence remains a formidable task, as demonstrated by the inadequate levels of trust observed in the digital economy.[51] The GDPR underscores the significance of data administrators in protecting user identities and privacy, highlighting the need for trust-based methodologies in data management. Strict data protection regulations can boost consumer confidence by promoting transparency, data security, and user autonomy regarding personal data.

Personal Data Privacy Regulation in India

The Internet of Things (IoT) and various technological phenomena lead the fee towards digitization. The aways-attaining implications of smart gadgets explain why the topic keeps making headlines, for higher or worse. The fundamental right to privacy is not expressly granted in the Indian constitution. However, courts have interpreted the right to privacy.[52] As the frequency of incidents and the potential consequences increase, data breaches within Indian organizations have emerged as a significant concern. Regarding cyber threats, India ranks highly internationally, with a substantial increase in data intrusions. These breaches frequently compromise sensitive data, such as pricing information, accounting transactions, and consumer information, posing severe business risks.[53] Data breaches often result from employee misconduct, exposing sensitive information

---

[49] Alharbi Nesreen Nasser A. and Yanhui Li, 'Effects of Privacy Policy and Government Regulation on Trust of Consumers in Saudi Arabia: An Empirical Study', *International Journal Of Innovation And Economic Development*, 5.4 (2019), 7–24 https://doi.org/10.18775/ijied.1849-7551-7020.2015.54.2001

[50] T. Tony Ke and K. Sudhir, 'Privacy Rights and Data Security: GDPR and Personal Data Markets', *Management Science*, 69.8 (2023), 4389–4412 https://doi.org/10.1287/mnsc.2022.4614

[51] Nurul Fibrianti and Amarru Holish, 'Consumer Personal Data Protection: Between Expectations and Reality', in *Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8-9 2021, Semarang, Indonesia* (EAI, 2022) https://doi.org/10.4108/eai.8-6-2021.2314376

[52] Claire Monique Segijn, Suzanna J. Opree, and Iris Van Ooijen, 'The Validation of the Perceived Surveillance Scale', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16.3 (2022) https://doi.org/10.5817/CP2022-3-9

[53] Vikram Sinha and Sharmadha Srinivasan, 'An Integrated Approach to Competition Regulation and Data Protection in India', *CSI Transactions on ICT*, 9.3 (2021), 151–58 https://doi.org/10.1007/s40012-021-00334-7

such as source code, intellectual property, and trade secrets without authorization. Cybercriminals' sophistication and the lack of stringent data security measures exacerbate Indian companies' susceptibility, necessitating more robust security protocols and awareness campaigns. Implementing comprehensive data protection strategies is critical to safeguard organizations' reputations and financial stability while mitigating the effects of data breaches.[54]

Worries about privateness are restrained to Indian residents, without a point out of other countries. Moreover, the research seeks to realize the issue of essential rights through the lens of the Indian Charter. Furthermore, the guidelines made to policymakers and different governments in India have some distance-reaching implications for improving recent policies and controlling private information; this is an excellent way to prevent it from falling into the wrong palms and protect residents' statistics and privacy.[55] India currently lacks express regulation governing facts protection or privacy. However, India's applicable data protection laws are the Information Generation Act of 2000 and the (Indian) Contract Act of 1872. A codified statistics protection law is probable to be enacted. Phase 43A of the (Indian) Facts Generation Act, 2000 states that a body company that possesses offers with, or handles any touchy non-public data or statistics and is negligent in implementing and keeping reasonable safety practices, resulting in wrongful loss or wrongful benefit to any individual, may be held prone to pay damages to the character so affected.[56] It is crucial to note that in such instances, there may be no top restriction on the amount of compensation claimed by the affected party.[57]

The data generation (affordable protection Practices and strategies and sensitive personal information or facts) was posted via the government. The most effective regulations protect "sensitive personal records or statistics of a person," including such records. The guidelines set up reasonable protection practices and strategies that the body corporate or any person who collects, receives, possesses, shops, deals with, or handles information on its behalf is required to observe when dealing with "personal sensitive statistics or records." within the event of a breach,

[54] Sukesh Smrithi, Hephzibah Miriam D. Doreen, and Robin C. R. Rene, 'An Analysis of the Increasing Cases of Data Breaches in India', *I-Manager's Journal on Software Engineering*, 17.3 (2023), 38 https://doi.org/10.26634/jse.17.3.19791

[55] Priya Shah, Neha Mehta, and Sweety Shah, 'Exploring the Factors That Drive Millet Consumption: Insights from Regular and Occasional Consumers', *Journal of Retailing and Consumer Services*, 76 (2024), 103598 https://doi.org/10.1016/j.jretconser.2023.103598

[56] Fatos Selita and others, 'Consensus Too Soon: Judges' and Lawyers' Views on Genetic Information Use', *New Genetics and Society*, 42.1 (2023) https://doi.org/10.1080/14636778.2023.2197583

[57] Jyoti Upadhyay, Avita Katal, and Preeti D Mehta, 'Self-Regulated Learning, an Important Tool to Improve Learning Capability: An Indian Case Study', *The International Journal of Learning in Higher Education*, 31.1 (2023), 69–95 https://doi.org/10.18848/2327-7955/CGP/v31i01/69-95

the body company or every other character acting on its behalf can be held vulnerable to pay damages to the person affected.[58]

Segment 72A of the (Indian) Facts Era Act, 2000 makes knowingly and deliberately disclosing statistics without the consent of the character involved and in breach of the lawful settlement punishable through imprisonment for a term of up to a few years and a pleasant of as much as Rs five, (about US$ 8,000). It should be noted that segment sixty-nine of the Act, which is an exception to the general rule of maintaining facts privateness and secrecy, gives that wherein the government is satisfied that it's far essential within the interest of the sovereignty or integrity of India, defense of India, security of the state, pleasant relations with foreign States, or public order, or for stopping incitement to the commission of any cognizable offense regarding the preceding, or for investigation.[59]

This segment authorizes the government to intercept, display, or decrypt records and non-public facts in any PC helpful resource. The government may additionally require disclosure of statistics if it's miles of any such nature that it has to be disclosed inside the public hobby. This category can also encompass statistics about anti-country-wide sports that violate countrywide protection, violations of the law or statutory responsibility, or fraud. Thousands and thousands of humans have submitted private information to an online platform. Moreover, a few government initiatives in India include the Aadhaar card, which collects biometric facts from Indian residents. In lots of instances, private facts are compromised in diverse situations. Because residents' non-public information is at stake, the look has immediate practical implications, especially for all citizens whose non-public facts are available online.[60]

Safeguarding information entails much more than simply preventing unauthorized access. It is also critical to reassure consumers that their trust in a specific consumer product manufacturer is well-placed. According to a recent poll of customers and executives, while customers are acutely aware of the risks associated with data privacy and security, many consumer product executives likely overestimate the degree to which their products meet consumer

[58] Ketki Ranade, Arjun Kapoor, and Tanya Nicole Fernandes, 'Mental Health Law, Policy & Program in India – A Fragmented Narrative of Change, Contradictions and Possibilities', *SSM - Mental Health*, 2 (2022), 100174 https://doi.org/10.1016/j.ssmmh.2022.100174

[59] Ajitabh Dash and Sandeep Kumar Mohanty, 'Technology Readiness and the Older Citizen's Acceptance of m-Health Services in India', *Digital Policy, Regulation and Governance*, 25.2 (2023), 169–83 https://doi.org/10.1108/DPRG-11-2022-0126

[60] Gianclaudio Malgieri and Frank Pasquale, 'Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology', *Computer Law & Security Review*, 52 (2024), 105899 https://doi.org/10.1016/j.clsr.2023.105899

expectations.[61] In contrast, many consumer product executives may underestimate the potential economic benefit of meeting customer data security and confidentiality requirements. Furthermore, based on their current data security and privacy strategies, policies, and systems, many consumer goods companies do not appear to be in a favorable position to gain consumer trust. [62]Consumer goods companies seem to have a significant opportunity to differentiate themselves by implementing cutting-edge data security and protection policies. Leaders in the consumer products industry would be wise to consider data security and privacy as a critical aspect of doing business and a potential source of competitive advantage.[63]

Figure 3 Challenge areas related to Data Privacy & Security

	Particularly challenging data privacy and security objectives for many consumer product companies
Vision and strategy	• Making data privacy and security a critical company-wide priority supported by adequate budget and resources • Maintaining an up to date strategy in the event that a breach is identified • Establishing a clear strategy for the collection and use of consumer data
Policies	• Crafting easy to understand consumer facing policies that emphasize opting in instead of opting out • Keeping policies up to date with changing technology and regulations
Organization and people	• Elevating a senior privacy officer to the C-suite with ultimate responsibility for data privacy and security and giving him/her the authority to carry out responsibilities
Processes and systems	• Restricting access to consumer data by business need to know • Tracking and monitoring all access to consumer data • Utilizing advanced cyber techniques (i.e., wargaming) to test security
Risk Management	• Identifying potential external and internal threats • Staying up to date on full range of tactics attackers may use • Monitoring third-party providers

Data source: Brijesh Singh, 2022

[61] Federico Costantini and Giada Soncini, 'Healthcare Data Governance in the EU: Main Challenges in Personal Data Protection', in *Endorobotics* (Elsevier, 2022), pp. 319–36 https://doi.org/10.1016/B978-0-12-821750-4.00014-1

[62] Sautma Ronni Basana, Mariana Ing Malelak, and Zeplin Jiwa Husada Tarigan, 'The Effect of Excessive Social Networking Sites on Credit Overuse Behavior through Money Trust, Money Anxiety, and Money Power', *International Journal of Data and Network Science*, 8.1 (2024), 655–66 https://doi.org/10.5267/j.ijdns.2023.8.020

[63] Nadine Pieper and David M. Woisetschläger, 'Customer Misbehavior in Access-Based Mobility Services: An Examination of Prevention Strategies', *Journal of Business Research*, 171 (2024), 114356 https://doi.org/10.1016/j.jbusres.2023.114356

India's digital economy is becoming increasingly crucial for the country's future. According to NASSCOM, India's technology industry grew 15.5% in the final year of the pandemic, reaching $227 billion in revenue in 2021-2022. Fintech, or financial technology, is at the forefront of this surge. Since 2016, when accurate time was introduced, Since the introduction of the Unified Payments Interface, or UPI payment system, more than 304 banks have signed on. In March 2022, approximately 5.4 billion transactions totaling $128 billion were completed, a staggering figure. Given India's 86% and nearly 800 million broadband subscribers, this will only grow.[64]

The rapid adoption of the digital economy in India poses challenges, particularly regarding data security. By 2024, 40% of large enterprises will use AI in all business-critical functions, such as marketing, legal, human resources, procurement, and supply chain logistics. This will increase data collection and utilization, including critical and sensitive information. As more data is stored, potential breaches raise the risk of identity theft, bank fraud, and economic destabilization, resulting in economic losses and political instability. Historically, cyber attackers have stolen strategic information and sensitive financial plans, but they have recently attacked critical infrastructure and stolen intellectual property (IP), particularly trade secrets.[65] Theft of necessary infrastructure IPs could have disastrous consequences for the global economy and national security. As a result, comprehensive records protection coverage with statistics safety regulations is crucial. Without a complete statistics protection regulation, regulators and government groups have issued zone-specific information privacy regulations, rules, standards, and quality practices, together with the subsequent. The facts era (reasonable security practices and procedures and sensitive personal statistics or records) policies, 2011. Records transferred outside India by author officers/departments are punishable if they violate the Public Facts Act 1993, the Respectable Secrets Act 1923, the email policy, or the government of India's coverage for the use of IT sources. Four ministries and departments may additionally host their servers with 0.33 parties, but the handiest in the Ministry of Home Affairs and CERT-IN hints). The Reserve Financial Institution of India (RBI) has permitted the status quo of an Account Aggregator framework.[66]

---

[64] Amparo Coiduras-Sanagustín, Eduardo Manchado-Pérez, and César García-Hernández, 'Understanding Perspectives for Product Design on Personal Data Privacy in Internet of Things (IoT): A Systematic Literature Review (SLR)', *Heliyon*, 10.9 (2024), e30357 https://doi.org/10.1016/j.heliyon.2024.e30357

[65] Tuulia Karjalainen, 'The Battle of Power : Enforcing Data Protection Law against Companies Holding Data Power', *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 47.August 2018 (2022), 105742 https://doi.org/10.1016/j.clsr.2022.105742

[66] Shivam Gupta and others, 'The Role of Innovation Ambidexterity on the Relationship between Cognitive Computing Capabilities and Entrepreneurial Quality: A Comparative Study of India and China', *Technovation*, 127 (2023), 102835 https://doi.org/10.1016/j.technovation.2023.102835

The RBI issued guidelines in March 2020 requiring payment aggregators to implement data security standards, including IT policy, cyber security audits, and reports. The RBI issued a circular in September 2021 mandating that, beginning in January 2022, (a) no entity other than card issuers or card networks be allowed to store card data, and (b) all such data stored before that date be purged. The Insurance Regulatory and Development Authority of India ("IRDAI") has issued information and cyber security guidelines for insurers. Similarly, the Securities and Exchange Board of India maintains data and cyber security guidelines for stockbrokers, exchanges, and depositories. The Ministry of Electronics and Information Technology (MeitY) of India issued a report on the Non-Personal Data Governance Framework in December 2020.[67]

MeitY has proposed a comprehensive data protection bill focusing on data localization. The first such regulation in India is modeled after the General Data Protection Regulations (GDPR). of the European Union, with specific provisions reflecting the California Privacy Act's guidelines. Apart from categorizing data into three broad categories, namely personal data, sensitive personal data, and critical sensitive personal data, it includes provisions on explicit consent for data sharing, data processing, and safeguards, including penalties for misuse. It also defines the government's and regulators' roles, making it easier for businesses to develop policies. It also addresses the ongoing global debate over the "Right to Be Forgotten" rule, which grants individuals the right to be forgotten.[68]

During bill consultations, corporations and the political opposition objected to data localization. The opposition also objected to Clause 35, which allows any agency to be exempt from all or any law provisions, particularly those concerning public order, sovereignty, and friendly relations with foreign states. In its most recent "Special 301" report, the US Trade Representative expressed concern about India's Personal Data Protection Bill and the draft of its non-personal data governance framework, claiming that they could jeopardize India's innovation and economic growth. The bill is expected to balance data localization and cross-border data flows well. The road to interoperability is a work in progress, especially since the Data Protection Bill is still being debated.[69] All Indian corporations are free to store data anywhere in the world. The proposed law change would keep data local, prohibiting both Indian and foreign companies

[67] Bhawana Sharma and others, 'Explainable Artificial Intelligence for Intrusion Detection in IoT Networks: A Deep Learning Based Approach', *Expert Systems with Applications*, 238 (2024), 121751 https://doi.org/10.1016/j.eswa.2023.121751

[68] Silvana Castano and others, 'Enforcing Legal Information Extraction through Context-Aware Techniques: The ASKE Approach', *Computer Law & Security Review*, 52 (2024), 105903 https://doi.org/10.1016/j.clsr.2023.105903

[69] Sylvia Divalona and Sfenrianto, 'An Empirical Study on the Factors Affecting Customer Satisfaction and Customer Loyalty in Online Transportation Apps', *Journal of System and Management Sciences*, 14.4 (2023) https://doi.org/10.33168/JSMS.2023.0406

from transferring data outside of Indian jurisdiction. The data localization provision is generally regarded favorably, as it may allow Indian entrepreneurs to develop an Indian data center industry.[70]

Encryption ensures the confidentiality and integrity of data flowing over networks, which policymakers and regulators may use to protect against potential threats and address critical concerns. Dynamic data masking, tokenization, and other technical safeguards against cyber threats. Creation of an overarching data protection act that goes beyond the piecemeal and incorporates principles of notice, choice, consent, collection and purpose limitation, access and correction, disclosure of information, security, openness, accountability, and a compliance enforcement mechanism.[71] The proposed law requires companies to store data within India's borders. Companies in India have attempted to increase consumer confidence by utilizing the Personal Data Protection Act. The purpose of the Act is to protect personally identifiable information. Ensuring adherence to data protection legislation is of the utmost importance for digital enterprises seeking to establish consumer confidence and safeguard privacy. Consistent with worldwide patterns in data privacy regulations, the Act emphasizes the importance of all-encompassing data safeguards. Adherence to data protection laws is critical for cultivating consumer confidence in India's swiftly progressing digital economy. By adhering to the protocols delineated in the Personal Data Protection Act, companies can exhibit their dedication to safeguarding consumer information and privacy, fortifying their standing and reputation within the marketplace.[72]

The 2022 Digital Personal Data Protection (DPDP) Bill marked a milestone in India's fast-expanding digital sector. Any company that collects or manages personal data must comply with India's new Digital Personal Data Protection Act of 2023. This law governs data processing in India and abroad. Companies in India have responded to personal data protection laws by implementing various strategies. The company implemented solutions for monitoring and enforcing data protection laws on an e-government interoperability platform by integrating integration mechanisms and utilizing recognized security standards.[73] In India, corporations have turned to private contracts to safeguard data, as the current legislation imposes certain restrictions. Indian companies have adopted a comprehensive approach to devising these strategies to navigate the dynamic

[70] Himani Maurya and Suneel Prasad, 'Data Protection Laws and a Comparative Analysis of GDPR and PDPB', 2022, p. 030077 https://doi.org/10.1063/5.0110597
[71] Fibrianti and Holish.
[72] Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law', *SSRN Electronic Journal*, 2018 https://doi.org/10.2139/ssrn.3244203
[73] Neelam Chawla and Basanta Kumar, 'E-Commerce and Consumer Protection in India: The Emerging Trend', *Journal of Business Ethics*, 180.2 (2022), 581–604 https://doi.org/10.1007/s10551-021-04884-3

realm of data protection regulations effectively. Furthermore, the organization employed an integrated collection of technologies called the Hippocratic Database (HDB) to ensure adherence to security and privacy regulations while minimizing disruption to information flow. This allowed for detailed disclosure policies and proactive enforcement of said policies. The prevailing practice of dominant corporations incorporating fundamental rights to exert control shaped the company's conduct, influencing the implementation of data protection and privacy legislation to ensure adherence to regulatory frameworks such as the GDPR.[74] As a result of implementing advanced technologies and adhering to data protection laws, the organization could effectively manage the complexities of data protection regulations and guarantee the appropriate use of information.

Personal Data Privacy Regulation in Indonesia

Indonesia enacted the private facts safety regulation in November 2020, establishing a legal framework for protecting personal records. The private information safety regulation applies to the processing of private records performed by way of people or entities, whether public or personal, inside or out of doors Indonesia, which is associated with Indonesian citizens, residents, or criminal entities in Indonesia. It aims to defend non-public data by requiring information controllers to attain consent, set up safeguards for processing private information, and offer individuals the proper entry to, accurate, and erase their non-public records.[75]

The law outlines several principles that organizations must comply with when processing non-public facts, along with facts minimization, reason obstacles, transparency, and accountability. The regulation additionally establishes a private data protection commission to oversee the implementation and enforcement of the regulation. Under the regulation, the processing of personal statistics is against the law, except the miles achieved with the consent of the statistics challenge or is vital for positive purposes, such as the achievement of a settlement, compliance with criminal responsibilities, or protection of critical pastimes.[76]

In terms of enforcement, the law imposes administrative sanctions, such as warnings, fines, and revocation of business licenses, for law violations. Additionally, individuals may seek compensation for damages resulting from breaches of their data rights. Indonesia's Personal Data Protection Law protects

[74] Afreen Nishat A. Nasabi and Sujaya H., 'Consumer Buying Behaviour Trends of E-Commerce in India- A Case Study', *International Journal of Management, Technology, and Social Sciences*, 2022, 736–50 https://doi.org/10.47992/IJMTS.2581.6012.0247

[75] Adi Prasetyo Tedjakusuma and others, 'Intention to Purchase Halal Health Supplement Online: Lessons Learned from the Health Crisis', *Heliyon*, 9.9 (2023), e19840 https://doi.org/10.1016/j.heliyon.2023.e19840

[76] 'Analysis Of Digital Marketing Quality Before and During the Covid-19 Pandemic on Frozen Food Consumers in West Java Region', *Quality-Access to Success*, 25.198 (2023) https://doi.org/10.47750/QAS/25.198.16

individuals' privacy and personal data rights. However, its implementation and enforcement will ensure that organizations comply with the law's requirements and that individuals' rights are adequately protected. In Indonesia, the implementation and regulation of personal data protection are typically governed by regulation No. 11 of 2008 on digital facts and transactions (EIT law) and authorities' law No. Seventy-one of 2019 is on implementing electronic systems and transactions (GR 71/2019).

The ITE law regulates the protection of private statistics and records processed via digital structures, together with records associated with people's personal lives, health, budget, and other touchy data. The ITE law calls for data controllers to acquire consent from statistics topics earlier than gathering, using, or disclosing their non-public statistics. It additionally requires statistics controllers to ensure the accuracy and safety of personal information and to inform facts subjects in case of a records breach. GR 71/2019 offers, in addition, info on the implementation of the EIT law, consisting of the necessities for statistics controllers to have privacy coverage and a security management plan in location. It also established the Indonesian country-wide Cyber and Encryption Organization (BSSN) because the regulator is responsible for overseeing the implementation of ITE law.[77]

Further to the ITE regulation and GR seventy-one/2019, there also are quarter-precise rules governing the safety of private statistics in Indonesia, inclusive of the Fitness Ministry regulation No. 20 of 2016 on non-public fitness information protection and the Economic Services Authority law No. 1/POJK.07/2013 on customer statistics privacy in monetary offerings.[78] Usually, the implementation and regulation of private data safety in Indonesia continue evolving, and there have been calls for more potent enforcement and extra comprehensive statistics safety laws. However, the existing legal framework gives a foundation for protecting personal information and records processed through electronic structures.

The enforcement of personal data protection in Indonesia has improved in recent years, but there is still much room for improvement. In 2016, Indonesia passed its first comprehensive facts protection regulation, the Non-public Data Protection Act (PDPA). The regulation calls for fact controllers to obtain consent from people before accumulating, using, or disclosing their private records. It also requires fact controllers to force appropriate security measures to shield personal

[77] Abdul Hadi and others, 'Undang-Undang Informasi Dan Transaksi Elektronik Dalam Konteks Maqasid Syari'ah', *Al-Manahij: Jurnal Kajian Hukum Islam*, 14.2 (2020), 211–24 https://doi.org/10.24090/mnh.v14i2.3582

[78] Reza Octavia Kusumaningtyas and others, 'Reduction of Digitalization Policy in Indonesian MSMEs and Implications for Sharia Economic Development', *JURIS (Jurnal Ilmiah Syariah)*, 21.2 (2022), 157 https://doi.org/10.31958/juris.v21i2.6855

facts from unauthorized admission or disclosure. However, there have been concerns about the enforcement of the PDPA. The Indonesian government has been criticized for not allocating sufficient resources to enforce the law, and there have been few prosecutions or fines for law violations. Moreover, some companies are non-compliant with the law, and data breaches in Indonesia have exposed individuals' personal information. In response to these issues, the government of Indonesia has taken steps to improve the enforcement of the PDPA.[79] In 2020, the government established a dedicated data protection agency, the Indonesian Data Protection Authority (IDPA), to oversee and enforce the PDPA. The IDPA can investigate complaints and issue fines for non-compliance with the law.[80]

On October 17, 2022, the President endorsed the Personal Data Protection Bill, marking a significant milestone in safeguarding personal data in Indonesia. The Lex specialist for personal data protection regulations in Indonesia, the Personal Data Protection Law (UU PDP). Because it is a compact regulation, the PDP Law necessitates many implementing rules, including sectoral regulations and provisions promulgated by institutions. Supporting the understanding and strengthening of all participants in the personal data protection ecosystem is necessary to achieve compliance by proactively lowering protection failures and unauthorized processing. The framework of data protection protocols should prioritize preventive measures. As a result, dialogues concerning safeguarding personal information persist in their dynamic nature in response to evolving legal and social trends.[81] The difficulties encountered pertain to law enforcement about the established regulations, specifically concerning how the substance of these regulations can guarantee the security of personal information in Indonesia. Furthermore, the apparatus's actions and the community's reaction have an impact.

One area of concern pertaining to the execution of Law No. 27 of 2022 on Personal Data Protection in Indonesia concerns the legal justifications employed in the processing of such information. The PDP Bill prioritizes consent as a prerequisite, but its implementation is still up for debate. Another obstacle is institutional regulation, which concerns the structure and authority of institutions tasked with implementing personal data protection. Law Number 27 of 2022 on Personal Data Protection has brought the safeguarding of personal information to

[79] Nania Nuzulita and Apol Pribadi Subriadi, 'The Role of Risk-benefit and Privacy Analysis to Understand Different Uses of Social Media by Generations X, Y, and Z in Indonesia', *The Electronic Journal Of Information Systems In Developing Countries*, 86.3 (2020) https://doi.org/10.1002/isd2.12122

[80] Almira Putri Aryani and Liana Endah Susanti, 'Pentingnya Perlindungan Data Pribadi Konsumen Dalam Transaksi Online Pada Marketplace Terhadap Kepuasan Konsumen', *Ahmad Dahlan Legal Perspective*, 2.1 (2022), 20–29 https://doi.org/10.12928/adlp.v2i1.5610

[81] Siti Yuniarti, 'Protection Of Indonesia's Personal Data After Ratification Of Personal Data Protection Act', *Progressive Law Review*, 4.02 (2022), 54–68 https://doi.org/10.36448/plr.v4i02.85

Indonesia. Nonetheless, numerous barriers persist in the way of execution, including a dearth of legal recourse and sectoral regulations that overlap.

At the same time, as there have been improvements in enforcing private information safety in Indonesia, paintings still need to be done to ensure that individual privacy rights are correctly covered. Consumers consider e-trade personal records protection an essential difficulty that can impact the fulfillment of online groups. With increasing private facts being shared online, clients have become more worried about protecting their records. In January 2022, the online forum raid forum sold 720 GB of sensitive information, including personal medical data. According to the GOD User account, this information originates from the Ministry of Health and BPJS Health servers. Then, over 160,000 files totaling 60 GB revealed the private information, including complete names, addresses, and phone numbers, of PT Pertamina Training & Consulting job applicants. Subsequently, Bjorka acquired 1.3 billion SIM card details in September 2022, selling them on the breach, to forum. This data includes the telephone number, Population Identification Number (NIK), and the registration date. Additionally, BPJS Employment users have been the target of data leaks, with an estimated 19.56 million data points exposed on dark web platforms on March 12, 2023.[82]

From the results of the research on consumer trust in e-commerce related to personal data protection. Here are some key findings: Indonesian purchasers are increasingly worried about information privacy, with 79% of Indonesians involved in how organizations utilize their private records. This shows that purchasers are increasingly privy to facts and privacy issues and seek more excellent protection of their personal information. Customers are much more likely to buy from sites they consider to defend their non-public facts.[83] 75% of clients in Indonesia could forestall the use of e-commerce if they discovered that their private records were compromised. This highlights the importance of preserving patron acceptance as accurate to maintain clients. Transparency can build agreement. The consequences show that 81% of humans accept as precise that the potential risks of fact collection outweigh the advantages. However, if organizations are prominent in their facts series and usage practices, purchasers can be extra willing to share their private information.[84]

In short, purchasers are increasingly involved in information privacy and consider it vital to e-trade success. Corporations that are obvious about their records series and utilization practices and take steps to guard consumer statistics

[82] Niebel.
[83] Rosnita Wirdiyanti and others, 'How Does E-Commerce Adoption Impact Micro, Small, and Medium Enterprises' Performance and Financial Inclusion? Evidence from Indonesia', *Electronic Commerce Research*, 23.4 (2023), 2485–2515 https://doi.org/10.1007/s10660-022-09547-7
[84] Wirdiyanti and others.

can construct and accept as accurate with clients and enhance their business performance. To complete patron belief, e-commerce companies must shield their clients' private facts. This could be done by implementing sturdy security features, including encryption, firewalls, and comfortable price processing structures.[85]

In addition, e-trade corporations may be transparent about their records safety rules and provide clean statistics to customers on how their records could be used. They ought to obtain express consent from clients before accumulating any private information and allow clients to enter and delete their data quickly. E-commerce agencies must also observe relevant statistics safety guidelines, consisting of the overall statistics safety regulation (GDPR) in the ECU Union, to ensure they assemble legal necessities for protecting client records. By those steps, e-commerce corporations can reveal their commitment to protecting their customers' private data and build trust with them. This can cause expanded purchaser loyalty and advanced commercial enterprise overall performance.

Consumers lack personal data protection expertise. Although supplying personal data is risky, consumers don't think it's excessively harmful. Even though e-commerce requires personal data to continue transactions, individuals are coerced and unwilling to offer it. The government should educate the public through public service ads about personal data protection and the PDP Law, create derivative regulations, and teach how to report e-commerce cases, especially data leaks. E-commerce and the government must collaborate to address the exploitation of customer data and enhance data security.[86]

The safeguarding of personal data in Indonesia has become a subject of considerable scrutiny due to cybercrimes such as doxing and breaches of personal data confidentiality. Current legislation, including the Electronic Information and Transaction Law, must be revised to address the constantly evolving nature of data intrusions. Critical issues, such as the Tokopedia data breach, have highlighted the need for more stringent regulations and supervision mechanisms to protect consumers' information in online applications. Contemporary legislative measures, such as Law Number 27 of 2022, endeavor to establish legal safeguards for personal information by human rights principles, focusing on social justice and dignity within legal structures. Furthermore, the potential misuse of personal data in online loan services has raised concerns. This has necessitated the implementation of stringent legal safeguards and penalties to deter the unauthorized collection and disclosure of data. In addition to adapting to rapid

[85] David Grande and others, 'Consumer Willingness to Share Personal Digital Information for Health-Related Uses', *JAMA Network Open*, 5.1 (2022), e2144787 https://doi.org/10.1001/jamanetworkopen.2021.44787

[86] Ayhan Serkan Şık, Arsev Umur Aydınoğlu, and Yeşim Aydın Son, 'Assessing the Readiness of Turkish Health Information Systems for Integrating Genetic/Genomic Patient Data: System Architecture and Available Terminologies, Legislative, and Protection of Personal Data', *Health Policy*, 125.2 (2021), 203–12 https://doi.org/10.1016/j.healthpol.2020.12.004

technological advancements, Indonesia's digital banking governance faces obstacles that necessitate new legislation to ensure adequate protection of personal data in the digital banking sector.

The PDP Law will enhance consumer confidence by guaranteeing data security and privacy. As a result, the PDP Law, which ensures the confidentiality and security of their data, has bolstered consumer confidence among Indonesian businesses. The companies listed below are examples of Indonesian organizations that have successfully implemented the Personal Data Protection Law and bolstered consumer confidence. Bank Indonesia has regulated consumer and transaction data used by the Personal Data Protection Law. Bank Indonesia has also enhanced data security measures by implementing more advanced technological systems and raising public awareness about the criticality of safeguarding personal information. By implementing the Personal Data Protection Law, Hootsuite Indonesia has begun to regulate the use of Internet user data. Additionally, Hootsuite Indonesia has improved data security by implementing more advanced technology and raising public awareness about the criticality of safeguarding personal information.

Roche Indonesia has established a privacy policy that is explicit and unambiguous. With compliance with this privacy policy, consumer information is handled securely and according to applicable laws. By safeguarding personal data against unauthorized use and infringement and ensuring that the constitutional rights of individuals whose personal data is being processed are respected, Law No. 27 of 2022 on Personal Data Protection has bolstered consumer confidence. In Indonesia, the implementation of Law No. 27 of 2022 on Personal Data Protection (UU PDP) has positively impacted consumer confidence. The PDP Law establishes strict requirements for security and transparency in the administration of personal data. Organizations must process data in a lawful, transparent, and purposeful manner. Furthermore, the PDP Law raises public awareness about the importance of protecting personal information and consumers' rights. By adhering to the PDP Law, businesses exhibit their dedication to safeguarding the personal information of consumers. This could boost client confidence and the company's reputation. The PDP Law imposes severe penalties for breaches of personal data protection regulations. This situation incentivizes organizations to exercise greater caution and proactivity in upholding data security, thereby bolstering the confidence and security of consumers.

4. Conclusion

Based on the analysis and discussion, a conclusion is drawn: *First*, digital technology and the Internet allow companies to acquire, transfer, and use consumer data for product development, pricing differentiation, targeted advertising, and establishing new revenue streams. Online cyber security dangers rise with company growth. Thus, firms must consider data theft risks. Consumer

trust in a company depends on data security. *Second*, despite advancements in various areas, personal data protection laws remain controversial globally, with challenges in implementation and enforcement persisting. The ratification and enforcement of data protection bills, such as India's Digital Personal Data Protection Act of 2023, are essential steps towards regulating data processing and ensuring consumer privacy rights. Whereas, the Indian government has taken steps to regulate personal data protection through the implementation of the Digital Personal Data Protection Act of 2023, which governs data processing within India and overseas. Companies in India have responded to personal data protection laws by implementing various strategies, such as monitoring and enforcing data protection laws through e-government interoperability platforms and recognized security standards to ensure comprehensive data safeguards and consumer confidence. Third, Indonesia has enacted the Private Data Protection Law No. 27 of 2022 to enhance public and investor confidence in digital firms by protecting personal data and privacy rights. But, challenges related to the structure and authority of institutions responsible for enforcing personal data protection laws hinder effective implementation in various regions. Continuous efforts are being made to strengthen the enforcement of personal data protection laws in Indonesia, with calls for more comprehensive regulations and improved compliance mechanisms to address evolving data security challenges and protect individuals' privacy rights. Based on researchs that have been conducted, effective implementation of personal data protection laws requires collaboration among government, industry, and civil society to establish a robust legal framework, increase awareness, and ensure reliable technological infrastructure to increase consumer confidence.

References

Aldboush, Hassan H. H., and Marah Ferdous, 'Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust', *International Journal of Financial Studies*, 11.3 (2023), 90 https://doi.org/10.3390/ijfs11030090

Alhaj-Yaseen, Yaseen S., John T. Barkoulas, and Arav Ouandlous, 'Liberalization and Asymmetric Information Flow Dynamics in the Chinese Equity Markets', *The Journal of Economic Asymmetries*, 21 (2020), e00151 https://doi.org/10.1016/j.jeca.2019.e00151

Alkatiri, Putri Hawa, Asep Muhamad Ramdan, and Faizal Mulia Z, 'Analysis of Advertising Effectiveness Free Shipping and Consumer Trust to Increase Purchase Decisions', *Almana : Jurnal Manajemen Dan Bisnis*, 6.2 (2022), 209–20 https://doi.org/10.36555/almana.v6i2.1633

'Analysis Of Digital Marketing Quality Before and During the Covid-19 Pandemic on Frozen Food Consumers in West Java Region', *Quality-Access to Success*, 25.198 (2023) https://doi.org/10.47750/QAS/25.198.16

Ariefulloh, Ariefulloh, Hibnu Nugroho, Angkasa Angkasa, and Riris Ardhanariswari, 'Restorative Justice-Based Criminal Case Resolution in Salatiga, Indonesia: Islamic Law Perspective and Legal Objectives', *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan*, 23.1 (2023), 19–36 https://doi.org/10.18326/ijtihad.v23i1.19-36

Arora, Ayesha, and Tarun Jain, 'Data Sharing between Platform and Seller: An Analysis of Contracts, Privacy, and Regulation', *European Journal of Operational Research*, 313.3 (2024), 1105–18 https://doi.org/10.1016/j.ejor.2023.09.035

Aryani, Almira Putri, and Liana Endah Susanti, 'Pentingnya Perlindungan Data Pribadi Konsumen Dalam Transaksi Online Pada Marketplace Terhadap Kepuasan Konsumen', *Ahmad Dahlan Legal Perspective*, 2.1 (2022), 20–29 https://doi.org/10.12928/adlp.v2i1.5610

Ashraf, Musaib, and Jayanthi Sunder, 'Can Shareholders Benefit from Consumer Protection Disclosure Mandates? Evidence from Data Breach Disclosure Laws', *The Accounting Review*, 98.4 (2023), 1–32 https://doi.org/10.2308/TAR-2020-0787

Bansal, Gaurav, and Fiona Fui-Hoon Nah, 'Internet Privacy Concerns Revisited: Oversight from Surveillance and Right To Be Forgotten as New Dimensions', *Information & Management*, 59.3 (2022), 103618 https://doi.org/10.1016/j.im.2022.103618

Basana, Sautma Ronni, Mariana Ing Malelak, and Zeplin Jiwa Husada Tarigan, 'The Effect of Excessive Social Networking Sites on Credit Overuse Behavior through Money Trust, Money Anxiety, and Money Power', *International Journal of Data and Network Science*, 8.1 (2024), 655–66 https://doi.org/10.5267/j.ijdns.2023.8.020

Büchi, Moritz, Noemi Festic, and Michael Latzer, 'The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda', *Big Data & Society*, 9.1 (2022), 205395172110653 https://doi.org/10.1177/20539517211065368

Castano, Silvana, Alfio Ferrara, Emanuela Furiosi, Stefano Montanelli, Sergio Picascia, Davide Riva, and others, 'Enforcing Legal Information Extraction through Context-Aware Techniques: The ASKE Approach', *Computer Law & Security Review*, 52 (2024), 105903 https://doi.org/10.1016/j.clsr.2023.105903

Chatsuwan, Panchapawn, Tanawat Phromma, Navaporn Surasvadi, and Suttipong Thajchayapong, 'Personal Data Protection Compliance Assessment: A Privacy Policy Scoring Approach and Empirical Evidence from Thailand's SMEs', *Heliyon*, 9.10 (2023), e20648 https://doi.org/10.1016/j.heliyon.2023.e20648

Chawla, Neelam, and Basanta Kumar, 'E-Commerce and Consumer Protection in India: The Emerging Trend', *Journal of Business Ethics*, 180.2 (2022), 581–604 https://doi.org/10.1007/s10551-021-04884-3

Chen, Lin, Guofang Nan, Minqiang Li, Bing Feng, and Qiurui Liu, 'Manufacturer's Online Selling Strategies under Spillovers from Online to Offline Sales', *Journal of the Operational Research Society*, 74.1 (2023), 157–80 https://doi.org/10.1080/01605682.2022.2032426

Chen, Yongmin, Xinyu Hua, and Keith E. Maskus, 'International Protection of Consumer Data', *Journal of International Economics*, 132 (2021), 103517

https://doi.org/10.1016/j.jinteco.2021.103517

Christensen, Tanja Kammersgaard, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective', *Computer Law & Security Review*, 53 (2024), 105980 https://doi.org/10.1016/j.clsr.2024.105980

Coiduras-Sanagustín, Amparo, Eduardo Manchado-Pérez, and César García-Hernández, 'Understanding Perspectives for Product Design on Personal Data Privacy in Internet of Things (IoT): A Systematic Literature Review (SLR)', *Heliyon*, 10.9 (2024), e30357 https://doi.org/10.1016/j.heliyon.2024.e30357

Costantini, Federico, and Giada Soncini, 'Healthcare Data Governance in the EU: Main Challenges in Personal Data Protection', in *Endorobotics* (Elsevier, 2022), pp. 319–36 https://doi.org/10.1016/B978-0-12-821750-4.00014-1

Dash, Ajitabh, and Sandeep Kumar Mohanty, 'Technology Readiness and the Older Citizen's Acceptance of m-Health Services in India', *Digital Policy, Regulation and Governance*, 25.2 (2023), 169–83 https://doi.org/10.1108/DPRG-11-2022-0126

Degutis, Mindaugas, Sigitas Urbonavičius, Linda D. Hollebeek, and Johan Anselmsson, 'Consumers' Willingness to Disclose Their Personal Data in e-Commerce: A Reciprocity-Based Social Exchange Perspective', *Journal of Retailing and Consumer Services*, 74 (2023), 103385 https://doi.org/10.1016/j.jretconser.2023.103385

Determann, Lothar, and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law', *SSRN Electronic Journal*, 2018 https://doi.org/10.2139/ssrn.3244203

Dinh, Van, Dao-Van Le, Duy Duong, and Dung Pham, 'Determinants Affecting Digital Financial Consumer Protection: Evidence from 135 Countries', *The Journal of Economic Asymmetries*, 27 (2023), e00301 https://doi.org/10.1016/j.jeca.2023.e00301

Divalona, Sylvia, and Sfenrianto, 'An Empirical Study on the Factors Affecting Customer Satisfaction and Customer Loyalty in Online Transportation Apps', *Journal of System and Management Sciences*, 14.4 (2023) https://doi.org/10.33168/JSMS.2023.0406

Esther Omolara, Abiodun, Aman Jantan, Oludare Isaac Abiodun, Humaira Arshad, Kemi Victoria Dada, and Etuh Emmanuel, 'HoneyDetails: A Prototype for Ensuring Patient's Information Privacy and Thwarting Electronic Health Record Threats Based on Decoys', *Health Informatics Journal*, 26.3 (2020), 2083–2104 https://doi.org/10.1177/1460458219894479

Fakhimi, Arezoo, Tony Garry, and Sergio Biggemann, 'The Effects of Anthropomorphised Virtual Conversational Assistants on Consumer Engagement and Trust During Service Encounters', *Australasian Marketing Journal*, 31.4 (2023), 314–24 https://doi.org/10.1177/14413582231181140

Fibrianti, Nurul, and Amarru Holish, 'Consumer Personal Data Protection: Between Expectations and Reality', in *Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8-9 2021, Semarang, Indonesia* (EAI, 2022) https://doi.org/10.4108/eai.8-6-2021.2314376

Firmansyah Putri, Deanne Destriani, and Muhammad Helmi Fahrozi, 'Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)', *Borneo Law Review*, 5.1 (2021), 46–68 https://doi.org/10.35334/bolrev.v5i1.2014

Georgiadis, Georgios, and Geert Poels, 'Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review', *Computer Law & Security Review*, 44 (2022), 105640 https://doi.org/10.1016/j.clsr.2021.105640

Grande, David, Nandita Mitra, Raghuram Iyengar, Raina M. Merchant, David A. Asch, Meghana Sharma, and others, 'Consumer Willingness to Share Personal Digital Information for Health-Related Uses', *JAMA Network Open*, 5.1 (2022), e2144787 https://doi.org/10.1001/jamanetworkopen.2021.44787

Guamán, Danny S., David Rodriguez, Jose M. del Alamo, and Jose Such, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications', *Computers & Security*, 130 (2023), 103262 https://doi.org/10.1016/j.cose.2023.103262

Guo, Zhilong, Jie Hao, and Lewis Kennedy, 'Protection Path of Personal Data and Privacy in China: Moving from Monism to Dualism in Civil Law and Then in Criminal Law', *Computer Law & Security Review*, 52 (2024), 105928 https://doi.org/10.1016/j.clsr.2023.105928

Gupta, Shivam, Sachin Modgil, Christina W.Y. Wong, and Arpan Kumar Kar, 'The Role of Innovation Ambidexterity on the Relationship between Cognitive Computing Capabilities and Entrepreneurial Quality: A Comparative Study of India and China', *Technovation*, 127 (2023), 102835 https://doi.org/10.1016/j.technovation.2023.102835

Hadi, Abdul, Bekti Taufiq Ari Nugroho, Ahmad Muntakhib, and Choeroni Choeroni, 'Undang-Undang Informasi Dan Transaksi Elektronik Dalam Konteks Maqasid Syari'ah', *Al-Manahij: Jurnal Kajian Hukum Islam*, 14.2 (2020), 211–24 https://doi.org/10.24090/mnh.v14i2.3582

HAYES, RACHEL M., FENG JIANG, and YIHUI PAN, 'Voice of the Customers: Local Trust Culture and Consumer Complaints to the CFPB', *Journal of Accounting Research*, 59.3 (2021), 1077–1121 https://doi.org/10.1111/1475-679X.12364

Hisbulloh, Moh Hamzah, 'Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi', *Jurnal Hukum*, 37.2 (2021), 119 https://doi.org/10.26532/jh.v37i2.16272

Huang, Yanting, and Yuqing Liang, 'Influence of Corporate Social Responsibility Considering Dual-Channel Recycling Competition and Privacy Information Protection', *Journal of Cleaner Production*, 373 (2022), 133850 https://doi.org/10.1016/j.jclepro.2022.133850

Juma'h, Ahmad H., and Yazan Alnsour, 'The Effect of Data Breaches on Company Performance', *International Journal of Accounting & Information Management*, 28.2 (2020), 275–301 https://doi.org/10.1108/IJAIM-01-2019-0006

Kadir Jaelani, Abdul, Reza Octavia Kusumaningtyas, and Asron Orsantinutsakul, 'The

Model of Mining Environment Restoration Regulation Based on Sustainable Development Goals', *Legality : Jurnal Ilmiah Hukum*, 30.1 (2022), 131–46 https://doi.org/10.22219/ljih.v30i1.20764

Kantachote, Krittiya, 'Micromanagement of Foreign Domestic Workers in Singapore: The Influence of State Regulations and Laws', *Heliyon*, 9.7 (2023), e17679 https://doi.org/10.1016/j.heliyon.2023.e17679

Karjalainen, Tuulia, 'The Battle of Power : Enforcing Data Protection Law against Companies Holding Data Power', *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 47.August 2018 (2022), 105742 https://doi.org/10.1016/j.clsr.2022.105742

Ke, T. Tony, and K. Sudhir, 'Privacy Rights and Data Security: GDPR and Personal Data Markets', *Management Science*, 69.8 (2023), 4389–4412 https://doi.org/10.1287/mnsc.2022.4614

Kusumaningtyas, Reza Octavia, Rahayu Subekti, Abdul Kadir Jaelani, Asron Orsantinutsakul, and Utkarsh K Mishra, 'Reduction of Digitalization Policy in Indonesian MSMEs and Implications for Sharia Economic Development', *JURIS (Jurnal Ilmiah Syariah)*, 21.2 (2022), 157 https://doi.org/10.31958/juris.v21i2.6855

Loertscher, Simon, and Leslie M. Marx, 'Digital Monopolies: Privacy Protection or Price Regulation?', *International Journal of Industrial Organization*, 71 (2020), 102623 https://doi.org/10.1016/j.ijindorg.2020.102623

Lohmöller, Johannes, Jan Pennekamp, Roman Matzutt, Carolin Victoria Schneider, Eduard Vlad, Christian Trautwein, and others, 'The Unresolved Need for Dependable Guarantees on Security, Sovereignty, and Trust in Data Ecosystems', *Data & Knowledge Engineering*, 151 (2024), 102301 https://doi.org/10.1016/j.datak.2024.102301

Malgieri, Gianclaudio, and Frank Pasquale, 'Licensing High-Risk Artificial Intelligence: Toward Ex Ante Justification for a Disruptive Technology', *Computer Law & Security Review*, 52 (2024), 105899 https://doi.org/10.1016/j.clsr.2023.105899

Masyhar, Ali, and Silaas Oghenemaro Emovwodo, 'Techno-Prevention in Counterterrorism: Between Countering Crime and Human Rights Protection', *Journal of Human Rights, Culture and Legal System*, 3.3 (2023), 625–55 https://doi.org/10.53955/jhcls.v3i3.176

Maurya, Himani, and Suneel Prasad, 'Data Protection Laws and a Comparative Analysis of GDPR and PDPB', 2022, p. 030077 https://doi.org/10.1063/5.0110597

Namysłowska, Monika, and Agnieszka Jabłonowska, 'Enforcement and Effectiveness of Consumer Law in Poland', 2018, pp. 433–55 https://doi.org/10.1007/978-3-319-78431-1_18

Nareswari, Ninditya, Małgorzata Tarczyńska-Łuniewska, and Rizqi Umar Al Hashfi, 'Analysis of Environmental, Social, and Governance Performance in Indonesia: Role of ESG on Corporate Performance', *Procedia Computer Science*, 225 (2023), 1748–56 https://doi.org/10.1016/j.procs.2023.10.164

Nasabi, Afreen Nishat A., and Sujaya H., 'Consumer Buying Behaviour Trends of E-Commerce in India- A Case Study', *International Journal of Management, Technology, and Social Sciences*, 2022, 736–50 https://doi.org/10.47992/IJMTS.2581.6012.0247

Nasser A., Alharbi Nesreen, and Yanhui Li, 'Effects of Privacy Policy and Government Regulation on Trust of Consumers in Saudi Arabia: An Empirical Study', *International Journal Of Innovation And Economic Development*, 5.4 (2019), 7–24 https://doi.org/10.18775/ijied.1849-7551-7020.2015.54.2001

Niebel, Crispin, 'The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy', *Computer Law & Security Review*, 40 (2021), 105523 https://doi.org/10.1016/j.clsr.2020.105523

Nuzulita, Nania, and Apol Pribadi Subriadi, 'The Role of Risk-benefit and Privacy Analysis to Understand Different Uses of Social Media by Generations X, Y, and Z in Indonesia', *The Electronic Journal Of Information Systems In Developing Countries*, 86.3 (2020) https://doi.org/10.1002/isd2.12122

Pieper, Nadine, and David M. Woisetschläger, 'Customer Misbehavior in Access-Based Mobility Services: An Examination of Prevention Strategies', *Journal of Business Research*, 171 (2024), 114356 https://doi.org/10.1016/j.jbusres.2023.114356

Ranade, Ketki, Arjun Kapoor, and Tanya Nicole Fernandes, 'Mental Health Law, Policy & Program in India – A Fragmented Narrative of Change, Contradictions and Possibilities', *SSM - Mental Health*, 2 (2022), 100174 https://doi.org/10.1016/j.ssmmh.2022.100174

Robertson, Viktoria H.S.E., 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data', *SSRN Electronic Journal*, 2019 https://doi.org/10.2139/ssrn.3408971

Rodríguez-Priego, Nuria, Lucia Porcu, and Philip J. Kitchen, 'Sharing but Caring: Location Based Mobile Applications (LBMA) and Privacy Protection Motivation', *Journal of Business Research*, 140 (2022), 546–55 https://doi.org/10.1016/j.jbusres.2021.11.022

Rodríguez-Priego, Nuria, Lucia Porcu, María Belén Prados Peña, and Esmeralda Crespo Almendros, 'Perceived Customer Care and Privacy Protection Behavior: The Mediating Role of Trust in Self-Disclosure', *Journal of Retailing and Consumer Services*, 72 (2023), 103284 https://doi.org/10.1016/j.jretconser.2023.103284

Rupp, Valentin, and Max von Grafenstein, 'Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection', *Computer Law & Security Review*, 52 (2024), 105932 https://doi.org/10.1016/j.clsr.2023.105932

Segijn, Claire Monique, Suzanna J. Opree, and Iris Van Ooijen, 'The Validation of the Perceived Surveillance Scale', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16.3 (2022) https://doi.org/10.5817/CP2022-3-9

Selita, Fatos, Robert Chapman, Yulia Kovas, Vanessa Smereczynska, Maxim Likhanov,

and Teemu Toivainen, 'Consensus Too Soon: Judges' and Lawyers' Views on Genetic Information Use', *New Genetics and Society*, 42.1 (2023) https://doi.org/10.1080/14636778.2023.2197583

Shah, Priya, Neha Mehta, and Sweety Shah, 'Exploring the Factors That Drive Millet Consumption: Insights from Regular and Occasional Consumers', *Journal of Retailing and Consumer Services*, 76 (2024), 103598 https://doi.org/10.1016/j.jretconser.2023.103598

Sharma, Bhawana, Lokesh Sharma, Chhagan Lal, and Satyabrata Roy, 'Explainable Artificial Intelligence for Intrusion Detection in IoT Networks: A Deep Learning Based Approach', *Expert Systems with Applications*, 238 (2024), 121751 https://doi.org/10.1016/j.eswa.2023.121751

Sinha, Vikram, and Sharmadha Srinivasan, 'An Integrated Approach to Competition Regulation and Data Protection in India', *CSI Transactions on ICT*, 9.3 (2021), 151–58 https://doi.org/10.1007/s40012-021-00334-7

Siti Yuniarti, 'Protection Of Indonesia's Personal Data After Ratification Of Personal Data Protection Act', *Progressive Law Review*, 4.02 (2022), 54–68 https://doi.org/10.36448/plr.v4i02.85

Şık, Ayhan Serkan, Arsev Umur Aydınoğlu, and Yeşim Aydın Son, 'Assessing the Readiness of Turkish Health Information Systems for Integrating Genetic/Genomic Patient Data: System Architecture and Available Terminologies, Legislative, and Protection of Personal Data', *Health Policy*, 125.2 (2021), 203–12 https://doi.org/10.1016/j.healthpol.2020.12.004

Smrithi, Sukesh, Hephzibah Miriam D. Doreen, and Robin C. R. Rene, 'An Analysis of the Increasing Cases of Data Breaches in India', *I-Manager's Journal on Software Engineering*, 17.3 (2023), 38 https://doi.org/10.26634/jse.17.3.19791

Soren, Anup Anurag, and Shibashish Chakraborty, 'Adoption, Satisfaction, Trust, and Commitment of over-the-Top Platforms: An Integrated Approach', *Journal of Retailing and Consumer Services*, 76 (2024), 103574 https://doi.org/10.1016/j.jretconser.2023.103574

Stapels, Julia G., Angelika Penner, Niels Diekmann, and Friederike Eyssel, 'Never Trust Anything That Can Think for Itself, If You Can't Control Its Privacy Settings: The Influence of a Robot's Privacy Settings on Users' Attitudes and Willingness to Self-Disclose', *International Journal of Social Robotics*, 15.9–10 (2023), 1487–1505 https://doi.org/10.1007/s12369-023-01043-8

'Strengthening the Security and Privacy of National Identity Numbers (NINs) in Smart Contract Mechanisms through AES Encryption', *Journal of Logistics, Informatics and Service Science*, 10.4 (2023) https://doi.org/10.33168/JLISS.2023.0412

Strycharz, J., J. Ausloos, and N. Helberger, 'Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR', *European Data Protection Law Review*, 6.3 (2020), 407–21 https://doi.org/10.21552/edpl/2020/3/10

Strycharz, Joanna, Eunah Kim, and Claire M. Segijn, 'Why People Would (Not) Change Their Media Use in Response to Perceived Corporate Surveillance', *Telematics and Informatics*, 71 (2022), 101838 https://doi.org/10.1016/j.tele.2022.101838

Strzelecki, Artur, and Mariia Rizun, 'Consumers' Security and Trust for Online Shopping after GDPR: Examples from Poland and Ukraine', *Digital Policy, Regulation and Governance*, 22.4 (2020), 289–305 https://doi.org/10.1108/DPRG-06-2019-0044

Tan, Alyssa Jean L., Lauren T. Yap, Elise Francesca L. Salud, and Mendiola Teng-Calleja, 'Leadership Experiences of Bicultural Business Leaders: An Interpretative Phenomenological Analysis', *Asian Journal of Social Psychology*, 26.4 (2023), 547–59 https://doi.org/10.1111/ajsp.12576

Tao, Shouzheng, Yezheng Liu, and Chunhua Sun, 'Understanding Information Sensitivity Perceptions and Its Impact on Information Privacy Concerns in E-Commerce Services: Insights from China', *Computers & Security*, 138 (2024), 103646 https://doi.org/10.1016/j.cose.2023.103646

Tedjakusuma, Adi Prasetyo, Hui Nee Au Yong, Erna Andajani, and Zam Zuriyati Mohamad, 'Intention to Purchase Halal Health Supplement Online: Lessons Learned from the Health Crisis', *Heliyon*, 9.9 (2023), e19840 https://doi.org/10.1016/j.heliyon.2023.e19840

Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies', *Computer Law & Security Review*, 34.1 (2018), 134–53 https://doi.org/10.1016/j.clsr.2017.05.015

Upadhyay, Jyoti, Avita Katal, and Preeti D Mehta, 'Self-Regulated Learning, an Important Tool to Improve Learning Capability: An Indian Case Study', *The International Journal of Learning in Higher Education*, 31.1 (2023), 69–95 https://doi.org/10.18848/2327-7955/CGP/v31i01/69-95

Wirdiyanti, Rosnita, Inka Yusgiantoro, Agus Sugiarto, Aprillia Dwi Harjanti, Indra Yudha Mambea, Subiakto Soekarno, and others, 'How Does E-Commerce Adoption Impact Micro, Small, and Medium Enterprises' Performance and Financial Inclusion? Evidence from Indonesia', *Electronic Commerce Research*, 23.4 (2023), 2485–2515 https://doi.org/10.1007/s10660-022-09547-7

Wu, Zihao, Siliang Lin, Tianhao Chen, Chunyang Luo, and Hui Xu, 'Does Effective Corporate Governance Mitigate the Negative Effect of ESG Controversies on Firm Value?', *Economic Analysis and Policy*, 80 (2023), 1772–93 https://doi.org/10.1016/j.eap.2023.11.018

Zhang, Jianxiong, Sa Li, Shichen Zhang, and Rui Dai, 'Manufacturer Encroachment with Quality Decision under Asymmetric Demand Information', *European Journal of Operational Research*, 273.1 (2019), 217–36 https://doi.org/10.1016/j.ejor.2018.08.002

Zhang, Shichen, Liqun Wei, and Jianxiong Zhang, 'Demand Forecast Sharing for a Dominant Retailer with Supplier Encroachment and Quality Decisions', *European Journal of Operational Research*, 301.1 (2022), 39–50 https://doi.org/10.1016/j.ejor.2021.09.024