SSJ
Social Sciences Journal
Volume 3 Issue 2, 2026 (367-372)
ISSN (*online*) : 3047-7646
Homepage : https://jurnalunived.com/index.php/SOSJ
Doi : https://doi.org/10.37676/sosj

Criminal Liability For The Misuse Of Personal Data: A Comparative Study Of Decision Number 628/PID.SUS/2020/PN.BTM And Number 541/PID.SUS/2022/PN.MDN Concerning Cybercrimes

Rifqi Fairuz Ula [1], Abdul Rahman Maulana Siregar [2], Sumarno [3]
Universitas Pembangunan Panca Budi, Medan, Indonesia
e-mail: rifqi.ula@gmail.com

Received [19-07-2026] Revised [22-08-2026] Accepted [25-082026)

Abstract. This study endeavors to scrutinize the criminal liability pertinent to the misuse of personal data as adjudicated in Decision Number 628/Pid.Sus/2020/PN.Btm and Decision Number 541/Pid.Sus/2022/PN.Mdn, specifically evaluated through the lens of the digital evidentiary system. Furthermore, it analyzes the congruence of this evidentiary framework with the evidentiary stipulations delineated in Law Number 20 of 2025 concerning the Criminal Procedure Code (the new KUHAP). The methodology employed is normative legal research, utilizing both a statutory approach and a case approach. Data analysis was executed qualitatively by meticulously processing and interpreting legal materials via a descriptive-analytical methodology. The findings reveal a discernible variance in interpretation and the trajectory of judicial reasoning (ratio decidendi) when appraising elements of unlawful acts, mens rea, and the probative value of electronic evidence within cybercrime adjudications. These divergent approaches are precipitated by a confluence of normative, juridical (case construction), and non-juridical variables. Ultimately, this comparative analysis elucidates the dichotomy between normative ideals (das Sollen) and judicial realities (das Sein), proposing recommendations for standardized legal enforcement to safeguard legal certainty and equity in the digital epoch.

Keywords: *Criminal Liability, Misuse of Personal Data, Digital Evidence, New Criminal Procedure Code.*

INTRODUCTION

The exponential advancement of information and communication technology has catalyzed a fundamental metamorphosis within modern society, particularly augmenting economic activities, governmental administration, and social interactions. The ubiquitous use of electronic systems, while facilitating unprecedented convenience and efficiency, has concurrently engendered novel forms of criminality, collectively designated as cybercrime. The accelerated technological progression invariably correlates with an escalation in electronic-based transgressions. This phenomenon dictates that the criminal evidentiary framework must possess the adaptive capacity to navigate these developments, thereby ensuring the administration of justice within the judicial process.

In criminal law, criminalization is a component of criminal policy. Criminal policy constitutes the state's strategic endeavor to combat criminality, functioning fundamentally as an integral facet of community protection initiatives oriented toward the realization of social well-being.

One of the most prevalent modalities of cybercrime is the illicit exploitation of personal data. Personal data constitutes information imbued with profound strategic and sensitive value, given its intrinsic correlation to an individual's identity. The misuse of such data—whether

through unauthorized acquisition, unlawful utilization, or illicit dissemination across electronic systems—is capable of inflicting severe detriments upon data subjects, encompassing both material and immaterial damages. Jurisprudentially, Indonesia has enacted a multiplicity of legal instruments to afford protection; nevertheless, the operationalization of these frameworks remains encumbered by systemic impediments, including suboptimal coordination and resource constraints. Consequently, the state is under an unequivocal obligation to institutionalize effective legal safeguards, notably through the apparatus of criminal law.

Prompted by these correlations, an imperative arises for the modernization and progressive evolution of the contemporary criminal justice system. This trajectory signifies a paradigm shift from a purely retributive approach, which predominantly fixates on retaliation, toward a more humanistic, dialogic, and restorative-oriented paradigm.

Before the promulgation of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), the regulatory framework governing personal data in Indonesia was fragmented across disparate legislative instruments. A primary locus was Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE), subsequently amended by Law Number 1

of 2024. In the realm of law enforcement practice, investigative and judicial apparatuses exhibited a propensity to invoke the penal provisions stipulated within the UU ITE to prosecute perpetrators of personal data misuse, notwithstanding the fact that the said provisions had not yet comprehensively codified the specific conceptual contours of personal data.

Judicial verdicts assume a pivotal function as the concrete manifestation of the application of penal norms to specific legal phenomena. Within the context of cybercrime, a judge's decision mirrors the architectural construction of criminal liability, encapsulating the hermeneutics applied to elements of unlawful acts, culpability, and the substantiation predicated on electronic evidence. Consequently, a rigorous examination of judicial decisions is profoundly pertinent for evaluating the consistency and evolutionary trajectory of cybercrime law enforcement in Indonesia.

Decision Number 628/Pid.Sus/2020/PN.Btm and Decision Number 541/Pid.Sus/2022/PN.Mdn represents two district court rulings adjudicating cybercrimes intertwined with the misuse of personal data. Despite sharing identical criminological characteristics, these cases were adjudicated by disparate judicial panels, yielding legal rationales that lack absolute uniformity. This discrepancy underscores a potential divergence in the formulation of criminal liability applied by judges in adjudicating offenses related to personal data exploitation.

From a critical scholarly vantage point, this incongruity in judicial reasoning constitutes the primary locus of inquiry for this research. The divergent verdicts in these respective cases illustrate the expansive interpretative latitude inherent in the application of criminal law, most notably concerning cybercrimes, which remain a relatively nascent and fluid domain within the Indonesian legal architecture. This paradigm provokes fundamental interrogations regarding the consistency of judges in applying the principles of criminal liability and the extent to which the maxims of legal certainty, justice, and utility are empirically actualized in judicial praxis.

Furthermore, the intellectual merit of this research transcends a mere rudimentary identification of divergent rulings; it systematically endeavors to anatomize the ratio decidendi underpinning each respective verdict. By doing so, this study aims to elucidate whether these divergences stem from normative variables (discrepant interpretations of statutory regulations), juridical factors (evidentiary appraisal and case construction), or non-juridical considerations, such as the ideological predispositions of the presiding judges toward cyber-criminality.

LITERATURE REVIEW

Theoretical Framework

Within the doctrinal framework of criminal law, the concept of criminal liability stands as a fundamental axiom dictating whether an individual is subject to penal sanctions for their conduct. The imposition of criminal liability inherently necessitates the concomitant presence of a prohibited act (actus reus) and a culpable state of mind (mens rea) residing within the perpetrator. In the specific context of personal data misuse, the theoretical construct of legal protection for personal data functions as an indispensable foundation for this scholarly inquiry. Personal data constitutes an integral manifestation of the individual right to privacy, an inalienable human right that the state is obligated to safeguard. The protection of personal data transcends mere administrative protocols; it inherently possesses a penal dimension when unlawful exploitation inflicts deleterious consequences upon the data subject.

METHODS

This study employs a normative legal research methodology, fundamentally concentrating on the rigorous examination of written legal norms enshrined within statutory regulations and judicial verdicts. The architectural design of this doctrinal research is not oriented towards the empirical evaluation of societal behavioral paradigms; rather, it is meticulously calibrated to profoundly analyze the law as an integrated, holistic system of norms (law in books). Acknowledging that normative legal research scrutinizes legal dogmatics and principles, conventional quantitative components such as statistical variables, population metrics, or sampling methodologies are explicitly excluded from this framework.

Statutory Approach

The statutory approach is operationalized through an exhaustive inventory, rigorous appraisal, and critical analysis of the constellation of regulations intrinsically linked to the jurisprudence of cyber law and personal data protection. The analytical locus is directed toward assessing the normative coherence and interplay between the Law on Information and Electronic Transactions (UU ITE), the Personal Data Protection Law (UU PDP), and the newly promulgated Criminal Procedure Code (Law Number 20 of 2025).

Case Approach

The case approach is instrumentalized through an intensive jurisprudential dissection of court decisions that have attained permanent legal force (inkracht van gewijsde). The empirical nexus of this case analysis focuses comparably on Decision Number 628/Pid.Sus/2020/PN.Btm and Decision Number 541/Pid.Sus/2022/PN.Mdn, aiming to anatomize the ratio decidendi specifically pertaining to the offense of personal data misuse.

RESULTS

Criminal Liability for the Misuse of Personal Data in Decision Number 628/Pid.Sus/2020/PN.Btm and Number 541/Pid.Sus/2022/PN.Mdn from the Perspective of the Digital Evidence Proof System

The omnipresence of information and communication technology within the dynamics of contemporary society has not merely reconfigured paradigms of social interaction but has simultaneously precipitated a profound transmutation in the typology of criminality, manifesting as cybercrime. Within the domain of criminal jurisprudence, the enforcement of law against this phenomenon mandates a comprehensive criminal policy meticulously architected to provide community protection, thereby ensuring the preservation of social welfare. Before the operationalization of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), law enforcement architectures predominantly relied on the hermeneutics of provisions

encapsulated within Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), as most recently amended by Law Number 1 of 2024. This paradigm introduced profound complexities, as the normative framework within the UU ITE had not yet conceptualized personal data protection in a highly specialized and integrative manner, consequently generating potential legal ambiguity in the adjudication of criminal liability.

The establishment of criminal liability in cybercrimes involving the exploitation of personal data as an economically lucrative asset necessitates an exacting examination of two foundational elements: the unlawful act (actus reus) and the psychological culpability of the perpetrator (mens rea). Anchored in the maxim 'geen straf zonder schuld' (no punishment without fault), adjudicating judges are compelled to transcend the mere objective-formal fulfillment of offense elements, being duty-bound to probe the subjective dimension, namely the intent or negligence of the offender. The intrinsic correlation between the perpetrator's inner disposition and the manipulation of electronic systems serves as the primordial basis for the judge to ascertain the reprehensibility of the act before the imposition of rehabilitative-oriented penal sanctions.

Commensurate with technological leaps, digital evidence has secured formidable juridical legitimacy within the Indonesian criminal justice ecosystem. However, the inherently volatile architecture of digital evidence—characterized by its susceptibility to modification and its intrinsic reliance on underlying hardware and software ecosystems—introduces acute technical and procedural convolutions upon its introduction in judicial

proceedings. The acquisition, processing, and evaluation of digital evidence strictly demand uncompromising adherence to the rigorous standards of admissibility, authenticity, and document integrity. Consequently, the adaptive proficiency of a judge in deciphering the technical specificities of electronic information is profoundly determinative of the probative weight of such evidence in forging an objective and incontrovertible judicial conviction.

DISCUSSION

The Conformity of the Digital Evidence Proof System in Decision Number 628/Pid.Sus/2020/PN.Btm and Number 541/Pid.Sus/2022/PN.Mdn with the Evidentiary Provisions under Law Number 20 of 2025 concerning the Criminal Procedure Code.

Empirical law enforcement praxis at the District Court tier illuminates a profoundly expansive interpretative latitude in the legal construction of the offense of personal data misuse. A comparative dissection of Decision Number 628/Pid.Sus/2020/PN.Btm (Batam District Court) and Decision Number 541/Pid.Sus/2022/PN.Mdn (Medan District Court) unveils palpable disparities in judicial reasoning (ratio decidendi). Despite the causative architecture of both cases being functionally identical—specifically, the illicit exploitation of individual data via electronic mediums—the respective judicial panels deployed discordant parameters in evaluating the probative efficacy of the digital evidence adduced by the public prosecutors. This judicial phenomenon robustly corroborates that Indonesian cyber criminal law remains in a developmental stage, a phase wherein law enforcement entities are frequently compelled to extrapolate from generalized norms to adequately address the multifaceted complexities of digital criminality.

The Indonesian criminal justice architecture has historically and consistently adhered to the negative statutory evidentiary doctrine (negatief wettelijk bewijs theorie). This jurisprudential doctrine imperatively dictates that a judge is authorized to pronounce a criminal conviction solely if said conviction is anchored upon a minimum of two legally valid pieces of evidence, unequivocally reinforced by the judge's subjective conviction, crystallized through meticulous evidentiary examination during the trial proceedings. The promulgation of Law Number 20 of 2025 concerning the Criminal Procedure Code (the new KUHAP) emerges as a highly critical

evaluative instrument to audit the degree of procedural conformity governing digital evidentiary protocols within the aforementioned court decisions.

The critical reconstruction and analysis of the adjudicators' rationale are of paramount essence. This scholarly undertaking seeks to bridge the juridical chasm between idealized normative constructs (das Sollen) and the empirical actualities of judicial administration (das Sein). Concurrently, it endeavors to propose a framework for legal harmonization designed to unequivocally guarantee legal certainty and substantive equity in the digital era.

CONCLUSION

The criminal liability attributed to perpetrators for the misuse of personal data in Decision Number 628/Pid.Sus/2020/PN.Btm and Decision Number 541/Pid.Sus/2022/PN.Mdn is substantively predicated upon the cumulative substantiation of the objective element, actus reus (the act of exploiting personal data electronically without lawful authorization), and the subjective element, mens rea (the culpability of the perpetrator driven by economic motives or unilateral advantage). However, at the empirical echelon, a significant disparity in legal reasoning (ratio decidendi) between the adjudicating panels is demonstrably evident. This divergence is largely attributable to the reality that cyber law enforcement during the judicial examination of these cases was strictly governed by the overarching provisions of the Law on Information and Electronic Transactions (UU ITE), predating the enactment of the more specialized Personal Data Protection Law (UU PDP). This historical context inadvertently afforded judges exceptionally broad interpretative discretion in constructing the parameters of the perpetrator's subjective fault and in calibrating the probative magnitude of the digital evidence presented in court.

Formally, the framework for assessing digital evidence in both verdicts successfully complied with the negative statutory evidentiary doctrine (negatief wettelijk bewijs theorie), thereby fulfilling the prerequisite of utilizing at least two legally admissible forms of evidence augmented by judicial conviction. Nonetheless, when subjected to scrutiny against the progressive stipulations of the newly enacted Law Number 20 of 2025 (the New KUHAP), the procedural management of digital evidence in these inherently conventional proceedings still exposes conspicuous procedural frailties. The novel KUHAP aggressively mandates a substantially more stringent and rigid standardization protocol governing the evaluation of electronic documents' admissibility, authenticity, and integrity.

Consequently, to effectively navigate and reconcile the juridical dichotomy between aspirational legal norms (das Sollen) and the pragmatic realities of the judiciary (das Sein), an imperative exigency exists for the harmonization and standardization of adaptive judicial parameters. Such an initiative is crucial to ensure that the orchestration of digital evidentiary procedures in future litigations is seamlessly and flawlessly aligned with the progressive trajectory of national criminal procedural reform.

LIMITATION

The scope of this study is limited to normative legal analysis of Decision Number 628/Pid.Sus/2020/PN.Btm and Decision Number 541/Pid.Sus/2022/PN.Mdn using statutory and case approaches, with emphasis on criminal liability, digital evidence, and their relationship to the evidentiary provisions of Law Number 20 of 2025 concerning the Criminal Procedure Code.

REFERENCES

Andoko. (2018). Kompetensi absolut peradilan agama dalam menyelesaikan persoalan ekonomi syariah pasca lahirnya Undang-Undang Nomor 3 Tahun 2006. Jurnal Hukum Responsif FH UNPAB, Medan.

Arief, B. N. (2018). Bunga rampai kebijakan hukum pidana. Jakarta: Kencana.

Aspan, H. (2023). Cyber notary issues authority certificate to provide legal protection in online selling. Journal of Law and Sustainable Development, Medan.
Chazawi, A. (2016). Pelajaran hukum pidana bagian 1. Jakarta: Raja Grafindo Persada.
Hamzah, A. (2017). Hukum acara pidana Indonesia. Jakarta: Sinar Grafika. Harahap, Y. (2018). Pembahasan permasalahan dan penerapan KUHAP. Jakarta: Sinar Grafika.
Hidayat, R. (2021). Pembuktian alat bukti elektronik dalam perkara tindak pidana siber. Jurnal Hukum IUS QUIA IUSTUM. Yogyakarta.
Hukum Online. (2026, 10 Januari). Alat bukti elektronik dalam perkara pidana. Diunduh dari: https://www.hukumonline.com
Ismaidar. (2018). Rekonstruksi sistem pembuktian dalam penanganan tindak pidana korupsi berbasis nilai keadilan. Jurnal Hukum Responsif FH UNPAB, Medan.
Kamus Besar Bahasa Indonesia. (2026, 10 Januari). Data pribadi. Diunduh dari: https://kbbi.kemdikbud.go.id
Kementerian Komunikasi dan Informatika RI. (2026, 11 Januari). Perlindungan data pribadi di Indonesia. Diunduh dari: https://www.kominfo.go.id
Lestari, D. (2022). Pertanggungjawaban pidana dalam penyalahgunaan data pribadi. Jurnal Legislasi Indonesia. Jakarta.
Mahkamah Agung RI. (2026, 12 Januari). Direktori putusan. Diunduh dari: https://putusan3.mahkamahagung.go.id
Makarim, E. (2019). Pengantar hukum telematika. Jakarta: Rajawali Pers. Marzuki, P. M. (2019). Penelitian hukum. Jakarta: Kencana.
Mertokusumo, S. (2015). Hukum acara pidana Indonesia. Yogyakarta: Liberty.
Moeljatno. (2016). Asas-asas hukum pidana. Jakarta: Rineka Cipta. Nugroho, S. A. (2022). Hukum siber dan perlindungan data pribadi. Jakarta: Kencana.
Pengadilan Negeri Batam. (2020). Putusan Nomor 628/Pid.Sus/2020/PN.Btm.
Pengadilan Negeri Medan. (2022). Putusan Nomor 541/Pid.Sus/2022/PN.Mdn.
Prasetyo, T. (2023). Urgensi pembaruan KUHAP dalam era digital. Jurnal Konstitusi. Jakarta.
Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
Republik Indonesia. (2025). Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.
Rosadi, S. D. (2015). Cyber law: Aspek data pribadi menurut hukum internasional, regional, dan nasional. Bandung: Refika Aditama.
Siregar, A. R. M. (2025). Legal analysis of the use of mediation in handling domestic violence crimes. Proceedings of the 2nd International Conference on Islamic Community Studies (ICICS). Medan: Universitas Pembangunan Panca Budi.
Siregar, F. R., dkk. (2024). Analysis of legal protection of street children victims of exploitation: A case study of the Medan City Social Service. Proceedings ICANEAT. Medan.
Siregar, M. (2022). Legalitas digital evidence dalam sistem peradilan pidana. Jurnal Rechtsvinding. Jakarta.
Siregar, M. A. (2025). Study of the benefits of law in the implementation of restorative justice for children as victims and perpetrators of criminal acts. Proceedings of the 2nd International Conference on Islamic Community Studies (ICICS). Medan: Universitas Pembangunan Panca Budi.
Sutarman. (2020). Cyber crime: Modus operandi dan penanggulangannya. Yogyakarta: LaksBang Pressindo.