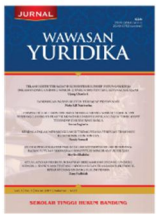
JURNAL

WAWASAN YURIDIKA

Vol. 7 | No. 1 | March 2023 | Page: 21-45

Nationally Accredited Journal Decree No. 36/E/KPT/2019, Dated 13rd December 2019

http://ejournal.sthb.ac.id/index.php/jwy



Enhancing Trade Secret Protection amidst E-commerce Advancements: Navigating the Cybersecurity Conundrum

Hari Sutra Disemadi[1], Henry Soelistyo Budi[2]

[1] Faculty of Law, Universitas Internasional Batam, Batam, Indonesia

2 Faculty of Law, Universitas Pelita Harapan, Jakarta, Indonesia

✉ Corresponding Author: hari@uib.ac.id

Info Artikel:

DOI: 10.25072/jwy.v7i1.608

Diterima: 26 January 2023 | Disetujui: 20 March 2023 | Dipublikasikan: 30 March 2023

Kata Kunci:

Cybersecurity; E-commerce; Intellectual Property; Trade Secrets.

Abstract

The e-commerce ecosystem has encompassed various aspects of life, giving rise to legal implications, particularly in the areas of intellectual property and personal data protection, which are now inseparable from Indonesia's economic system in the digital age. This research aims to elucidate the legal relationship between trade secrets as a crucial form of intellectual property to be safeguarded in the digital era and analyze Indonesia's legal capability to protect trade secrets amidst the escalating challenges of cybersecurity due to the widespread use of various forms of e-commerce. The research employs a normative legal research method to analyze the protection and legal certainty concerning trade secrets, which can be subject to unauthorized access or theft through cyberattacks. Utilizing a legislative approach, the research relies on secondary data in the form of primary legal sources. The findings of this research reveal political-legal issues and normative shortcomings in regulating e-commerce and trade secrets, often underestimating the digital threats that can harm individuals' intellectual property rights.

A. INTRODUCTION

The current development of technology has brought humanity to the stage of digitalization, which, in various aspects that support life, can be accessed digitally, and several daily activities can be shifted into digital form.[1] The grand goal of digitalization is to make everyone's daily activities a breeze, with the ambitious aim of boosting both social and economic mobility for tech-savvy individuals embracing this digital transformation. At the heart of this process lies the key to work wizardry – increasing work efficiency by empowering individuals with access to cutting-edge technologies to effortlessly juggle multiple

[1] Safira Dhea Fitriani *et al.*, "Digitalisasi Ekonomi Syariah Penerapan Hukum-Hukum Islam Dalam Jual Beli Online," *JURNAL EKONOMI SYARIAH* 6, No. 1 (2021): 51–59, https://doi.org/10.37058/jes.v6i1.2542., p. 52.

tasks and work processes, ultimately supercharging productivity levels.

The efficiency brought forth by digitalization, an inextricable aspect of modern daily life, has empowered individuals to interlink diverse activities and critical productivity factors within a network. A prime example of such interconnection is e-commerce, seamlessly integrating numerous social media platforms into its service framework.[2] Not only are products or services offered, but businesses can also utilize e-commerce as a medium for disseminating content, whether directly related to their business or not, thereby ultimately bolstering engagement of prospective consumers with the seller. Furthermore, this interconnected network system exhibits remarkable flexibility, as it can be implemented through e-commerce as the principal platform or via social media as the primary platform.

Digital services, an integral part of the global and Indonesian economic systems akin to traditional physical services, find their impetus in various elements. Notably, e-commerce stands out as a prime example, harnessing the power of data as one of its fundamental pillars.[3] Information or data stands as a vital cornerstone in the progression of knowledge, thereby wielding substantial influence over the growth of all technological endeavors borne from existing scientific advancements. Its pertinence becomes even more pronounced in the wake of rapid data processing systems like the Internet of Things (IoT) and Big Data, where information assumes a paramount role.[4] With the rapid evolution of data processing techniques and systems, the efficiency in managing vast amounts of data has significantly improved. This technological advancement gains momentum as it expedites the identification

---

[2] Sefiya Nur Farichin, "Pengaruh Digitalisasi Dalam Bidang E-Commerce Terhadap Perilaku Konsumtif Mahasiswa UIN Sunan Ampel," *JURNAL SOSIAL Jurnal Penelitian Ilmu-Ilmu Sosial* 23, No. 1 (2022): 34–39, https://doi.org/10.33319/sos.v23i1.108, p. 34.

[3] Ruilin Zhu, Aashish Srivastava, and Juliana Sutanto, "Privacy-Deprived e-Commerce: The Efficacy of Consumer Privacy Policies on China's e-Commerce Websites from a Legal Perspective," *Information Technology and People* 33, No. 6 (2020): 1601–26, https://doi.org/10.1108/ITP-03-2019-0117., p. 1620. This research does not explicitly state that data is the driving force behind e-commerce but rather highlights that cybersecurity significantly contributes to the development of e-commerce. Presently, data represents the key element and the primary object of protection within the cybersecurity domain. *See* Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7 (2021): 8176-8186, https://doi.org/10.1016/j.egyr.2021.08.126., p. 8183.

[4] Rahmi Ayunda and Rusdianto, "Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence Dalam Aktifitas Perbankan Di Indonesia," *Jurnal Komunikasi Hukum* 7, No. 2 (2021): 663–677, https://doi.org/10.23887/jkh.v7i2.37995., pp. 664-665.

of various legal issues, harnessing the power of abundant data resources. In the domain of e-commerce, data assumes an increasingly pivotal role, empowering e-commerce platforms to elevate service quality[5], gain profound insights into consumer behavior, and make well-informed decisions concerning targeted marketing strategies.[6]

The evolution of data relevance in the contemporary economic system, driven by digital technology, significantly amplifies the necessity to safeguard various forms of existing data. Within this context, cybersecurity emerges as an indispensable framework for protecting all types of data present in the digital network, playing a critical role in fostering the growth of the data-dependent e-commerce ecosystem. Much like information in the physical world, data in the digital realm is also susceptible to various attempts of theft and breaches, commonly referred to as cyberattacks. Consequently, cybersecurity serves as the digital world's defensive bulwark against ever-evolving cyber threats, paralleling the rapid advancements in knowledge and technology. The protection of data as the primary focal point stems from its inherent value, regardless of its scale. These values hold distinct commercial implications, particularly concerning digital services that store and leverage such data. In the context of e-commerce development, data intertwines with the factors influencing a country's economic progress, becoming inseparable from the growth of its economic system. Therefore, users of e-commerce platforms should be entitled to data protection related to their activities within these platforms, regardless of their roles as buyers or sellers.

Intellectual property rights, being a cornerstone of economic progress[7], have garnered unprecedented significance amidst the dawn of the digital economic era. The pervasive presence of diverse e-commerce services has become an integral part of Indonesian society, magnifying the importance of safeguarding intellectual

---

5 B. Palese and A. Usai, "The Relative Importance of Service Quality Dimensions in E-Commerce Experiences," *International Journal of Information Management* 40 (2018): 132–140, https://doi.org/10.1016/j.ijinfomgt.2018.02.001., p. 137.

6 Safa Kaabi and Rim Jallouli, "Overview of E-Commerce Technologies, Data Analysis Capabilities and Marketing Knowledge," in *Lecture Notes in Business Information Processing* 358 (2019): 183–193, https://doi.org/10.1007/978-3-030-30874-2_14, p. 176.

7 Hari Sutra Disemadi, "Contextualization of Legal Protection of Intellectual Property in Micro Small and Medium Enterprises in Indonesia," *LAW REFORM* 18, No. 1 (2022): 89–110, https://doi.org/10.14710/lr.v18i1.42568., p. 91.

property rights. Notably, these rights serve as a catalyst for stimulating the inventive spirit among all economic players within the system. As the digital economy unfolds and novel economic realms (digital spaces) emerge, the role of intellectual property rights takes on an even more paramount role. The proliferation of various forms of intellectual property rights violations underscores the pressing need to fortify and protect these rights diligently.

Cybersecurity assumes an indispensable role in upholding the sustainability of diverse e-commerce ecosystems, with direct implications for the prosperity and continuity of numerous enterprises. Given the considerable impact of e-commerce on Indonesia's economic landscape, safeguarding the fundamental tenets of e-commerce assumes paramount importance within the ambit of cybersecurity, a responsibility incumbent upon extant e-commerce service providers in Indonesia. Among these foundational tenets, intellectual property rights find themselves in a precarious position. The data stored and utilized across various e-commerce platforms may encompass elements protected under intellectual property rights, owing to their significant influence and pertinence in the creation or finalization of products offered through these platforms. This intricate interconnection underscores the indispensability of a multidimensional cybersecurity approach, one that not only shields buyers but also safeguards sellers, who serve as users of the e-commerce platform.

Numerous prior inquiries have been conducted to explore the significance of safeguarding intellectual property in the digital era, as accomplished through the evolution of legal systems in Indonesia. One such study revealed endeavors to adapt to the advancements in information technology, uncovering various intellectual property rights violations, particularly in the music industry. This research underscores the pressing need to adjust Indonesia's legal framework to effectively tackle these emerging challenges.[8] Another study delves into the intriguing phenomenon of the cultural development surrounding intellectual property rights violations. It uncovers that the proliferation

[8] Iin Indriani, "Hak Kekayaan Intelektual: Perlindungan Hukum Terhadap Hak Cipta Karya Musik," *Jurnal Ilmu Hukum* 7, No. 2 (2018): 246–263, http://dx.doi.org/10.30652/jih.v7i2.5703., p. 248.

of the intellectual property legal culture might adversely impact society's perception of law enforcement and the value of intellectual property protection in Indonesia.[9] Nevertheless, these investigations have yet to explore other critical challenges in the current digital era, most notably, the realm of cybersecurity and its intricate relationship with intellectual property rights, especially concerning trade secrets within Indonesia's legal system.

In this study, we will conduct a comprehensive examination of the literature gap to foster the development of cutting-edge concepts and analyses that can be instrumental for Indonesia in updating its existing legal framework. The aim is to effectively facilitate the advancement of technology, which wields a significant impact on society's way of life. Our analysis will delve deeply into the legal politics of cybersecurity within Indonesia, shedding light on the trajectory of legal development in the country and the government's level of awareness concerning cybersecurity challenges. Furthermore, this research will shed light on the pivotal role played by e-commerce in the advancement of intellectual property law and personal data protection within Indonesia. Subsequently, we will integrate both conceptual analyses with normative analysis, meticulously exploring the norms embedded within the normative structure of the legal framework pertaining to trade secrets and cybersecurity in Indonesia. The primary objective here is to identify any gaps and normative limitations that might pose implications for trade secret protection amidst the burgeoning growth of e-commerce. Through this study, we aspire to furnish Indonesia with valuable insights, thereby facilitating the refinement of its legal landscape to adapt effectively to the ever-evolving technological landscape and its influence on society.

B. RESEARCH METHODS

This research constitutes a doctrinal inquiry with the primary objective of examining the correlation between cybersecurity and the safeguarding of intellectual property amid the rapid growth of the digital economy in Indonesia. To undertake this analysis, the study employs normative legal methodologies to delve into

[9] Muhammad Deovan Reondy Putra and Hari Sutra Disemadi, "Counterfeit Culture Dalam Perkembangan UMKM: Suatu Kajian Kekayaan Intelektual," *KRTHA BHAYANGKARA* 16, No. 2 (2022): 297–314, https://doi.org/10.31599/krtha.v16i2.1151., p. 307.

the existing statutory laws in Indonesia and to scrutinize the normative framework that establishes the link between cybersecurity and intellectual property rights within the country's legal system. The research adopts a legislative approach and primarily relies on secondary data sourced from essential legal documents. Among the pivotal regulations utilized in this study are: Law No. 30 of 2000 on Trade Secrets; Law No. 11 of 2008 on Electronic Information and Transactions; Law No. 19 of 2016, which serves as an amendment to Law No. 11 of 2008 on Electronic Information and Transactions; Law No. 27 of 2022 pertaining to Personal Data Protection; Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions; and Minister of Communication and Information Technology Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems. The research is based on a comprehensive literature review to gather the requisite secondary data and legal materials. Subsequently, a qualitative descriptive analysis is applied to ensure precision in drawing conclusive insights. By utilizing these methods, this study aims to contribute significantly to the understanding of the intricate relationship between cybersecurity and the protection of intellectual property in the context of Indonesia's evolving digital landscape.

C. RESULTS AND DISCUSSIONS

1. The Legal Landscape of Cybersecurity in Indonesia

Cybersecurity emerges as a paramount response to the multifaceted challenges stemming from the relentless process of digitalization, which continues to permeate every aspect of our daily lives. In essence, Cybersecurity encompasses the proactive measures and defensive strategies employed to shield systems, networks, and software applications from insidious digital attacks. These malevolent cyber-attacks invariably strive to obtain unauthorized access, manipulate or obliterate sensitive information, extort financial gains from unsuspecting users, or wreak havoc on normal business operations.[10] The term "Cybersecurity" significantly expands upon the conventional notion of "security" or "keamanan" in Indonesian, attuned to the evolving landscape of digital technology,

[10] Basie von Solms and Rossouw von Solms, "Cybersecurity and Information Security–What Goes Where?," *Information and Computer Security* 26, No. 1 (2018): 2–9, https://doi.org/10.1108/ICS-04-2017-0025., p. 6.

and signifies a comprehensive array of endeavors directed towards safeguarding invaluable assets within the intricate fabric of digital networks.

In the realm of legal academia, cybersecurity encompasses a comprehensive array of endeavors aimed at countering diverse manifestations of criminal conduct in the digital realm. Its focal objective lies in thwarting attempts to breach the fortified boundaries of digital networks, which harbor vital and confidential information safeguarded by robust network systems. The essence of cybersecurity's protective framework centers on fortifying against cyberattacks, particularly concerning the identification and understanding of the motives driving such assaults on data and information integrity.

Cybersecurity poses a multifaceted and intricate dimension due to its technical intricacies. Within the legal framework of Indonesia, the realm of cybersecurity lacks a singular, all-encompassing regulation dedicated solely to addressing cyber safety and its nuances. Instead, Indonesia has multiple regulations that pertain to distinct facets of cybersecurity, each catering to the safeguarding of specific elements within the cyber domain. This discourse primarily delves into the sphere of data protection, shedding light on the pertinent matters at hand.

Data protection represents a tangible legal response to actions that target specific objectives, constituting a defensive mechanism against hacking activities.[11] In Indonesia, the legal framework governing data protection is referred to as "the use of personal data", and it has been in effect since 2008, established within the provisions of Law No. 11 of 2008 concerning Electronic Information and Transactions. This law explicitly addresses the safeguarding of personal data in Article 26, paragraph (1), which stipulates that "Unless otherwise mandated by the Legislation, the utilization of any information concerning an individual's Personal Data through electronic media must be conducted with the explicit consent of the affected individual". The provisions within this article not only govern the use of personal data but also underscore the criticality of

[11] Ilya Kabanov and Stuart Madnick, "Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense," *MIS Quarterly Executive* 20, No. 2 (2021): 109–125, https://doi.org/10.17705/2msqe.00044., pp. 112-118.

obtaining informed consent from the concerned individuals.[12]

The normative clarity of Article 26 paragraph (1) presents a significant challenge, as it fails to elucidate the term "orang yang bersangkutan" (the individual concerned). This lack of specificity holds profound implications, considering the intricate interplay of personal data within network systems employed for data storage and service execution. The entanglement of one's personal data with that of others is highly plausible, leading to an interdependence of data ownership among individuals. Moreover, the proliferation of data servers, adept at accumulating and classifying vast amounts of information, accentuates the visibility of this interconnected data. These data repositories are extensively utilized across diverse digital services throughout Indonesia. As such, the need for a comprehensive legal framework addressing data ownership becomes increasingly paramount to elevate the significance of cybersecurity in contemporary digital society.[13] Hence, data ownership stands as a paramount aspect within data regulation, seeking to forge a robust legal framework that elevates the paramountcy of cybersecurity in the contemporary digital era of society.[14]

The legal ramifications of cybersecurity go beyond the scope of this law and are further elucidated in Article 32 paragraphs (2) and (3). Paragraph (2) stipulates that any individual who intentionally and without authorization, or in violation of the law, transfers Electronic Information and/or Electronic Documents to another person's Electronic System without proper authority commits an offense. On the other hand, paragraph (3) addresses situations where such actions as described in paragraph (1) lead to the exposure of confidential Electronic Information and/or Electronic Documents, allowing public access with compromised data integrity. While this law addresses data regulation and its implications concerning cybersecurity, it highlights certain normative ambiguities

[12] Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridikta* 5, No. 2 (2021): 177–199, http://dx.doi.org/10.25072/jwy.v5i2.460., pp. 184-185.

[13] Wisnu Prabowo, Satriya Wibawa, and Fuad Azmi, "Perlindungan Data Personal Siber Di Indonesia," *Padjadjaran Journal of International Relations* 1, No. 3 (2020): 218–239, https://doi.org/10.24198/padjir.v1i3.26194., pp. 232-233.

[14] Lailatur Rahmi and Guruh Tri Nugroho, "Kepemilikan Data Di Universitas : Salah Satu Isu Dalam Kebijakan Informasi," *Shaut Al Maktabah* 8, No. 2 (2017): 155–168, https://doi.org/10.15548/shaut.v9i2.114., p. 167.

that necessitate clarification for bolstering the implementation of a more comprehensive cybersecurity system in Indonesia.

Moreover, the provisions of the aforementioned law underwent revision through Law No. 19 of 2016, which pertains to Amendments to Law No. 11 of 2008 on Electronic Information and Transactions. Notably, Article 26 of the ITE Law was augmented with the addition of three paragraphs, as follows (1) Every Electronic System Provider is under an obligation to expunge irrelevant Electronic Information and/or Electronic Documents under their control upon the request of the concerned party, subject to a court order, (2) Every Electronic System Provider is mandated to establish a mechanism for the deletion of Electronic Information and/or Electronic Documents that are no longer relevant, in strict accordance with the prevailing laws and regulations, and (3) The procedures governing the deletion of Electronic Information and/or Electronic Documents, as referred to in paragraphs (3) and (4), shall be regulated by the government. These enhancements to Article 26 are praiseworthy as they bestow data owners with increased authority over the storage and utilization of their data. The supplementary regulatory provisions are replete with elements for effective implementation, particularly concerning technical aspects pertaining to data control and deletion mechanisms.

The inclusion of these normative constructs showcases the government's steadfast commitment to shaping concrete legal policies concerning cybersecurity and data protection. This commitment is further elucidated through the enactment of Government Regulation No. 71 of 2019, which centers on the implementation of Electronic Systems and Transactions and emphasizes adherence to the legal principles outlined in the ITE Law, particularly those related to data processing and protection.[15] The regulations pertaining to Article 26 of the ITE Law are enshrined in Article 14, encompassing paragraphs (3) to (6), which encompass the following key points: "(3) Personal Data processing must adhere to the prerequisite of obtaining valid consent from the Data Subject, specifying one or multiple specific purposes that have

[15] Muhamad Hasan Rumlus and Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik," *Jurnal HAM* 11, No. 2 (2020): 285-299, https://doi.org/10.30641/ham.2020.11.285-299., pp. 294-295.

been duly communicated to the Data Subject, (4) In addition to the consent mentioned in paragraph 3, Personal Data processing must meet necessary requirements to fulfill contractual obligations, should the Data Subject be a party to an agreement, or to comply with the Data Subject's explicit request during the agreement's formation. Moreover, the processing must align with the legal obligations of the Personal Data Controller, as stipulated in the prevailing laws and regulations. It must also serve the protection of the Data Subject's legitimate interests (vital interest), implement the authority of the Personal Data Controller in accordance with the prevailing legal provisions, fulfill obligations of the Personal Data Controller in public services for the public interest, and/or meet other legitimate interests of the Personal Data Controller and/or Data Subject, (5) In the unfortunate event of any breach leading to the inadequate protection of Personal Data under their management, the Electronic System Provider must promptly communicate this incident to the Data Subject in written form, and (6) Technical aspects pertaining to the processing of Personal Data are governed and guided by the provisions set forth in the prevailing laws and regulations".

The incorporation of Article 14 introduces a novel term in the domain of personal data governance, known as the "data controller," representing an evolution in data processing systems. This progressive development reflects the government's keen interest in the transformation of data processing methods. This normative framework serves as the foundational concept for defining the authority and obligations of data controllers, encompassing the legal responsibilities arising from the diverse digitization processes prevalent in Indonesian society.[16] Additionally, this regulation is intrinsically linked to paragraph (5), which specifically addresses instances of data breach and protection lapses. Significantly, this marks the first instance within Indonesia's legal framework wherein the explicit regulation of data controller's responsibilities in ensuring data security is enshrined. In essence, it mandates data controllers to institute robust cybersecurity systems to safeguard personal data effectively.

[16] Nurhidayati, Sugiyah, and Kartika Yuliantari, "Pengaturan Perlindungan Data Pribadi Dalam Penggunaan Aplikasi Pedulilindungi," *Widya Cipta: Jurnal Sekretari dan Manajemen* 5, No. 1 (2021): 39–45, https://doi.org/10.31294/widyacipta.v5i1.9447., p. 40.

The landscape of cybersecurity regulation in Indonesia is undergoing dynamic changes, mirroring the swift advancement of digitalization, which has been further expedited by the COVID-19 pandemic. The pandemic has acted as a catalyst, propelling all sectors of society to embrace digital technologies, aiming to curtail physical interactions and mitigate the spread of COVID-19. At present, the latest regulation that prominently delves into cybersecurity concerns, with a specific focus on establishing a robust data protection framework as a vital component of cybersecurity, is Law No. 27 of 2022 on Personal Data Protection (PDP Law).

The provisions within the PDP Law signify a notable advancement in the concept of data controller accountability, encompassing supplementary regulations pertaining to failures in safeguarding personal data, as stipulated in Article 46. According to this article, "In the event of a failure in Personal Data Protection, the Personal Data Controller is mandated to provide written notification within 3 x 24 (three times twenty-four) hours to the Data Subjects and relevant Authorities. The written notification, as mentioned in paragraph (1), shall contain essential information, including details of the disclosed Personal Data, the circumstances surrounding the disclosure, and the measures undertaken by the Personal Data Controller to address and recover from the data breach. Furthermore, in certain situations, the Personal Data Controller must also inform the public about the failure in Personal Data Protection". These regulations, encompassed in the recent data protection legislation, elevate the level of complexity concerning data controller's accountability and responsibilities in the event of cybersecurity failures within digital services, with a particular focus on prioritizing public interests, as explicitly stated in paragraph (3) as "the public". Such regulations hold great relevance to the ongoing development of digital technology, which has become deeply intertwined with people's lives in the digital era. As various segments of society have significantly heightened their digital literacy, driven by the adaptation to social and economic functions through accelerated digitalization processes, advanced knowledge, effective data management, and the necessity to adapt due to the COVID-19 pandemic have

played pivotal roles in shaping the current landscape.[17]

The longstanding normative ambiguity surrounding the definition and legal framework of "failure in personal data protection" in Indonesia's data protection laws has finally been elucidated through the explanation found in Article 46, paragraph (1). It states: "The term 'failure in Personal Data Protection' refers to the inadequacy in safeguarding an individual's Personal Data concerning confidentiality, integrity, and availability. This encompasses both deliberate and unintended security breaches, which may result in the destruction, loss, alteration, disclosure, or unauthorized access to the transmitted, stored, or processed Personal Data". This clarification is indeed praiseworthy as it offers a lucid comprehension of the elements constituting a failure in protecting personal data, while also integrating the notion of "security." This fortifies the interconnection between personal data protection and cybersecurity as crucial components in data protection within the digital era.

The dynamic progression of the legal framework concerning cybersecurity, with a specific focus on data protection, demonstrates the rapid and accelerating development of strong normative constructs. This remarkable advancement represents a praiseworthy response to the increasing legal requirements driven by the ever-expanding integration of digitalization into all facets of societal existence.

2. E-commerce: The Key Catalyst for Advancing Intellectual Property Law and Personal Data Protection in Indonesia

The pervasive influence of information technology extends to various facets of life, particularly in the realm of business. The rapid development of information technology has revolutionized the selling and marketing of goods and services, eradicating spatial, temporal, and distance barriers. Information technology's prowess in disseminating diverse data forms, including texts, graphics, audio, video, and animations, has led to profound transformations in the economic and business sectors. A noteworthy manifestation of information technology in

[17] Iqbal Faza Ahmad, "Urgensi Literasi Digital Di Indonesia Pada Masa Pandemi COVID-19: Sebuah Tinjauan Sistematis," *Nusantara: Jurnal Pendidikan Indonesia* 2, No. 1 (2022): 1–18, https://doi.org/10.14421/njpi.2022.v2i1-1., p. 4.

the business landscape is electronic commerce (e-commerce). In parallel with the continuous strides in information technology, the realm of business is witnessing a surge in competitive allure. This competition transcends the confines of traditional offline markets and thrives in the domain of online markets as well. As a result, business stakeholders find themselves engaged in intense competitive rivalries. Consequently, enterprises of all sizes are urged to cultivate creativity, foster innovation, and consistently deliver top-tier products to compete effectively and elevate overall business competitiveness.[18] Beyond mere product orientation, companies must strategically contemplate approaches to attain their objectives, as a growing number of prominent corporations presently harness the potential of the internet or the widely known e-commerce platform.

E-commerce stands as a remarkable reflection of the digital transformation within society, bringing forth significant implications.[19] It has firmly ingrained itself in Indonesia's economic framework.[20] As an ever-evolving product of continuous societal digitalization, e-commerce offers a wealth of opportunities for Indonesia's economy, seamlessly integrating into business operations. As a result, e-commerce has become an indispensable component, particularly for Micro, Small, and Medium Enterprises (MSMEs), which constitute the prevailing business scale in Indonesia.[21] Leveraging user-friendly technology, e-commerce has fostered financial inclusivity among Indonesian business stakeholders, empowering enterprises of all sizes to effectively compete in marketing and vending top-tier products, alongside long-established corporations that have historically dominated both local and global markets.[22]

Various forms of elements, opportunities, and other influencing factors

---

[18] Melisa Setiawan Hotana, "Industri E-Commerce Dalam Menciptakan Pasar yang Kompetitif Berdasarkan Hukum Persaingan Usaha," *Jurnal Hukum Bisnis Bonum Commune* 1, No. 1 (2018): 28-38, https://doi.org/10.30996/jhbbc.v0i0.1754., p. 29.

[19] Margaretha Rosa Anjani and Budi Santoso, "Urgensi Rekonstruksi Hukum E-Commerce di Indonesia," *LAW REFORM* 14, No. 1 (2018): 89-103, https://doi.org/10.14710/lr.v14i1.20239., p. 90-91.

[20] Imam Lukito, "Tantangan Hukum dan Peran Pemerintah Dalam Pembangunan E-Commerce," *Jurnal Ilmiah Kebijakan Hukum* 11, No. 3 (2017): 349–67, http://dx.doi.org/10.30641/kebijakan.2017.V11.349-367., p. 351.

[21] Moh. Kurdi *et al*., "The Government's Role in MSMEs Development Through E-Commerce in Sumenep Regency," in *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021*, (2021): 1–5, https://doi.org/10.4108/eai.6-3-2021.2306388., pp. 1-2.

[22] Florentina Kurniasari, Ardi Gunardi, Farica Perdana Putri, and Andy Firmansyah, "The Role of Financial Technology to Increase Financial Inclusion in Indonesia," *International Journal of Data and Network Science* 5, No. 3 (2021): 391–400, https://doi.org/10.5267/j.ijdns.2021.5.004., pp. 393-394.

in e-commerce play a critical role and require constant monitoring due to their direct impact on Indonesian society. The significant influence of e-commerce on society necessitates a vigilant observation of its development. It becomes evident that all aspects influencing e-commerce development encounter distinct challenges, stemming from the multidimensional nature of its integration into society's life. As e-commerce becomes increasingly inseparable from daily life, it intertwines with societal factors, each presenting its unique set of challenges.

The continuous monitoring of various elements, opportunities, and factors that shape e-commerce is crucial as they directly affect society, considering the substantial impact of e-commerce on the lives of Indonesians today. A closer examination of e-commerce development reveals that these elements, opportunities, and influencing factors encounter distinct challenges. These challenges are inherent in the multidimensional nature of e-commerce, which progressively intertwines with societal life. As e-commerce becomes more inseparable, it intricately connects with different facets of society, giving rise to its distinct set of challenges.[23]

The challenges that e-commerce development encounters will inevitably lead to distinct legal consequences, aligning with legal domains associated with the arising issues. These challenges and their corresponding legal implications play a pivotal role in shaping the course of legal evolution in Indonesia. The ongoing process is dedicated to fostering societal advancement, especially amidst the profound influence of the digital economy on both Indonesia's domestic economic system and the global economy.

Challenges may arise from the very aspects that make e-commerce advantageous, especially when it comes to business competition. While e-commerce generally enhances the level of business competition in Indonesia's economic landscape, unregulated development of large corporations adopting e-commerce systems can create an uneven playing field.[24] There is an ongoing discourse on updating regulations to address

[23] Ida Ayu Eka Pradnyaswari and I Ketut Westra, "Upaya Perlindungan Hukum Bagi Konsumen Dalam Transaksi Jual Beli Menggunakan Jasa E-Commerce," *Kertha Semaya,* 8, No. 5 (2020): 758–766, https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/59414., pp. 759-761.

[24] Rodiatn Adawiyah Wiya, "Analisis Tantangan E-Commerce dalam Mengimplementasikan Hukum Persaingan Usaha di Indonesia," *Ilmu Hukum Prima (IHP)* 4, No. 3 (2022): 1-13, https://doi.org/10.34012/jihp.v4i3.2152., p. 4.

monopolistic practices and unfair competition within Indonesia's legal framework, and this discourse is now supported by a draft law. However, conceptualizing fair competition still encounters hurdles due to the intricate nature of the business world and competition, inseparable from other legal dimensions such as intellectual property law, consumer protection, and various other legal fields entwined with Indonesian society. Particularly within the realm of intellectual property law, the e-commerce growth through the lens of business competition significantly impacts the development of various businesses in Indonesia, predominantly small-scale, as intellectual property law directly influences the conducive or detrimental business competition climate in the country's economic system.[25]

Challenges may also arise from inherent limitations within the e-commerce system itself. E-commerce has brought forth numerous advantages for businesses, including expanded choices, easy accessibility, product exploration, convenient online shopping, and increased efficiency. However, alongside these benefits, there are also certain drawbacks, notably privacy infringements and security risks, which render data a critical economic commodity susceptible to various forms of data breaches.[26] Therefore, the substantial growth in the adoption of electronic services and products must be complemented by the development of mechanisms and frameworks to safeguard against diverse security risks. This becomes particularly crucial as most digital services, especially e-commerce, heavily rely on data to offer personalized services to individual users, known as data-driven services.[27] In response to security challenges arising from the rapidly evolving and all-encompassing digital landscape, which influences Indonesian society, Indonesia's legal policy is strategically aimed at facilitating the use of existing digital platforms and ensuring the advancement of digital services, with a specific focus on e-commerce. This direction in legal policy is evident through the

[25] Zen Umar Purba, "Hak Kekayaan Intelektual & Persaingan Usaha Ikhtisar Tiga UU Baru HaKI," *Jurnal Hukum & Pembangunan* (2017): 85-96, https://doi.org/10.21143/jhp.vol0.no0.1408., p. 88.

[26] Rahmawati Nafi'ah, "Pelanggaran Data dan Pencurian Identitas pada E-Commerce," *Cyber Security Dan Forensik Digital* 3, No. 1 (2020): 7–13, https://doi.org/10.14421/csecurity.2020.3.1.1980., p. 8.

[27] Can Azkan, lennart Iggena, Frederik Moller, and Borris Otto, "Towards Design Principles for Data-Driven Services in Industrial Environments," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, (2021): 1789–1798, https://doi.org/10.24251/hicss.2021.217., pp. 1789-1790.

gradual formulation of various regulations to establish a cybersecurity legal framework in Indonesia.

One fascinating illustration of this legal policy direction is exemplified by the issuance of Minister of Communication and Informatics Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. This regulation serves to reinforce the implementation of various legal principles enshrined in the ITE Law (Information and Electronic Transactions Law). Furthermore, subsequent progress occurred with the amendment of the ITE Law through Law No. 19 of 2016, focusing on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. Although this amendment did not explicitly address cybersecurity regulations, it significantly contributed to the conceptualization and evolution of the legal interpretation of cybercrime, which indeed presents a substantial challenge in the realm of cybersecurity. Both legal instruments distinctly emphasize the utmost importance of safeguarding data and ensuring data protection measures are in place.

The regulation issued by the Minister of Communication and Information Technology (Permenkominfo) on the Protection of Personal Data in Electronic Systems presents an intriguing aspect within the realm of law. Article 1 number 5 of this regulation opens up possibilities for the normative advancement of cybersecurity. It defines "Electronic system" as a series of electronic devices and procedures with various functions such as preparing, collecting, processing, analyzing, storing, displaying, announcing, transmitting, and/or distributing electronic information. This connection to cybersecurity arises from the regulation's primary objective of safeguarding data security within electronic systems, necessitating the reinforcement of mechanisms and protective frameworks within the cybersecurity domain. [28] The significance of this regulation concerning electronic systems cannot be understated, as it establishes the electronic system operator as the principal entity responsible for data security in digital services, as specified in Article 1 number 6 of the same Permenkominfo. Conceptually,

[28] Vina Himmatus Sholikhah, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah, "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia," *Indonesian Scholars Scientific Summit Taiwan Proceeding* 3 (2021): 54–63, https://doi.org/10.52162/3.2021112., p. 55.

cybersecurity must encompass all elements of an electronic network to ensure comprehensive protection.

The emphasis on data protection as a crucial element in the development of e-commerce in Indonesia continues to drive the progress and legal policies in the country.[29] This has become even more evident as data has evolved into a commodity, leading to the statement that "data is the new oil," signifying the significance of data in this digital era, with data value rivaling that of fossil fuels that once dominated the global society.[30] As a manifestation of this legal policy direction and concerns about privacy and data protection in the digital economy era dominated by e-commerce, the Indonesian Government has taken action by issuing a new legal instrument specifically addressing data protection, namely Law No. 27 of 2022 concerning Personal Data Protection (PDP Law).

As previously elaborated, the Personal Data Protection Law (PDP Law) elucidates the accountability mechanism of electronic system providers who, according to the law, also function as "data controllers." This legal framework is crucial in Indonesia's cybersecurity development and can be found in Article 4, which stipulates: "(1) Personal Data comprises: a. specific personal data; and b. general personal data; (2) Specific personal data as referred to in paragraph (l) letter a includes health data and information; biometric data; genetic data; criminal records; child data; personal financial data; and/or other data in accordance with the provisions of the regulations; (3) General personal data as referred to in paragraph (l) letter b includes full name; gender; nationality; religion; marital status; and/or combined Personal Data used to identify a person". The legal construct concerning data and its classification as described in Article 4 of the PDP Law is highly praiseworthy as it establishes a framework for safeguarding relevant data, which, in reality, varies significantly depending on the electronic system used to operate an e-commerce service. The regulation pertaining to personal financial data is particularly emphasized here due to its utmost importance in the context of cybersecurity and its frequent targeting for data theft. The

[29] Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *LAW REFORM* 18, No. 2 (2022): 144–163, https://doi.org/10.14710/lr.v18i2.43307., pp. 145-146.

[30] M. Popescu, L. Baruh, P. Messaris, and L. Humphreys, "Consumer Surveillance and Distributive Privacy Harms in the Age of Big Data," in *Digital Media. Transformations in Human Communication* (2017): 313–327, pp. 318-319.

term "personal financial data" is subsequently elucidated in the explanatory section, which states, "the term 'personal financial data' includes, but is not limited to, data on the amount of savings in banks, including savings accounts, deposits, and credit card data".

Many data that fall under the provisions of Article 4 of the Personal Data Protection Law (PDP Law) are categorized as mandatory data that e-commerce service users must submit. These comprehensive regulations pave the way for a wider scope of cybersecurity regulation in the future, given the ever-growing utilization and recycling of data.[31] This is further fueled by the interconnectivity between diverse digital services and e-commerce platforms within the Indonesian economic ecosystem.

3. Guarding Trade Secrets: Legal Implications of Cybersecurity in the E-Commerce Ecosystem

E-commerce, being a significant facet of technological advancement and digitization, plays a vital role in Indonesia's economic framework. It effectively integrates diverse aspects of digitalization into the daily lives of people, including social media and various communication platforms. By revolutionizing payment systems and marketplaces, e-commerce has profoundly impacted various business sectors within Indonesia's economy, as they have eagerly adopted this digital evolution to tackle the intricacies of the digital market. As a result, e-commerce has evolved into a domain where its legal landscape consistently intertwines with Indonesia's legal policies, engaging multiple legal domains simultaneously.

One intriguing aspect of e-commerce is its strong association with intellectual property law. This natural relationship stems from the fact that e-commerce, as a catalyst for economic advancement, is inherently tied to creativity and innovation. In fact, creativity is frequently regarded as a valuable resource in the modern economy.[32] Consequently, it becomes imperative to continually evolve and enhance the protection of intellectual property in alignment with the digital economic growth within the realm of e-commerce, ultimately

[31] Žarko Đorić, "Digital Economy: Basic Aspects and the Case of Serbia," *Ekonomski Pogledi* 22, No. 2 (2020): 73–96, https://doi.org/10.5937/ekopog2002073q., p. 91.

[32] Maciej Czaplewski, "The Use of E-Commerce in the Promotion and Sale of Hand Made Products," *Management* 22, No. 1 (2018): 154–62, https://doi.org/10.2478/manment-2018-0011., p. 154.

safeguarding Indonesia's economic progress.

The ongoing progress of technology and digitalization has brought about a remarkable surge in data utilization, leading to a vast expansion in the types and amounts of data collected. To continually improve data-driven services, it is essential to consistently enhance the diversity and volume of data employed for market analysis and understanding consumer behavior.[33] Recognizing the utmost importance of intellectual property rights and the protective mechanisms within an economic framework, data, being a fundamental element of e-commerce, is intricately connected to intellectual property rights.

The rising frequency of data usage presents potential risks in the dissemination of data containing protected elements under Indonesia's legal system for intellectual property protection. One of these essential elements is trade secrets, which, as the name implies, are confidentially kept due to their vital role in defining a product's intellectual property. The continuous expansion of e-commerce service quality has driven the extensive adoption of various e-commerce networks in Indonesia, but it has also raised concerns about privacy due to the substantial data requirements of digital services. Among the information that can be included in this data are trade secrets, making them vulnerable to misuse and theft through cybercrime. Moreover, beyond the domain of data-driven e-commerce, the security of intellectual property forms like trade secrets is significantly influenced by cybersecurity measures implemented in data storage networks.[34]

Given the e-commerce industry's heavy reliance on data collection and processing, the urgency to enhance various cybersecurity mechanisms is increasing. In the corporate scale of the creative industry, the loss of trade secrets through theft can result in the loss of contracts, competitive advantages, and even the identity of specific products to be released. In the realm of digital security breaches, trade secrets frequently become the prime target of cyberattacks, ranging from smaller interests, such as stealing product-related

[33] Can Azkan *et al.*, *op.cit.,* p. 1787.

[34] Riccardo Vecellio Segate, "Securitizing Innovation to Protect Trade Secrets Between 'the East' and 'the West': A Neo-Schumpeterian Public Legal Reading," *UCLA Pacific Basin Law Journal* 37, No. 1 (2020): 59–126, https://doi.org/10.5070/p8371048804., p. 74.

information[35], to larger interests, like economic espionage typically conducted by a state-backed entity with the aim of obtaining information about the industrial developments of a competing foreign country.[36]

The PDP Law governs the significance of national interests and national security in safeguarding personal data. However, it imposes normative restrictions on regulating national security, particularly concerning denying access to modifications in personal data. These normative limitations are further constrained by the limited scope of data covered under this law, primarily focusing on individual identification. The association between trade secrets as an intellectual property right and the protection of personal data is solely addressed in Article 4 paragraph (1) letter g, underscoring the necessity for additional normative advancements.

Law No. 30 of 2000 concerning Trade Secrets provides a compelling framework for normative development, as articulated in Article 2. The article emphasizes the broad scope of protection granted to Trade Secrets, encompassing valuable economic information in the realms of technology and business that remains undisclosed to the public. This well-crafted regulation not only extends its protective measures to physical trade secrets but also effectively adapts to the digital landscape, ensuring the safeguarding of confidential data in the digital realm. The inclusivity of this regulation allows for the implementation of robust trade secret protection mechanisms, covering a wide array of confidential information, including production, processing, sales methods, and other economically significant data. It is worth noting that there are no specific provisions in other regulations addressing the position of trade secrets in the electronic system. The reason behind this absence is attributed to the age of the law, enacted at a time when digitalization had not yet significantly impacted society. However, in the contemporary context, data has emerged as a highly valuable commodity in the digital economy era. Consequently, Law No. 30 of 2000 now gains renewed relevance, as it seamlessly encompasses the evolving

[35] Michael Ettredge, Feng Guo, and Yijun Li, "Trade Secrets and Cyber Security Breaches," *Journal of Accounting and Public Policy* 37, No. 6 (2018): 564–585, https://doi.org/10.1016/j.jaccpubpol.2018.10.006., p. 569.

[36] Julien Chaisse and Cristen Bauer, "Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration," *Vanderbilt Journal of Entertainment & Technology Law* 21, No. 3 (2017): 549–590, https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss3/5.

significance of data within the dynamic e-commerce ecosystem. The regulation provides a much-needed framework to address the protection of trade secrets in the digital world, ensuring their confidentiality and secure handling amidst the ever-expanding digital landscape.

D. CONCLUSIONS

The analysis results reveal the significant role of e-commerce in Indonesia's economy, impacting the country's legal development. Despite Indonesia having a well-established legal framework, the government has not effectively utilized it through the Personal Data Protection Law (PDP Law). Normative analysis identifies limitations in the PDP Law, particularly concerning the classification of data forms in today's technology landscape, which could affect the protection of trade secrets, an important aspect of intellectual property rights. This issue arises partly due to the outdated Trade Secret Law, which fails to address technical aspects related to data that have become crucial in operating e-commerce systems. To address these challenges, there is a need to expand the scope of the regulations within the PDP Law and update the Trade Secret Law to encompass various technical aspects of data. Future regulations should prioritize the enhancement of cybersecurity frameworks to provide better protection for trade secrets.

REFERENCES

Ahmad, Iqbal Faza. "Urgensi Literasi Digital Di Indonesia Pada Masa Pandemi COVID-19: Sebuah Tinjauan Sistematis." *Nusantara: Jurnal Pendidikan Indonesia* 2, No. 1 (2022): 1–18. https://doi.org/10.14421/njpi.2022.v2i1-1.

Anjani, Margaretha Rosa, and Budi Santoso. "Urgensi Rekonstruksi Hukum E-Commerce Di Indonesia." *LAW REFORM* 14, No. 1 (2018): 89-103. https://doi.org/10.14710/lr.v14i1.20239.

Ayunda, Rahmi. "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *LAW REFORM* 18, No. 2 (2022): 144–63. https://doi.org/10.14710/lr.v18i2.43307.

Ayunda, Rahmi, and Rusdianto. "Pelindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence Dalam Aktifitas Perbankan Di Indonesia." *Jurnal Komunikasi Hukum* 7, No. 2 (2021): 663–677. https://doi.org/10.23887/jkh.v7i2.37995.

Azkan, Can, Lennart Iggena, Frederik Möller, and Boris Otto. "Towards Design Principles for Data-Driven

Services in Industrial Environments." In *Proceedings of the 54th Hawaii International Conference on System Sciences*, (2021) :1789–1798. https://doi.org/10.24251/hicss.2021.217.

Chaisse, Julien, and Cristen Bauer. "Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration." *Vanderbilt Journal of Entertainment & Technology Law* 21, No. 3 (2017): 549–590. https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss3/5.

Czaplewski, Maciej. "The Use of E-Commerce in the Promotion and Sale of Hand Made Products." *Management* 22, No. 1 (2018): 154–162. https://doi.org/10.2478/manment-2018-0011.

Disemadi, Hari Sutra. "Contextualization of Legal Protection of Intellectual Property in Micro Small and Medium Enterprises in Indonesia." *LAW REFORM* 18, No. 1 (2022): 89–110. https://doi.org/10.14710/lr.v18i1.42568.

Đorić, Žarko. "Digital Economy: Basic Aspects and the Case of Serbia." *Ekonomski Pogledi* 22, No. 2 (2020): 73–96. https://doi.org/10.5937/ekopog2002073q.

Ettredge, Michael, Feng Guo, and Yijun Li. "Trade Secrets and Cyber Security Breaches." *Journal of Accounting and Public Policy* 37, No. 6 (2018): 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006.

Farichin, Sefiya Nur. "Pengaruh Digitalisasi Dalam Bidang E-Commerce Terhadap Perilaku Konsumtif Mahasiswa UIN Sunan Ampel." *JURNAL SOSIAL Jurnal Penelitian Ilmu-Ilmu Sosial* 23, No. 1 (June 2022): 34–39. https://doi.org/10.33319/sos.v23i1.108.

Fitriani, Safira Dhea, Margi Rizki Satriana M, Titin Retnosari, and Nur Rohmawati. "Digitalisasi Ekonomi Syariah Penerapan Hukum-Hukum Islam Dalam Jual Beli Online." *JURNAL EKONOMI SYARIAH* 6, No. 1 (2021): 51–59. https://doi.org/10.37058/jes.v6i1.2542.

Hotana, Melisa Setiawan. "Industri e-Commerce Dalam Menciptakan Pasar yang Kompetitif Berdasarkan Hukum Persaingan Usaha." *Jurnal Hukum Bisnis Bonum Commune* 1, No. 1 (2018): 28–38. https://doi.org/10.30996/jhbbc.v0i0.1754.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Indonesia. Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang.

Indonesia. Peraturan Menteri Komunikasi

dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Indriani, Iin. "Hak Kekayaan Intelektual: Perlindungan Hukum Terhadap Hak Cipta Karya Musik." *Jurnal Ilmu Hukum* 7, No. 2 (2018): 246–263. http://dx.doi.org/10.30652/jih.v7i2.5703.

Kaabi, Safa, and Rim Jallouli. "Overview of E-Commerce Technologies, Data Analysis Capabilities and Marketing Knowledge." In *Lecture Notes in Business Information Processing* 358, (2019): 183–93. https://doi.org/10.1007/978-3-030-30874-2_14.

Kabanov, Ilya, and Stuart Madnick. "Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense." *MIS Quarterly Executive* 20, No. 2 (2021): 109–125. https://doi.org/10.17705/2msqe.00044.

Kurdi, Moh., Dina Kurniawati, Very Andrianingsih, Astri Furqani, Nur Alfiyah, and Miftahol Arifin. "The Government's Role in MSMEs Development Through E-Commerce in Sumenep Regency." In *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021,* (2021): 1–5. https://doi.org/10.4108/eai.6-3-2021.2306388.

Kurniasari, Florentina, Ardi Gunardi, Farica Perdana Putri, and Andy Firmansyah. "The Role of Financial Technology to Increase Financial Inclusion in Indonesia." *International Journal of Data and Network Science* 5, No. 3 (2021): 391–400. https://doi.org/10.5267/j.ijdns.2021.5.004.

Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." *Energy Reports* 7 (2021): 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126.

Lukito, Imam. "Tantangan Hukum dan Peran Pemerintah Dalam Pembangunan E-Commerce." *Jurnal Ilmiah Kebijakan Hukum* 11, No. 3 (2017): 349–367. http://dx.doi.org/10.30641/kebijakan.2017.V11.349-367.

Nafi'ah, Rahmawati. "Pelanggaran Data dan Pencurian Identitas pada E-Commerce." *Cyber Security Dan Forensik Digital* 3, No. 1 (2020): 7–13. https://doi.org/10.14421/csecurity.2020.3.1.1980.

Nurhidayati, Sugiyah, and Kartika Yuliantari. "Pengaturan Pelindungan Data Pribadi Dalam Penggunaan Aplikasi Pedulilindungi." *Widya Cipta: Jurnal Sekretari Dan Manajemen* 5, No. 1 (2021): 39–45. https://doi.org/10.31294/widyacipta.v5i1.9447.

Palese, B., and A. Usai. "The Relative Importance of Service Quality Dimensions in E-Commerce Experiences." *International Journal of Information Management* 40 (2018): 132–140.

https://doi.org/10.1016/j.ijinfomgt.2018.02.001.

Popescu, M., L. Baruh, P. Messaris, and L. Humphreys. "Consumer Surveillance and Distributive Privacy Harms in the Age of Big Data." In *Digital Media. Transformations in Human Communication*, (2017): 313–327. https://www.academia.edu/32080668/Consumer_Surveillance_and_Distributive_Privacy_Harms_in_the_Age_of_Big_Data.

Prabowo, Wisnu, Satriya Wibawa, and Fuad Azmi. "Pelindungan Data Personal Siber Di Indonesia." *Padjadjaran Journal of International Relations* 1, No. 3 (2020): 218–239. https://doi.org/10.24198/padjir.v1i3.26194.

Pradnyaswari, Ida Ayu Eka, and I Ketut Westra. "Upaya Pelindungan Hukum Bagi Konsumen Dalam Transaksi Jual Beli Menggunakan Jasa E-Commerce." *Kertha Semaya,* 8, No. 5 (2020): 758–66. https://ojs.unud.ac.id/index.php/kerthasemaya/article/view/59414.

Purba, Zen Umar. "Hak Kekayaan Intelektual ^ Persaingan Usaha: Ikhtisar Tiga UU Baru HaKI." *Jurnal Hukum & Pembangunan*, (2017): 85–96. https://doi.org/10.21143/jhp.vol0.no0.1408.

Putra, Muhammad Deovan Reondy, and Hari Sutra Disemadi. "Counterfeit Culture Dalam Perkembangan UMKM: Suatu Kajian Kekayaan Intelektual." *KRTHA BHAYANGKARA* 16, No. 2 (2022): 297–314. https://doi.org/10.31599/krtha.v16i2.1151.

Rahmi, Lailatur, and Guruh Tri Nugroho. "Kepemilikan Data Di Universitas : Salah Satu Isu Dalam Kebijakan Informasi." *Shaut Al Maktabah* 8, No. 2 (2017): 155–168. https://doi.org/10.15548/shaut.v9i2.114.

Rumlus, Muhamad Hasan, and Hanif Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik." *Jurnal HAM* 11, No. 2 (2020): 285–99. https://doi.org/10.30641/ham.2020.11.285-299.

Sholikhah, Vina Himmatus, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah. "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia." *Indonesian Scholars Scientific Summit Taiwan Proceeding* 3 (2021): 54–63. https://doi.org/10.52162/3.2021112.

Solms, Basie von, and Rossouw von Solms. "Cybersecurity and Information Security – What Goes Where?" *Information and Computer Security* 26, No. 1 (2018): 2–9. https://doi.org/10.1108/ICS-04-2017-0025.

Sutra Disemadi, Hari. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Pelindungan Data Pribadi Di Indonesia." *Wawasan Yuridikta* 5, No. 2 (2021): 177–199. http://dx.doi.org/10.25072/jwy.v5i2.460.

Vecellio Segate, Riccardo. "Securitizing Innovation to Protect Trade Secrets Between 'the East' and 'the West': A Neo-Schumpeterian Public Legal Reading." *UCLA Pacific Basin Law Journal* 37, No. 1 (2020): 59–126. https://doi.org/10.5070/p8371048804.

Wiya, Rodiatn Adawiyah. "Analisis Tantangan E-Commerce Dalam Mengimplementasikan Hukum Persaingan Usaha Di Indonesia." *Ilmu Hukum Prima (IHP)* 4, No. 3 (2022): 1–13. https://doi.org/10.34012/jihp.v4i3.2152.

Zhu, Ruilin, Aashish Srivastava, and Juliana Sutanto. "Privacy-Deprived e-Commerce: The Efficacy of Consumer Privacy Policies on China's e-Commerce Websites from a Legal Perspective." *Information Technology and People* 33, No. 6 (2020): 1601–1626. https://doi.org/10.1108/ITP-03-2019-0117.