A Legal Analysis of Criminal Liability for Perpetrators of Personal Data Misuse (A Case Study of Decision Number 541/Pid.Sus/2022/PN. Mdn)

Rifqi Fairuz Ula, Abdul Rahman Maulana Siregar, Sumarno

Abstract

This study aims to analyze the form of criminal liability and the legal considerations of judges in adjudicating personal data misuse in Verdict Number 541/Pid.Sus/2022/PN. Mdn. Employing a normative legal research method with case and statutory approaches, this study examines secondary data comprising court decisions and relevant legal literature. The findings reveal that the defendant was legally and convincingly proven to have met both the material and formal elements of cybercrime through unauthorized data access and manipulation. Criminal liability was imposed based on the presence of fault (*mens rea*) and the perpetrator's legal capacity. This study concludes that while the imposition of criminal sanctions in this verdict aligns with the prevailing positive law, the judicial interpretation remains textually normative. The implication of this research is expected to contribute theoretically to the development of cyber law and serve as a practical reference for law enforcement officers in optimizing evidentiary standards and data privacy protection in Indonesia.

Keywords: *Criminal Liability, Personal Data Misuse, Cybercrime, Court Verdict.*

Rifqi Fairuz Ula[1]
[1]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: rifqi.ula@gmail.com[1]

Abdul Rahman Maulana Siregar[2], Sumarno[3]
[2,3]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: abdulrahmanms@dosen.pancabudi.ac.id[2], sumarno@dosen.pancabudi.ac.id[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The proliferation of information technology has disrupted multifaceted sectors of life, catalyzing a massive transition from conventional administrative systems to the digitalization of data ecosystems. Within this landscape, personal data has metamorphosed into a highly valuable asset profoundly susceptible to threats of exploitation and illicit access [1]. Cybercrimes featuring the modus operandi of personal data misuse are becoming increasingly escalatory and intricate, thereby demanding the preparedness of both material and formal criminal law instruments to provide integrative protection. The scope of these transgressions is no longer confined to physical identity theft but has proliferated into the interception and manipulation of electronic systems, inflicting multifaceted detriments upon data subjects [2]. Consequently, law enforcement through judicial verdicts assumes a pivotal role as the manifestation of repressive legal protection.

A review of prior literature (state of the art) indicates that the discourse surrounding personal data protection remains predominantly monopolized by studies encompassing civil law and state administrative law dimensions. Previous research conducted by [3], for instance, places greater emphasis on the exigency of formulating comprehensive personal data protection regulations. Meanwhile, another study by [4] focuses on the civil liability of electronic system operators for negligence resulting in data breaches. Specific inquiries dissecting the anatomy of individual perpetrators' criminal liability, particularly concerning the substantiation of malicious intent (mens rea) in Indonesian cybercrimes, remain relatively nascent and are generally confined to theoretical echelons [5].

In constructing criminal liability for cybercrimes, it is imperative to anchor it upon general criminal law doctrines. As asserted, the determination of absolute criminal liability must deliberate the fulfillment of the elements of unlawful acts, the presence of fault on the part of the perpetrator, and the perpetrator's capacity for legal responsibility. [6]

Departing from these literature gaps, the scientific novelty of this article lies in its object of study, which exclusively scrutinizes the application of law in concreto. Diverging from preceding research which tended to be macro and purely normative in nature, this study microscopically dissects the application of criminal elements and legal liability through a case study of the Medan District Court Decision Number 541/Pid.Sus/2022/PN. Mdn. The nucleus of this research is directed toward how Indonesian positive law responds to and accommodates the complexities of data-misuse-based cybercrimes within the realities of judicial proceedings.

Based on the aforementioned background, the primary issue addressed in this research is the form of criminal liability imposed upon perpetrators of personal data misuse crimes according to Decision Number 541/Pid.Sus/2022/PN. Mdn. In alignment with this formulation of the problem, the writing of this scientific article aims to juridically analyze the implementation of criminal liability and the foundational judicial reasoning in adjudicating the a quo case. The results of this analysis are anticipated to furnish theoretical prescriptions for the development of cyber-criminal law and function as a practical touchstone for handling analogous cases in the future.

Literature Review

A. The Concept of Criminal Liability

The study of criminal liability is rooted in the fundamental principle of geen straf zonder schuld, signifying "no punishment without fault." Within criminal law doctrine, penalization cannot merely rely on the occurrence of an outward act prohibited by law (actus reus), but must be accompanied by a wicked or reprehensible state of mind of the perpetrator (mens rea) [7]. Fault in this context encompasses both intent (dolus) and negligence (culpa), as well as the legal subject's competence to bear responsibility for their actions [8]. Furthermore, the element of unlawfulness (wederrechtelijkheid) dictates whether an act satisfying the formulation of the offense can truly be subjected to criminal sanctions or whether penal abolition grounds exist

[9]. These foundational concepts serve as the primary analytical scalpel to ascertain whether data misusers in cyberspace can be legitimately held liable before the law.

B. Personal Data Misuse in the Cyber Legal Ecosystem

Cybercrimes possess borderless and anonymous characteristics, significantly distinguishing them from conventional crimes. Technological penetration mandates a paradigm shift in criminal law to accommodate new legal objects in the form of electronic data. Dogmatically, the misuse of personal data constitutes an infringement of privacy rights possessing a criminal dimension if it satisfies the elements of illegal access, interception, or manipulation of data without lawful authority [10].

In an increasingly integrated digital ecosystem, personal data has metamorphosed into a crucial asset harboring both economic value and profound vulnerability. As articulated by Fitrianto et al., this acceleration of digitalization entails the logical consequence of heightened cybersecurity risks, wherein sensitive data is highly susceptible to illicit utilization through identity manipulation, theft, and hacking by irresponsible entities. [11] In Indonesia, the normative framework to prosecute these crimes historically rested upon the Law on Information and Electronic Transactions (UU ITE), before ultimately being specifically fortified by the Personal Data Protection Law (UU PDP). The legal construct within these regulations accentuates the protection of the integrity, confidentiality, and availability of data from any form of exploitation detrimental to the data subject [12].

C. Review of Previous Literature (State of the Art)

As a comparative foundation and theoretical stepping stone, this research navigates a plethora of relevant prior literature. A study conducted by [13] underscores the vulnerabilities of conventional criminal evidentiary systems when confronted with the characteristics of electronic evidence prone to degradation. On a divergent focus, [14] analyzes the disparity in judicial decisions regarding cybercrime penalization, where a lack of uniformity is frequently observed in interpreting the element "intentionally and without rights" in illegal access offenses. Meanwhile, a study by [15] dissects corporate criminal liability in data breach cases, highlighting the paradigm shift from individual perpetrators to business entities.

From this literature mapping, it is evident that the majority of studies remain confined to the echelons of general regulatory and evidentiary analysis. Therefore, this research is positioned to bridge the literature gap by constructing a specific analysis of the legal reasoning of first-instance judges. The exclusive examination of Decision Number 541/Pid.Sus/2022/PN. Mdn is functionalized to empirically observe how the panel of judges assembles legal facts, appraises digital evidence, and determines the criminal liability of individual personal data offenders within the contemporary Indonesian criminal justice system.

Research Methodology

This research is constructed as normative legal research, positioning the law as an edifice of normative systems. The approaches utilized to resolve the legal issues encompass the statute approach and the case approach. The statute approach is employed to scrutinize the coherence of positive legal regulations pertinent to cybercrimes and data protection. Concurrently, the case approach serves as the principal instrument to meticulously dissect the ratio decidendi or judicial reasoning of the judges in the Medan District Court Decision Number 541/Pid.Sus/2022/PN. Mdn.

Given the doctrinal nature of the research, the primary instruments emanate from the compilation of legal materials divided into two classifications. Primary legal materials encompass authoritative regulations such as the Penal Code (KUHP), the Criminal Procedure Code (KUHAP), the Law on Information and Electronic Transactions, alongside the authentic document constituting the official transcript of Decision Number 541/Pid.Sus/2022/PN. Mdn. Conversely, secondary legal materials are acquired through academic literature, criminal law

textbooks, and cutting-edge scientific journals that provide elucidations regarding the correlated primary legal materials.

The technique for collecting legal materials is executed through a documentary study by inventorying literature and decision dossiers relevant to the focal point of the study. Furthermore, the analytical technique employed is qualitative analysis. All collated legal materials are not evaluated utilizing mathematical or statistical models but are instead explicated in a descriptive-analytical manner. The deductive reasoning process underpins the drawing of conclusions, specifically by intertwining the major premise—consisting of propositions and general principles of criminal liability—with the minor premise—comprising legal facts and evidentiary proceedings in the concrete case at the Medan District Court—to engender a precise conclusion.

Results

Based on the exploration of trial facts revealed in the Medan District Court Decision Number 541/Pid.Sus/2022/PN. Mdn, the judex facti panel of judges has comprehensively delineated the anatomy of the personal data misuse crime perpetrated by the defendant. Objectively (actus reus), the defendant's actions of possessing, manipulating, and transmitting the victim's electronic information without authorization were legally and conclusively proven to fulfill the offense formulation within the Law on Information and Electronic Transactions (UU ITE). In its deliberations, the panel of judges gravitated towards the material acts of data exploitation that inflicted both financial and immaterial detriments upon the data subject, wherein the digital footprints presented by the Public Prosecutor at the trial were deemed to possess valid and incontrovertible evidentiary weight in accordance with the cyber evidentiary legal regime.

In constructing the criminal liability, the panel of judges predicated their decision on the fulfillment of the fault element (mens rea) in the form of intent as a purpose (opzet als oogmerk). The defendant consciously intended the act of accessing another party's personal data and was fully cognizant of the legal ramifications of said action. Although technology affords copious conveniences, the vulnerability of privacy systems in the digital realm is inescapable. As expounded by Muhammad Arif Sahlepi et al., in the contemporary era of globalization, cybercrime has transmuted into a profoundly significant and massive peril worldwide, encompassing Indonesia [16].

Furthermore, the panel of judges discerned no presence of justification grounds (rechtvaardigingsgrond) nor excusatory grounds (schulduitsluitingsgrond) capable of obliterating the unlawful nature (wederrechtelijkheid) of the defendant's actions. This corroborates that the defendant possessed full capacity for responsibility (toerekeningsvatbaarheid) both psychologically and cognitively at the time of committing the criminal offense, rendering the imposition of imprisonment and fines a proportional juridical consequence.

The efficacy of imposing criminal sanctions in Decision Number 541/Pid.Sus/2022/PN. Mdn must be scrutinized. As elucidated by Ali Yusran Gea, "A good law is a law that is just, lucid, and enforceable, while also being capable of furnishing legal certainty and protection for society." The verdict of the judicial panel ought to be capable of representing such legal certainty to ensure no further latitude remains for abusers of electronic data. [17]

When the phenomenon of legal reasoning in this decision is comparatively juxtaposed with the findings of earlier research, a sufficiently significant paradigm shift becomes apparent. In prior comparative studies conducted by [18], judges were frequently ensnared by technical evidentiary impediments and rigid interpretations of the "intentionally" element in information technology crimes. However, in the in casu decision, the panel of judges has exhibited a more progressive comprehension by accommodating electronic evidence not merely as supplementary indicia, but rather as paramount, independent instruments of evidence. If juxtaposed with research [19] which critiques the leniency toward cybercrimes in Indonesia,

this Medan District Court decision reflects an endeavor to optimize the deterrent effect, wherein the judges employ a penalization approach oriented toward both retribution and societal protection.

In every asymmetrical legal relationship, the state is obligated to intervene to protect the more vulnerable party, as in the case of victims of personal data exploitation. This resonates with the perspective of Rika Jamin Marbun et al., who assert that the existence of legal regulations and government intervention are unconditionally necessitated to respond to positional disparities among parties, ensuring citizens' rights remain recognized and equitably protected. [20]

As an intellectual contribution and projection for future law enforcement, the analysis of this decision yields a pivotal note concerning the transition of the regulatory ecosystem. A quo decision was pronounced utilizing the instruments of the ITE Law because the criminal event (tempus delicti) transpired prior to the full enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Moving forward, law enforcement apparatuses are mandated to transition to utilizing the Lex specialist of the UU PDP, which dictates substantially more rigorous and specific criminal sanctions against both corporate entities and individual data leakers. The implications of these findings necessitate the harmonization of comprehension among law enforcement personnel to avert overlapping application of articles between the ITE Law and the UU PDP, aiming to guarantee legal certainty and more substantive privacy protection for the Indonesian populace in the digital era.

Conclusion

Predicated on the elucidated analysis of problem resolution, this research concludes that the architecture of criminal liability for perpetrators of personal data misuse in Decision Number 541/Pid.Sus/2022/PN. Mdn is coherently constructed through the cumulative substantiation of the elements of a criminal act and the element of fault. The panel of judges has precisely qualified the defendant's material actions as a manifestation of illegal access and exploitation that fulfills the offense qualifications stipulated in the Law on Information and Electronic Transactions. The imposition of criminal sanctions was legitimately executed because, dogmatically, the defendant was proven to possess malicious intent (mens rea) in the form of intent as a purpose, possessed full legal capacity to be held accountable for their actions, and due to the absence of penal abolition grounds capable of nullifying the unlawful nature (wederrechtelijkheid) of said act.

The pronouncement of this verdict corroborates that extant positive legal instruments can be straightforwardly implemented to respond to and prosecute crimes possessing a cyber dimension. As an implication of this study's findings, the a quo decision empirically affirms that electronic evidence instruments and digital footprints possess robust evidentiary status and validity within the framework of modern Indonesian criminal procedural law. The evolution of these findings projects an urgent exigency for a paradigm shift in future law enforcement, preeminently following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Jurisprudence and progressive penalization approaches, such as those manifests in this decision, must be integrated with the Lex specialis provisions encapsulated in the newly established UU PDP. Therefore, law enforcement apparatuses are compelled to perpetually recalibrate their investigative capacities and prosecutorial standardization to engender legal harmonization capable of providing data privacy protection that is more comprehensive, equitable, and maximizes the deterrent effect in the digital era.

References

[1] A. S. R. Sinaga dan M. H. Siregar, "Perlindungan hukum terhadap data pribadi sebagai hak privasi di era ekonomi digital," *J. Huk. & Pembang.*, vol. 50, no. 2, pp. 312–328, 2020.

[2] D. N. E. P. Litaay, "Anatomi kejahatan siber dan penegakan hukum pidana di Indonesia," *J. Huk. Ius Quia Iustum*, vol. 25, no. 1, pp. 112–130, 2018.
[3] S. R. P. Tampubolon and E. S. K. B. Ginting, "Urgensi pengesahan rancangan undang-undang perlindungan data pribadi di Indonesia," *J. Penelit. Huk. De Jure*, vol. 21, no. 3, pp. 345–358, 2021.
[4] E. Y. L. Nabila, "Tanggung jawab perdata penyelenggara sistem elektronik atas kegagalan perlindungan data pribadi," *J. Huk. Bisnis Bonum Commune*, vol. 3, no. 2, pp. 210–225, 2020.
[5] M. A. Nawawi, "Pembuktian unsur mens rea dalam tindak pidana penyalahgunaan data elektronik," *J. Kriminologi Indonesia.*, vol. 16, no. 1, pp. 45–60, 2020.
[6] R. R. H. Sitorus, M. A. Siregar, and F. Rafianti, "The Problem of Classification of Perpetrators in Narcotics Crimes During the Investigation Stage at the North Sumatra Regional Police," in *2nd International Conference on Islamic Community Studies (ICICS)*, 2024, pp. 7134–7139.
[7] Moeljatno, *Asas-Asas Hukum Pidana*. Jakarta, Indonesia: Rineka Cipta, 2018.
[8] E. O. S. Hiariej, *Prinsip-Prinsip Hukum Pidana*, Edisi Revisi. Yogyakarta, Indonesia: Cahaya Atma Pustaka, 2016.
[9] B. N. Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta, Indonesia: Kencana, 2017.
[10] I. G. B. A. Dharmawan, "Kualifikasi delik akses ilegal terhadap data pribadi berdasarkan undang-undang Informasi dan Transaksi Elektronik," *J. Magister Huk. Udayana (Udayana Master Law J.)*, vol. 11, no. 2, pp. 321–335, 2022.
[11] B. Fitrianto, A. S. P. Gaja, A. F. Dalimunthe, A. V. R. B. Manurung, and A. S. Harahap, "Kerangka Regulasi Open Banking dan Perlindungan Data Pribadi Nasabah," Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, vol. 4, no. 1, pp. 536–550, 2026.
[12] R. A. Gani, "Transisi rezim perlindungan data pribadi dari UU ITE menuju UU PDP: Sebuah tinjauan yuridis," *J. Legislasi Indonesia.*, vol. 19, no. 4, pp. 489–502, 2022.
[13] A. Setyawan, "Validitas dan kekuatan pembuktian alat bukti elektronik dalam persidangan pidana," *J. Huk. Acara Pidana*, vol. 5, no. 1, pp. 77–92, 2019.
[14] D. H. Permana and L. A. Wibowo, "Disparitas putusan hakim dalam perkara tindak pidana siber: Analisis unsur dengan sengaja dan tanpa hak," *J. Yudisial*, vol. 14, no. 2, pp. 199–218, 2021.
[15] F. T. Alamsyah, "Pertanggungjawaban pidana korporasi dalam kasus kebocoran data konsumen pada aplikasi digital," *J. Huk. Pidana dan Kriminologi*, vol. 2, no. 2, pp. 150–167, 2021.
[16] H. Y. Prasetyo, "Kendala pembuktian niat jahat (mens rea) dalam kejahatan teknologi informasi: Studi komparatif putusan Pengadilan Negeri," *J. Huk. Progresif*, vol. 9, no. 1, pp. 88–104, 2021.
[17] W. Fahriza, M. A. Sahlepi, and Rahmayanti, "Effectiveness of Law Enforcement against Cybercrime in Indonesia: Study on Hacking Crimes and the Role of the ITE Law," *Law Synergy Conference (LSC)*, vol. 1, no. 1, 2024.
[18] A. Y. Gea, "Analisis Konflik Pengaturan Tindak Pidana Penggelapan Objek Fidusia dalam UU Fidusia dan KUHP," *Rewang Rencang : Jurnal Hukum Lex Generalis*, vol. 6, no. 7, pp. 1–10, 2025.
[19] B. Susanti, "Kritik terhadap kebijakan pemidanaan tindak pidana siber di Indonesia: Antara efek jera dan keadilan," *J. Huk. Pidana Islam*, vol. 6, no. 2, pp. 211–228, 2020.
[20] R. J. Marbun, Rahmayanti, and M. R. Faisal, "Penerapan Hukum Ketenagakerjaan Terhadap Pekerja/Buruh Yang Mengalami Pemutusan Hubungan Kerja (PHK) Pasca Berlakunya Undang-Undang Nomor 11 Tahun 2020 Tentang Cipta Kerja," *Jurnal Darma Agung*, vol. 32, no. 1, pp. 420–430, 2024.