



Research Article



Digital Defense Drives Economic Growth in Indonesia and Uzbekistan

Arief Budiono ^{1,2*}, Gradia Okultra Alba ¹, Said Saidakhrarovich Gulyamov ², Turdialiev Mukhammad Ali Polatjon Ogli ²

¹ Faculty of Law, Universitas Muhammadiyah Surakarta, Sukoharjo, Indonesia.

² Department of Cyber Law, Tashkent State Law University, Taskent, Uzbekistan.

*Correspondence: ab368@ums.ac.id

Received: July 25, 2024 / Revised: May 18, 2025 / Accepted: May 18, 2025

Abstract: Digital technologies drive economic growth in both Indonesia and Uzbekistan. The global economy increasingly depends on the digital economy, reflected in the rise of blockchain systems, digital banking, and other digital activities in the economic sector. This research highlights the importance of digital personal data protection in Uzbekistan and Indonesia and examines its connection to digital economic development in both countries. The study uses a normative legal method that combines statutory and conceptual approaches. The authors examine the relevant laws and explore the concept of personal data protection in each country. The findings present two main points. First, the laws in both countries regulate personal data protection and assign institutional responsibilities across administrative, civil, and criminal domains. Second, when conflicts, data breaches, or criminal actions involving personal data occur, the legal systems provide for resolution through court litigation. Although both countries have implemented personal data protection laws that support digital economic development, they differ in institutional structure, legal procedures, and the scope of authority. Weak personal data protection may hinder the growth of the digital economy in both nations.

Keywords: Data; Economic; Legal Entity; Mechanism; Personal Data Protection Act;



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

INTRODUCTION

Change has been occurring since the era before Christ up to now and becoming more advanced from year to year. These changes result in shifts in human beings' interaction patterns and certainly leading to a domino effect on Indonesia. The aforementioned interaction pattern refers to the shift from direct interaction to indirect interaction facilitated by technologies, a prominent characteristic of the current digital era, which certainly did not all the sudden emerge.¹ The current era, which is called the 5.0 Society Era, has experienced a long journey to reach this point.² It was initiated by Japan, specifically in 2019, and presented new ideas compared to the previous era, i.e., the era of the Industrial Revolution 4.0. The focus point of this era was the balance between technological usage and technological advancement. Before this, there was surely the 1.0 era, where humans only started to create and use alphabets. Then, it was followed by the Society 2.0 era, which was characterized with the development of the human activity, especially in the

¹ Sandryones Palinggi, Srivan Palelleng, and Lutma Ranta Allolinggi, 'Peningkatan Rasio Kejahatan Cyber Dengan Pola Interaksi Sosio Engineering Pada Periode Akhir Era Society 4.0 Di Indonesia', *Jurnal Ilmiah Dinamika Sosial*, 4.1 (2020), 145 <https://doi.org/10.38043/jids.v4i1.2314>

² Luluk Setyowati and Deni Nasir Ahmad, 'Pemanfaatan Big Data Dalam Era Teknologi 5.0', *ABDINE: Jurnal Pengabdian Masyarakat*, 1.2 (2021), 117–22 <https://doi.org/10.52072/abdine.v1i2.205>



agricultural sector. In that era, there was less focus on consumptive activities,³ meaning that the society started to plant and produce their own food. Then, the next era was called Society 3.0, which was characterized by the discovery of machines to aid activities in daily life.⁴

The emergence of a new digital economic ecosystem has driven developments in digital activities that significantly impact economic growth. However, this progress has also increased the risk of data violations, particularly involving personal data. Between 2019 and 2021, at least 29 cases of personal data breaches were reported. Specifically, authorities recorded three cases in 2019, twenty in 2020, and six in 2021.⁵ New data shown that huge amounts of data were leaked from BSI (*Bank Syariah Indonesia*/The Indonesian Sharia Bank), with a total of 15 million data.⁶ The worst case of data leakage happened to BPJS Kesehatan (The Social Security Administering Agency for Health), which reached 274 million data in 2024.⁷ However, the most embarrassing case was the leakage of the temporary National Data Center which happened in 2024, where data from 210 national institutions were leaked.⁸ It is crucial to pay attention to these cases as the writers saw that 93% of these cases concerned the cases of personal data leakage, while the rest (7%) were violations against other protection principles.⁹

Meanwhile, most recently in 2025, there was a case of DKI Bank (The Special Capital Region Bank) data leakage with a significant amount of data leakage.¹⁰ It was shown that the most embarrassing data leakage case was perpetrated by the National Data Center, while the case with the biggest data leaked happened to the National Healthcare of the Indonesian government. The rest were data leakage cases from governmental banks (BSI and DKI Bank), followed by data leakage of e-commerce sites. An example that caused an uproar among the general public in Indonesia was the data leakage which happened to the National Data Center and the government's national healthcare data (in 2024). Over 274 million users' personal data leaked from

³ Hari Sutra Disemadi and Cindy Kang, 'Tantangan Penegakan Hukum Hak Kekayaan Intelektual Dalam Pengembangan Ekonomi Kreatif Di Era Revolusi Industri 4.0', *Jurnal Komunikasi Hukum (JKH)*, 7.1 (2021), 54 <https://doi.org/10.23887/jkh.v7i1.31457>

⁴ i-Scoop, 'From Industry 4.0 to Society 5.0: The Big Societal Transformation Plan of Japan', *I-Scoop.Eu*, 2017.

⁵ Lia Sautunnida, 'Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia', *Kanun Jurnal Ilmu Hukum*, 20.2 (2018), 369–84 <https://doi.org/10.24815/kanun.v20i2.11159>

⁶ Vanesha Marcelliana and others, 'Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah (Implementation of Consumer Protection for PT Customers. Indonesian Sharia Bank in Customer Data Leak Case)', *Deposisi: Jurnal Publikasi Ilmu Hukum*, 1.2 (2023), 180–94 <https://doi.org/10.59581/deposisi.v1i2.562>

⁷ Arief Budiono, A. S. Nurrizky, and others, 'Lessons from Indonesian National Healthcare Security (BPJS Kesehatan): HIV/AIDS Patient Medical Data Protection Policies', *Malaysian Journal of Medicine and Health Sciences*, 20.9 (2024), 201–8 <https://doi.org/10.47836/mjmh/20.s9.33>

⁸ E.F. Astuti and others, 'Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001:2013', *International Journal of Safety and Security Engineering*, 14.5 (2024), 1559–1567 <https://doi.org/10.18280/ijss.140523>

⁹ Mirnayanti Mirna, Judhariksawan, and Maskum, 'Analisis Pengaturan Keamanan Data Pribadi Di Indonesia', *Jurnal Ilmiah Living Law*, 15.1 (2023), 16–30. <https://doi.org/10.30997/jill.v15i1.4726>

¹⁰ Theresia Silalahi, 'Police Investigate Alleged Data Breach at Bank DKI', *Jakarta Globe* <https://jakartaglobe.id/business/police-investigate-alleged-data-breach-at-bank-dki>



BPJS only,¹¹ and the stolen data were then sold to the dark web. BPJS Kesehatan and BSI are government-owned institutions, while Tokopedia is one of the largest e-commerce companies in Indonesia which is called the Tokopedia Limited Company. At the time of the data leakage's occurrence, Indonesia still did not have integrated legal acts on personal data. In consequence, there was no solution to this case and it ended without any clarity.¹² The lack of data or personal data protection will harm the development of the digital economic ecosystem. If the government is not serious in addressing this issue, many digital startups or investors will risk their investment, which may lead them to withdraw their investments in Indonesia and switching to other countries with a stronger law enforcement regarding personal data protection. Therefore, personal data protection is crucial in digital economic growth.

In the context of data storage, Indonesia has enacted the Electronic Information and Transaction Act (i.e., the Republic of Indonesia's Law No. 11 of 2008 on Electronic Information and Transaction), which experienced an amendment with the enactment of the revision law, i.e., Law No. 19 of 2016.¹³ Apart from that, Indonesia has also issued Law No. 27 of 2022 on the Personal Data Protection. The writers also saw that the forms of sanctions in these legal regulations were not yet adequate to show legal responsibility because massive data leakage continuously happens and there have been no serious efforts to arrest the perpetrators under the reason that they are anonymous (the data of the perpetrators are unknown). It is a shame that the law is ineffective in punishing the perpetrators, failing to provide justice to society as victims of data theft. There is a gap between what is written and the reality (*das sollen* and *das sein*), as these laws fail to create a deterrent effect by letting perpetrators walk free. Data leakage cases bring economic losses as institutions which became victims of these crimes must spend a great amount of money to fix the system, not to mention losing the trust of investors to the Indonesian global digital economy due to its incapability to create a clear law in the digital data protection.¹⁴

This research studies a comparison between Indonesia and Uzbekistan concerning the topic of personal data protection laws and their application. Uzbekistan was chosen as the object as the authors have created a Memorandum of Understanding (MoU) for joint research with this country. Apart from that, in terms of the research, the authors see that Uzbekistan has a fairly good digital economy development and digital protection, rendering it appropriate to be researched. Aside from that, there have been no previous researches which directly study such a topic with the same objects, making this current research unique and novel. Regarding Uzbekistan, the main legal act governing the processing and protection of personal data in Uzbekistan is the Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data" ("Law on

¹¹ Budiono, Nurriszky, and others.

¹² Rahmawati Nafi'ah, 'Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce Data Breach and Identity Theft on E-Commerce', *CyberSecurity Dan Forensik Digital*, 3.1 (2020), 7–13. <https://doi.org/10.14421/csecurity.2020.3.1.1980>

¹³ Rony Mart Panjaitan, 'Pertanggungjawaban Pidana Korporasi Sebagai Penyelenggara Sistem Elektronik Dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik', *Jurnal Hukum Adigama*, 4.2 (2021), 2624–43. <https://journal.untar.ac.id/index.php/adigama/article/view/17761/9805>

¹⁴ Wardah Yuspin and others, 'The Law Alteration on Artificial Intelligence in Reducing Islamic Bank's Profit and Loss Sharing Risk', *Legality: Jurnal Ilmiah Hukum (Scientific Journal of Law)*, 30.2 (2022), 267–282 <https://doi.org/10.22219/ljih.v30i2.23051>



Personal Data"), which was adopted on July 2nd, 2019 and effective from October 1st, 2019.¹⁵ The Law on Personal Data's application has a rather broad scope, as it applies to relations arising from the processing and protection of personal data, regardless of the applied means of processing, including information technologies. This law on data protection is also related to Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12th, 2002; Law No. 560-II 'On Informatization' dated December 11th, 2003; and Law No. ZRU-1015 'On Telecommunications' dated December 28th, 2024, under which all operators and service providers are obliged to ensure the secrecy of communications.¹⁶

Uzbekistan has enacted laws to safeguard the privacy of its citizens' personal data as it understands the significance of this issue. Uzbekistan's new personal data law (Law on Personal Data issued in 2019) sets the ground rules for how we collect, store, analyze, and share information on living individuals. Data protection measures are also addressed in the Cybersecurity Law of Uzbekistan, which went into effect on July 17th, 2022 (Cyber-Security Law of 2022). The privacy conundrum is an intricate predicament that calls for a multifaceted solution to properly solve this worldwide problem, affecting governments, organizations, and specialists throughout Uzbekistan. This law ensured that the safety of the personal data is very crucial.

Related to this topic, previous research conducted by Utami et al.¹⁷ focused on data leakage from the pure perspective of the PDP Law, different from the authors' current research which also analyzes the law's implementation. Another previous research was written by Prastyanti et al.,¹⁸ which discussed consumer data protection strategies from the perspective of the PDP Law, while the authors' current research discusses personal data leakage and how it affects the economy. Next, previous research was conducted by Prastyanti and Sharma,¹⁹ which analyzed the PDP Law as a competitive advantage in gaining public trust. However, the authors' current research shows a difference as the authors analyze that even though the Indonesian PDP Law is good, its practice is not according to the stipulations. Next, Rizal, Rosadi, and Taryana²⁰ wrote a paper which analyzed the PDP Law's framework for developing MSMEs' digital businesses in Indonesia, while the authors' current research discusses the PDP Law's implementation that is not according to its stipulations, making Indonesia lose

¹⁵ M. Mukhammedov and others, 'Development of Public Regulatory Strategies to Incentivise Investment in Human Capital', *Scientific Bulletin of Mukachevo State University Series Economics*, 11.4 (2024), 133–146 <https://doi.org/10.52566/msu-econ4.2024.133>

¹⁶ M. Fayzieva, G. Abdurakhmanova, and others, 'The Role of Digital Development in the Reinforcement of the Government Social Protection System of Uzbekistan', in *ACM International Conference Proceeding Series* (Dubai: 7th International Conference on Future Networks and Distributed Systems, ICFNDS, 2023), pp. 42–50 <https://doi.org/10.1145/3644713.3644720>

¹⁷ Tanti Kirana Utami and others, 'Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law', *Journal Customary Law*, 2.2 (2025), 21 <https://doi.org/10.47134/jcl.v2i2.3742>

¹⁸ Rina Arum Prastyanti and others, 'Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia', *Jurnal Jurisprudence*, 11.1 (2021), 82–99 <https://doi.org/10.23917/jurisprudence.v11i1.14756>

¹⁹ Rina Arum Prastyanti and Ridhima Sharma, 'Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India', *Journal of Human Rights, Culture and Legal System*, 4.2 (2024), 354–90 <https://doi.org/10.53955/jhcls.v4i2.200>

²⁰ M. Rizal, S. D. Rosadi, and A. Taryana, 'Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia', *Journal of Law and Sustainable Development*, 12.1 (2024), e2809 <https://doi.org/10.55908/sdgs.v12i1.2809>



trust in the ecosystem of digital economy. Next, in his research, Yashnarovna²¹ found that the digital law transformation in Uzbekistan is categorized as a transformation of the data protection law due to artificial intelligence in Uzbekistan, whereas the authors' current research focuses on the legal responsivity of Indonesia and Uzbekistan related to data leakage violations. Another research on the comparison of personal data laws was conducted by Maleno and Kusumawati²², who discussed the comparison of PDP Laws in Indonesia, the European Union, and California, the United States, in terms of the best application of privacy protection. It was found that the Indonesian PDP Law had the worst application compared to other examples as there have been frequent cases of data leakage. This previous research was different from the current research as the authors compare Indonesia with Uzbekistan and the effects of data leakage on the economy.

Another research on the comparison of PDP Laws was conducted by Shahrullah et al.,²³ which analyzed the comparison of the PDP Laws in Indonesia and South Korea in terms of their capabilities in fulfilling privacy rights, and it was found that South Korea's Law was more effective in protecting data privacy. The difference between the previous research and the authors' current research was that the latter analyzes the comparison between the PDP Laws in Indonesia and Uzbekistan and their impacts to the economy. Even so, the authors also found that Indonesia's PDP Law was ineffective and that such a condition impacts the economy. Next, Yuspin et al.²⁴ conducted research which discussed the security of data in banks, including the personal data of bank customers. This previous research was different from the authors' research as the former was micro research on the scale of bank customers' personal data, while the authors' current research analyzes these cases at a macro scale, namely the comparison of the PDP Laws between two countries. Then, Nofie²⁵ published research which discussed the PDP Law and its economic impacts, specifically analyzing the effect of personal data and its privacy on the economy in digital platforms. Meanwhile, the authors' current research analyzes the effect of data leakage towards the economy in Indonesia and Uzbekistan. Research concerning the comparison between the PDP Law in Indonesia and Malaysia has been written by Prasetyoningsih et al.,²⁶ which discussed this topic from the aspect of its regulations

²¹ Isokhujaeva Munira Yashnarovna, 'AI Transforms E-Commerce Management and Regulation in Uzbekistan', *Indonesian Journal of Law and Economics Review*, 19.2 (2024) <https://doi.org/10.21070/ijler.v19i2.1054>

²² M. Maleno and A. Kusumawati, 'Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights', *Indonesia Law College Association Law Journal*, 3.2 (2024), 91–98 <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>

²³ Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment', *Hasanuddin Law Review*, 10.1 (2024), 1–20 <https://doi.org/10.20956/halrev.v10i1.5016>

²⁴ W. Yuspin and others, 'Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities', *International Journal of Safety and Security Engineering*, 14.6 (2024), 1699–1706 <https://doi.org/10.18280/ijse.140605>

²⁵ Iman Nofie, 'The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms', *International Journal of Law and Management*, 66.6 (2024), 774–791 <https://doi.org/10.1108/IJLMA-12-2022-0258>

²⁶ Nanik Prasetyoningsih and others, 'Legal Protection for the Personal Data in Indonesia and Malaysia', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and*



and implementation. It was found that the PDP Law in Indonesia is not specifically implemented by a special institution, leading to frequent overlaps. This was according to the authors' current research which also found that the implementation and regulations of the Indonesian PDP Law are not specially tasked to certain institutions, making them ineffective. The difference between the previous research and the current research is that the latter also analyzes the difference between this condition in Uzbekistan and their effects on the economy.

The problem in Uzbekistan is that the ever-shifting nature of regulations presents still another difficulty.²⁷ Multinational corporations for economic benefits have unique challenges in ensuring compliance with the data protection laws and regulations of each country and jurisdiction in which they operate.²⁸ Data privacy problems in a global environment are made worse by the fact that certain legislation cannot be applied outside national borders. Data privacy issues have also arisen due to the increasing volume of data being collected and the widespread use of Internet of Things (IoT) devices. Due to the nature of the data that IoT devices gather and send, security and data protection are key concerns. Several cases of data leaking from multiple companies arise, causing problems for personal data protection.

The urgency of this research is that personal data protection is one of the important factors in developing the digital economy which is experiencing rapid advancement. The digital economy experiences a steep increase in quality and quantity, affecting the economy as a whole. Thus, if the PDP Law does not run well, it will be difficult for the digital economy to grow. There are at least two main legal issues that the authors will discuss in this paper. The first is the form of legal responsibility towards legal entities on personal data protection in Indonesia and Uzbekistan. The second part of legal issues is how to drive an inclusive digital economy through strong data protection.

METHOD

This research was a normative type of research³⁰ which employed the comparison, statutory, and conceptual approaches.³¹ Using the normative-juridical method, the authors analyzed data leakage cases which happened in Indonesia and Uzbekistan. The authors compared the two laws in these two countries in an effort to specifically protect personal data and the institutions that are appointed or are given the authority to implement the PDP Law. The authors also analyzed the effectiveness in

Lecture Notes in Bioinformatics), 14728 (2024), 161 – 169 https://doi.org/10.1007/978-3-031-61379-1_11

²⁷ M. Fayzieva, M. Sanjar, and others, 'The Study of the Impact of the Digital Economy on the Growth of E-Government Services in Uzbekistan', in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (New York: Springer, 2023), pp. 208–17 https://doi.org/10.1007/978-3-031-30258-9_18

²⁸ M.P. Eshov and D.S. Nasirkhodjaeva, 'Conditions And Factors Of Forming A Digital Economy In Uzbekistan', in *ACM International Conference Proceeding Series* (ACM, 2022), pp. 81–86 <https://doi.org/10.1145/3584202.3584215>

³⁰ Kornelius Benur and Muhamad Azhar, 'Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer', *Gema Keadilan*, 7.1 (2020), 20–33 <https://doi.org/10.14710/GK.7.1.20-33>

³¹ Kelik Wardiono, 'Prophetic: An Epistemological Offer for Legal Studies', *Journal of Transcendental Law*, 1.1 (2019), 17–41 <https://doi.org/10.23917/jtl.v1i1.8797>



handling data protection and how these institutions handle data leakage. Then, the authors also analyzed whether or not the PDP Laws in these countries are effective enough in handling such cases. Next, the authors also compared the legal effects, authorized institutions, as well as data protection handling in these two countries and how they affect the economy. The researcher implemented the comparison approach, the statutory approach, and the conceptual approach as they are deemed suitable for the issue analyzed in this research, namely the law and the authority of legal entities in protecting personal data as well as its impacts on the economy of these two countries.³²

RESULT AND DISCUSSION

Legal Entities Authorized on Personal Data Protection in Indonesia and Uzbekistan

The first part of this paper discusses the forms of legal liability of legal entities on personal data protection. The writer will start this discussion by stating the legal subjects mentioned in the PDPA. The Law on Personal Data has specifically regulated the existence of personal data protection. The contents of the PDPA specifically contain the existence of legal subjects in data protection, the rights of data subjects, as well as the obligations of personal data controllers and personal data processors.³³ It also contains applicable regulations on personal data as well as sanctions for legal subjects which violate the stipulations of that law. Therefore, before stepping further, the researcher will describe and explain the legal subjects in that law. In Uzbekistan, personal data is regulated by the Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data" ("Law on Personal Data"). It was adopted on July 2nd, 2019 and effective from October 1st, 2019. The Law on Personal Data's application has a rather broad scope, as it applies to relations arising from the processing and protection of personal data, regardless of the applied means of processing, including information technologies.

This law on data protection is also related to Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12th, 2002; Law No. 560-II 'On Informatization' dated December 11th, 2003; and Law No. ZRU-1015 'On Telecommunications' dated December 28th, 2024. In this regulation, it is stated that the power to handle personal data is carried out under a special institution, namely the Cyber Security Center, which is under the auspices of the Ministry of Digital Technologies of the Republic of Uzbekistan in the field of personal data (Article 7 of Law No. ZRU-547). The similarity between all these regulations is that there is one single institution that handles personal data and data leakage. This single authority, namely the Cyber Security Center, under the auspices of the Ministry of Digital Technologies, has full authority in handling data leakage cases.

Disputes and violations against personal data will be imposed with legal sanctions (Articles 34 and 35). However, there is no clear stipulation on what the sanctions are.

³² Yati Nurhayati, Ifrani Ifrani, and M. Yasir Said, 'Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum', *Jurnal Penegakan Hukum Indonesia*, 2.1 (2021), 1–20 <https://doi.org/10.51749/jphi.v2i1.14>

³³ Olisias Gultom, Auditya Firza Saputra, and Muhammad Faiz Aziz, 'Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital', 2021, 1–135. <https://igj.or.id/2022/08/27/perlindungan-datapribadi-diindonesiamenyikapi-liberalisasi-ekonomi-digital/>



Such sanctions are regulated in Law ZRU-752, "About modification and amendments in some legal acts of the Republic of Uzbekistan in connection with further strengthening of guarantees of the rights of citizens and subjects of entrepreneurship", of May 17th, 2022. Penalties for illegal collection, systematization, storage, modification, addition, use, sharing, distribution, transfer, depersonalization and destruction of personal data, non-compliance with their processing using information technologies, including on the Internet, requirements for the collection, systematization and storage of personal data on technical means located on the territory of the republic, and in the databases of personal data registered in the State register of databases of personal data have been increased to 7 Basic Calculation Value (the "BCV") (UZS 1 890 000 or approximately USD 176) for individuals and to 50 BCV (UZS 13 500 000 or approximately USD 1 257) for officials under the Article 46 of the Administrative Code.³⁴

The same wrongdoings repeated after the application of an administrative penalty are subject to a penalty in the amount of 100 BCV (UZS 2 700 000 or approximately USD 252) to 150 BCV (UZS 1 611 750 or approximately USD 150) or deprivation of certain rights for up to three years or correctional labour up to three years. The penalty for commitment of the aforementioned actions in the group is set from 150 BCV (UZS 1 611 750 or approximately USD 150) to 200 BCV (UZS 2 149 000 or approximately USD 200) or correctional labor for two to three years or restriction of freedom from one to three years or imprisonment for up to three years.³⁵

In Indonesia, there is the PDP Law and the Law on Electronic Information and Transaction and a ministry that handles this sector, namely the Ministry of Communication and Digital Affairs. However, the authority to handle data is divided into several institutions, such as the State Cyber and Password Agency. This institutional overlapping leads to a highly ineffective coordination process. As there is more than one institution, there is confusion on whose authority such issues are. Even though a single institution, i.e., the Institution of the Personal Data Protection Authority has been given the mandate to handle such affairs, this institution has not been formed. There is unclear authority (there must be changes to the law); thus, the handling of data leakage cases becomes undirected, allowing data leakage perpetrators to repetitively hack into various institutions' systems to steal data, each case worse than the last.³⁶

From the aspect of internet access, the prevalence of Indonesians that may access the internet reaches 79.9%, while in Uzbekistan, it is 88.6%. This data shows that Uzbekistan has higher access to the internet compared to Indonesia. However, the prevalence of data leakage in Indonesia is very high. In Uzbekistan, in case there is

³⁴ Jamshid Sodikov, 'Roads Infrastructure Digital Twin Case Study: Uzbekistan', *Urban Sustainability*, F3988 (2024), 209 – 230 https://doi.org/10.1007/978-981-97-8483-7_10

³⁵ Askarova Mavluda, Choriev Fazliddin, and Khayitov Saidjon, 'The Importance of Digitalization in Economic Development of the Government', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14543 (2024), 196 – 204 https://doi.org/10.1007/978-3-031-60997-8_17

³⁶ Faiz Rahman, 'Safeguarding Personal Data In The Public Sector: Unveiling The Impact Of The New Personal Data Protection Act In Indonesia', *UUM Journal of Legal Studies*, 16.1 (2025), 1 – 18 <https://doi.org/10.32890/uumjls2025.16.1.1>



massive data leakage, the cyber security center quickly notifies those whose data were stolen via telegram. It will also announce to all citizens who access the telegram to be more aware. This strategy is difficult to apply in Indonesia, as there have been several cases of data leakage with millions of data leaked. In terms of the sanctions for this crime, the sanction in Indonesia is actually more severe (both in terms of imprisonment and fines) but this norm is ineffective as there are institutional and regulatory overlaps. Therefore, there have been no massive data leakage cases which end with the arrest of the perpetrator.

The nomenclature of the legal subject certainly brings up various opinions from many legal experts. There are many terms for legal subjects, which certainly require comprehensive understanding.³⁷ The clause of legal subjects can be defined as a legal individual (as stated by Oentari Sadino and St. K Malikul Adil), a legal person (Soerjono Soekanto), etc.³⁸ Legal subjects are perceived as legal individuals, which means that everything has legal authority or *persoonlijkheid*.³⁹ The meaning of the aforementioned legal authority is the capability to become supporters of a legal subject which is given by the objective law. Then, Algra also defines that a legal subject or *rechtsubject* is every person who has rights and responsibilities which may lead to legal competence. In this case, legal competence is the authority to become a subject of the occurring rights. Therefore, in carrying out or in implementing their legal actions, legal subjects have competence, which are divided into two. First, the competence to have a right (*rechts-bevoegdheid*). Second, the competence to implement legal subjects and the factors that influence it.

Meanwhile, Sudikno Mertokusumo expresses a different opinion. He stated that legal subjects are everything that may obtain rights and obligations from the existing law. In line with that, Subekti states that legal subjects are right-bearers. This, according to him, is attached to people. When seeing the definition from the international stipulations stated in Arum et al., legal subjects are explained as follows: owes allegiance and is governed by his law. For instance, the natives of Great Britain are subjects of the British Government. Men in free governments are subjects as well as citizens: as they enjoy rights and franchises, while they are bound to obey the law.⁴⁰ Based on the definition above, it is shown that legal subjects are regulated by the law of the state. Legal subjects are also citizens and these subjects can enjoy their rights as they are bound to obey the law. Apart from that, it should be known that in Dutch, legal subjects are called *rechtsubject*. In general, the origin of that word in Dutch can be defined as supporters of rights and obligations, i.e., humans and legal entities.

³⁷ Moh Indra Bangsawan and others, 'Personal Data Protection Policy during Covid-19 Pandemic Era', *Law and Justice*, 8.1 (2023), 21–31 <https://doi.org/10.23917/laj.v8i1.1558>

³⁸ Doli Witro, Mhd Rasidin, and Muhamad Izazi Nurjaman, 'Subjek Hukum Dan Objek Hukum: Sebuah Tinjauan Hukum Islam, Pidana Dan Perdata', *Asy Syar'iyah: Jurnal Ilmu Syari'ah Dan Perbankan Islam*, 6.1 (2021), 43–64 <https://doi.org/10.32923/asy.v6i1.1611>

³⁹ Dyah Hapsari Prananingrum, 'Penegakan Hukum Jabatan Notaris Dalam Pembuatan Perjanjian Berdasarkan Pancasila Dalam Rangka Kepastian Hukum', *Refleksi Hukum: Jurnal Ilmu Hukum*, 8.1 (2014), 73–92. <https://doi.org/10.33476/ajl.v2i3.846>

⁴⁰ Prastyanti and others.



Therefore, from the various definitions above, the writer tries to conclude that a legal subject is anything that has or owns legal authority. It may also be defined as holders or owners of rights and obligations in undergoing legal actions. In bearing their rights and obligations, legal subjects are attached and connected to their legal capabilities or *rechtsbekwaam*. Apart from the existence of legal subjects' capabilities, this also relates to various legal relationships. These legal relationships are linked to other legal subjects. Referring to the definition of the legal subject, the PDPA regulates some legal subjects. There are at least three types of legal subjects regulated in the PDPA, which are explicitly mentioned in Article 1 numbers 7 to 10 of this act. The legal subjects mentioned encompass every person, legal entity, and international organization.⁴²

“Every person” in the PDPA is defined as individuals or corporations. PDPA defines corporations as a well-organized group of people and/or wealth that are either legal entities or non-legal entities. Corporations have a very extensive definition and it encompasses many parties according to the PDPA. Corporations are not only viewed as institutions with a legal entity in the PDPA, but it also encompasses business entities that are non-legal entities. Apart from that, there is the public entity legal subject that needs to be described.⁴³

The public entity legal subject in the PDPA is defined as the executive, legislative, and judicative institutions, as well as other entities whose functions and main tasks regard the state establishment,⁴⁴ whose part or all of its funds, are sourced from the state or regional expenditures or non-governmental organizations so long as part or all of its funds are sourced from the state or regional expenditures, donations from the public, and/or from foreign countries.⁴⁵ The definition of the public entity legal subject shows that all non-governmental organizations whose funds are sourced from the state or regional expenditures are included as public entity legal subjects which must comply with the PDPA. Apart from the public entity, there is the international organization which is a type of legal subject in the PDPA. An international organization is defined as an organization that is acknowledged as an international legal subject and which has the capacity to make international treaties.⁴⁶ The PDPA stipulates obligations for personal data controllers,⁴⁷ which according to the authors

⁴² Wahyudi Djafar, ‘Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan’, *Jurnal Becoss*, 1.1 (2019), 147–54. <https://learning.hukumonline.com/wp-content/uploads/2022/09/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>

⁴³ A. A. Dhewa and Herkin Yossyafaat Program, ‘Aspek Hukum Perlindungan Konsumen Pada Transfer Data Pribadi Oleh Korporasi Dalam Hukum Positif Indonesia’, *Lontar Merah*, 6.1 (2023), 619–29. <https://doi.org/10.31002/lm.v6i1.3807>

⁴⁴ Rina Arum Prastyanti and Prattana Srisuk, ‘Achieving Sustainable Consumer Protection in the Era of Social Media’, *Journal of Sustainable Development and Regulatory Issues*, 3.1 (2025), 121–46 <https://doi.org/10.53955/jsderi.v3i1.52>

⁴⁵ Anindita Kusumowijoyo, Anjani Marta, and Kimberly Natali Boasrifa, ‘The Artificial Intelligence as a One-Stop Point for Dealing with Online Human Trafficking Scams in Indonesia’, *Journal of Sustainable Development and Regulatory Issues*, 1.3 (2023), 189–211 <https://doi.org/10.53955/jsderi.v1i3.18>

⁴⁶ Trisa Tampubolon and Rizki Ramadhan, ‘ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara’, *Padjadjaran Journal of International Relations*, 1.3 (2020), 270 <https://doi.org/10.24198/padjir.v1i3.26197>

⁴⁷ Erlina Maria Christin Sinaga, ‘Formulasi Legislasi Perlindungan Data Pribadi’, *Jurnal RechtVinding*, 9.2 (2020), 237–56. <https://dx.doi.org/10.33331/rechtsvinding.v9i2.428>



imply the birth of attached legal obligations. Obligations are certainly very closely related to responsibilities. There are at least some obligations related to this research that require further analysis. Article 20 clauses (1) and (2) of the PDPA state that there is an obligation to fulfill the protection of personal data subjects' vital interests.

This obligation leads to the existence of a legal responsibility to implement the protection of the interests of the personal data subjects. This certainly shows the importance of personal data protection, especially regarding vital things.⁴⁸ The next clearly stipulated obligation concerns the responsibility to validly and transparently process personal data according to the law. The specific and limited processing must be valid according to the law and legal regulations. This obligation is certainly closely related to the personal data controllers' obligation to validly process data as nothing should be kept secret from the personal data owners.

In Uzbekistan, personal data of more than 200,000 Uzbek users has been leaked to the Internet. Experts told Kun.uz that the leaked information includes passwords to the OneID system, the State Testing Center, and many public and educational organizations, as well as search and payment systems. The Cybersecurity Center noted that this poses a cyber threat to the users, especially on economic terms and issued advices.⁴⁹ Most of the leaked data consisted of access codes for banks and payment systems as well as control panels of various economic sites. In total, the information of hundreds of thousands of Uzbek users has been leaked.

The Center of the Cyber Security of Uzbekistan launched advice via telegram with an Uzbekistan number via the bot (@CSEC_Login_Bot) to recommend that users take certain steps to ensure the protection of their confidential information.⁵⁰ An advice was to always set a strong password of at least 8 characters as well as use upper- and lower-case letters, numbers, and special characters (e.g., @, #, \$, %, &, etc.). Also, users are recommended to avoid setting a password that can be easily guessed; update their password every 2-3 months, except for complex passwords; while avoiding setting a password similar to the previous one. Users are advised to not use the same password to register on different websites, to not use free password managers, and to not save passwords in browsers. Then, they should always use two-step verification features as well as use only licensed operating systems, software, and anti-virus software, and update them regularly. Users should not click on suspicious web links or download unknown software. When users open web pages, before entering their logins and passwords, they must pay attention to the address of the website and check to make sure that it is valid.

⁴⁸ Dinda Agustin Wulandari, Abdul Kadir Jaelani, and Ong Argo Victoria, 'Income Tax Regulations for Child Content Creators of TikTok Platform: Inefficacy of Indonesian Legal Frameworks', *Journal of Sustainable Development and Regulatory Issues*, 2.2 (2024), 145–57 <https://doi.org/10.53955/jsderi.v2i2.35>

⁴⁹ J. Kambarov and others, 'Problems and Solutions for the Implementation of the Industry-4.0 Program in Uzbekistan', *Journal of Advanced Research in Dynamical and Control Systems*, 12.2 (2020), 2677–2683 <https://doi.org/10.5373/JARDCS/V12I2/S20201321>

⁵⁰ N. Karimov and others, 'Impact of Mobile Applications on Tourism Development in Uzbekistan', *Indian Journal of Information Sources and Services*, 14.4 (2024), 175 – 181 <https://doi.org/10.51983/ijiss-2024.14.4.27>



This condition may be compared to the situation in Indonesia, where there have been many cases of data leakage with a very significant number of leaked data. However, the government has never carried out any serious efforts to provide information up to the people's personal level such as what was carried out by the Center of Cyber Security of Uzbekistan. This Center of Cyber Security of Uzbekistan showed responsibility by taking measures to provide information to the personal level by utilizing the telegram technology (considering that almost 90% of its citizens utilize telegram).⁵¹ The advice that was broadcasted to the personal level is one of the accountabilities of the Uzbek authority.

The form of responsibility that comes with the next obligation concerns the responsibility to process personal data based on its original goal.⁵² The aim of the data processing must be stated beforehand, and the processing must be carried out based on the initial goal. Controllers must be held accountable if the data processing was not according to the initial goal of that personal data. The discussion on the forms of liability is at least divided into three forms, i.e., administrative, civil, and criminal liabilities. Further, the authors will discuss the administrative and civil forms of legal liability.

There is the administrative aspect of liability in the case of the failure to protect personal data in the form of data leakage. Based on the law in the PDPA, it can be seen that administrative sanctions are attached to personal data controllers and personal data processors. These two special subjects are borne with administrative liability. Some articles may be imposed to demand administrative liability such as Article 35 which shows that Personal Data Controllers must protect and make sure of the safety of the personal data they process. Then, Article 36 imposes the responsibility to keep the confidentiality of personal data.

Article 38 imposes the responsibility to protect personal data from invalid processing. Then, Article 39 Clause (1) of the PDPA gives the responsibility to prevent invalid access to personal data. Then, Article 46 clauses (1) and (3) of the PDPA give the responsibility to provide a written warning in the case of personal data leakage. Apart from that, personal data controllers have the obligation to notify society in the case of personal data leakage.⁵³ Article 47 strictly regulates that personal data controllers must exhibit liability in protecting personal data. Apart from that, the writer also deems that personal data processors also borne the responsibilities of personal data controllers as stipulated in Article 52. The author also found that there are various forms of administrative sanctions which will be imposed or applied to personal data controllers or processors. The administrative sanctions according to Article 57 clause (2) of the PDPA are as follows: (1) Written warning; (2) Temporarily

⁵¹ Tuja Khaund and others, 'Telegram: Data Collection, Opportunities and Challenges', *Communications in Computer and Information Science*, 1410 (2020), 513 – 526 https://doi.org/10.1007/978-3-030-76228-5_37

⁵² Maichle Delpiero and others, 'Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data', *Padjadjaran Law*, 9.1 (2021), 1–22. <https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509>

⁵³ M Rafifnafia Hertianto, 'Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia', *Kertha Patrika*, 43.1 (2021), 93 <https://doi.org/10.24843/kp.2021.v43.i01.p07>



terminating personal data processing activities; (3) Deleting or exterminating personal data; and (4) Administrative fines.

Here in Indonesia, notifications that should ideally be given to citizens according to the PDPA in case of data leakage have never been given. There is no general release, notification or warning (moreover at the personal level) as a responsibility of the governmental authority. Such a notification has been carried out by the Uzbek authority even though its law does not oblige the spread of this warning or notification. Such a warning or notification is very useful, especially in the economic sector, if the leaked data is related to the finances or economics, such as the leakage of bank data (including identity, etc.). This will make society more aware of this issue and immediately change the security of their bank accounts, passwords, and usernames or add security facilities to prevent economic disaster.

The form of legal liability towards personal data leakage is categorized as strict liability. This is because it refers to the condition where there is a causal relationship between the action and the impact it generates which must be viewed proportionally. There is still a chance for resistance from the party of the defendant, in this case, the personal data controllers or processors. Strict liability is given to protect personal data subjects,⁵⁴ considering that personal data controllers may be in the form of corporations or public entities. Edmon Makarim also stated that the burden of proof in this limited legal liability uses the mechanism of reversed evidence.⁵⁵ In this case, perpetrators must prove that they are not guilty to elude themselves from this strict legal liability.

Driving Inclusive Digital Economy Through Strong Data Protection

The development of the digital economy is one of the great opportunities for an inclusive economy, where every person has the chance to grow and develop. This is one of the main focuses of the Sustainable Development Goals (SDGs), specifically SDG 8. SDG 8 aims to promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all.⁵⁶ Digital economy is an inclusive economy that can be accessed so long as one has the appropriate device, electricity, and internet signals. The development of the digital economy in Indonesia and Uzbekistan has a very good opportunity, especially with the fact that these electronic systems have been regulated in the law.⁵⁷ This law establishment was very important for the digital economic ecosystem as it will lead to economic growth.

To develop an inclusive economy, there needs to be strong legal protection, especially regarding personal data protection. In Uzbekistan, the Law on

⁵⁴ Josephine Josephine, Sinta Dewi Rosadi, and Sudaryat Sudaryat, 'Perlindungan Konsumen Daring Dan Tanggung Jawab Perusahaan Marketplace Atas Data Privasi Konsumen', *Jurnal Suara Keadilan*, 21.1 (2020), 97–112 <https://doi.org/10.24176/sk.v21i1.5686>

⁵⁵ Johannes Gunawan, 'Kontroversi Strict Liability Dalam Hukum Perlindungan Konsumen', *Veritas et Justitia*, 4.2 (2018), 274–303 <https://doi.org/10.25123/vej.3082>

⁵⁶ Ardak N Turginbayeva and others, 'Digital Inclusion as a Way to Deal with the Mismatch Between the Higher Education Market and the Labour Market', *Education in the Asia-Pacific Region*, 73 (2025), 93 – 100 https://doi.org/10.1007/978-981-96-1933-7_11

⁵⁷ K. F. Dantes, 'Engaturan Sistem Elektronik Dalam Pengambilan Keputusan Rapat Umum Pemegang Saham (Rups) Perseroan Terbatas Yang Berkepastian', *Jurnal Komunikasi Hukum (JKH)*, 8.1 (2022), 527–36 <https://doi.org/10.23887/jkh.v8i1.50941>



Cybersecurity mostly regulates the State Security Service of the Republic of Uzbekistan's mechanisms of exercising duties. It directly states that either such mechanisms are regulated 'in accordance with legislation', or are 'developed by the Regulatory authority'. It should be also noted that the Law on Cybersecurity introduced substantial notions and consolidated the bare minimum of cybersecurity legislation which was scattered among several sector-specific laws, as well as presidential and government by-laws. This mechanism certainly needs to be refined as the authority in various laws (the Cyberlaw, the Law on Information, etc.)⁵⁸ is handled by a single institution, namely the Cyber Security Center. However, it becomes an effective foundation that may influence Uzbekistan's digital economy, considering that there is clear coordination and authority of the institution to protect personal data.

The researchers opine that in the context of the development of an inclusive digital economy that is according to the SDGs, there needs to be strong data protection.⁵⁹ In Uzbekistan, data leakage cases are handled with the Cyber Security Center. Then, they are handled by the general court, which is a place to file a lawsuit on the law-violating action on personal data leakage perpetrators by personal data controllers and processors in this context, personal data protection system establishers. In this case, the personal data protection establishment mandated by the law is implemented by an institution called cyber security center under ministry of digital technologies,⁶⁰ that is especially determined by the president. Personal data institutions will then have a responsibility towards the president and the ministers. Further technicalities will be described in detail in the Presidential Regulation. In the current condition in Indonesia, the PDPA has effectively been implemented. There are still many legal voids in the technical scope that have not officially been covered, making digital-based investors reluctant to invest in Indonesia as they are not covered by the PDPA and this hinders the development of an inclusive digital economy.

The researchers perceive that Indonesian business institutions will at least consider how legal entities carry out some activities to protect personal data. Article 59 of the PDPA states as follows: (1) Formulating and determining policies and strategies; (2) Protecting personal data which becomes guidelines for personal data subjects, personal data controllers, and personal data processors; (3) Supervising the organization of personal data protection; (4) Enforcing the administrative law on violations against this law; and (5) Facilitating a non-litigation dispute resolution. Even though such stipulations exist, there are no clear institutions that have the authority to act upon them, leading to their ineffectiveness.⁶¹

⁵⁸ Dilafruz Jabborova and others, 'Possibilities of Using Technologies in Digital Transformation of Sustainable Development', *E3S Web of Conferences*, 49121 (2024) <https://doi.org/10.1051/e3sconf/202449101002>

⁵⁹ F.K. Agyekum and others, 'Does Technological Inclusion Promote Financial Inclusion among SMEs? Evidence from South-East Asian (SEA) Countries', *Global Finance Journal*, 53.100618 (2022) <https://doi.org/10.1016/j.gfj.2021.100618>

⁶⁰ Muhammad Fikri, 'Ruang Lingkup Perlindungan Data Pribadi', *Ganesha Law Review*, 5.1 (2023), 13–17. <https://doi.org/10.23887/glr.v5i1.2237>

⁶¹ I. Trinugroho and others, 'Adoption of Digital Technologies for Micro and Small Business in Indonesia', *Finance Research Letters*, 45.102156 (2022), 1–7 <https://doi.org/10.1016/j.frl.2021.102156>



Uzbekistan has taken a step by carrying out reformation to clarify this mechanism with the aim of developing the digital economy. The presidential decree in 2022 of the “Digital Uzbekistan-2030” Strategy was approved, which provides for the implementation of over 280 projects (including the clear mechanism for digital leaking data and its responsibility) for digital transformation sectors in the next two years. In Uzbekistan, the state is successfully coping with its role of creating the necessary conditions for the development of the inclusive digital economy, as evidenced by the results achieved and the ambitious goals set for the near future. The year 2024 was a successful one for the economy of Uzbekistan and turned out to be decisive in achieving one of the main goals of the ongoing reforms - strengthening the digital economy, maintaining high economic growth rates with clear responsibility for digital security or cyber security.

As a result of this cyber security reform, Uzbek households will have access to the Internet with a speed of at least 10 Mbit/s in each settlement and access increased to 79%. This is still deemed slow compared to the internet speed in Indonesia but is a significant jump in access in Uzbekistan. This is crucial in cyber security and data leakage prevention while developing the Law on Information Communication Technologies (ICT) in the country. The Cyber Security Center focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access and its responsible authority. Meanwhile, in Indonesia, the PDPA mandates the formation of a personal data protection institution to handle and protect personal data. However, this institution has not been established, even after several years, leading to ineffective law enforcement.⁶²

Generally, in the effort to develop an inclusive digital economy in Uzbekistan, the government combined all authorities in a single institution, namely the Cyber Security Center. Law enforcement is implemented in case of data leakage or violations, as the cyber security center has the statutory duty to notify the DXX (person or company) about the cybersecurity incidents and cybercrimes that have occurred. It also has corresponding duties. Cybersecurity takes measures to prevent the loss of relevant digital traces to fully disclose these incidents. It is to ensure the permanent storage of information necessary for analysis.⁶³ Cyber security center also had responsibility for cybersecurity incidents and investigating cybercrimes, including terrorism⁶⁴ (this new responsibility is regulated in clause 4 part 2 of Article 16 of the Law on Cyber security) and to notify the DXX on the results of investigation of the owner of an information resource or system in which a cyber security incident occurred (part 2 of Article 22 of the Law on Cyber security). Cyber security has become increasingly important recently as governments, corporations, and people collect, process, and store vast

⁶² Rakhmatillo Djuraevich Aloev and Mirkhon Mukhammadovich Nurullaev, ‘Software, Algorithms and Methods of Data Encryption Based on National Standards’, *IIUM Engineering Journal*, 21.1 (2020) <https://doi.org/10.31436/iiumej.v21i1.1179>

⁶³ O. Z. Maratdaevna, M. K. Kholdarovna, and A.T. Kalmakhanovna, ‘Features of Digital Employment in the Republic of Uzbekistan’, in *International Conference on Mathematical Applications in Science and Technology* (Applications of Mathematics in Science and Technology, 2025), pp. 95 – 97 <https://doi.org/10.1201/9781003606659-17>

⁶⁴ Arief Budiono, Absori, and others, ‘Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice’, *Journal of Human Rights, Culture and Legal System*, 3.3 (2023), 441–475 <https://doi.org/10.53955/jhcls.v3i3.127>



amounts of confidential information and transmit that data across networks. The reformation of cyber security through laws and concrete steps will develop the digital inclusive economy according to the goal of SDG 8.

This is something that Indonesia still has not succeeded in carrying, as national-scale data leakage keeps on occurring. Indonesia has not carried out adequate reformation in laws and actions to act upon and prevent the occurrence of data leakage. A fundamental thing that it still fails to do is notify citizens, companies, or institutions in case of data leakage as Uzbekistan has succeeded in doing even though the penal sanctions in Uzbekistan are less severe than those in Indonesia. This shows that the mere threat of punishment does not create a deterrent effect.

The mechanism for handling leaked data in Indonesia as illustrated by the writer starts from the first stage, where the personal data is leaked. The victim experiences confusion and files a complaint to the Personal Data Institution (that is still non-existent), even though it should already be established according to the mandate of the PDPA through the Presidential Regulation. Thus, the victim files a complaint to the police force (which is still unfamiliar with digital data issues).⁶⁵ Second, after the complaint is processed, the parties will be summoned, especially the personal data subject (personal data holder). The personal data institution will facilitate a resolution (either chasing the data leaker or other methods), because data breakers or data thieves in Indonesia would usually seek ransom). Finally, if the perpetrator is caught, the litigation method will be carried out through court which usually takes years. Thus, it does not provide a quick solution for digital-based businesses. This may become an obstacle to digital-based investment, making investors reluctant to invest in Indonesia due to its weak data security law in protecting data and personal data and finally this is not good for the digital inclusive economic as the goal of SDG 8.⁶⁶ This is a terrible condition for the national digital ecosystem. The writer certainly suggests that the lawsuit used concerns the law-violating actions of the legal entities that fail to protect personal data.

In Uzbekistan, the mechanism of resolution related to personal data (digital data) is carried out solely by an institution called the Cyber Security Center. In cases where it is proven that cybercrimes have occurred (data leakage, phishing, scamming, and cracking), the cyber security will process them using criminal law. However, if there are cases of related to business data, personal data, or business disputes, it will be processed through the private law mechanism in Uzbekistan. This guarantees that there is a clear sole institution with clear responsibility to handle the protection of personal data. This ease is the key to the data protection law reformation in Uzbekistan in supporting the development of the digital inclusive economy according to the SDGs.

⁶⁵ Sidik Prabowo and others, 'Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia', *International Journal of Safety and Security Engineering*, 15.1 (2025), 113 – 126 <https://doi.org/10.18280/ijssse.150113>

⁶⁶ I. Aprilianti and S. A. Dina, 'Co-Regulating the Indonesian Digital Economy', *CIPS Indonesia*, 2021 <https://repository.cipsindonesia.org/media/publications/332998-co-regulating-the-indonesian-digital-eco-30376717.pdf> [accessed 15 April 2025].



CONCLUSION

Based on the discussion above, the authors conclude that the legal responsibilities of entities regarding personal data are reflected in the obligations outlined in the laws of both Indonesia and Uzbekistan. However, in Indonesia, the lack of clarity regarding the institution responsible for managing personal data issues whether it is the State Cyber and Password Agency, the National Police, or the Ministry of Communication and Digital Affairs remains a significant problem. Although the Personal Data Protection Act (PDPA) mandates the establishment of a dedicated data protection authority, the government has yet to form this institution, even years after the law's enactment. This institutional vacuum has resulted in legal uncertainty and the continued occurrence of large-scale data breaches. In contrast, Uzbekistan has established a clear institutional framework through the Cyber Security Center, which holds explicit authority over data protection matters and has demonstrated greater effectiveness in handling such cases. Furthermore, the protection of personal data plays a vital role in fostering an inclusive digital economy, as emphasized in Sustainable Development Goal 8. Failure to ensure data protection in Indonesia will significantly hinder digital economic growth, as recurring data breaches could expose millions or even hundreds of millions of personal records. Since personal data forms the backbone of digital business operations, inadequate protection will ultimately obstruct the rapid development of an inclusive and secure digital economy.

ACKNOWLEDGMENT

The authors would like to thank Universitas Muhammadiyah Surakarta and Tashkent State Law University in this research for their cooperation in comparing the personal data protection laws in Indonesia and Uzbekistan as pioneering (the first) research which directly compares legal norms, implementation, and effectiveness of the PDP Law in these two countries, with the conclusion that these two countries have laws regarding this issue with different effectiveness and implementation.

REFERENCES

- Agyekum, F.K., K. Reddy, D. Wallace, and N.H. Wellalage, 'Does Technological Inclusion Promote Financial Inclusion among SMEs? Evidence from South-East Asian (SEA) Countries', *Global Finance Journal*, 53.100618 (2022) <https://doi.org/10.1016/j.gfj.2021.100618>
- Aloev, Rakhmatillo Djuraevich, and Mirkhon Mukhammadovich Nurullaev, 'Software, Algorithms and Methods of Data Encryption Based on National Standards', *IJUM Engineering Journal*, 21.1 (2020) <https://doi.org/10.31436/iiumej.v21i1.1179>
- Aprilianti, I., and S. A. Dina, 'Co-Regulating the Indonesian Digital Economy', *CIPS Indonesia*, 2021 <https://repository.cipsindonesia.org/media/publications/332998-co-regulating-the-indonesian-digital-eco-30376717.pdf> [accessed 15 April 2025]
- Astuti, E.F., A.N. Hidayanto, S. Nurwardani, and A.Z. Salsabila, 'Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001:2013', *International Journal of Safety and Security Engineering*, 14.5 (2024), 1559–1567 <https://doi.org/10.18280/ijssse.140523>



- Bangsawan, Moh Indra, Budi Santoso, M Junaidi, Dewi Kusuma Diarti, Sandya Mahendra, and Engine Kubota, 'Personal Data Protection Policy during Covid-19 Pandemic Era', *Law and Justice*, 8.1 (2023), 21–31 <https://doi.org/10.23917/laj.v8i1.1558>
- Benuf, Kornelius, and Muhamad Azhar, 'Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer', *Gema Keadilan*, 7.1 (2020), 20–33 <https://doi.org/10.14710/GK.7.1.20-33>
- Budiono, Arief, Absori, Kelik Wardiono, Wardah Yuspin, and Said Saidakhrarovich Gulyamov, 'Cyber Indoctrination Victims in Indonesia and Uzbekistan: Victim Protection and Indoctrination in Practice', *Journal of Human Rights, Culture and Legal System*, 3.3 (2023), 441–475 <https://doi.org/10.53955/jhcls.v3i3.127>
- Budiono, Arief, A. S. Nurrizky, F. Fairuzzaman, S. S. Gulyamov, A. L. Prakoso, Wardah Yuspin, and others, 'Lessons from Indonesian National Healthcare Security (BPJS Kesehatan): HIV/AIDS Patient Medical Data Protection Policies', *Malaysian Journal of Medicine and Health Sciences*, 20.9 (2024), 201–8 <https://doi.org/10.47836/mjmhs/20.s9.33>
- Dantes, K. F., 'Engaturan Sistem Elektronik Dalam Pengambilan Keputusan Rapat Umum Pemegang Saham (Rups) Perseroan Terbatas Yang Berkepastian', *Jurnal Komunikasi Hukum (JKH)*, 8.1 (2022), 527–36 <https://doi.org/10.23887/jkh.v8i1.50941>
- Maichle Delpiero and others, 'Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data', *Padjadjaran Law*, 9.1 (2021), 1–22. <https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509>
- A. A. Dhewa and Herkin Yossyafaat Program, 'Aspek Hukum Perlindungan Konsumen Pada Transfer Data Pribadi Oleh Korporasi Dalam Hukum Positif Indonesia', *Lontar Merah*, 6.1 (2023), 619–29. <https://doi.org/10.31002/lm.v6i1.3807>
- Wahyudi Djafar, 'Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan', *Jurnal Becoss*, 1.1 (2019), 147–54. <https://learning.hukumonline.com/wp-content/uploads/2022/09/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf>
- Eshov, M.P., and D.S. Nasirkhodjaeva, 'Conditions And Factors Of Forming A Digital Economy In Uzbekistan', in *ACM International Conference Proceeding Series* (ACM, 2022), pp. 81–86 <https://doi.org/10.1145/3584202.3584215>
- Faiz Rahman, 'Safeguarding Personal Data In The Public Sector: Unveiling The Impact Of The New Personal Data Protection Act In Indonesia', *UUM Journal of Legal Studies*, 16.1 (2025), 1 – 18 <https://doi.org/10.32890/uumjls2025.16.1.1>
- Fayzieva, M., G. Abdurakhmanova, M. Eshov, Sadirdin Khudoykulov, Samandar Kurbonov, S. Goyipnazarov, and others, 'The Role of Digital Development in the Reinforcement of the Government Social Protection System of Uzbekistan', in *ACM International Conference Proceeding Series* (Dubai: 7th International Conference



- on Future Networks and Distributed Systems, ICFNDS, 2023), pp. 42–50 <https://doi.org/10.1145/3644713.3644720>
- Fayzieva, M., M. Sanjar, S. Kongratbay, Y. Maksudjon, B. Iroda, K. Iroda, and others, 'The Study of the Impact of the Digital Economy on the Growth of E-Government Services in Uzbekistan', in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (New York: Springer, 2023), pp. 208–17 https://doi.org/10.1007/978-3-031-30258-9_18
- Muhammad Fikri, 'Ruang Lingkup Perlindungan Data Pribadi', *Ganesha Law Review*, 5.1 (2023), 13–17. <https://doi.org/10.23887/glr.v5i1.2237>
- Olisias Gultom, Auditya Firza Saputra, and Muhammad Faiz Aziz, 'Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital', 2021, 1–135. <https://igj.or.id/2022/08/27/perlindungan-datapribadi-diindonesiamenyikapi-liberalisasi-ekonomi-digital/>
- Gunawan, Johannes, 'Kontroversi Strict Liability Dalam Hukum Perlindungan Konsumen', *Veritas et Justitia*, 4.2 (2018), 274–303 <https://doi.org/10.25123/vej.3082>
- Hertianto, M Rafifnafia, 'Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia', *Kertha Patrika*, 43.1 (2021), 93 <https://doi.org/10.24843/kp.2021.v43.i01.p07>
- i-Scoop, 'From Industry 4.0 to Society 5.0: The Big Societal Transformation Plan of Japan', *I-Scoop.Eu*, 2017
- Iman Nofie, 'The Fight for Our Personal Data: Analyzing the Economics of Data and Privacy on Digital Platforms', *International Journal of Law and Management*, 66.6 (2024), 774–791 <https://doi.org/10.1108/IJLMA-12-2022-0258>
- Jabborova, Dilafroz, Dilfuza Mamurova, Khushvakht Khakimovna Umurova, Umida Ulasheva, Sevara Xolmuradovna Jalalova, and Azizbek Khurramov, 'Possibilities of Using Technologies in Digital Transformation of Sustainable Development', *E3S Web of Conferences*, 49121 (2024) <https://doi.org/10.1051/e3sconf/202449101002>
- Jamshid Sodikov, 'Roads Infrastructure Digital Twin Case Study: Uzbekistan', *Urban Sustainability*, F3988 (2024), 209 – 230 https://doi.org/10.1007/978-981-97-8483-7_10
- Josephine, Josephine, Sinta Dewi Rosadi, and Sudaryat Sudaryat, 'Perlindungan Konsumen Daring Dan Tanggung Jawab Perusahaan Marketplace Atas Data Privasi Konsumen', *Jurnal Suara Keadilan*, 21.1 (2020), 97–112 <https://doi.org/10.24176/sk.v21i1.5686>
- Kambarov, J., U. Rakhmatov, N. Rakhmonov, and Y. Sultanova, 'Problems and Solutions for the Implementation of the Industry-4.0 Program in Uzbekistan', *Journal of Advanced Research in Dynamical and Control Systems*, 12.2 (2020), 2677–2683 <https://doi.org/10.5373/JARDCS/V12I2/S20201321>



- Karimov, N., M. Kalandarova, N. Makhkamova, M. Karshiboeva, and B. Odilov, 'Impact of Mobile Applications on Tourism Development in Uzbekistan', *Indian Journal of Information Sources and Services*, 14.4 (2024), 175 – 181 <https://doi.org/10.51983/ijiss-2024.14.4.27>
- Khaund, Tuja, Muhammad Nihal Hussain, Mainuddin Shaik, and Nitin Agarwal, 'Telegram: Data Collection, Opportunities and Challenges', *Communications in Computer and Information Science*, 1410 (2020), 513 – 526 <https://doi.org/10.1007/978-3-030-76228-5_37>
- Kusumowijoyo, Anindita, Anjani Marta, and Kimberly Natali Boasrifa, 'The Artificial Intelligence as a One-Stop Point for Dealing with Online Human Trafficking Scams in Indonesia', *Journal of Sustainable Development and Regulatory Issues*, 1.3 (2023), 189–211 <https://doi.org/10.53955/jsderi.v1i3.18>
- Maleno, M., and A. Kusumawati, 'Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights', *Indonesia Law College Association Law Journal*, 3.2 (2024), 91–98 <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>
- Maratdaevna, O. Z., M. K. Kholdarovna, and A.T. Kalmakhanovna, 'Features of Digital Employment in the Republic of Uzbekistan', in *International Conference on Mathematical Applications in Science and Technology* (Applications of Mathematics in Science and Technology, 2025), pp. 95 – 97 <https://doi.org/10.1201/9781003606659-17>
- Marcelliana, Vanesha, Salsabila Muthia Zahra, Ninda Nur Adzani, Hanif Nur Massaid, Nurhasna Badriyyah, Raina Benita, and others, 'Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah (Implementation of Consumer Protection for PT Customers. Indonesian Sharia Bank in Customer Data Leak Case)', *Deposisi: Jurnal Publikasi Ilmu Hukum*, 1.2 (2023), 180–94 <https://doi.org/10.59581/deposisi.v1i2.562>
- Mavluda, Askarova, Choriev Fazliddin, and Khayitov Saidjon, 'The Importance of Digitalization in Economic Development of the Government', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14543 (2024), 196 – 204 https://doi.org/10.1007/978-3-031-60997-8_17
- Mirnayanti Mirna, Judhariksawan, and Maskum, 'Analisis Pengaturan Keamanan Data Pribadi Di Indonesia', *Jurnal Ilmiah Living Law*, 15.1 (2023), 16–30. <https://doi.org/10.30997/jill.v15i1.4726>
- Mukhammedov, M., A. Nizamov, Z. Mukhammedova, S. Iskhakova, and A. Nizamov, 'Development of Public Regulatory Strategies to Incentivise Investment in Human Capital', *Scientific Bulletin of Mukachevo State University Series Economics*, 11.4 (2024), 133–146 <https://doi.org/10.52566/msu-econ4.2024.133>
- Rahmawati Nafi'ah, 'Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce Data Breach and Identity Theft on E-Commerce', *CyberSecurity Dan Forensik*



- Digital*, 3.1 (2020), 7–13. <https://doi.org/10.14421/csecurity.2020.3.1.1980>
- Nurhayati, Yati, Ifrani Ifrani, and M. Yasir Said, ‘Metodologi Normatif Dan Empiris Dalam Perspektif Ilmu Hukum’, *Jurnal Penegakan Hukum Indonesia*, 2.1 (2021), 1–20 <https://doi.org/10.51749/jphi.v2i1.14>
- Palinggi, Sandryones, Srivan Palelleng, and Lutma Ranta Allolinggi, ‘Peningkatan Rasio Kejahatan Cyber Dengan Pola Interaksi Sosio Engineering Pada Periode Akhir Era Society 4.0 Di Indonesia’, *Jurnal Ilmiah Dinamika Sosial*, 4.1 (2020), 145 <https://doi.org/10.38043/jids.v4i1.2314>
- Panjaitan, Rony Mart, ‘Pertanggungjawaban Pidana Korporasi Sebagai Penyelenggara Sistem Elektronik Dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik’, *Jurnal Hukum Adigama*, 4.2 (2021), 2624–43 <https://journal.untar.ac.id/index.php/adigama/article/view/17761/9805>
- Prabowo, Sidik, Maman Abdurrohman, Hilal Hudan Nuha;, and Sarwono Sutikno, ‘Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia’, *International Journal of Safety and Security Engineering*, 15.1 (2025), 113 – 126 <https://doi.org/10.18280/ijssse.150113>
- Prananingrum, Dyah Hapsari, ‘Penegakan Hukum Jabatan Notaris Dalam Pembuatan Perjanjian Berdasarkan Pancasila Dalam Rangka Kepastian Hukum’, *Refleksi Hukum: Jurnal Ilmu Hukum*, 8.1 (2014), 73–92 <https://doi.org/10.33476/ajl.v2i3.846>
- Prasetyoningsih, Nanik, Nazli Ismail Nawang, Windy Virdinia Putri, and Muhammad Nur Rifqi Amirullah, ‘Legal Protection for the Personal Data in Indonesia and Malaysia’, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14728 (2024), 161 – 169 https://doi.org/10.1007/978-3-031-61379-1_11
- Prastyanti, Rina Arum, Istiyawati Rahayu, Eiad Yafi, Kelik Wardiono, and Arief Budiono, ‘Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia’, *Jurnal Jurisprudence*, 11.1 (2021), 82–99 <https://doi.org/10.23917/jurisprudence.v11i1.14756>
- Prastyanti, Rina Arum, and Ridhima Sharma, ‘Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India’, *Journal of Human Rights, Culture and Legal System*, 4.2 (2024), 354–90 <https://doi.org/10.53955/jhcls.v4i2.200>
- Prastyanti, Rina Arum, and Prattana Srisuk, ‘Achieving Sustainable Consumer Protection in the Era of Social Media’, *Journal of Sustainable Development and Regulatory Issues*, 3.1 (2025), 121–46 <https://doi.org/10.53955/jsderi.v3i1.52>
- Rizal, M., S. D. Rosadi, and A. Taryana, ‘Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia’, *Journal of Law and Sustainable Development*, 12.1 (2024), e2809 <https://doi.org/10.55908/sdgs.v12i1.2809>
- Sautunnida, Lia, ‘Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia:



- Studi Perbandingan Hukum Inggris Dan Malaysia', *Kanun Jurnal Ilmu Hukum*, 20.2 (2018), 369–84 <https://doi.org/10.24815/kanun.v20i2.11159>
- Setyowati, Luluk, and Deni Nasir Ahmad, 'Pemanfaatan Big Data Dalam Era Teknologi 5.0', *ABDINE: Jurnal Pengabdian Masyarakat*, 1.2 (2021), 117–22 <https://doi.org/10.52072/abdine.v1i2.205>
- Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah, 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment', *Hasanuddin Law Review*, 10.1 (2024), 1–20 <https://doi.org/10.20956/halrev.v10i1.5016>
- Silalahi, Theresia, 'Police Investigate Alleged Data Breach at Bank DKI', *Jakarta Globe* <https://jakartaglobe.id/business/police-investigate-alleged-data-breach-at-bank-dki>
- Sinaga, Erlina Maria Christin, 'Formulasi Legislasi Perlindungan Data Pribadi', *Jurnal RechtVinding*, 9.2 (2020), 237–56 <https://dx.doi.org/10.33331/rechtsvinding.v9i2.428>
- Sutra Disemadi, Hari, and Cindy Kang, 'Tantangan Penegakan Hukum Hak Kekayaan Intelektual Dalam Pengembangan Ekonomi Kreatif Di Era Revolusi Industri 4.0', *Jurnal Komunikasi Hukum (JKH)*, 7.1 (2021), 54 <https://doi.org/10.23887/jkh.v7i1.31457>
- Tampubolon, Trisa, and Rizki Ramadhan, 'ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital Pada Asia Tenggara', *Padjadjaran Journal of International Relations*, 1.3 (2020), 270 <https://doi.org/10.24198/padjir.v1i3.26197>
- Trinugroho, I., P. Pamungkas, J. Wiwoho, S.M. Damayanti, and T. Pramono, 'Adoption of Digital Technologies for Micro and Small Business in Indonesia', *Finance Research Letters*, 45.102156 (2022), 1–7 <https://doi.org/10.1016/j.frl.2021.102156>
- Turginbayeva, Ardak N, Zhanna V Gornostaeva, Vera Yu Rudakova, and Tatiana A Dugina, 'Digital Inclusion as a Way to Deal with the Mismatch Between the Higher Education Market and the Labour Market', *Education in the Asia-Pacific Region*, 73 (2025), 93 – 100 https://doi.org/10.1007/978-981-96-1933-7_11
- Utami, Tanti Kirana, Kayla Andini Putri, Salsa Octaviani Suryanto, and Fina Asriani, 'Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law', *Journal Customary Law*, 2.2 (2025), 21 <https://doi.org/10.47134/jcl.v2i2.3742>
- Wardiono, Kelik, 'Prophetic: An Epistemological Offer for Legal Studies', *Journal of Transcendental Law*, 1.1 (2019), 17–41 <https://doi.org/10.23917/jtl.v1i1.8797>
- Witro, Doli, Mhd Rasidin, and Muhamad Izazi Nurjaman, 'Subjek Hukum Dan Objek Hukum: Sebuah Tinjauan Hukum Islam, Pidana Dan Perdata', *Asy Syar'iyah: Jurnal Ilmu Syari'ah Dan Perbankan Islam*, 6.1 (2021), 43–64 <https://doi.org/10.32923/asy.v6i1.1611>



- Wulandari, Dinda Agustin, Abdul Kadir Jaelani, and Ong Argo Victoria, 'Income Tax Regulations for Child Content Creators of TikTok Platform: Inefficacy of Indonesian Legal Frameworks', *Journal of Sustainable Development and Regulatory Issues*, 2.2 (2024), 145–57 <https://doi.org/10.53955/jsderi.v2i2.35>
- Yashnarovna, Isokhujaeva Munira, 'AI Transforms E-Commerce Management and Regulation in Uzbekistan', *Indonesian Journal of Law and Economics Review*, 19.2 (2024) <https://doi.org/10.21070/ijler.v19i2.1054>
- Yuspin, W., A.O. Putri, A. Fauzie, and J. Pitaksantayothin, 'Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities', *International Journal of Safety and Security Engineering*, 14.6 (2024), 1699–1706 <https://doi.org/10.18280/ijssse.140605>
- Yuspin, Wardah, Kelik Wardiono, Arief Budiono, and Said Saidarakhrovich Gulyamov, 'The Law Alteration on Artificial Intelligence in Reducing Islamic Bank's Profit and Loss Sharing Risk', *Legality: Jurnal Ilmiah Hukum (Scientific Journal of Law)*, 30.2 (2022), 267–282 <https://doi.org/10.22219/ljih.v30i2.23051>