Jurnal Hukum UNISSULA

Volume 40 No. 2, December
P-ISSN: 1412-2723

LEGAL SAFEGUARDS FOR VICTIMS OF DATA DISSEMINATION CRIMES AND CYBERCRIME PROTECTION

Umi Enggarsasi
Universitas Wijaya Kusuma Surabaya, Indonesia, Email: umienggarsasi.uwks@gmail.com
Nur Khalimatus Sa'diyah
Universitas Wijaya Kusuma Surabaya, Indonesia, Email: nurkhalimatussadiyah_fh@uwks.ac.id
Pratama Alifiandi Martio
Universitas Wijaya Kusuma Surabaya, Indonesia, Email: alfian.alfiandi55@gmail.com

ARTICLE INFO

Keywords:
Personal Data Protection; Data Theft; Legal Safeguards; Cybercrime; Digital Age.

DOI:
10.26532/jh.v40i2.39974

ABSTRACT

In the digital age, legal protections for personal data are insufficient, leaving individuals vulnerable to financial losses from data theft and criminal dissemination of personal information. This research focuses on assessing the effectiveness of existing regulations, such as Law Number 27 of 2022 Concerning Personal Data Protection. Employing an empirical juridical approach for field research and a conceptual approach for theoretical analysis. The analysis underscores that personal data, crucial for identification, is a frequent target for malevolent actors seeking financial gain, leading to profound consequences for victims. Incidents of personal data theft, often orchestrated by fraudsters, extend beyond financial losses, compromising personal information available for purchase on clandestine online platforms like the dark web. Despite existing regulations, the research identifies a significant gap in providing clear guidelines for safeguarding individuals in the digital era. The study concludes that the current legal framework, while foundational, requires a more comprehensive focus on the Personal Data Protection Law due to inherent weaknesses. This research contributes valuable insights into the evolving legal landscape surrounding personal data crimes in Indonesia, ensuring a comprehensive understanding of legal protections for victims amidst technological advancements.

1. Introduction

The progression from the Fourth Industrial Revolution (4.0) towards the emerging Fifth Industrial Revolution (5.0) signifies a paradigm where remote control of various aspects is enabled through web connectivity and associated devices. The widespread adoption of technology-driven innovations in daily life, such as enhancing work efficiency, establishing financial connections, and facilitating

various tasks, has led to substantial consequences.[1] The swift development of computer-based information technology innovations among the public has simplified the experiences of community groups. This ease of access, however, has resulted in a notable lack of attention to security, particularly concerning the protection of personal identity.[2] In Indonesia, it has become commonplace for individuals to freely disclose personal information, including their residence, date of birth, and social connections. Displaying personal identification, like identity card, to outsiders when entering different premises has become a societal norm. Additionally, online media users in Indonesia often openly share details such as their place of birth, date of birth, telephone number, and familial relationships[3]. An examination conducted by the Association of Indonesian Network Access Providers (APJII) reveals a continuous growth in internet access users over the years. In 2016, there were 132.7 million internet users, constituting 51.7% of the total population of 256.2 million.[4] The following year, 2017, saw an increase to 143.26 million users, accounting for 54.68% of the total population of 262 million.[5] By 2018, the number of internet users had risen to 171.17 million, marking a 10.12% increase from the previous year and representing 67.2% of the population, which had reached 254.16 million.[6] The accumulation of personal information in these records underscores the need for heightened security measures to safeguard individuals from potential harm. Concerns regarding the misuse of personal information are evident, with 59% of internet users expressing discomfort at the prospect of their data being exploited by certain entities for purposes that primarily benefit the data owner.[7]

---

[1] Anran Xiao, Zeshui Xu, Marinko Skare, Yong Qin, and Xinxin Wang., Bridging the digital divide: the impact of technological innovation on income inequality and human interactions, *Humanities and Social Sciences Communications*, Vol.11, no.1, 2024, page.11, See to, Ayesha Afzal, Saba Fazal Firdousi, Ayma Waqar, and Minahil Awais., The influence of internet penetration on poverty and income inequality, *Sage Open*, Vol.12, no.3, 2022, page.21582440221116104. See to, Robin Mansell., Inequality and digitally mediated communication: Divides, contradictions and consequences, In *Critical Perspectives on Media, Power and Change*, pp. 1-16. London, Routledge, 2018, page.142. See to, Tewathia, Nidhi, Anant Kamath, and P. Vigneswara Ilavarasan., Social inequalities, fundamental inequities, and recurring of the digital divide: Insights from India, *Technology in Society*, Vol.61, 2020, page.101251.

[2] Jiesen Lin, Lemuria Carter, and Dapeng Liu., Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app, *European Journal of Information Systems*, Vol.30, no.4, 2021, page.399. See to, Ömer Aslan, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin., A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, *Electronics*, Vol.12, no.6, 2023, page.1333.

[3] Mona Natasha Siahaan, Putu Wuri Handayani, and Fatimah Azzahro., Self-disclosure of social media users in Indonesia: the influence of personal and social media factors, *Information Technology & People,* Vol.35, no.7, 2022, page 1940.

[4] Bethani Suryawardani and Astri Wulandari., Determinant factors of customers switching behavior to customer satisfaction and loyalty in online transportation users in bandung, *JDM (Jurnal Dinamika Manajemen),* Vol.11, no.1, 2020, page.19.

[5] Nur Aini Fitriya Ardiani Aniqoh., The role of digital economy to enhancing sustainable economic development, *International Journal of Social Science and Business*, Vol.4, no.4, 2020, page.523.

[6] Palupi Anggraheni, Novi Tri Setyowati, and Harry Harry., Social media and political participation in indonesia: restrictions access at announcement results of 2019 presidential election, *Aspiration Journal*, Vol.2, no.1, 2021, page.115.

[7] Bagus Satryo Ramadha., *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia*, Master Theses, Yogyakarta, Universitas Isam Indonesia, 2021, Page.241.

Indonesia possesses numerous regulations pertaining to the protection of individual data, yet these regulations are dispersed across various legal frameworks. Currently, explicit regulations and guidelines addressing the legal safeguarding of individual data, which could serve as solutions for diverse cases involving the misuse of personal identity, are lacking. Although Indonesia has enacted Law Number 27 of 2022 Concerning Personal Data Protection, there is a need for a more comprehensive focus on this law, given its inherent weaknesses in providing clear guidelines. Individuals have the autonomy to safeguard their personal information, and the reckless provision of information to others can potentially lead to legal repercussions, including imprisonment. Regulation number 24 of 2013, which concerns population organizations, permits certain state organizations to disclose population data. Legal principles governing the dissemination of others' data and identities are outlined in statutory regulations, including the Electronic Information and Transactions Law. According to administrative regulations, individuals who unlawfully share someone's personal information without consent can face a maximum sentence of 2 years and 8 months in prison. In this context, the wrongful dissemination of an individual's data satisfies the essential elements of criminal acts, encompassing elements akin to theft, fraud, and other criminal activities, both in terms of objective and subjective criteria. The criminal act of revealing identity confidentiality stems from the era of information technology, particularly with the widespread use of social media, where personal information becomes exposed in the cyberspace domain.

The reviewed literature highlights significant gaps in addressing legal protection for victims of personal data dissemination in Indonesia. Gojali emphasizes corporate vulnerabilities but does not consider the direct impact of personal data breaches on individual victims.[8] Rosadi et al. and Hisbulloh analyze the Personal Data Protection Bill but lack focus on victim-centered safeguards or remedies for data dissemination harms.[9] Hasbullah explores corporate compliance with cybersecurity laws without addressing how these frameworks protect victims of personal data breaches.[10] Sitompul proposes a legal framework for data protection within criminal law but omits specific protections for victims of personal data violations.[11] Nugroho and Chandrawulan discuss cybercrime trends but do not explore how legal frameworks support victims of data dissemination.[12] Similarly,

[8] Djoni Sumardi Gojali., Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective, *International Journal of Cyber Criminology*, Vol.17, no.1, 2023, page.9.

[9] Sinta Dewi Rosadi, Andreas Noviandika, Robert Walters, and Firsta Rahadatul Aisy., Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?, *International Review of Law, Computers & Technology*, Vol.37, no.1, 2023, page.89. See to, Moh Hamzah Hisbulloh., Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi, *Jurnal Hukum,* Vol.37, no.2, 2021, page.121.

[10] M. Afif Hasbullah., Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers, *International Journal of Cyber Criminology*, Vol.16, no.2, 2022, page.123.

[11] Josua Sitompul., Developing a Legal Framework of Personal Data Protection in the Indonesian Criminal Procedure Law, *Indonesia Law Review,* Vol.9, no.3, 2019, page.201.

[12] Agus Nugroho and An An Chandrawulan., Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries, *Security Journal*, Vol.36, no.4,

Angkasa et al. focus on enforcement in illegal online loans while neglecting data dissemination issues.[13] Lastly, Manthovani assesses cybercrime prosecution but fails to consider the legal remedies available to victims of personal data breaches.[14] Thus, this research is conducted to fill the gap by focusing on legal protections for victims of personal data dissemination, ensuring their rights and remedies are adequately addressed in the Indonesian legal framework.

2. Research Methods

The research design incorporates the normative and conceptual elements. The normative approach aims to analyze the legal provisions of victims of personal data crimes. Simultaneously, the conceptual aspect employs a statutory approach, delving into the relevant laws governing personal data protection. This dual approach aims to provide a comprehensive understanding of the legal landscape surrounding the crime of personal data dissemination and its effects on victims. This research delves into the critical issue of legal protection for victims of the dissemination of personal data, with a particular focus on identity theft and doxing. The study underscores the pervasive influence of digital technology in facilitating unauthorized access to personal information, leading to potential financial exploitation and reputational harm. The legal framework in Indonesia, represented by regulations such Law Number 27 of 2022 Concerning Personal Data Protection, provides a foundation for addressing these challenges. Data analysis in this study follows a descriptive approach. It involves systematically examining and summarizing the findings from both empirical and conceptual investigations. The descriptive analysis aims to present a clear and comprehensive picture of the legal protection scenario for victims of personal data crimes.

3. Results and Discussion

3.1. Criminal Acts and Legal Challenges in Protecting Personal Data Confidentiality

Various criminal acts related to the dissemination of personal data confidentiality include cyberstalking, which constitutes a form of criminal behavior involving unwarranted threats or excessive attention in internet and computer communication, severely impacting the victim.[15] Cyberstalking, when viewed literally, can be interpreted as a manifestation of online harassment aimed at extracting personal.[16] Perpetrators of online stalking exhibit diverse motives,

2022, page.651. See to, Hamed Taherdoost., Insights into Cybercrime Detection and Response: A Review of Time Factor, *Information*, Vol.15, no.5, 2024, page.273.

[13] Angkasa Angkasa, Filep Wamafma, Ogiandhafiz Juanda, and Bhanu Prakash Nunna., Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim, *Lex Scientia Law Review*, Vol.7, no.1, 2023, page.121.

[14] Reda Manthovani., Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law, *International Journal of Criminal Justice Sciences*, Vol.18, no.1, 2023, page.449.

[15] Iñigo Gordon Benito., Online harassment and cyberstalking: a case study, *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, Vol.13, no.2, 2023, page.248.

[16] Waheeb Abu-Ulbeh, Maryam Altalhi, Laith Abualigah, Abdulwahab Ali Almazroi, Putra Sumari, and Amir H. Gandomi., Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations, *Electronics*, Vol.10, no.14, 2021, page.1670. See to, Noora Al Mutawa, Joanne Bryce, Virginia NL Franqueira, and Andrew Marrington., Forensic investigation of cyberstalking cases using behavioural evidence analysis, *Digital investigation*, Vol.16, no.21, 2016, page.99. See to, Aimee Mirto., *Detecting*

typically initiating the process by mining the victim's information, including social media connections, friends, and family, to acquire additional personal details such as phone numbers and email addresses. Subsequently, armed with the obtained information, the perpetrator often proceeds to terrorize or harass the victim through means like incessant messaging, continuous calls, and the issuance of threats or unwanted demands. Cyberstalking is often coupled with other offenses, including threats, harassment, and the continuous dissemination of false accusations (defamation) using electronic devices or internet platforms, perpetrated by an individual unknown to or not previously acquainted with the victim. In the context of spreading the confidentiality of a person's identity, cyberstalking involves the perpetrator stalking the victim in cyberspace through tactics such as creating an anonymous social media account or pseudonym, utilizing this account to stalk individuals. The perpetrator then communicates with the victim, presenting messages that may be in the form of invitations, deception, or threats, intending to coerce the victim into ongoing interaction for the purpose of extracting personal data information. Unbeknownst to the victim, participation in these interactions inadvertently results in the widespread dissemination of their identity confidentiality due to the allure of invitations or threats made by the perpetrator. These elements collectively contribute to the broad dissemination of an individual's identity confidentiality.

Furthermore, the dissemination of personal data confidentiality involves data commercialization, which refers to the utilization of an individual's personal data in the business domain without obtaining the owner's consent. In this scenario, business entities derive economic benefits from someone's personal data, while the data owner receives no compensation for the use of their personal information.[17] Exploiting or misusing personal data in this manner is deemed a criminal act, particularly when it involves the buying and selling of data or unauthorized data usage.[18] This business practice creates a conflict between privacy protection and economic interests. On one hand, business entities gain economic advantages by leveraging personal data from individuals. On the other hand, the individuals who own the data do not reap any benefits from the commercial use of their personal information.[19] The commercialization of data in the context of spreading identity confidentiality has implications for individuals, such as receiving targeted product offers or facing threats, such as solicitation for credit.[20] It opens the possibility for groups or individuals to gather data from

*cyberstalking from social media platform (s) using data mining analytic*s, PhD. Dissertation, London, University of West London, 2022, page.132.

[17] Jason Aaron Gabisch, and George R. Milne., The impact of compensation on information ownership and privacy control, *Journal of Consumer Marketing*, Vol.31, no.1, 2014, page.20. See to, Francesco Banterle., Data ownership in the data economy: a European dilemma, *EU Internet Law in the Digital Era: Regulation and Enforcement*, Vol.5, no.12, 2020, page.217.

[18] Alicia Nakhjavan., The Worst Law in Technology: How the Computer Fraud and Abuse Act Allows Big Businesses to Collect and Sell Your Personal Information, *Brooklyn Law Review,* Vol.87, no.21, 2021, page.1077.

[19] Bryan Pratama., *Data Pribadi, Data Privasi Dan Komersialisasinya*, Semarang, Binus University, 2019, page.123.

[20] Shaukat Ali, Naveed Islam, Azhar Rauf, Ikram Ud Din, Mohsen Guizani, and Joel JPC Rodrigues., Privacy and security issues in online social networks, *Future Internet*, Vol.10, no.12, 2018, page.114.

sources like the internet and social media, subsequently selling this information. Consequently, individuals may unknowingly become targets of various acts of harassment, even when they have not willingly shared their data. In situations related to banking, commercialized data can manifest in offers such as loans or gold loan solicitations. In corporate settings, where consumer data is involved, companies may request data for specific purposes, but then engage in commercializing or trading the data for unauthorized purposes. The act of data commercialization without the owner's consent exhibits clear elements constituting a criminal offense.

Moreover, Data Interception, or interception in the confidential distribution of personal data, encompasses the activities of listening, recording, distorting, altering, inhibiting, and/or capturing the transmission of non-public electronic information and/or electronic documents through communication cable networks or wireless networks, such as electromagnetic radiation or radio frequency.[21] Wiretapping, in essence, involves the installation of additional tools or equipment on a telecommunications network to illicitly acquire information, constituting an unauthorized and prohibited activity.[22] The information owned by an individual is considered a personal right that warrants protection, making wiretapping a forbidden practice. The significance of data interception or tapping in the context of spreading identity confidentiality is evident in regulatory frameworks, where wiretapping is defined as the installation of additional tools or equipment on a telecommunications network for the purpose of unauthorized information acquisition.[23] This implies that if an individual taps into another person's communication device with the intention of obtaining information unlawfully, deliberately and without the knowledge of the person being tapped, using various methods such as installing network equipment on telecommunications or employing additional devices, eavesdroppers can easily access information and maintain the confidentiality of someone's identity. Engaging in wiretapping without proper authorization is unequivocally classified as a criminal act.

Furthermore, phishing in the context of disseminating the confidentiality of personal data is a method employed by online identity thieves to illicitly acquire sensitive information such as online banking passwords or credit card details from users.[24] This deceptive activity utilizes various means, including the use of

[21] Caitlin E. Jokubaitis., There and Back: Vindicating the Listener's Interests in Targeted Advertising in the Internet Information Economy, *Colum. Columbia Journal of Law & the Arts*, Vol.42, no.34, 2018, page.85.

[22] Paul AC. Duijn, and Peter PHM Klerks., Social network analysis applied to criminal networks: recent developments in Dutch law enforcement, *Networks and network analysis for defence and security*, Vol.13, no.7, 2014, page.134. See to, Joseph Fitsanakis., *Redesigning Wiretapping: The Digitization of Communications Interception*. Springer Nature, 2020.; Stephen C. Thaman., The Use of Information and Communications Technology in Criminal Procedure in the USA, *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Vol.3, no.17, 2017, page.118.

[23] Susan Landau., *Surveillance or security?: The risks posed by new wiretapping technologies*, Cambridge, Mit Press, 2011, page.198.

[24] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan., Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science*, Vol.3, no.4, 2021, page.563060. See to, L. Joy Singh, and N. I. E. L. I. T. Imphal., A survey on phishing and anti-phishing techniques, *International Journal of Computer Science Trends and Technology (IJCST)*, Vol.6, no.2, 2018, page.65. See to, Lauren L. Sullins., "Phishing" for a solution: domestic and

applications or sending links to individuals, with the objective of stealing their information. Phishing can be characterized as a deceptive service that falsely assures the validity and security of data transfer.[25] In the context of spreading identity confidentiality, phishing involves hackers tricking targets into using a counterfeit login form on a fraudulent website that closely resembles the original site. The modus operandi of phishing entails the hacker inducing the target to click on a link to their fraudulent website, often presented through an enticing image or reference in an email. Subsequently, unwittingly, users enter their username and password, compromising their identity confidentiality. Through this method, hackers can easily gain control of user accounts, enabling them to engage in criminal activities and misuse the compromised information. Consequently, this qualifies as a criminal offense.[26]

Subsequently, in the context of disseminating the confidentiality of personal data, Doxing, derived from the term "dox" denoting documents, involves an internet-based activity that entails researching and publicly disclosing personal information, including personal data, about an individual or organization.[27] Doxing predominantly occurs in forums or online communities where users commonly utilize aliases for interaction, as opposed to platforms like Facebook where users generally employ their real identities, including photos and names. Essentially, the act of publishing personal information about others, in any form and on any platform, falls within the definition of doxing.[28] The consideration of doxing in terms of spreading identity confidentiality is crucial due to its utilization in victimizing individuals through the internet. Doxing involves the exposure of an individual's identifying information, such as their real name, email address, workplace, phone number, financial details, and other personal information, which is then disseminated to the public without the victim's consent.[29] An instance of doxing includes a netizen revealing someone's identity, thereby violating privacy by sharing the personal data of others. The act of divulging someone else's identity without their consent is highly perilous and can lead to undesirable consequences in cyberspace.

Finally, cyber-hacking in the context of disseminating the confidentiality of personal data demands careful consideration.[30] The emergence of cyber-hacking

international approaches to decreasing online identity theft, In *Computer Crime*, pp. 73-110. Routledge, 2017, page.198.

[25] Diksha Goel, and Ankit Kumar Jain., Mobile phishing attacks and defence mechanisms: State of art and open research challenges, *Computers & Security*, Vol.73, no.4, 2018, page.527.

[26] Tri Rudiyanto, Halley Kunda, Amy Dunn, Sharon Shenderovskiy, and Rondarrius Gibson., Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States, *Lex Publica*, Vol.10, no.1, 2023, page.91.

[27] Teguh Cahya Yudiana, Sinta Dewi Rosadi, and Enni Soerjati Priowirjanto., The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia, *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, Vol.9, no.1, 2022, page.32.

[28] Julia M. MacAllister., The doxing dilemma: seeking a remedy for the malicious publication of personal information, *Fordham Law Review,* Vol.85, no.2, 2016, page.2451.

[29] Lachlan Jaccoud, Lorena Molnar, and Marcelo F. Aebi., Antifa's political violence on Twitter: A grounded theory approach, *European Journal on Criminal Policy and Research*, Vol.29, no.3, 2023, page.506.

[30] Oksidelfa Yanto., Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development, *Lex Publica*, Vol.7, no.2, 2020, page.35.

is directly linked to the compromise of identity confidentiality and warrants close attention. Article 30, paragraph 3 of the Information and Electronic Transactions Law provides clarification on a security system, defining it as a mechanism that restricts or prohibits computer access based on user categorization, coupled with assigned levels of authority. This legal provision asserts that intentionally accessing a computer or electronic system by bypassing or violating the security measures established by the owner or user constitutes a criminal act referred to as "cracking".[31] Crackers engage in such activities with the objective of personal gain, either financially by exploiting vulnerabilities to amass wealth through the unauthorized access of banking or credit card passwords, or non-financially by indulging in acts that gratify their own desires, such as disrupting computer networks. Acquiring knowledge of passwords or other secret identities empowers crackers to easily commit crimes.[32]

3.2. The Right to Privacy and Identity Protection

Identity confidentiality is synonymous with privacy and is intricately linked to the protection of personal information.[33] When discussing an individual's personal identity, we inherently address the associated privacy that warrants safeguarding and reverence. The term "privacy" has been widely utilized in developed nations to denote personal identity as an inherent right deserving protection. The right to privacy, as a fundamental aspect of individual freedom and dignity, plays a pivotal role in preserving identity.[34] The Constitution of the Republic of Indonesia of 1945, commonly referred to as the 1945 Constitution, governs the protection of personal identity. This legal framework, articulated in Article 28G, paragraph (1), explicitly declares, "Every person has the right to protection of himself, his family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear of doing or not doing something which is a human right." In essence, the protection of personal identity manifests in two forms: securing physical identity, encompassing both visible and explicitly identifiable aspects, and establishing regulatory measures to govern the use of identity by unauthorized individuals, prevent identity misuse for specific interests, and mitigate the destruction of identity. Internally, the government is tasked with ensuring the institutionalization of the significance of protecting personal identity for citizens through comprehensive legislation aligned with the principles of identity protection.[35]

Concerning the constraints on the use of other data or identity, such information may not be disclosed to the public or employed for purposes beyond specific

[31] Orin S. Kerr., Cybercrime's scope: interpreting access and authorization in computer misuse statutes, *New York University Law Review,* Vol.78, no.6, 2003, page.1596.

[32] Dittrich, David, and Kenneth Einar Himma., *Hackers, crackers, and computer criminals, Handbook of Information Security,* Bakersfield, California State University, 2006, page.165.

[33] Maree Bernoth, Elaine Dietsch, Oliver Kisalay Burmeister, and Michael Schwartz., Information management in aged care: Cases of confidentiality and elder abuse, *Journal of Business Ethics*, Vol.122, no.3, 2014, page.457.

[34] Ana Beduschi., Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations, *Data & Policy*, Vol.3, no.2, 2021, page.15.

[35] Edmon Makarim., Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach, *Data Protection Around the World: Privacy Laws in Action*, Vol.22, no.6, 2021, page.142.

intentions without the explicit consent of the involved party, except with the authorization of the data owner or legal authorities. In the context of safeguarding personal data identity, this aligns with the privacy principle, signifying that personal data cannot be made public without a specified purpose and requisite permission from the concerned individual.[36] The principle of restriction on data collection and privacy identity underscores that the acquisition of data must adhere to legally valid, fair, and necessary methods, grounded in the knowledge and consent of the individual involved. This principle elucidates that the limitation on collecting personal data is confined to data collected for expressly stated purposes, in compliance with both legal provisions and the consent of the data owner. When collecting data or identity, a clear and specific purpose must be outlined, and any subsequent use of the data is restricted to align with the specified purpose. This implies that data utilization requires a well-defined reason and purpose, provided it remains within the bounds of applicable regulations. In the context of the principle related to specifying objectives in protecting personal data, the controller or electronic system administrator must articulate a distinct and specific objective regarding data or identity collection, ensuring compliance with established regulations through procedural and technological support. Any additional data or identity must be safeguarded with protective measures to prevent loss, damage, use, alteration, or distribution, whether intentional or inadvertent.[37] The imperative nature of the security principle in personal data protection is underscored by the existence of regulatory and technological procedures in response to intentional or unintentional threats such as damage, loss, alteration, or leakage, aiming to shield data from cybercrime and misuse by irresponsible entities.

The escalating demands and initiatives for information disclosure have introduced new tensions in the safeguarding of the right to privacy, particularly concerning the personal data and information of citizens. This situation exacerbates the challenge of protecting the right to privacy in Indonesia, as the public exhibits weak awareness regarding the safeguarding of their personal data. Provisions addressing the protection of personal data, especially in electronic form, are confined to Article 26 of the Information and Electronic Transactions Law.[38] The government, functioning as the custodian of public data for data collection and policymaking, faces vulnerability in terms of personal data leakage, especially under the pretext of public information disclosure. Consequently, the current challenge revolves around striking a balance between the imperative to protect privacy and the need for open access to public information. In the Indonesian context, the adopted arrangement is the second model, where information disclosure is governed by Law No. 14 of 2008 concerning Openness of Public Information, while privacy protection is delineated in Minister of Communication and Information Regulation Number 20 of 2016 regarding Protection of Personal Data in Electronic Systems. The concept of data protection implies that individuals

[36] Bart Van der Sloot., Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol.5, no.5, 2014, page.230.

[37] Andhira Wardani, Mahrus Ali, and Jaco Barkhuizen., Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act, *Lex Publica*, Vol.9, no.2, 2022, page.58.

[38] Abdul Kadir Jaelani, and Resti Dian Luthviati., The Crime of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017, *Journal of Human Rights, Culture and Legal System*, Vol.1, no.1, 2021, page.36.

possess the right to decide whether to share or exchange their personal data. Hence, individuals have the authority to determine the conditions under which the transfer of personal data occurs. Privacy protection, as an extension of the right to privacy, has evolved to encompass the right to safeguard personal data. Every individual is entitled to access information regarding their personal data and has the right to rectify or delete any inaccuracies. The principle of individual participation in personal data protection underscores that individuals have the right to express their opinions in decision-making processes that concern their interests, both directly and indirectly.[39] In this context, individuals determine the extent to which decisions regarding personal data will be made.

The government holds the responsibility of managing population data for various developmental purposes, serving as the cornerstone for public service planning, democratic development, legal protection, and the integration of cross-sector systems and administrative levels. The enduring accuracy of population data relies on the state's commitment to respecting, safeguarding, and fulfilling the right to data protection for all. The government's accountability in personal data protection is characterized by key principles: ensuring universal registration coverage without discrimination; removing barriers and gaps in information and technology accessibility; developing a secure and unique identity system; establishing a cross-operational and responsive system; using openly available standards ensuring neutrality between technology providers; prioritizing personal privacy and user control in system design; planning for financial and operational sustainability while maintaining accessibility; safeguarding personal data confidentiality, security, and user rights through a comprehensive legal framework; establishing a comprehensive mandate and accountability; and upholding the legal framework and trust through monitoring and independent complaint mechanisms. The government, in terms of safeguarding an individual's personal data, bears full responsibility for its protection.[40] In the event of a breach, as observed in recent incidents, pertinent government agencies and state institutions are legally obligated, as stipulated in existing laws and regulations. Several aspects demand attention in light of various instances of personal data leaks. Firstly, the vigilance of relevant agencies or institutions is crucial.[41] These entities must remain vigilant and promptly implement necessary security measures to prevent the further dissemination of suspected leaked personal data. Despite the technical nature of these measures, they fundamentally embody principles of integrity and confidentiality.

3.3. Legal Protection for Victims of Dissemination of Personal Data

Identity theft or dissemination refers to the unauthorized transfer or use of an individual's means of identification for illicit purposes. Therefore, it is strongly

[39] Reza Mousavi, Rui Chen, Dan J. Kim, and Kuanchin Chen., Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory, *Decision Support Systems*, Vol.135, no.3, 2020, page.113323.

[40] Ahmad Syaufi, Aurora Fatimatuz Zahra, and Fatham Mubina Iksir Gholi., Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes, *International Journal of Cyber Criminology*, Vol.17, no.1, 2023, page.92.

[41] Nik Thompson, Ravi Ravindran, and Salvatore Nicosia., Government data does not mean data governance: Lessons learned from a public sector application audit, *Government information quarterly*, Vol.32, no.3, 2015, page.319.

advised against sharing any information related to one's identity publicly, be it through social media or messaging applications. Even the slightest details of one's identity can be exploited by criminals for wrongful activities.[42] The pervasive influence of digital technology in people's lives facilitates quick access to information, enabling fraudsters to gradually collect a person's personal identity, which may be utilized for impersonation, leading to financial exploitation of the victim or unauthorized access to personal accounts. The concept of dissemination of personal data, commonly known as doxing, involves the internet-based research and public disclosure of personal information, including personal data, pertaining to individuals or organizations. Douglas stated that doxing originated from dropping documents, signifying a form of revenge in the 1990s.[43] Government regulations in Indonesia, such as Law Number 27 of 2022 Concerning Personal Data Protection, define personal data as information that can be identified individually or in combination with other data, either directly or indirectly, through electronic and/or non-electronic systems.

Deanonymization doxing, or simply deanonymizing, involves the public disclosure of information that unveils the true identity of an individual previously known only by a pseudonym. This category of doxing encompasses situations where someone's identity is revealed to the public, regardless of whether the person intentionally concealed their identity or not. On the other hand, targeting doxing entails the exposure of an individual's identity through various means, such as phone numbers or email addresses, with the specific objective of increasing the subject's physical accessibility. Unlike deanonymizing doxing, targeting doxing differs in the type of personal data disseminated, sharing information such as home addresses, campus addresses, college majors, or office locations.[44] Both deanonymizing doxing and targeting doxing share the common goal of spreading personal information to tarnish an individual's reputation, character, or credibility, often resulting in an attempt to embarrass the person. This particular form of doxing is also commonly referred to as a violation of social norms.

In the realm of disseminating identity confidentiality, preventive efforts play a crucial role in averting potential harm and data leaks. The government, recognizing the significance of protecting personal data and fostering awareness, has implemented guidelines and regulations to address this concern. The Personal Data Protection Law, in particular, outlines preventive measures in Article 17 Paragraph 2. This provision delineates principles governing the processing of personal data, emphasizing limited and specific data collection that is legally valid, transparent, and appropriate. Furthermore, it stresses the alignment of data processing with its intended purpose, ensuring the rights of the data owner, maintaining accuracy, completeness, and relevance, and safeguarding data security against unauthorized access, disclosure, modification, misuse, destruction, or loss. The responsible processing of personal data involves notifying individuals about purposes and processing activities while adhering to the principles of data protection and proving this responsibility clearly.

[42] Sodiki, Achmad., *Kejahatan Mayantara*, Bandung, PT. Refika Aditama, 2010, page.212.
[43] David M. Douglas., Doxing: a conceptual analysis, *Ethics and information technology*, Vol.18, no.3, 2016, page.205.
[44] Jason RC. Nurse., Cybercrime and you: How criminals attack and the human factors that they seek to exploit, *arXiv preprint arXiv:1811.06624*, Vol.45, no.7, 2018, page.133.

These preventive measures also include the timely destruction or deletion of personal data after the retention period or at the request of the data owner, unless statutory regulations dictate otherwise. Ultimately, responsible processing in accordance with the principles of data protection is emphasized, requiring clear evidence of adherence to these principles. These preventive measures within the legal framework aim to guide and steer anticipatory actions, ensuring that issues related to personal data dissemination are addressed proactively, reducing the likelihood of adverse consequences.[45] The processing of personal data is designed to proactively prevent the leakage of such data. This involves collecting personal data in a manner that is limited, specific, legally valid, appropriate, and transparent. The processing ensures the rights of the personal data owner, maintaining accuracy and responsibility. Security measures are in place to protect personal data from unauthorized access, disclosure, misuse, destruction, or loss. Additionally, the processing includes informing individuals about the purposes and activities related to personal data, as well as addressing failures in personal data protection. The Ministerial Regulation on Personal Data Protection for Electronic Systems highlights the obligations of electronic system operators regarding the failure to protect personal data for their users. This can be viewed as a preventive effort, as stated in Article 28, letter c of the Regulation. However, the effectiveness of this preventive protection aspect is deemed premature by the author, considering the ongoing prevalence of data leaks and evolving cybercrimes in the current digital landscape.[46]

Article 28, letter c stipulates the protocol for notifying the owner of personal data in the event of a failure to protect the confidentiality of such data in the managed electronic system. The notification must be in writing and include explicit reasons or causes for the failure. If the Personal Data Owner has given consent, electronic notification is permissible, provided it has been accepted by the owner and is sent no later than 14 days after the discovery of the failure. This preventive measure ensures that the data owner is promptly informed of any breach in data protection, fostering transparency and accountability. The notification process involves clear communication, obtaining consent, and timely delivery of information to address potential losses. Additionally, the Personal Data Protection Law outlines other effective preventive measures to safeguard data processing. This includes the preparation and implementation of technical operational steps to protect personal data from interference that goes against statutory regulations. Moreover, it emphasizes the determination of the security level for personal data, considering the nature and associated risks in the data processing.[47] These measures collectively aim to fortify the protection and security of processed personal data, aligning with the legal framework and addressing potential threats to data integrity.

[45] Sri Ayu Astuti., Penerapan Uu Ite Dan Surat Edaran Kapolri Mengenai Ujaran Kebencian Hate Speech Terhadap Penyimpangan Penggunaan Kebebasan Berekspresi Dalam Kajian Pasal 28 Uud 1945 Tentang Ham Di Ruang Maya Cyber Space, *Lex Publica*, Vol.2, no.2, 2016, page.334.

[46] Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah., Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data, *Padjadjaran Law Review*, Vol.9, no.1, 2021, page.167.

[47] Kumalaratri, Giosita., Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia, *Jurnal Hukum*, Vol.37, no.1, 2021, page.11.

3.4. Balancing Preventive and Repressive Measures in Personal Data Protection

Balancing preventive and repressive measures in personal data protection requires a nuanced approach that incorporates legal, technological, and educational strategies. On the preventive front, a comprehensive legal framework should be established to define clear protocols for responsible data handling and processing. Organizations should prioritize educating individuals on the significance of safeguarding their personal data, encouraging prudent data-sharing practices, and conducting regular privacy assessments to identify and address potential risks. Simultaneously, implementing robust encryption methods and cybersecurity measures is essential to fortify the security of stored and transmitted personal data, mitigating the risk of unauthorized access. Transparency is crucial, necessitating clear notification procedures in the event of a data breach, ensuring individuals are informed promptly about any compromise and the actions taken to address the situation. Government oversight and collaboration with various stakeholders are vital components, establishing regulatory bodies to monitor personal data protection and fostering cooperation between the public and private sectors.

Repressive measures, within this framework, play a critical role in enforcing compliance and accountability. Establishing legal consequences, including sanctions and penalties for data breaches, serves as a deterrent, creating a strong incentive for organizations to adhere to privacy laws. Dispute resolution mechanisms should be outlined, allowing for the swift and fair resolution of violations, reinforcing accountability. Moreover, continuous monitoring, adaptation, and international cooperation are imperative to stay ahead of evolving threats. User empowerment, through tools and knowledge for active data management, and public awareness campaigns contribute to a holistic strategy. By carefully integrating these elements, a balanced approach to personal data protection can be achieved, effectively safeguarding privacy while holding organizations accountable for responsible data handling.

Repressive actions are characterized by their restrictive and oppressive nature, seeking to restore disrupted harmony by imposing sanctions aligned with the committed violation. This repressive approach serves a dual purpose: to address the immediate violation and to act preventively against potential breaches of societal norms.[48] Regulations exist that outline repressive measures for safeguarding the confidentiality of personal data. However, with the enactment of the Personal Data Protection Law, specific provisions for dispute resolution and procedural law have been introduced, as outlined in Article 56. Dispute resolution concerning the protection of Personal Data under the Personal Data Protection Law may involve arbitration, court proceedings, or other alternative dispute resolution mechanisms, all governed by statutory provisions. The procedural law applicable in dispute resolution and court proceedings adheres to statutory provisions and ensures that the process aligns with the principles outlined in the

[48] Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah., Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data, *Padjadjaran Law Review*, Vol.9, no.1, 2021, page.167.

law. In instances necessitating the protection of Personal Data, the hearing process is conducted behind closed doors, emphasizing confidentiality during legal proceedings.

Dispute resolution concerning the protection of Personal Data can be conducted through various channels such as arbitration, court proceedings, or alternative dispute resolution institutions, ensuring compliance with statutory regulations.[49] In instances where safeguarding Personal Data is deemed necessary, the process is supported by valid evidence and electronic information and/or documents. Notably, trial proceedings are conducted in a confidential manner, behind closed doors. Furthermore, the Ministerial Regulation on Personal Data Protection in Electronic Systems introduces an additional protective measure by outlining a dispute resolution mechanism through complaints to the Minister of Communications. Article 29, paragraph 3, of the regulation specifies the grounds for filing a complaint, including instances where the Electronic System Operator fails to provide written notification of the failure to protect the confidentiality of Personal Data to the concerned individual or another Electronic System Operator, regardless of the potential for causing harm. Additionally, complaints can be filed if there has been a loss for the Personal Data Owner or another Electronic System Operator related to the failure in safeguarding the confidentiality of Personal Data, even if a written notification was issued, but the timing of the notification was delayed.

In the event of a failure to protect the confidentiality of personal data, individuals are entitled to file complaints with the Minister. These complaints may be grounded in the failure to issue written notifications about the breach to the data owner or other electronic system operators linked to the personal data, irrespective of the potential for causing harm. Alternatively, complaints may be lodged if there has been a loss for the personal data owner or another electronic system operator connected to the failure in safeguarding the confidentiality of the personal data, even if written notification of the data breach has been provided, but the timing of the notification is belated.[50] In cases where a data leak is attributed to government negligence, the primary responsibility lies with the initial data controller. This accountability extends to both the private and public sectors when the government is involved. Subsequently, the supervisory authority must possess competence and independence to identify errors in both public and private sectors.[51] Ideally, direct communication with the data owner should occur if a data breach occurs.

In essence, legal protection for victims of personal data dissemination encompasses both preventive and repressive measures. In a preventive capacity, victims are afforded safeguards under the Personal Data Protection Law, granting

[49] Borut Stražišar., Alternative dispute resolution, *Право. Журнал Высшей Школы Экономики*, Vol.3, no.2, 2018, page.224.

[50] Maichle Delpiero, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah., Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data, *Padjadjaran Law Review*, Vol.9, no.1, 2021, page.167.

[51] Mahardika, Ahmad Mahardika., Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia, *Jurnal Hukum*, Vol.37, no.2, 2021, page.111.

them the right to rectify inaccuracies and access their personal data. Additionally, repressive efforts involve the right of the data owner to receive written notifications from electronic system operators. As part of preventive measures, the government must intensify supervision of personal data dissemination, particularly by overseeing the security of electronic systems to prevent data leaks. It is crucial for entities handling personal data to align their privacy policies with existing Indonesian laws and regulations. Government initiatives to safeguard personal data and foster awareness include the formulation of guidelines, derivative regulations, educational programs, and awareness campaigns through various media channels. Furthermore, national and international collaboration is imperative. To counter identity theft of personal data, the public is urged to comprehend the types and relevance of personal data, limit its exposure on the internet, understand application permissions, and regularly update anti-theft and security software for operating systems.

4. Conclusion

Cyberstalking, data commercialization, phishing, doxing, and cyber-hacking all contribute to the illegal dissemination of personal data, compromising privacy and exposing individuals to financial gain, harassment, and defamation. Despite existing legal frameworks, such activities continue to pose significant challenges, highlighting the need for a more comprehensive approach to personal data protection. Identity theft and doxing, involving unauthorized use of personal information for malicious purposes, remain pressing concerns.

Legal frameworks like the Indonesian Constitution and the Information and Electronic Transactions Law emphasize the right to privacy, requiring consent for data use and implementing specific regulations to protect personal information. Indonesia's Personal Data Protection Law aims to prevent breaches by ensuring responsible data processing, transparency, and timely destruction of personal data. It also mandates breach notifications and security measures, but concerns over its effectiveness in combating ongoing cybercrimes and data leaks persist. However, issues like public awareness and ongoing data leaks persist, demanding stronger safeguards and effective monitoring.

Balancing preventive and repressive measures in data protection requires a multifaceted strategy involving legal, technological, and educational elements. Preventive actions should include clear protocols for data handling, transparency, cybersecurity measures, and regular privacy assessments. Timely breach notifications and government oversight are essential to prevent data misuse. Repressive measures, including sanctions, effective dispute resolution, and complaint mechanisms, are necessary to enforce compliance. The law mandates confidential hearings and dispute resolution procedures. The government is also tasked with intensifying oversight of electronic systems to prevent leaks. Public awareness campaigns and international cooperation are vital to strengthening personal data protection and preventing identity theft.

References

Books:

Dittrich, David, and Kenneth Einar Himma., 2006, *Hackers, crackers, and computer criminals, Handbook of Information Security,* Bakersfield, California State University;

Fitsanakis, Joseph., 2020, *Redesigning Wiretapping: The Digitization of Communications Interception*. Berlin, Springer Nature;

Landau, Susan., 2011, *Surveillance or security?: The risks posed by new wiretapping technologies*. Mit Press.

Pratama, Bryan., 2019, *Data Pribadi, Data Privasi Dan Komersialisasinya*, Semarang, Binus University;

Sodiki, Achmad., 2010, *Kejahatan Mayantara*, Bandung, PT. Refika Aditama;

Master Theses and PhD Dissertation:

Mirto, Aimee., 2022, *Detecting cyberstalking from social media platform (s) using data mining analytic*s, PhD. Dissertation, London, University of West London;

Ramadha, Bagus Satryo., 2021, *Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi Di Indonesia*, Master Theses, Yogyakarta, Universitas Isam Indonesia;

Conference Proceeding:

Mansell, Robin., 2018, Inequality and digitally mediated communication: Divides, contradictions and consequences, In *Critical Perspectives on Media, Power and Change*, pp. 1-16. London, Routledge, 2018;

Sullins, Lauren L., Phishing for a solution: domestic and international approaches to decreasing online identity theft, In *Computer Crime*, pp. 73-110. London, Routledge, 2017;

Journals:

Abu-Ulbeh, Waheeb, Maryam Altalhi, Laith Abualigah, Abdulwahab Ali Almazroi, Putra Sumari, and Amir H. Gandomi., Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations, *Electronics*, Vol.10, no.14, 2021, https://doi.org/10.3390/electronics10141670;

Afzal, Ayesha, Saba Fazal Firdousi, Ayma Waqar, and Minahil Awais., The influence of internet penetration on poverty and income inequality, *Sage Open*, Vol.12, no.3, 2022, page.21582440221116104, https://doi.org/10.1177/21582440221116104;

Al Mutawa, Noora, Joanne Bryce, Virginia NL Franqueira, and Andrew Marrington. "Forensic investigation of cyberstalking cases using behavioural evidence analysis." *Digital investigation*, Vol.16, no.21, 2016, https://doi.org/10.1016/j.diin.2016.01.012;

Ali, Shaukat, Naveed Islam, Azhar Rauf, Ikram Ud Din, Mohsen Guizani, and Joel JPC Rodrigues., Privacy and security issues in online social networks, *Future Internet*, Vol.10, no.12, 2018, https://doi.org/10.3390/fi10120114;

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, aand Imtiaz Khan., Phishing attacks: A recent comprehensive study and a new anatomy, *Frontiers in Computer Science*, Vol.3, no.4, 2021, https://doi.org/10.3389/fcomp.2021.563060;

Anggraheni, Palupi, Novi Tri Setyowati, and Harry Harry., Social media and political participation in indonesia: restrictions access at announcement results of 2019 presidential election, *Aspiration Journal*, Vol.2, no.1, 2021, https://doi.org/10.56353/aspiration.v2i1.23;

Angkasa, Angkasa, Filep Wamafma, Ogiandhafiz Juanda, and Bhanu Prakash Nunna., Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim, *Lex Scientia Law Review*, Vol.7, no.1, 2023, https://doi.org/10.15294/lesrev.v7i1.67558;

Aniqoh, Nur Aini Fitriya Ardiani., The role of digital economy to enhancing sustainable economic development, *International Journal of Social Science and Business*, Vol.4, no.4, 2020, https://doi.org/10.23887/ijssb.v4i4.28881;

Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin., A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, *Electronics*, Vol.12, no.6, 2023, https://doi.org/10.3390/electronics12061333;

Astuti, Sri Ayu., Penerapan Uu Ite Dan Surat Edaran Kapolri Mengenai Ujaran Kebencian Hate Speech Terhadap Penyimpangan Penggunaan Kebebasan Berekspresi Dalam Kajian Pasal 28 Uud 1945 Tentang Ham Di Ruang Maya Cyber Space, *Lex Publica*, Vol.2, no.2, 2016;

Banterle, Francesco., Data ownership in the data economy: a European dilemma, *EU Internet Law in the Digital Era: Regulation and Enforcement*, Vol.5, no.12, 2020, https://doi.org/10.1007/978-3-030-25579-4_9;

Beduschi, Ana., Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations, *Data & Policy*, Vol.3, no.2, 2021, https://doi.org/10.1017/dap.2021.15;

Benito, Iñigo Gordon., Online harassment and cyberstalking: a case study, *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, Vol.13, no.2, 2023;

Bernoth, Maree, Elaine Dietsch, Oliver Kisalay Burmeister, and Michael Schwartz., Information management in aged care: Cases of confidentiality and elder abuse, *Journal of Business Ethics*, Vol.122, no.3, 2014, https://doi.org/10.1007/s10551-013-1770-7;

Delpiero, Maichle, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah., Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data, *Padjadjaran Law Review*, Vol.9, no.1, 2021;

Douglas, David M., Doxing: a conceptual analysis, *Ethics and information technology*, Vol.18, no.3, 2016, https://doi.org/10.1007/s10676-016-9406-0;

Duijn, Paul AC, and Peter PHM Klerks., Social network analysis applied to criminal networks: recent developments in Dutch law enforcement." *Networks and network analysis for defence and security*, Vol.13, no.7, 2014, https://doi.org/10.1007/978-3-319-04147-6_6;

Fitsanakis, Joseph. *Redesigning Wiretapping: The Digitization of Communications Interception*. Springer Nature, 2020.; Stephen C. Thaman., The Use of Information and Communications Technology in Criminal Procedure in the USA, *Cybercrime, Organized Crime, and Societal Responses: International*

Approaches, Vol.3, no.17, 2017, https://doi.org/10.1007/978-3-030-39919-1;

Gabisch, Jason Aaron, and George R. Milne., The impact of compensation on information ownership and privacy control, *Journal of Consumer Marketing*, Vol.31, no.1, 2014, https://doi.org/10.1108/JCM-10-2013-0737;

Goel, Diksha, and Ankit Kumar Jain., Mobile phishing attacks and defence mechanisms: State of art and open research challenges, *Computers & Security*, Vol.73, no.4, 2018, https://doi.org/10.1016/j.cose.2017.12.006;

Gojali, Djoni Sumardi., Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective, *International Journal of Cyber Criminology*, Vol.17, no.1, 2023;

Hasbullah, M. Afif., Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers, *International Journal of Cyber Criminology*, Vol.16, no.2, 2022;

Hisbulloh, Moh Hamzah., Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi, *Jurnal Hukum,* Vol.37, no.2, 2021, http://dx.doi.org/10.26532/jh.v37i2.16272;

Jaccoud, Lachlan, Lorena Molnar, and Marcelo F. Aebi., Antifa's political violence on Twitter: A grounded theory approach, *European Journal on Criminal Policy and Research*, Vol.29, no.3, 2023, https://doi.org/10.1007/s10610-023-09558-6;

Jaelani, Abdul Kadir, and Resti Dian Luthviati., The Crime of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017, *Journal of Human Rights, Culture and Legal System*, Vol.1, no.1, 2021, https://doi.org/10.53955/jhcls.v1i1.5;

Jokubaitis, Caitlin E., There and Back: Vindicating the Listener's Interests in Targeted Advertising in the Internet Information Economy, *Colum. Columbia Journal of Law & the Arts*, Vol.42, no.34, 2018;

Kerr, Orin S., Cybercrime's scope: interpreting access and authorization in computer misuse statutes, *New York University Law Review,* Vol.78, no.6, 2003;

Kumalaratri, Giosita., Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia, *Jurnal Hukum*, Vol.37, no.1, 2021, http://dx.doi.org/10.26532/jh.v37i1.13604;

Lin, Jiesen, Lemuria Carter, and Dapeng Liu., Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app, *European Journal of Information Systems*, Vol.30, no.4, 2021, https://doi.org/10.1080/0960085X.2021.1920857;

MacAllister, Julia M., The doxing dilemma: seeking a remedy for the malicious publication of personal information, *Fordham Law Review,* Vol.85, no.2, 2016;

Mahardika, Ahmad Mahardika., Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia, *Jurnal Hukum*, Vol.37, no.2, 2021, http://dx.doi.org/10.26532/jh.v37i2.16994;

Makarim, Edmon., Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach, *Data Protection Around the World: Privacy Laws in Action*, Vol.22, no.6, 2021, https://doi.org/10.1007/978-94-6265-407-5_6;

Manthovani, Reda., Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law, *International Journal of Criminal Justice Sciences*, Vol.18, no.1, 2023;

Mousavi, Reza, Rui Chen, Dan J. Kim, and Kuanchin Chen., Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory, *Decision Support Systems*, Vol.135, no.3, 2020, https://doi.org/10.1016/j.dss.2020.113323;

Nakhjavan, Alicia., The Worst Law in Technology: How the Computer Fraud and Abuse Act Allows Big Businesses to Collect and Sell Your Personal Information, *Brooklyn Law Review,* Vol.87, no.21, 2021;

Nugroho, Agus, and An An Chandrawulan., Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries, *Security Journal*, Vol.36, no.4, 2022, https://doi.org/10.1057/s41284-022-00357-y;

Nurse, Jason RC., Cybercrime and you: How criminals attack and the human factors that they seek to exploit, *arXiv preprint arXiv:1811.06624*, Vol.45, no.7, 2018, https://doi.org/10.48550/arXiv.1811.06624;

Rosadi, Sinta Dewi, Andreas Noviandika, Robert Walters, and Firsta Rahadatul Aisy., Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?, *International Review of Law, Computers & Technology*, Vol.37, no.1, 2023, https://doi.org/10.1080/13600869.2022.2114660;

Rudiyanto, Tri, Halley Kunda, Amy Dunn, Sharon Shenderovskiy, and Rondarrius Gibson., Ethical and Legal Concerns of Artificial Intelligence in the Workplace: Examining Current Legislations in the United States, *Lex Publica*, Vol.10, no.1, 2023;

Siahaan, Mona Natasha, Putu Wuri Handayani, and Fatimah Azzahro., Self-disclosure of social media users in Indonesia: the influence of personal and social media factors, *Information Technology & People*, Vol.35, no.7, 2022, https://doi.org/10.1108/ITP-06-2020-0389;

Singh, L. Joy, and N. I. E. L. I. T. Imphal., A survey on phishing and anti-phishing techniques, *International Journal of Computer Science Trends and Technology (IJCST)*, Vol.6, no.2, 2018;

Sitohang, Bertrand Silverius, Sahata Manalu, Mancur Sinaga, and Niswan Harefa., The Validity of Marriage Through Constitutional Court Decision Number 69/Puu-XIII/2015 Reviewed from Law Number 1 Of 1974, *Jurnal Pendidikan Tambusai,* Vol.7, no.3, 2023, https://doi.org/10.31004/jptam.v7i3.9541;

Sitompul, Josua., Developing a Legal Framework of Personal Data Protection in the Indonesian Criminal Procedure Law, *Indonesia Law Review,* Vol.9, no.3, 2019;

Sloot, Bart Van der., Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol.5, no.5, 2014;

Stražišar, Borut., Alternative dispute resolution, *Право. Журнал Высшей Школы Экономики*, Vol.3, no.2, 2018, https://doi.org/10.17323/2072-8166.2018.3.214.233;

Suryawardani, Bethani, and Astri Wulandari., Determinant factors of customers switching behavior to customer satisfaction and loyalty in online transportation users in bandung, *JDM (Jurnal Dinamika Manajemen)*, Vol.11, no.1, 2020, https://doi.org/10.15294/jdm.v11i1.21432;

Suyaman, Prahasti, and Temmy Fitriah Alfiany., Polemics of Interfaith Marriage Reviewed from the Perspectives of Marriage Law and the Compilations of Islamic Law, *KnE Social Sciences*, Vol.13, 2022, https://doi.org/10.18502/kss.v7i15.12129;

Syaufi, Ahmad, Aurora Fatimatuz Zahra, and Fatham Mubina Iksir Gholi., Employing

Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes, *International Journal of Cyber Criminology*, Vol.17, no.1, 2023;

Tabroni, Imam, Hisam Ahyani, and Dian Permana., Philosophical Review of Materialism and Idealism Limits of Wedding Age in Indonesia; Study of Article 7 Paragraph (1) of Law 16 of 2019 Jo. Law 1 of 1974 Concerning Marriage, *Muttaqien: Indonesian Journal of Multidiciplinary Islamic Studies,* Vol.2, no.1, 2021, https://doi.org/10.52593/mtq.02.1.01;

Taherdoost, Hamed., Insights into Cybercrime Detection and Response: A Review of Time Factor, *Information*, Vol.15, no.5, 2024, https://doi.org/10.3390/info15050273;

Tewathia, Nidhi, Anant Kamath, and P. Vigneswara Ilavarasan., Social inequalities, fundamental inequities, and recurring of the digital divide: Insights from India, *Technology in Society*, Vol.61, 2020, https://doi.org/10.1016/j.techsoc.2020.101251;

Thaman, Stephen C., The Use of Information and Communications Technology in Criminal Procedure in the USA, *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Vol.3, no.17, 2017, https://doi.org/10.1007/978-3-319-44501-4_6;

Thompson, Nik, Ravi Ravindran, and Salvatore Nicosia., Government data does not mean data governance: Lessons learned from a public sector application audit, *Government information quarterly*, Vol.32, no.3, 2015, https://doi.org/10.1016/j.giq.2015.05.001;

Van der Sloot, Bart., Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data, *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol.5, no.5, 2014;

Wardani, Andhira, Mahrus Ali, and Jaco Barkhuizen., Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act, *Lex Publica*, Vol.9, no.2, 2022;

Wati, Reka Desrina., The Marriage Agreement in Article 29 of Law Number 1 of 1974 is Reviewed According to Islamic Law, *Al Hurriyah: Jurnal Hukum Islam,* Vol.7, no.2, 2022, https://doi.org/10.30983/alhurriyah.v7i2.4125;

Widiani, Ah Kholish Hayatuddin Desti., Socio-Juridical Analysis on Polygamy Requirements in the Compilation of Islamic Law (KHI), *Al-'Adalah,* Vol.19, no.1, 2022, https://dx.doi.org/10.24042/adalah.v19i1.10266;

Xiao, Anran, Zeshui Xu, Marinko Skare, Yong Qin, and Xinxin Wang., Bridging the digital divide: the impact of technological innovation on income inequality and human interactions, *Humanities and Social Sciences Communications*, Vol.11, no.1, 2024, https://doi.org/10.1057/s41599-024-03307-8;

Yanto, Oksidelfa., Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development, *Lex Publica*, Vol.7, no.2, 2020;

Yudiana, Teguh Cahya, Sinta Dewi Rosadi, and Enni Soerjati Priowirjanto., The urgency of doxing on social media regulation and the implementation of right to be forgotten on related content for the optimization of data privacy protection in Indonesia, *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, Vol.9, no.1, 2022.