ADLIYA: Jurnal Hukum dan Kemanusiaan –ISSN: 1978-8312 (p), 2657-2125 (e)
Vol. 18, no. 1 (March 2024), pp. 25-46, doi: 10.15575/adliya.v18i1.43758

TRANSPARENCY AND CONSENT FOR THE USE OF *DATA ANALYTICS* IN INDONESIA

Hari Sutra Disemadi[1]*, Rufinus Hotmaulana Hutauruk[2], Ninne Zahara Silviani[3], David Tan[4]

[1234] *Faculty of Law, Universitas Internasional Batam, Indonesia*
* Correspondence: hari@uib.ac.id

Received: 19 Mei 2023; Accepted: 25 March 2024; Published: 30 March 2024

Abstract

The digital economy era has driven the use of technology that relies on data utilization to support various economic activities, such as the use of data analytics. The use of data analytics to provide more relevant features and ads to users of various online platforms has legal implications that must be supported by a legal framework for personal data protection in Indonesia. This study is done to analyze the gap in the development of legal framework in Indonesia in regards to the use of data analytics. Using normative legal research, this study explains the legal implications and outlines the legal issues related to the use of data analytics and the risks faced by online platform users as data owners. The analysis using the statutory approach in this research found that there are several legal issues and normative limitations that make it difficult to implement the concept of transparency and consent in efforts to protect personal data of online platform users, which is the main target of the use of data analytics. The findings of this study also indicate that the use of more complex technical terms is not found in regulations governing the protection of personal data, and hinders further normative exploration related to the use of data analytics that distinguish the types of data used into more complex terms and classifications.

Keywords: personal data protection; legal framework; *data analytics*; digital economy; transparency and consent

Abstrak

Era ekonomi digital telah mendorong penggunaan teknologi yang mengandalkan pemanfaatan data untuk mendukung berbagai aktivitas ekonomi, seperti penggunaan *data analytics*. Pemanfaatan *data analytics* untuk menyediakan fitur dan iklan yang lebih relevan bagi pengguna berbagai platform *online* memiliki implikasi hukum yang harus didukung oleh kerangka hukum perlindungan data pribadi di Indonesia. Penelitian ini dilakukan untuk menganalisis kesenjangan dalam perkembangan kerangka hukum di Indonesia terkait penggunaan *data analytics*. Dengan menggunakan metode penelitian hukum normatif, studi ini menjelaskan implikasi hukum serta memetakan isu-isu hukum terkait penggunaan *data analytics* dan risiko yang dihadapi oleh pengguna platform *online* sebagai pemilik data. Analisis dengan pendekatan peraturan perundang-undangan dalam penelitian ini menemukan bahwa terdapat beberapa permasalahan hukum dan keterbatasan normatif yang mempersulit implementasi konsep transparansi dan persetujuan dalam upaya perlindungan data pribadi pengguna platform *online*, yang menjadi sasaran utama dari penggunaan *data analytics*. Hasil penelitian ini juga menunjukkan bahwa penggunaan istilah teknis yang lebih kompleks belum ditemukan dalam regulasi yang mengatur perlindungan data pribadi, yang pada akhirnya menghambat eksplorasi normatif lebih lanjut terkait penggunaan *data analytics* yang membedakan jenis data yang digunakan ke dalam istilah dan klasifikasi yang lebih kompleks.

Kata Kunci: perlindungan data pribadi; kerangka hukum; *data analytics*; ekonomi digital; transparansi dan persetujuan

Introduction

The use of *data analytics* to target advertising is an effort by various businesses to improve the accuracy and efficiency of advertising in various *online* spaces in this digital economy era.[1] This effort, in addition to assisting in running a business, must also consider the interests of potential consumers as the target of various *online* advertisements. From the perspective of users of an *online* platform, transparency and consent from users are two important aspects of using this technology. Since users must give their consent before their personal data is collected and used for advertising purposes, transparency in communicating information related to data collection and usage is crucial. However, this can be challenging as many users may not fully understand the implications of data collection and may not be aware of their rights in controlling their data.[2]

The collection of users' personal data by *online* platform providers must comply with relevant legislation and regulations, such as the General Data Protection Regulation (GDPR) in effect in the European Unio[3] or the California Consumer Privacy Act (CCPA) which applies in California, United States.[4] Both regulations emphasize that the collection of personal data can only be done if *online* platform providers have obtained user consent and have provided sufficient information regarding the collection, usage, and protection of user personal data. Along with the increasing relevance of data in the digital economy era, awareness of the importance of data protection from various factors that may harm data owners continues to grow. Furthermore, with the emergence of the popular term "data is the new oil," the importance of data in the economy has increased, which then influences the development of data protection standards worldwide.[5] Furthermore, *online* platform providers must ensure that users give their consent knowingly and voluntarily,

[1] Nicholas Economides and Ioannis Lianos, "Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective," *Journal of Competition Law and Economics* 17, no. 4 (2021): 765–847, https://doi.org/10.1093/joclec/nhab007.

[2] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, "Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society," in *Aufwachsen in Überwachten Umgebungen*, 2021, 219–36, https://doi.org/10.5771/9783748921639-219.

[3] Aggeliki Tsohou et al., "Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform," *Information and Computer Security* 28, no. 4 (2020): 531–53, https://doi.org/10.1108/ICS-01-2020-0002.

[4] Jeeyun (Sophia) Baik, "Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)," *Telematics and Informatics* 52 (2020): 1–33, https://doi.org/10.1016/j.tele.2020.101431.

[5] Andrej Zwitter and Jilles Hazenberg, "Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation," in *Blockchain, Law and Governance*, 2021, 87–97, https://doi.org/10.1007/978-3-030-52722-8_6.

without coercion or threat.[6] These companies must also provide users with the option to refuse data collection or to delete their data if they change their minds about previously given consent. The forms of coercion or threat must meet certain elements to be considered as such, and must have a direct impact on how *online* platform users decide to consent to the use of their data.

When an *online* platform provider collects user data, they must provide sufficient clear and understandable information about the data collection, such as the type of data collected, the purpose of data collection, and third parties who may receive such data.[7] In addition, the platform provider must ensure that the information provided to users is easily accessible and understandable, avoiding technical terms that may be difficult for ordinary users to understand. If the platform provider fails to meet the required transparency and consent standards, they may be subject to sanctions by the authorities, such as fines or bans on the use of personal data. Therefore, transparency and good consent from users are crucial in the use of *data analytics* to target ads accurately and legally from a legal perspective.

The use of *data analytics* is becoming increasingly important in the digital era, but it also brings special attention to the risks involved in data protection. In Indonesia, data protection issues are important because there is no clear regulation on the use of *data analytics*. Therefore, it is important to analyze this issue from the perspective of data protection law. Several studies have been conducted on data protection issues and the use of *data analytics* in Indonesia. Previous studies have explained how the legal framework governing personal data protection and data privacy in Indonesia is insufficient compared to some other countries.[8] Other studies have also found that there is a tendency to overlook data protection policies and only focus on developing functionality from a technological aspect.[9]

In addition, other studies have found that digital literacy does not significantly increase perceptions of security and data privacy, particularly regarding risks that can threaten e-commerce ecosystem users.[10] They also found that *online* platform

[6] Princess Alafaa, "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World," *SSRN Electronic Journal*, 2022, 1–12, https://doi.org/10.2139/ssrn.4005750.

[7] Christian Kurtz, Martin Semmann, and Tilo Böhmann, "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors," in *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, 2018.

[8] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (2022): 1443–57, https://doi.org/10.1108/JFC-09-2021-0193.

[9] Yudy Setiawan and Anita Maharani, "Unboxing Employees Perspectives on Factors Affecting Their Compliance to Organizational Information Security Policies," in *SMARTCYBER 2021: Proceedings of 2nd International Conference on Smart Computing and Cyber Security*, 2022, 182–93, https://doi.org/10.1007/978-981-16-9480-6_17.

[10] Ayasha Nadira Widyadhana, Putu Wuri Handayani, and Pramitha Dwi Larasati, "Influence of Technological, Social, and Individual Factors on Security and Privacy Take-up of Digital Banking,"

providers in Indonesia need to increase awareness of data protection and improve their privacy policies. In the context of data protection law, the study also states that Indonesia as a whole still lacks strong regulations on data protection. Another study found that there needs to be a distinction between perceived threats and preparedness, to better fight against many cybersecurity threats.[11] Therefore, clear and comprehensive regulations are needed to address data protection issues in the use of *data analytics.*

However, there are also studies that reveal that data protection issues are not just a regulatory problem, but also an issue of awareness and organizational culture within the *online* platform provider environment.[12] Another similar research found this to be the case, along with the importance of understanding security risks, particularly with the increasing use of data collection techniques with very large volumes, such as Big Data.[13] A solution such as cybersecurity disclosure has been proposed by a study, particularly to increase transparency through the act of organizational compliance.[14] Fundamentally, data protection issues in the use of *data analytics* in Indonesia remain an important concern. While data protection regulations in Indonesia are still inadequate, it is important to increase awareness and organizational culture in managing *data analytics* and data protection. This can help organizations, in this case *online* platform providers, to improve their privacy policies and effectively protect their customer data.

The novelty of this study lies in its focus on transparency and consent aspects regarding the use of data for analyzing the legal aspects of data protection in the context of *data analytics* in Indonesia. While some previous studies have highlighted the importance of privacy and data protection in Indonesia, this research takes a unique perspective by examining the legal framework surrounding *data analytics* and privacy, particularly regarding the compliance framework directly related to the concepts of transparency and consent in data usage. Additionally, this study also recognizes the need for increased awareness and culture of privacy and data protection in the *online* platform provider environment, which is a relatively unexplored area in previous legal research. The findings of this study have the potential

in *2022 International Conference on Information Management and Technology (ICIMTech)* (IEEE, 2022), 33–38, https://doi.org/10.1109/ICIMTech55957.2022.9915231.

[11] Taewoo Nam, "Understanding the Gap between Perceived Threats to and Preparedness for Cybersecurity," *Technology in Society* 58 (August 2019): 1–10, https://doi.org/10.1016/j.techsoc.2019.03.005.

[12] Khikmatul Islah, "Peluang Dan Tantangan Pemanfaatan Teknologi Big Data Untuk Mengintegrasikan Pelayanan Publik Pemerintah," *Jurnal Reformasi Administrasi: Jurnal Ilmiah Untuk …* 5, no. 1 (2018): 130–38.

[13] Paulo Costa et al., "The Security Challenges Emerging from the Technological Developments," *Mobile Networks and Applications* 24, no. 6 (December 2019): 2032–37, https://doi.org/10.1007/s11036-018-01208-0.

[14] Maricela Ramírez et al., "The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index," *Sustainability* 14, no. 3 (January 2022): 1–23, https://doi.org/10.3390/su14031390.

to contribute to the development of regulations and guidelines related to *data analytics* and privacy in Indonesia, as well as provide insights for *online* platform providers to enhance their privacy policies and practices. Therefore, this study can fill existing literature gaps and offer valuable insights for policymakers, researchers, and practitioners working in the field of *data analytics* and privacy in Indonesia.

Methods

This study employed a normative legal research method to examine the existing legal norms within the relevant legal framework in Indonesia,[15] particularly the ones regarding the protection of personal data. Typically, a normative legal study, at least in its purest sense, involves the analysis of a particular legal issue, viewed by the lens of secondary data in the form of primary law sources.[16] By utilizing a statutory approach, this research analyzed the legal issues and normative limitations that affect the use of personal data in *data analytics* in Indonesia and how it may threaten the interests of *online* platform users as owners of personal data used. Secondary data in the form of primary legal sources, namely Law No. 27 of 2022 on Personal Data Protection, was utilized in this study.

Results and Discussion

The Significance of Transparency and Consent in the Use of *Data analytics* within the Legal Domain

Data analytics has revolutionized the way businesses interact with their customers, especially in the field of targeted advertising.[17] With the help of *data analytics*, various *online* platform providers can gain insights into the behavior, preferences, and interests of their customers.[18] By analyzing data from various sources such as social media platforms, search engines, and *online* marketplaces, businesses can identify patterns and trends that can inform their advertising strategies.

One of the key benefits of *data analytics* in advertising is the ability to create ads specifically targeted to individual users. These targeted ads are customized for each user based on their browsing history, search engine queries, and social media activity. The ads are designed to be relevant to the user's interests and, as a result, tend to be

[15] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289–304, https://doi.org/10.37253/jjr.v24i2.7280.

[16] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78.

[17] Arshia Rehman, Saeeda Naz, and Imran Razzak, "Leveraging Big *Data analytics* in Healthcare Enhancement: Trends, Challenges and Opportunities," in *Multimedia Systems*, vol. 28, 2022, https://doi.org/10.1007/s00530-020-00736-8.

[18] Marcello M. Mariani and Samuel Fosso Wamba, "Exploring How Consumer Goods Companies Innovate in the Digital Age: The Role of Big *Data analytics* Companies," *Journal of Business Research* 121 (2020), https://doi.org/10.1016/j.jbusres.2020.09.012.

clicked on more often, resulting in higher conversion rates.[19] *Data analytics* can also help businesses track the effectiveness of their advertising campaigns. By analyzing metrics such as click-through rates, conversion rates, and return on investment, *online* platform providers can identify which ads are performing well and which are not. This data can be used to make informed decisions about where advertising spend should be allocated and which ads should be modified or discontinued.

In addition to enhancing the effectiveness of advertising campaigns, *data analytics* can also help *online* platform providers identify opportunities for new customer growth. By analyzing customer data, various forms of business can identify gaps in the market or new trends that can be leveraged.[20] For example, if *data analytics* show that a specific demographic is interested in a particular type of product, *online* platform providers can create new product lines to target that demographic. *Data analytics* also play a crucial role in creating a seamless customer experience. By tracking customer interactions at various touchpoints, businesses can identify areas of friction or confusion and address them. This can improve customer satisfaction and loyalty, which in turn can drive sales and revenue.

Data analytics has become an integral aspect of business operations and decision-making processes in various industries. *Data analytics* involves the use of software tools, algorithms, and statistical models to analyze and draw insights from large volumes of data. The use of *data analytics* has enabled *online* platform providers to improve their operations, increase efficiency, and make better-informed decisions.[21] However, the use of *data analytics* also poses significant legal and ethical issues, particularly with regards to the collection, use, and disclosure of personal information. Privacy laws require users to be informed about how their personal information is collected, used, and disclosed, and that they provide their consent for such collection, use, and disclosure. Failure to comply with these legal requirements can result in significant legal and reputational consequences for *online* platform providers.

Transparency is an essential aspect of all forms of data and privacy protection as it enables users to understand and control how their personal information is used.[22] It is important for *online* platform providers to provide clear and concise information about their *data analytics* practices to ensure that users are informed about

[19] Xin Zhang, Wei Thoo Yue, and Yugang Yu, "Compete, Cooperate, or Coopete? The Strategic Role of *Data analytics* in Targeted Advertising," *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3549642.

[20] Saeid Sadeghi Darvazeh, Iman Raeesi Vanani, and Farzaneh Mansouri Musolu, "Big *Data analytics* and Its Applications in Supply Chain Management," in *New Trends in the Use of Artificial Intelligence for the Industry 4.0*, 2020, https://doi.org/10.5772/intechopen.89426.

[21] Yanfang Niu et al., "Organizational Business Intelligence and Decision Making Using Big *Data analytics*," *Information Processing and Management* 58, no. 6 (2021), https://doi.org/10.1016/j.ipm.2021.102725.

[22] Yang Liu and Connor Greene, "The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination," in *Digital Transformation in Business and Society: Theory and Cases*, 2019, 145–53, https://doi.org/10.1007/978-3-030-08277-2_9.

the purposes of collecting, using, and disclosing their personal information. *Online* platform providers should strive to ensure that this information is easily accessible to users and communicated in plain language to facilitate their understanding. One of the key benefits of transparency is building trust between *online* platform providers as data controllers and platform users themselves.[23] When users are aware of how their personal information is being used, they are more likely to trust *online* platform providers and feel more comfortable sharing their personal information. By providing transparency, *online* platform providers can not only comply with legal and ethical obligations but also improve their relationships with their customers.

Transparency is also important to ensure that *online* platform providers are accountable for their *data analytics* practices. When *online* platform providers provide clear and concise information about their *data analytics* practices, they can be held accountable for their actions. This accountability promotes responsible and ethical behavior by *online* platform providers and helps prevent the misuse of personal information. Additionally, transparency is crucial for users to effectively exercise their privacy rights. If users do not know how their personal information is being used, they cannot make informed decisions about whether to give their consent. By providing clear and concise information about their *data analytics* practices, *online* platform providers can enable users to effectively exercise their privacy rights and control their personal information.

The importance of a well-defined concept of transparency is a key aspect of all regulations related to data and privacy protection.[24] The presence of a good and clear conceptualization of transparency can ensure that users know how their personal information is being used. *Online* platform providers should provide clear and concise information about their *data analytics* practices in simple language and make it easily accessible to users. Transparency fosters trust, promotes accountability, and enables users to effectively exercise their privacy rights.

Consent is equally important in ensuring that users have control over their personal information and how it will be used after consent is given.[25] *Online* platform providers must obtain clear and informed consent from users before collecting, using, or disclosing their personal information for *data analytics* purposes. Consent should be specific, meaning it should be related to a particular purpose and should not be overly broad. Additionally, it should ensure that users understand the implications of giving their consent, including potential risks and benefits.

[23] Sandra Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model," *Law, Innovation and Technology* 10, no. 2 (2018): 266–94, https://doi.org/10.1080/17579961.2018.1527479.

[24] Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99, https://doi.org/10.25072/jwy.v5i2.460.

[25] Michael Birnhack, "A Process-Based Approach to Informational Privacy and the Case of Big Medical Data," *Theoretical Inquiries in Law* 20, no. 1 (2019): 257–90, https://doi.org/10.1515/til-2019-0009.

Consent can also be referred to as one of the fundamental principles of data protection and related legal regulations regarding privacy, as it enables users to know why their data is being collected and how it will impact their experience using a particular *online* platform. Obtaining clear and informed consent is crucial for *online* platform providers who collect, use, or disclose personal information for *data analytics* purposes.[26] *Online* platform providers must strive to obtain specific consent, meaning it is related to a particular purpose and not overly broad. Consent must also be obtained in a clear and understandable manner, so that users can make decisions based on information about whether to give their consent.

Furthermore, obtaining consent is not a one-time obligation but an ongoing process that requires *online* platform providers to ensure that users continue to receive information about the use of their personal information.[27] This ongoing process involves regularly reviewing and updating the purposes of collecting, using, and disclosing personal information, and ensuring that users are notified of any changes to these purposes. *Online* platform providers must also ensure that users are given the opportunity to withdraw their consent at any time.

Consent is also important to ensure that personal information is collected, used, and disclosed in a proportional manner and based on legitimate reasons under the law, without violating the interests of the data owner.[28] Obtaining clear and informed written consent ensures that *online* platform providers use personal information in a manner consistent with user expectations and not excessive or unnecessary. Furthermore, obtaining consent is crucial in protecting users' privacy rights and preventing the misuse of personal information. Consent requirements provide a legal framework for users to exercise their privacy rights and control their personal information. By obtaining consent, *online* platform providers can ensure that personal information is collected, used, and disclosed in a transparent, accountable, and ethical manner.

Obtaining consent is a crucial aspect of data protection and privacy laws that must be clearly explained and linked to all aspects of data usage. This concept plays a fundamental role in ensuring that users have control over their personal information. *Online* platform providers must obtain explicit and informed consent in a clear and understandable manner, and ensure that users remain informed about the use of their personal information. Consent requirements ensure that personal information is collected, used, and disclosed in a proportional, necessary, transparent, and ethical manner.

[26] Vrinda Bhandari and Renuka Sane, "Protecting Citizens From the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018," *Socio Legal Review* 14, no. 2 (October 2018): 143–69.

[27] Tharuka Rupasinghe, Frada Burstein, and Carsten Rudolph, "Blockchain Based Dynamic Patient Consent: A Privacy-Preserving Data Acquisition Architecture for Clinical *Data analytics*," in *40th International Conference on Information Systems, ICIS 2019*, 2019.

[28] Martin Abrams et al., "Artificial Intelligence, Ethics, and Enhanced Data Stewardship," *IEEE Security and Privacy* 17, no. 2 (2019): 17–30, https://doi.org/10.1109/MSEC.2018.2888778.

From a legal perspective, failure to provide transparency and obtain consent can essentially result in significant legal and reputational consequences for *online* platform providers. The legal framework for the protection of personal data essentially imposes strict requirements on *online* platform providers regarding the collection, use, and disclosure of personal information. Failure to comply with these requirements can result in fines, penalties, and legal liability for *online* platform providers. Furthermore, failure to respect user privacy rights can result in reputetional damage and loss of consumer trust, which can have long-term consequences for *online* platform providers.

In general, the concept transparency and consent are paramount to ensuring the lawful and ethical use of *data analytics*. *Online* platform providers that collect, use, and disclose personal information for *data analytics* purposes must comply with applicable privacy laws and ensure that users are aware of and have control over their personal information. Failure to do so can result in significant legal and reputational consequences for *online* platform providers.

Legal Issues and Normative Limitations in Regulation Regarding *Data analytics*

There are several common legal challenges that arise in the context of using *data analytics* and personal information, particularly related to transparency and consent. One of the most significant challenges is ensuring that *online* platform providers provide adequate transparency about their *data analytics* practices. This includes providing clear and concise information about what data is collected, how that data is used, and to whom the data is disclosed. Failure to provide adequate transparency can result in legal challenges, such as issues regarding the inconsistency of data collection and usage practices with the claims made by *online* platforms that use *data analytics* to provide specifically targeted advertisements to certain users.[29]

Another common legal challenge is obtaining valid consent from individuals.[30] Providers of various forms of *online* platforms must ensure that consent is obtained in a clear, understandable, and specific manner for the purpose of using personal information. Consent should also be given freely, meaning that individuals as users of an *online* platform should be able to refuse to give their consent without facing negative consequences. Failure to obtain valid consent can result in legal challenges, such as claims of unauthorized access to personal information or violations of data protection and privacy laws.

Furthermore, there are legal challenges related to the scope of consent. *Online* platform providers must ensure that consent is not overly broad, meaning that the

[29] Dorota Habrat, "Legal Challenges of Digitalization and Automation in the Context of Industry 4.0," in *Procedia Manufacturing*, vol. 51, 2020, 938–42, https://doi.org/10.1016/j.promfg.2020.10.132.

[30] Maja Nišević, "A Study on the Personal Data Processing and the UCPD Focused on Italy, Germany and the UK," *Maastricht Journal of European and Comparative Law* 28, no. 1 (2021): 7–29, https://doi.org/10.1177/1023263X20961493.

consent is specific to the purpose of using personal information. This can conflict with the context of *data analytics*, where personal information can be used for various purposes. *Online* platform providers must also ensure that users are informed of any changes in the purpose of using their personal information, and that they have the opportunity to withdraw their consent if they do not agree with these changes. In other words, there must be clear consistency in the purpose of data usage, in line with the statements provided to *online* platform users when requesting consent.[31]

As a consequence of the aforementioned issues, there are also issues related to accountability and enforcement. *Online* platform companies must be able to demonstrate that they have obtained valid consent and provided adequate transparency about their *data analytics* practices. There needs to be good coordination between legislative bodies and the public so that the government can investigate complaints or initiate legal enforcement actions against companies that fail to comply with data protection and privacy laws. Companies may also face legal challenges, such as class action lawsuits, if it is found that they have violated the privacy rights of consumers or users of their platforms.

Overall, ensuring transparency and obtaining valid consent are important aspects of data protection and privacy laws. *Online* platform providers that fail to provide transparency or obtain valid consent may face legal challenges and enforcement actions, as well as damage to their reputation and customer trust. Companies using *data analytics* must be proactive in addressing these legal challenges and implementing effective privacy and data protection policies and practices.

Furthermore, there are normative limitations related to transparency and consent within the legal framework for the protection of personal data in Indonesia. Transparency requires various *online* platform providers that use *data analytics* to be transparent about the data they collect, how they use it, and with whom they share it. Indonesia uses Law No. 27 of 2022 on Personal Data Protection (PDP Law) as the main legal source that regulates how personal data is collected, processed, and utilized. The PDP Law emphasizes the importance of transparency in processing personal data, through Article 27 which states that "the Personal Data Controller is obligated to process Personal Data in a limited and specific manner, legally valid, and transparent."

It's then further explained in the explanation of Article 27 of the PDP Law, that "transparency means that the processing of Personal Data is carried out by ensuring that the Personal Data Subject is aware of the Personal Data being processed and how the Personal Data is being processed, as well as any information and communication related to the processing of Personal Data that is easily accessible and understood, using clear language."

[31] Duc Bui et al., "Consistency Analysis of Data-Usage Purposes in Mobile Apps," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2021, 2824–43, https://doi.org/10.1145/3460120.3484536.

Article 16 paragraph (2) letter a also regulates the same matter, but with a focus on the collection process. It states that "the collection of Personal Data is carried out in a limited and specific manner, legally valid, and transparent." Overall, the concept of transparency has been well-reflected with various regulations found in the PDP Law, including regulations that do not explicitly mention the terms "transparency" or "transparent", but regulate the importance of notifying data owners about various collection and processing processes that will be carried out using their data. This is in line with the concept of transparency, which is essentially designed to ensure that users have a clear understanding of how their personal information is being used and can make informed decisions about whether to provide it or not.

However, the criminal provisions related to the concept of transparency are unfortunately not directly related to the criminal provisions in the PDP Law regarding responsibility for data transparency. Article 67 paragraph (1) only regulates the collection of personal data that is normatively illegal. Article 67 paragraph (1) jo. Article 16 paragraph (2) letter a state "Article 67: Anyone who intentionally and unlawfully obtains or collects Personal Data that does not belong to them with the intention of benefiting themselves or others that can cause harm to the Personal Data Subject as referred to in Article 65 paragraph (1) is punishable by imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp5.000.000.000,00 (five billion rupiah). Article 16 paragraph (2) letter a: (2) Processing of Personal Data as referred to in paragraph (1) is carried out in accordance with the principle of Protection of Personal Data, which includes "Personal Data is processed in a limited and specific manner, lawful, and transparent." The PDP Law does not regulate accountability regarding data misuse, particularly those that do not conform to the information provided as part of fulfilling the transparent aspect as mentioned in Article 16 paragraph (2) letter a.

The next normative limitation related to *data analytics* is the requirement for consent. This means that data owners must give their consent before their personal information can be collected, used, or shared for *data analytics* purposes. This requirement is designed to give users control over their personal information and to ensure that their privacy rights are respected. The PDP Law regulates consent in detail, beginning with Article 20 paragraph (2) which states, "(2) The basis for processing Personal Data as referred to in paragraph (1) includes explicit, valid consent from the Data Subject for one or more specific purposes communicated by the Personal Data Controller to the Data Subject".

Furthermore, the same regulation describes its elements through Article 20 paragraph (1) which reads, "(1) In the case of processing Personal Data based on consent as referred to in Article 20 paragraph (2) letter a, the Personal Data Controller is required to provide Information regarding 1) the legality of processing Personal Data; 2) the purpose of processing Personal Data; 3) the type and relevance of Personal Data to be processed; 4) the retention period of documents containing Personal Data; 5) details of Information on the processing period of Personal Data; and 6) the rights of the Data Subject."

This regulation actually stems from the concept of transparency, which is reflected in the form of an agreement between the data collector and the data owner. However, it is not explained what obligations the data collector must fulfill. Assuming that this refers to the regulations contained in this legislation, the agreement on the consent of data collection and processing can easily be manipulated to only benefit the data processor. In addition, there is still a legal vacuum regarding the accountability of the misuse of data collected lawfully, as it is not discussed in the criminal provisions of the PDP Law as previously explained.

The biggest normative problem of the PDP Law is the lack of detailed regulation regarding the highly technical aspects of data collection and processing in various digital spaces. *Data analytics* can provide highly accurate information about consumer behavior and interests by using data that indicates such behavior. Such data is typically found in the form of cache and cookies.[32] Cache stores various types of files from browsers or specific devices to speed up and facilitate the process of opening an *online* platform at a later time,[33] while cookies make tracking mechanisms easier by providing location information, browsing history, and improving the performance of various additional features available on an *online* platform.[34] It is essential that highly technical regulations related to such matters are included in the PDP Law, given that it is a newly enacted regulation. Through the PDP Law, the Indonesian government has missed the opportunity to improve privacy standards in Indonesia, which are becoming increasingly complex due to the growing reliance on data in the digital economy.

There are also other normative limitations that apply to the use of *data analytics* in Indonesia. For instance, *online* service providers are required to ensure that the personal information they collect is accurate, relevant, and up-to-date. They must also take appropriate measures to protect personal information from unauthorized access, use, or disclosure. Conceptually, transparency and consent also remain influential in this regard, as users whose data is used in *data analytics* must be informed.

Overall, normative limitations on transparency and consent in the use of *data analytics* in Indonesia are designed to protect the privacy rights of users and ensure that their personal information is not misused or abused. *Online* platform providers that utilize *data analytics* must be aware of these limitations and ensure that they comply with them to avoid legal and reputational risks. Furthermore, effective law enforcement mechanisms regarding data protection in Indonesia are still lacking.

[32] Liu and Greene, "The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination."

[33] Mulki Indana Zulfa, Rudy Hartanto, and Adhistya Erna Permanasari, "Caching Strategy for Web Application – a Systematic Literature Review," *International Journal of Web Information Systems* 16, no. 5 (January 2020): 545–69, https://doi.org/10.1108/IJWIS-06-2020-0032.

[34] Rienties Bart et al., "Effective Usage of Learning Analytics: What Do Practitioners Want and Where Should Distance Learning InBart, R., Olney, T., Nichols, M., & Herodotou, C. (2020). Effective Usage of Learning Analytics: What Do Practitioners Want and Where Should Distance Le," *Open Learning* 35, no. 2 (2020): 178–95, https://doi.org/10.1080/02680513.2019.1690441.

Government agencies responsible for enforcing data protection regulations often lack the necessary resources and expertise to do so effectively. This results in a lack of accountability among *online* platform providers, and the interests of individual users of such platforms become threatened.

Strategies to Protect the Interests of *Online* Platform Users in the Use of *Data analytics*

As the trend of using *data analytics* in various industries in Indonesia continues to grow, there is increasing concern about privacy and ethical implications of collecting and using personal data. In Indonesia, this issue is further complicated by the lack of comprehensive regulations and guidelines related to data protection that complexly regulate the use of *data analytics*. However, there are strategies that can be applied to address this issue and ensure the protection of personal data and privacy. Two important strategies are transparency and consent.

The use of *data analytics* from the perspective of users of various *online* platforms can pose a number of potential dangers that should be carefully considered. One prominent risk involves the possibility of exploitation of personal information by immoral individuals. Given the large amount of data collected, customers may find that their sensitive data, such as financial information, social security numbers, or health records, can be accessed without their knowledge or consent. This can lead to a series of harmful outcomes, including identity theft, financial fraud, or other dangerous activities.[35]

Another risk of *data analytics* is the potential for generating inaccurate or misleading insights, which can negatively impact customer decision-making. The use of incorrect or incomplete data sets, faulty algorithms, or other technical disruptions can result in misinterpretations of customer behavior, preferences, or needs.[36] This can lead businesses to make ill-informed decisions that harm their customers, such as recommending unsuitable products, offering suboptimal services, or providing misleading advertisements. This issue is particularly relevant given the widespread use of Big Data as the primary source of *data analytics*, which technically utilizes vast amounts of data and is therefore susceptible to data interpretation errors if not carefully verified by those carrying out the process.

Furthermore, there are concerns about the potential of *data analytics* to undermine privacy and autonomy. *Online* platform users may feel that their personal data is being used without their knowledge or consent, or that they are the targets of unfair data collection schemes based on their data profiles. This can erode trust from a business perspective and damage the ability of *online* platform providers to build long-

[35] Ben Falchuk, Shoshana Loeb, and Ralph Neff, "The Social Metaverse: Battle for Privacy," *IEEE Technology and Society Magazine* 37, no. 2 (2018): 52–61, https://doi.org/10.1109/MTS.2018.2826060.

[36] Mohammad I. Merhi and Klajdi Bregu, "Effective and Efficient Usage of Big *Data analytics* in Public Sector," *Transforming Government: People, Process and Policy* 14, no. 4 (2020): 605–22, https://doi.org/10.1108/TG-08-2019-0083.

term relationships with their users, which then impacts revenue from advertising, the primary source of income for various forms of *online* platforms.[37]

Overall, although *data analytics* offers many potential benefits for businesses and customers, it is crucial to recognize and address potential risks involved. By adopting transparent and ethical practices for data collection, analysis, and use, businesses can build trust with their customers and foster a culture of responsible data management.[38] There are several strategies that can be applied to address normative limitations related to *data analytics* and privacy in Indonesia.

The most important thing to do is to increase awareness and promote education. Efforts should be made to raise awareness among users and *online* platform providers about data protection and the importance of safeguarding personal data. This can be achieved through education and training programs that equip users with the knowledge and skills needed to protect their personal data. Enhancing enforcement mechanisms: To ensure compliance with data protection regulations, it is important to have effective enforcement mechanisms. This can be achieved by empowering government agencies responsible for enforcing data protection regulations, with the necessary resources and expertise.[39] With increased awareness of the importance of privacy among users of *online* platforms and the importance of compliance with privacy standards among *online* platform providers, Indonesia's legal culture in the field of personal data protection will automatically improve.

Building a culture of data protection is equally important. *Online* platform providers must prioritize data protection and embed it into their culture and values. This can be achieved by developing policies and practices that prioritize data protection and implementing training programs to educate employees on the importance of protecting personal data. The efforts to establish a strong legal culture regarding data protection are increasingly important in contemporary society.[40] As *online* platform providers collect, store, and use personal data in large amounts, the risks of data breaches and privacy violations increase accordingly. As a result, the development of a legal framework aimed at protecting data privacy becomes crucial. However, it is still unclear how the reputation of *online* platform providers correlates with their commitment to enhancing a legal culture related to data protection.

[37] Xin Zhang et al., "To Partner or Not to Partner? The Partnership Between Platforms and Data Brokers in Two-Sided Markets," *Information System Research* Ahead-of-p, no. Ahead-of-print (August 2022): 1–39, https://doi.org/10.2139/ssrn.4189518.

[38] Ram Mohan Rao P, S. Murali Krishna, and AP Siva Kumar, "Modern Privacy Threats and Privacy Preservation Techniques in *Data analytics*," in *Factoring Ethics in Technology, Policy Making, Regulation and AI*, 2021, https://doi.org/10.5772/intechopen.99160.

[39] Frauke Kreuter, Rayid Ghani, and Julia Lane, "Change Through Data: A *Data analytics* Training Program for Government Employees," *Harvard Data Science Review*, 2019, https://doi.org/10.1162/99608f92.ed353ae3.

[40] Xuanting Wu and Yi Chen, "Research on Personal Data Privacy Security in the Era of Big Data," *Journal of Humanities and Social Sciences Studies* 4, no. 3 (September 2022): 228–35, https://doi.org/10.32996/jhsss.2022.4.3.24.

On the one hand, *online* platform providers that value the importance of data protection and invest in a legal culture that respects it can gain a reputation as responsible and trustworthy entities. By implementing strong data protection policies and complying with relevant regulations, such companies can demonstrate their commitment to protecting personal data. In addition, companies that comply with the principles of data protection law can enhance their reputation by demonstrating ethical and socially responsible behavior, thus potentially attracting a customer base that values data protection.

On the other hand, *online* platform providers who prioritize profit over privacy can damage their reputation if they ignore data protection laws or experience data breaches. Negative publicity can quickly spread on social media and other *online* platforms, potentially damaging the company's reputation and eroding the trust of *online* platform users, who are essentially also consumers. Users may view a platform provider with a low compliance history regarding privacy as an unethical or untrustworthy service provider, resulting in loss of revenue and potential legal penalties for the platform provider.

Encouraging accountability is also a strategy that can improve the standards of personal data protection in Indonesia. *Online* platform providers should be encouraged to be transparent about their data collection and usage practices, so that they can be held accountable for any data protection violations. This can be achieved by implementing mechanisms to report and investigate privacy violations, as well as imposing penalties for non-compliance. This strategy requires an adequate normative framework, which includes technical issues that unfortunately have not yet been included in the personal data protection legal framework in Indonesia. Overall, implementing this strategy can help address the normative limitations related to *data analytics* and privacy in Indonesia, as well as ensure personal data protection and privacy for *online* platform users.

The Crucial Role of Transparency and Consent in Developing a Legal Framework for *Data analytics*

Typically, Indonesia can regulate emerging technologies through the development of with sector-specific frameworks. However, specific legal aspect of a particular emerging technology might need a more subtle approach. Transparency is an even more complex legal aspect to regulate, as it is often found as an important aspect of many utilizations of digital technology.[41] Transparency and consent are crucial in addressing the normative limitations related to *data analytics* and privacy in Indonesia. Here are some ways in which they can help: ***First***, increasing awareness and understanding of data privacy risks among the public: The public is essentially the primary subject in all efforts to protect personal data. As users of various *online* platforms, prevailing societal attitudes have a significant influence on various aspects

[41] Afif Noor and Dwi Wulandari, "Regulation of Sharia Information Technology-Based Peer-To-Peer Financing Services in POJK No. 10/POJK.05/2022," *ADLIYA: Jurnal Hukum Dan Kemanusiaan* 17, no. 1 (March 2023): 1–18. https://doi.org/10.15575/adliya.v17i1.21887

of life, including the technology industry. With increased public understanding of the dangers of data misuse and the importance of protection from such risks, there will be a growing demand in the technology industry related to all forms of data processing to improve data protection standards. This can lead to a culture of transparency and accountability, where *online* platform providers prioritize data protection in their operations, and users become more aware of their rights and how to protect their personal data.

Second, building trust: Transparency and consent can help build trust between users and *online* platform providers. When users know how their personal data is being used and have given consent, they are more likely to trust the *online* platform providers handling their data. This can lead to greater customer loyalty and enhance business relationships. By improving compliance standards in the context of data protection, the public as users of *online* platforms will be relieved of some of the anxieties that may arise from the risks associated with the continuous use of data in large volumes.

Third, legal compliance: In Indonesia, regulations regarding data protection are still in the process of development and implementation. By being transparent about data collection and usage practices and obtaining consent, *online* platform providers can ensure that they comply with existing regulations and avoid potential legal issues in the future. Legal compliance should be supported by more structured criminal provisions, particularly regarding the use of data, which is currently a normative gap in the PDP Law.

Fourth, improving data quality: When users give their consent to the use of their personal data, this can lead to improved data quality. Poor data quality can cause issues that can continue to grow as Big Data and data-sharing practices evolve, which can be used by other industries, such as the healthcare industry.[42] *Online* platform providers can collect more relevant and useful data, which can result in better decision-making processes and better business outcomes. The concept of transparency should be supported by clear normative structures regarding the quality and accuracy of collected and processed data. Improving data quality is primarily the responsibility of the *online* platform provider, and can be achieved by constantly innovating and improving service quality through technical server and storage enhancements.[43]

Fifth, minimizing risk: Transparency and consent can help minimize risks related to data protection violations. When users are informed about the collection and use of their data, they are more likely to detect and report any unauthorized or suspicious activities related to their personal data. This can help *online* platform

[42] Valentina Bellini, Jonathan Montomoli, and Elena Bignami, "Poor Quality Data, Privacy, Lack of Certifications: The Lethal Triad of New Technologies in Intensive Care," *Intensive Care Medicine* 47, no. 9 (2021): 1052–53, https://doi.org/10.1007/s00134-021-06473-4.

[43] N. Deepa et al., "A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions," *Future Generation Computer Systems* 131 (2022): 209–26, https://doi.org/10.1016/j.future.2022.01.017.

providers to respond quickly and prevent further damage. From the perspective of *online* platform providers, with the existence of transparency and consent mechanisms supported by clear legal frameworks, companies will be automatically driven to improve their data protection standards to minimize the risk of data breaches and other forms of violations that may occur as a result.[44]

Conclusion

Given Indonesia's entry into the digital economy era, it is important for the government to protect the interests of society in the digital spaces of Indonesia. This is increasingly relevant with the continuing development of various technologies that are becoming increasingly integrated into various aspects of people's lives. The development of technology, accompanied by the development of various forms and types of data that are constantly used, must be accompanied by adequate legal development. The use of *data analytics* is not yet fully embedded in the latest regulation related to data protection, namely the Personal Data Protection Law (PDP Law). Although the concept of transparency and consent is partially reflected in various regulations contained in the PDP Law, there are still important elements such as responsibility in the use of data and changes in the use of data that may differ from the consent obtained from users of an *online* platform. Analysis also found that another reason for the inability to fully fulfill the concept of transparency and consent is the absence of regulations regarding technical terms that need to be distinguished from the general meaning of "data" such as cache and cookies. Normative regulatory issues that are technical in nature like this need to be given more attention by the government because these forms of data are the main source of data used by *data analytics* in helping *online* platform providers provide relevant services and ads based on the behavior of users of the *online* platform.

References

Abrams, Martin, John Abrams, Peter Cullen, and Lynn Goldstein. "Artificial Intelligence, Ethics, and Enhanced Data Stewardship." *IEEE Security and Privacy* 17, no. 2 (2019): 17–30. https://doi.org/10.1109/MSEC.2018.2888778.

Alafaa, Princess. "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World." *SSRN Electronic Journal*, 2022, 1–12. https://doi.org/10.2139/ssrn.4005750.

Baik, Jeeyun (Sophia). "Data Privacy against Innovation or against

[44] Robert Steinbuch and Richard Peltz-Steele, "Ongoing Challenges In Researching Affirmative Action In Legal Education: Maximizing Public Welfare Through Transparency.," *Texas Hispanic Journal of Law & Policy* 25/26, no. 2/1 (2019): 57–84. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=144538040&site=ehost-live

Discrimination?: The Case of the California Consumer Privacy Act (CCPA)." *Telematics and Informatics* 52 (2020): 1–33. https://doi.org/10.1016/j.tele.2020.101431.

Bart, Rienties, Tom Olney, Mark Nichols, and Christothea Herodotou. "Effective Usage of Learning Analytics: What Do Practitioners Want and Where Should Distance Learning InBart, R., Olney, T., Nichols, M., & Herodotou, C. (2020). Effective Usage of Learning Analytics: What Do Practitioners Want and Where Should Distance Le." *Open Learning* 35, no. 2 (2020): 178–95. https://doi.org/10.1080/02680513.2019.1690441.

Bellini, Valentina, Jonathan Montomoli, and Elena Bignami. "Poor Quality Data, Privacy, Lack of Certifications: The Lethal Triad of New Technologies in Intensive Care." *Intensive Care Medicine* 47, no. 9 (2021): 1052–53. https://doi.org/10.1007/s00134-021-06473-4.

Bhandari, Vrinda, and Renuka Sane. "Protecting Citizens From the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018." *Socio Legal Review* 14, no. 2 (October 2018): 143–69.

Birnhack, Michael. "A Process-Based Approach to Informational Privacy and the Case of Big Medical Data." *Theoretical Inquiries in Law* 20, no. 1 (2019): 257–90. https://doi.org/10.1515/til-2019-0009.

Bui, Duc, Yuan Yao, Kang G. Shin, Jong Min Choi, and Junbum Shin. "Consistency Analysis of Data-Usage Purposes in Mobile Apps." In *Proceedings of the ACM Conference on Computer and Communications Security*, 2824–43, 2021. https://doi.org/10.1145/3460120.3484536.

Costa, Paulo, Ricardo Montenegro, Teresa Pereira, and Pedro Pinto. "The Security Challenges Emerging from the Technological Developments." *Mobile Networks and Applications* 24, no. 6 (December 2019): 2032–37. https://doi.org/10.1007/s11036-018-01208-0.

Deepa, N., Quoc Viet Pham, Dinh C. Nguyen, Sweta Bhattacharya, B. Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, and Pubudu N. Pathirana. "A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions." *Future Generation Computer Systems* 131 (2022): 209–26. https://doi.org/10.1016/j.future.2022.01.017.

Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. https://doi.org/10.37253/jjr.v24i2.7280.

———. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. https://doi.org/10.25072/jwy.v5i2.460.

Economides, Nicholas, and Ioannis Lianos. "Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective."

Journal of Competition Law and Economics 17, no. 4 (2021): 765–847. https://doi.org/10.1093/joclec/nhab007.

Falchuk, Ben, Shoshana Loeb, and Ralph Neff. "The Social Metaverse: Battle for Privacy." *IEEE Technology and Society Magazine* 37, no. 2 (2018): 52–61. https://doi.org/10.1109/MTS.2018.2826060.

Habrat, Dorota. "Legal Challenges of Digitalization and Automation in the Context of Industry 4.0." In *Procedia Manufacturing*, 51:938–42, 2020. https://doi.org/10.1016/j.promfg.2020.10.132.

Islah, Khikmatul. "Peluang Dan Tantangan Pemanfaatan Teknologi Big Data Untuk Mengintegrasikan Pelayanan Publik Pemerintah." *Jurnal Reformasi Administrasi: Jurnal Ilmiah Untuk …* 5, no. 1 (2018): 130–38.

Kreuter, Frauke, Rayid Ghani, and Julia Lane. "Change Through Data: A Data Analytics Training Program for Government Employees." *Harvard Data Science Review* 1, no. 2 (2019): 1–24. https://doi.org/10.1162/99608f92.ed353ae3.

Kurtz, Christian, Martin Semmann, and Tilo Böhmann. "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors." In *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, 2018.

Liu, Yang, and Connor Greene. "The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination." In *Digital Transformation in Business and Society: Theory and Cases*, 145–53, 2019. https://doi.org/10.1007/978-3-030-08277-2_9.

Livingstone, Sonia, Mariya Stoilova, and Rishita Nandagiri. "Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society." In *Aufwachsen in Überwachten Umgebungen*, 219–36, 2021. https://doi.org/10.5771/9783748921639-219.

Mariani, Marcello M., and Samuel Fosso Wamba. "Exploring How Consumer Goods Companies Innovate in the Digital Age: The Role of Big Data Analytics Companies." *Journal of Business Research* 121 (2020): 338–52. https://doi.org/10.1016/j.jbusres.2020.09.012.

Merhi, Mohammad I., and Klajdi Bregu. "Effective and Efficient Usage of Big Data Analytics in Public Sector." *Transforming Government: People, Process and Policy* 14, no. 4 (2020): 605–22. https://doi.org/10.1108/TG-08-2019-0083.

Mohan Rao P, Ram, S. Murali Krishna, and AP Siva Kumar. "Modern Privacy Threats and Privacy Preservation Techniques in Data Analytics." In *Factoring Ethics in Technology, Policy Making, Regulation and AI*, 1–10, 2021. https://doi.org/10.5772/intechopen.99160.

Nam, Taewoo. "Understanding the Gap between Perceived Threats to and Preparedness for Cybersecurity." *Technology in Society* 58 (August 2019): 1–10. https://doi.org/10.1016/j.techsoc.2019.03.005.

Nišević, Maja. "A Study on the Personal Data Processing and the UCPD Focused on Italy, Germany and the UK." *Maastricht Journal of European and Comparative Law* 28, no. 1 (2021): 7–29. https://doi.org/10.1177/1023263X20961493.

Niu, Yanfang, Limeng Ying, Jie Yang, Mengqi Bao, and C. B. Sivaparthipan. "Organizational Business Intelligence and Decision Making Using Big Data Analytics." *Information Processing and Management* 58, no. 6 (2021): 1–13. https://doi.org/10.1016/j.ipm.2021.102725.

Noor, Afif, and Dwi Wulandari. "Regulation of Sharia Information Technology-Based Peer-To-Peer Financing Services in POJK No. 10/POJK.05/2022." *ADLIYA: Jurnal Hukum Dan Kemanusiaan* 17, no. 1 (March 2023): 1–18. https://doi.org/10.15575/adliya.v17i1.21887

Ramírez, Maricela, Lázaro Rodríguez Ariza, María Elena Gómez Miranda, and Vartika. "The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index." *Sustainability* 14, no. 3 (January 2022): 1–23. https://doi.org/10.3390/su14031390.

Rehman, Arshia, Saeeda Naz, and Imran Razzak. "Leveraging Big Data Analytics in Healthcare Enhancement: Trends, Challenges and Opportunities." In *Multimedia Systems*, 28:1339–71, 2022. https://doi.org/10.1007/s00530-020-00736-8.

Rupasinghe, Tharuka, Frada Burstein, and Carsten Rudolph. "Blockchain Based Dynamic Patient Consent: A Privacy-Preserving Data Acquisition Architecture for Clinical Data Analytics." In *40th International Conference on Information Systems, ICIS 2019*, 1–9, 2019.

Sadeghi Darvazeh, Saeid, Iman Raeesi Vanani, and Farzaneh Mansouri Musolu. "Big Data Analytics and Its Applications in Supply Chain Management." In *New Trends in the Use of Artificial Intelligence for the Industry 4.0*, 1–26, 2020. https://doi.org/10.5772/intechopen.89426.

Setiawan, Yudy, and Anita Maharani. "Unboxing Employees Perspectives on Factors Affecting Their Compliance to Organizational Information Security Policies." In *SMARTCYBER 2021: Proceedings of 2nd International Conference on Smart Computing and Cyber Security*, 182–93, 2022. https://doi.org/10.1007/978-981-16-9480-6_17.

Steinbuch, Robert, and Richard Peltz-Steele. "Ongoing Challenges In Researching Affirmative Action In Legal Education: Maximizing Public Welfare Through Transparency." *Texas Hispanic Journal of Law & Policy* 25/26, no. 2/1 (2019): 57–84.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2022): 1443–57. https://doi.org/10.1108/JFC-09-2021-0193.

Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu*

Pengetahuan Sosial 8, no. 5 (2021): 2463–78.

Tsohou, Aggeliki, Emmanouil Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni, and Beatriz Gallego-Nicasio Crespo. "Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform." *Information and Computer Security* 28, no. 4 (2020): 531–53. https://doi.org/10.1108/ICS-01-2020-0002.

Wachter, Sandra. "The GDPR and the Internet of Things: A Three-Step Transparency Model." *Law, Innovation and Technology* 10, no. 2 (2018): 266–94. https://doi.org/10.1080/17579961.2018.1527479.

Widyadhana, Ayasha Nadira, Putu Wuri Handayani, and Pramitha Dwi Larasati. "Influence of Technological, Social, and Individual Factors on Security and Privacy Take-up of Digital Banking." In *2022 International Conference on Information Management and Technology (ICIMTech)*, 33–38. IEEE, 2022. https://doi.org/10.1109/ICIMTech55957.2022.9915231.

Wu, Xuanting, and Yi Chen. "Research on Personal Data Privacy Security in the Era of Big Data." *Journal of Humanities and Social Sciences Studies* 4, no. 3 (September 2022): 228–35. https://doi.org/10.32996/jhsss.2022.4.3.24.

Zhang, Xin, Lihong Cheng, Yugang Yu, and Yong Tan. "To Partner or Not to Partner? The Partnership Between Platforms and Data Brokers in Two-Sided Markets." *Information System Research* Ahead-of-p, no. Ahead-of-print (August 2022): 1–39. https://doi.org/10.2139/ssrn.4189518.

Zhang, Xin, Wei Thoo Yue, and Yugang Yu. "Compete, Cooperate, or Coopete? The Strategic Role of Data Analytics in Targeted Advertising." *SSRN Electronic Journal*, 2020. https://doi.org/10.2139/ssrn.3549642.

Zulfa, Mulki Indana, Rudy Hartanto, and Adhistya Erna Permanasari. "Caching Strategy for Web Application – a Systematic Literature Review." *International Journal of Web Information Systems* 16, no. 5 (January 2020): 545–69. https://doi.org/10.1108/IJWIS-06-2020-0032.

Zwitter, Andrej, and Jilles Hazenberg. "Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation." In *Blockchain, Law and Governance*, 87–97, 2021. https://doi.org/10.1007/978-3-030-52722-8_6.

[This page intentionally left blank]