Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2776-771X (Online)
ISSN 2962-570X (Printed)
6 (2) 2026, Page: 41087-41099

Analisis Yuridis Pertanggungjawaban Pidana terhadap Pelaku Penyalahgunaan Data Pribadi dalam Transaksi Elektronik di Indonesia

M. Resko, Siti Rahmah, Bambang Sasmita Adi Putra
[1,2,3] **Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Islam Indragiri**
mrezkoo876@gmail.com, raturahmahdaeng@gmail.com, bambangsasmitaadiputra@gmail.com

Published: July , 2025

ABSTRACT
The rapid growth of digital technology has increased the risk of personal data misuse in electronic transactions, creating significant legal challenges in Indonesia. This study aims to analyze criminal liability for perpetrators of personal data misuse, examine the application of the *lex specialis derogat legi generali* principle between the Personal Data Protection Law and the Electronic Information and Transactions Law, and identify obstacles to law enforcement. This research employed a normative juridical method using statutory, conceptual, and case approaches. Legal materials consisted of primary, secondary, and tertiary legal sources analyzed qualitatively through a prescriptive approach. The findings indicate that criminal liability may be imposed on both individuals and corporations that unlawfully obtain, disclose, or misuse personal data. Although the Personal Data Protection Law provides a more specific legal framework, practical implementation still encounters regulatory overlap, limited institutional capacity, digital evidence challenges, and inadequate cyber law expertise among law enforcement officers. Therefore, harmonization of regulations, institutional strengthening, and enhancement of digital forensic capabilities are essential to ensure effective legal protection and legal certainty.
Keywords: Personal Data Protection; Criminal Liability; Electronic Transactions; Electronic Information and Transactions Law; Legal Certainty.

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN
Indonesia merupakan negara hukum sebagaimana ditegaskan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menempatkan hukum sebagai landasan utama dalam penyelenggaraan kehidupan berbangsa dan bernegara. Prinsip negara hukum tersebut mengandung konsekuensi bahwa setiap warga negara berhak memperoleh perlindungan atas hak-hak konstitusionalnya, termasuk hak atas privasi dan pelindungan data pribadi. Di era transformasi digital, data pribadi telah berkembang menjadi aset yang memiliki nilai ekonomi tinggi sekaligus menjadi bagian dari hak asasi manusia yang harus dijamin keberadaannya. Perlindungan terhadap data pribadi menjadi semakin penting karena berbagai aktivitas masyarakat, seperti perdagangan elektronik (*e-commerce*), layanan perbankan digital, *financial technology*, media sosial, hingga layanan publik berbasis elektronik, mengandalkan pengumpulan dan pemrosesan data pribadi pengguna (Hadjon, 1987; Greenleaf, 2023).

Perkembangan teknologi informasi telah mendorong peningkatan transaksi elektronik secara signifikan di Indonesia. Berdasarkan laporan **e-Conomy SEA 2024**, nilai ekonomi digital Indonesia terus mengalami pertumbuhan dan diproyeksikan menjadi yang terbesar di kawasan Asia Tenggara. Kondisi tersebut memberikan dampak positif terhadap perkembangan ekonomi nasional, namun pada saat yang sama juga meningkatkan risiko penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab. Berbagai bentuk penyalahgunaan data pribadi, seperti pencurian identitas (*identity theft*), penyebaran informasi pribadi tanpa persetujuan, penjualan data konsumen secara ilegal, hingga penggunaan data untuk pembukaan rekening maupun pinjaman daring tanpa izin pemilik data,

semakin sering ditemukan dalam praktik transaksi elektronik di Indonesia (Google, Temasek, & Bain & Company, 2024; Solove, 2021).

Sebagai respons terhadap perkembangan tersebut, pemerintah Indonesia telah membentuk berbagai regulasi yang mengatur pelindungan data pribadi. Pengaturan awal terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir Undang-Undang Nomor 1 Tahun 2024. Selanjutnya, pemerintah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai regulasi khusus (*lex specialis*) yang mengatur hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data pribadi, hingga pengenaan sanksi administratif maupun pidana terhadap pelanggaran data pribadi. Kehadiran UU PDP menunjukkan komitmen negara dalam memperkuat sistem pelindungan data pribadi agar selaras dengan perkembangan hukum internasional (Koops, 2022; Greenleaf, 2023).

Meskipun demikian, keberadaan berbagai regulasi tersebut belum sepenuhnya mampu memberikan kepastian hukum dalam praktik penegakan hukum pidana terhadap penyalahgunaan data pribadi. Dalam praktiknya, satu perbuatan penyalahgunaan data pribadi sering kali memenuhi unsur tindak pidana yang diatur dalam dua regulasi sekaligus, yaitu Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi. Kondisi tersebut menimbulkan persoalan mengenai penerapan asas *lex specialis derogat legi generali*, khususnya dalam menentukan ketentuan hukum yang lebih tepat digunakan oleh aparat penegak hukum. Ketidakjelasan tersebut berpotensi menimbulkan disparitas penegakan hukum, mengurangi kepastian hukum, serta memengaruhi efektivitas perlindungan terhadap korban penyalahgunaan data pribadi (Mertokusumo, 2005; Ali, 2017).

Permasalahan tersebut semakin kompleks karena penyalahgunaan data pribadi tidak hanya dilakukan oleh individu, tetapi juga dapat melibatkan korporasi sebagai pengendali maupun pemroses data pribadi. Kebocoran data yang terjadi pada berbagai platform digital menunjukkan bahwa lemahnya sistem keamanan informasi dapat mengakibatkan kerugian material maupun immaterial bagi masyarakat. Selain kerugian ekonomi, korban juga menghadapi risiko penyalahgunaan identitas, penipuan daring, hingga pelanggaran terhadap hak privasi. Oleh karena itu, pertanggungjawaban pidana tidak hanya harus diarahkan kepada pelaku perseorangan, tetapi juga terhadap badan hukum yang terbukti lalai atau dengan sengaja melakukan penyalahgunaan data pribadi (Azhar & Mahyani, 2023; Ahmad Ibrahim, 2025).

Beberapa penelitian terdahulu telah mengkaji mengenai pelindungan data pribadi dan pertanggungjawaban pidana terhadap penyalahgunaan data pribadi. Penelitian oleh Azhar dan Mahyani (2023) lebih memfokuskan kajian pada pertanggungjawaban pidana korporasi dalam penyebaran data pribadi konsumen. Penelitian lain yang dipublikasikan dalam **PAMPAS: Journal of Criminal Law** membahas pertanggungjawaban pidana terhadap penyalahgunaan data pribadi pada tindak pidana dunia maya secara umum. Sementara itu, penelitian yang dimuat dalam **Syntax Literate: Jurnal Ilmiah Indonesia** menitikberatkan pada harmonisasi pengaturan hukum siber mengenai data pribadi. Namun demikian, penelitian-penelitian tersebut belum secara komprehensif mengkaji penerapan pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi yang secara khusus terjadi dalam transaksi elektronik dengan menganalisis hubungan antara UU ITE dan UU PDP berdasarkan asas *lex specialis derogat legi generali* (Azhar & Mahyani, 2023; PAMPAS, 2023; Syntax Literate, 2024).

Berdasarkan uraian tersebut, terdapat **research gap** berupa masih terbatasnya penelitian yang secara khusus mengintegrasikan analisis pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dalam transaksi elektronik dengan pendekatan normatif yang mengombinasikan analisis ketentuan dalam UU ITE, UU PDP, serta penerapan asas *lex specialis derogat legi generali* dalam praktik penegakan hukum di Indonesia. Sebagian besar penelitian terdahulu masih bersifat deskriptif mengenai pelindungan data pribadi atau hanya berfokus pada aspek korporasi maupun kejahatan siber secara umum, sehingga belum memberikan analisis yang mendalam mengenai mekanisme pertanggungjawaban pidana dalam transaksi elektronik.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis pengaturan pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi elektronik

di Indonesia, mengkaji penerapan asas *lex specialis derogat legi generali* dalam penyelesaian perkara penyalahgunaan data pribadi berdasarkan UU ITE dan UU PDP, serta mengidentifikasi berbagai kendala yang dihadapi dalam penegakan hukum pidana guna mewujudkan kepastian hukum dan perlindungan hukum yang efektif terhadap masyarakat sebagai pemilik data pribadi.

METODE

2.1 Jenis Penelitian

Penelitian ini menggunakan metode **penelitian hukum normatif (yuridis normatif)**, yaitu penelitian yang menitikberatkan pada pengkajian norma-norma hukum positif, asas hukum, doktrin hukum, serta putusan pengadilan yang berkaitan dengan pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi elektronik di Indonesia. Penelitian hukum normatif dipilih karena permasalahan yang dikaji berfokus pada sinkronisasi dan penerapan norma hukum yang terdapat dalam berbagai peraturan perundang-undangan, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana (KUHP), serta berbagai peraturan pelaksana yang berkaitan dengan pelindungan data pribadi. Melalui penelitian hukum normatif, analisis dilakukan terhadap ketentuan hukum yang berlaku untuk memperoleh argumentasi hukum mengenai bentuk pertanggungjawaban pidana serta kepastian hukum dalam penegakan tindak pidana penyalahgunaan data pribadi (Marzuki, 2021).

2.2 Pendekatan Penelitian

Penelitian ini menggunakan beberapa pendekatan hukum (*multiple approaches*) agar analisis yang dihasilkan lebih komprehensif. Pendekatan pertama adalah **pendekatan perundang-undangan (*statute approach*)**, yaitu menelaah seluruh ketentuan peraturan perundang-undangan yang mengatur pelindungan data pribadi dan transaksi elektronik di Indonesia. Pendekatan ini digunakan untuk mengidentifikasi dasar hukum pertanggungjawaban pidana serta hubungan antara UU ITE dan UU PDP.

Pendekatan kedua adalah **pendekatan konseptual (*conceptual approach*)**, yaitu mengkaji berbagai teori dan doktrin hukum mengenai pertanggungjawaban pidana, perlindungan hukum, kepastian hukum, serta teori mengenai pelindungan data pribadi yang berkembang dalam literatur hukum pidana dan hukum siber. Pendekatan ini digunakan untuk membangun kerangka konseptual dalam menganalisis permasalahan penelitian (Soekanto & Mamudji, 2019).

Pendekatan ketiga adalah **pendekatan kasus (*case approach*)**, yaitu menganalisis putusan pengadilan yang berkaitan dengan tindak pidana penyalahgunaan data pribadi dalam transaksi elektronik. Analisis terhadap putusan pengadilan dilakukan untuk mengetahui bagaimana hakim menerapkan ketentuan pidana dalam praktik, sekaligus mengidentifikasi penerapan asas *lex specialis derogat legi generali* dalam penyelesaian perkara yang melibatkan ketentuan UU ITE dan UU PDP (IRAC Centre, 2023).

2.3 Jenis dan Sumber Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta berbagai putusan pengadilan yang relevan mengenai penyalahgunaan data pribadi dalam transaksi elektronik.

Bahan hukum sekunder terdiri atas buku-buku hukum, jurnal ilmiah nasional maupun internasional, hasil penelitian terdahulu, artikel ilmiah, serta pendapat para ahli yang berkaitan dengan hukum pidana, hukum siber, pelindungan data pribadi, dan pertanggungjawaban pidana. Sementara itu, bahan hukum tersier berupa kamus hukum, ensiklopedia hukum, serta berbagai dokumen resmi yang memberikan petunjuk terhadap bahan hukum primer dan sekunder (Marzuki, 2021).

2.4 Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum dilakukan melalui **studi kepustakaan (*library research*)**, yaitu dengan menelusuri, mengumpulkan, mengidentifikasi, serta mengklasifikasikan berbagai bahan hukum yang relevan dengan fokus penelitian. Penelusuran dilakukan terhadap peraturan perundang-undangan, putusan pengadilan, jurnal ilmiah nasional dan internasional, buku referensi, serta dokumen resmi yang berkaitan dengan pelindungan data pribadi dan transaksi elektronik. Seluruh bahan hukum yang diperoleh kemudian diklasifikasikan berdasarkan relevansinya terhadap rumusan masalah penelitian sehingga memudahkan proses analisis secara sistematis (Zainuddin Ali, 2021).

2.5 Teknik Analisis Bahan Hukum

Analisis bahan hukum dilakukan secara **kualitatif** dengan menggunakan metode **analisis preskriptif**, yaitu memberikan argumentasi hukum terhadap permasalahan yang diteliti berdasarkan norma hukum yang berlaku. Analisis diawali dengan menginventarisasi seluruh ketentuan hukum yang berkaitan dengan penyalahgunaan data pribadi dalam transaksi elektronik, kemudian dilakukan interpretasi hukum melalui pendekatan gramatikal, sistematis, dan teleologis untuk memperoleh makna yang utuh terhadap norma yang berlaku.

Selanjutnya dilakukan analisis terhadap penerapan asas **lex specialis derogat legi generali** guna menentukan ketentuan hukum yang tepat diterapkan apabila terdapat pengaturan yang saling berkaitan antara UU ITE dan UU PDP. Hasil analisis tersebut kemudian dibandingkan dengan praktik penegakan hukum melalui studi putusan pengadilan sehingga dapat diperoleh gambaran mengenai efektivitas pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi elektronik. Tahap akhir analisis dilakukan dengan menarik kesimpulan secara **deduktif**, yaitu dari ketentuan hukum yang bersifat umum menuju penyelesaian terhadap permasalahan hukum yang bersifat khusus sesuai dengan rumusan masalah penelitian (IRAC Centre, 2023; Marzuki, 2021).

HASIL DAN PEMBAHASAN

3.1 Pengaturan Pertanggungjawaban Pidana terhadap Pelaku Penyalahgunaan Data Pribadi dalam Transaksi Elektronik di Indonesia

Perkembangan teknologi informasi telah mengubah pola interaksi masyarakat dalam berbagai sektor, seperti perdagangan elektronik (*e-commerce*), perbankan digital, layanan pinjaman daring (*peer-to-peer lending*), *financial technology* (fintech), hingga pelayanan publik berbasis elektronik. Seluruh aktivitas tersebut memerlukan pengumpulan, penyimpanan, pengolahan, dan distribusi data pribadi pengguna sehingga meningkatkan risiko terjadinya penyalahgunaan data pribadi. Penelitian ini menunjukkan bahwa Indonesia telah memiliki landasan hukum yang relatif komprehensif dalam mengatur perlindungan data pribadi, namun pengaturan mengenai pertanggungjawaban pidana masih tersebar dalam beberapa peraturan perundang-undangan sehingga berpotensi menimbulkan tumpang tindih dalam penerapannya.

Landasan konstitusional perlindungan data pribadi berakar pada Pasal 28G ayat (1) dan Pasal 28D ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin hak atas perlindungan diri pribadi, rasa aman, serta kepastian hukum bagi setiap warga negara. Ketentuan tersebut kemudian diimplementasikan melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kehadiran kedua regulasi tersebut menunjukkan adanya komitmen negara dalam memberikan perlindungan hukum terhadap data pribadi sebagai bagian dari hak asasi manusia di era digital.

Berdasarkan hasil analisis terhadap ketentuan peraturan perundang-undangan, bentuk pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dapat dikenakan apabila pelaku secara melawan hukum memperoleh, mengakses, mengungkapkan, menggunakan, memindahkan, menjual, maupun memalsukan data pribadi milik orang lain tanpa persetujuan yang sah. UU PDP secara tegas mengatur larangan tersebut dalam Pasal 65 yang selanjutnya diikuti dengan ancaman pidana sebagaimana diatur dalam Pasal 67 sampai dengan Pasal 70. Selain menjangkau pelaku perseorangan, UU PDP juga mengakui korporasi sebagai subjek hukum pidana yang dapat dimintai pertanggungjawaban apabila penyalahgunaan data dilakukan dalam ruang lingkup kegiatan korporasi.

Di sisi lain, UU ITE juga mengatur berbagai bentuk tindak pidana yang berkaitan dengan akses ilegal terhadap sistem elektronik, intersepsi, perubahan, penghilangan, maupun pemindahan informasi elektronik yang memuat data pribadi. Dengan demikian, apabila suatu penyalahgunaan data pribadi dilakukan melalui akses ilegal terhadap sistem elektronik, maka pelaku tidak hanya berpotensi dijerat menggunakan ketentuan dalam UU PDP, tetapi juga dapat dikenakan pasal-pasal pidana dalam UU ITE. Kondisi tersebut menunjukkan bahwa perlindungan hukum terhadap data pribadi di Indonesia tidak hanya diberikan melalui satu instrumen hukum, melainkan melalui kombinasi berbagai regulasi yang saling berkaitan.

Berdasarkan hasil kajian normatif, penelitian ini menemukan bahwa pertanggungjawaban pidana dalam penyalahgunaan data pribadi memenuhi unsur-unsur pertanggungjawaban pidana sebagaimana dikemukakan oleh Moeljatno, yaitu adanya perbuatan melawan hukum (*actus reus*), adanya kesalahan (*mens rea*), kemampuan bertanggung jawab, serta tidak adanya alasan pemaaf maupun alasan pembenar. Dengan demikian, seseorang hanya dapat dipidana apabila seluruh unsur tersebut terbukti secara sah dalam proses pembuktian di persidangan. Hal ini menunjukkan bahwa sistem hukum pidana Indonesia tetap berpegang pada asas **geen straf zonder schuld** (tiada pidana tanpa kesalahan).

Selain pertanggungjawaban pidana terhadap individu, hasil penelitian juga menunjukkan bahwa korporasi memiliki tanggung jawab yang cukup besar dalam menjamin keamanan data pribadi pengguna. Korporasi sebagai pengendali data (*data controller*) maupun pemroses data (*data processor*) wajib menerapkan sistem keamanan informasi yang memadai, memperoleh persetujuan pemilik data sebelum melakukan pemrosesan data, serta segera memberitahukan kepada subjek data apabila terjadi kebocoran data pribadi. Kelalaian dalam memenuhi kewajiban tersebut dapat mengakibatkan dikenakannya sanksi administratif maupun sanksi pidana sesuai dengan ketentuan UU PDP.

Untuk memberikan gambaran yang lebih sistematis mengenai pengaturan pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dalam transaksi elektronik, hasil analisis dapat disajikan pada Tabel 1 berikut.

Tabel 1. Pengaturan Pertanggungjawaban Pidana terhadap Penyalahgunaan Data Pribadi dalam Transaksi Elektronik

Aspek	UU ITE	UU PDP	Hasil Analisis
Objek yang Dilindungi	Sistem elektronik dan informasi elektronik	Data pribadi sebagai hak subjek data	Kedua regulasi saling melengkapi dalam memberikan perlindungan hukum.
Perbuatan yang Dilarang	Akses ilegal, intersepsi, manipulasi data elektronik	Memperoleh, menggunakan, mengungkapkan, menjual, memalsukan data pribadi	Banyak perbuatan memenuhi unsur kedua undang-undang sekaligus.
Subjek Hukum	Individu dan korporasi	Individu dan korporasi	Pertanggungjawaban pidana dapat dikenakan kepada kedua subjek hukum.
Jenis Sanksi	Pidana penjara dan denda	Pidana penjara, denda, dan pidana terhadap korporasi	UU PDP mengatur lebih rinci mengenai sanksi terhadap penyalahgunaan data pribadi.
Tujuan Pengaturan	Menjamin keamanan sistem elektronik	Menjamin perlindungan hak atas data pribadi	Kedua regulasi memiliki tujuan yang saling mendukung dalam perlindungan data digital.

Sumber: Hasil analisis penulis berdasarkan UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (2026).

Berdasarkan Tabel 1 terlihat bahwa pengaturan pertanggungjawaban pidana terhadap penyalahgunaan data pribadi di Indonesia telah memiliki dasar hukum yang cukup kuat. Namun demikian, pengaturan tersebut masih tersebar dalam beberapa regulasi sehingga berpotensi menimbulkan perbedaan penafsiran dalam praktik penegakan hukum. UU ITE lebih berorientasi pada perlindungan sistem elektronik, sedangkan UU PDP secara khusus mengatur hak-hak subjek data beserta bentuk pertanggungjawaban pidana atas penyalahgunaan data pribadi. Oleh karena itu, diperlukan

sinkronisasi penerapan kedua regulasi agar tidak menimbulkan ketidakpastian hukum ketika suatu perbuatan memenuhi unsur pidana dalam kedua undang-undang tersebut.

3.2 Penerapan Asas *Lex Specialis Derogat Legi Generali* dalam Penyelesaian Tindak Pidana Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi

Hasil penelitian menunjukkan bahwa salah satu persoalan utama dalam penegakan hukum terhadap penyalahgunaan data pribadi di Indonesia adalah adanya pengaturan yang saling berkaitan antara Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kedua regulasi tersebut sama-sama mengatur perbuatan yang berkaitan dengan akses, penggunaan, maupun penyebaran data pribadi secara melawan hukum. Akibatnya, dalam praktik penegakan hukum sering ditemukan kondisi di mana satu perbuatan memenuhi unsur tindak pidana sebagaimana diatur dalam kedua undang-undang tersebut secara bersamaan.

Secara teoritis, penyelesaian konflik norma tersebut dapat dilakukan melalui penerapan asas **lex specialis derogat legi generali**, yaitu ketentuan hukum yang bersifat khusus mengesampingkan ketentuan hukum yang bersifat umum. Dalam konteks perlindungan data pribadi, UU PDP merupakan regulasi yang secara khusus mengatur hak subjek data, kewajiban pengendali data, mekanisme pemrosesan data, hingga sanksi administratif maupun pidana atas penyalahgunaan data pribadi. Sebaliknya, UU ITE memiliki ruang lingkup yang lebih luas karena mengatur seluruh aktivitas yang berkaitan dengan informasi elektronik dan transaksi elektronik, termasuk keamanan sistem elektronik. Oleh karena itu, apabila suatu perkara secara khusus menyangkut penyalahgunaan data pribadi, maka UU PDP pada prinsipnya lebih tepat dijadikan dasar hukum utama, sedangkan UU ITE dapat berfungsi sebagai ketentuan pendukung apabila perbuatan tersebut juga melibatkan akses ilegal atau gangguan terhadap sistem elektronik.

Berdasarkan hasil analisis terhadap berbagai putusan pengadilan dan ketentuan normatif, penelitian ini menemukan bahwa penerapan asas *lex specialis* belum dilakukan secara konsisten. Sebagian perkara masih menggunakan ketentuan UU ITE meskipun substansi perkaranya berkaitan langsung dengan penyalahgunaan data pribadi. Kondisi tersebut dipengaruhi oleh beberapa faktor, antara lain karena UU PDP masih tergolong regulasi baru, belum terbentuknya seluruh kelembagaan pelaksana sebagaimana diamanatkan UU PDP, serta masih terbatasnya pedoman teknis bagi aparat penegak hukum dalam menentukan dasar hukum yang paling tepat digunakan pada setiap perkara.

Selain itu, penelitian ini menunjukkan bahwa dalam praktik penyalahgunaan data pribadi sering kali terdapat rangkaian perbuatan yang saling berkaitan. Sebagai contoh, pelaku terlebih dahulu melakukan akses ilegal terhadap sistem elektronik, kemudian mengambil data pribadi pengguna, selanjutnya menggunakan data tersebut untuk mendaftarkan layanan pinjaman daring atau menjualnya kepada pihak lain. Dalam kondisi demikian, unsur tindak pidana tidak hanya memenuhi ketentuan dalam UU PDP mengenai perolehan dan penggunaan data pribadi secara melawan hukum, tetapi juga memenuhi unsur pidana dalam UU ITE mengenai akses ilegal terhadap sistem elektronik. Oleh karena itu, aparat penegak hukum harus mampu membedakan **perbuatan pokok** dengan **perbuatan penyerta** agar penerapan pasal tidak menimbulkan tumpang tindih maupun pelanggaran terhadap asas kepastian hukum.

Penelitian ini juga menemukan bahwa penerapan asas *lex specialis* tidak berarti mengesampingkan seluruh ketentuan dalam UU ITE. Kedua undang-undang tersebut justru memiliki hubungan yang saling melengkapi (*complementary regulation*). UU ITE memberikan perlindungan terhadap keamanan sistem elektronik, sedangkan UU PDP memberikan perlindungan terhadap hak pemilik data pribadi. Dengan demikian, apabila penyalahgunaan data pribadi dilakukan melalui pembobolan sistem elektronik, maka aparat penegak hukum tetap dapat menerapkan ketentuan dalam kedua undang-undang sepanjang tidak terjadi *double punishment* terhadap perbuatan yang sama dan tetap memperhatikan prinsip proporsionalitas dalam pemidanaan.

Hasil penelitian selanjutnya menunjukkan bahwa penerapan asas *lex specialis derogat legi generali* memiliki peran penting dalam menciptakan kepastian hukum. Kepastian hukum akan tercapai apabila aparat penegak hukum memiliki pedoman yang jelas mengenai kapan UU PDP digunakan sebagai dasar

utama, kapan UU ITE diterapkan sebagai ketentuan pendukung, serta bagaimana konstruksi dakwaan disusun ketika suatu tindak pidana memenuhi unsur kedua undang-undang tersebut. Tanpa adanya pedoman tersebut, akan muncul disparitas penanganan perkara yang dapat mengurangi efektivitas perlindungan terhadap hak-hak subjek data pribadi.

Untuk memperjelas hasil analisis, penerapan asas *lex specialis derogat legi generali* dapat dirangkum pada Tabel 2 berikut.

Tabel 2. Analisis Penerapan Asas *Lex Specialis Derogat Legi Generali* pada Penyalahgunaan Data Pribadi

Aspek Analisis	UU ITE	UU PDP	Hasil Analisis
Ruang lingkup pengaturan	Informasi dan transaksi elektronik secara umum	Perlindungan data pribadi secara khusus	UU PDP merupakan pengaturan yang lebih spesifik terhadap data pribadi.
Objek perlindungan	Sistem elektronik dan informasi elektronik	Hak pemilik data pribadi	UU PDP menjadi dasar utama apabila objek yang dirugikan adalah data pribadi.
Fokus tindak pidana	Akses ilegal, intersepsi, manipulasi sistem elektronik	Perolehan, penggunaan, pengungkapan, pemalsuan data pribadi	Kedua regulasi dapat diterapkan secara komplementer sesuai karakteristik perkara.
Penerapan asas *lex specialis*	Sebagai aturan umum pada transaksi elektronik	Sebagai aturan khusus terhadap data pribadi	UU PDP lebih tepat digunakan apabila inti perkara adalah penyalahgunaan data pribadi.
Permasalahan praktik	Masih digunakan pada sebagian perkara penyalahgunaan data pribadi	Belum sepenuhnya diterapkan secara optimal	Diperlukan pedoman teknis bagi aparat penegak hukum agar tidak terjadi tumpang tindih norma.

Sumber: Hasil analisis penulis berdasarkan UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, dan berbagai putusan pengadilan yang relevan (2026).

Berdasarkan Tabel 2 dapat diketahui bahwa UU PDP memiliki karakter sebagai **lex specialis** dalam pengaturan pelindungan data pribadi, sedangkan UU ITE tetap memiliki fungsi penting dalam melindungi keamanan sistem elektronik yang menjadi media terjadinya penyalahgunaan data pribadi. Oleh karena itu, hubungan antara kedua regulasi tersebut tidak bersifat saling meniadakan, melainkan saling melengkapi dalam mewujudkan perlindungan hukum yang efektif terhadap masyarakat. Hasil penelitian ini menegaskan bahwa penerapan asas *lex specialis derogat legi generali* harus dilakukan secara proporsional dengan mempertimbangkan objek hukum yang dilindungi, karakteristik perbuatan pidana, serta tujuan pemidanaan sehingga mampu memberikan kepastian hukum sekaligus keadilan bagi seluruh pihak yang terlibat.

3.3 Kendala Penegakan Hukum terhadap Pelaku Penyalahgunaan Data Pribadi dalam Transaksi Elektronik di Indonesia

Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki kerangka regulasi yang lebih komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), implementasi penegakan hukum terhadap penyalahgunaan data pribadi dalam transaksi elektronik masih menghadapi berbagai kendala. Hambatan tersebut tidak hanya berasal dari aspek substansi hukum, tetapi juga mencakup struktur kelembagaan, sumber daya manusia, pembuktian,

perkembangan teknologi informasi, hingga rendahnya kesadaran hukum masyarakat. Berbagai kendala tersebut berdampak pada belum optimalnya perlindungan hukum terhadap korban penyalahgunaan data pribadi.

Kendala pertama adalah **belum optimalnya harmonisasi regulasi** antara UU PDP dengan UU ITE. Kedua regulasi tersebut sama-sama mengatur tindak pidana yang berkaitan dengan data pribadi, namun memiliki ruang lingkup dan karakteristik pengaturan yang berbeda. Dalam praktiknya, aparat penegak hukum masih menghadapi kesulitan dalam menentukan dasar hukum yang paling tepat digunakan ketika suatu perbuatan memenuhi unsur tindak pidana dalam kedua undang-undang tersebut. Kondisi tersebut berpotensi menimbulkan perbedaan penafsiran, inkonsistensi penerapan pasal, serta ketidakpastian hukum bagi pelaku maupun korban (Ali, 2017).

Kendala kedua adalah **belum optimalnya kelembagaan pelindungan data pribadi** sebagaimana diamanatkan dalam UU PDP. Meskipun undang-undang telah mengatur pembentukan lembaga yang memiliki fungsi pengawasan terhadap pelindungan data pribadi, implementasi kelembagaan tersebut masih memerlukan penguatan dari aspek regulasi teknis, koordinasi antarlembaga, serta mekanisme pengawasan yang efektif. Akibatnya, proses penanganan pelanggaran data pribadi masih sangat bergantung pada aparat penegak hukum konvensional, seperti Kepolisian Negara Republik Indonesia, Kejaksaan, dan Pengadilan Negeri, sehingga mekanisme perlindungan administratif belum berjalan secara optimal (Greenleaf, 2023).

Kendala ketiga berkaitan dengan **pembuktian tindak pidana digital**. Berbeda dengan tindak pidana konvensional, penyalahgunaan data pribadi dalam transaksi elektronik memerlukan alat bukti elektronik yang memiliki karakteristik khusus. Proses memperoleh, mengamankan, dan menganalisis barang bukti digital membutuhkan kemampuan forensik digital (*digital forensic*) yang memadai. Selain itu, pelaku sering menggunakan teknologi enkripsi, identitas anonim, *virtual private network* (VPN), maupun server yang berada di luar wilayah Indonesia sehingga menyulitkan proses identifikasi dan pembuktian di persidangan. Kondisi tersebut menyebabkan proses penyidikan memerlukan waktu yang lebih lama dibandingkan tindak pidana konvensional (Brenner, 2018).

Kendala berikutnya adalah **keterbatasan sumber daya manusia aparat penegak hukum** dalam menghadapi perkembangan kejahatan siber. Tidak seluruh penyidik, penuntut umum, maupun hakim memiliki kompetensi yang memadai mengenai hukum siber, pelindungan data pribadi, serta teknik investigasi digital. Perkembangan teknologi informasi yang berlangsung sangat cepat menyebabkan modus operandi penyalahgunaan data pribadi terus mengalami perubahan sehingga memerlukan peningkatan kapasitas aparat penegak hukum secara berkelanjutan melalui pendidikan, pelatihan, dan sertifikasi di bidang forensik digital maupun hukum teknologi informasi (Wall, 2021).

Selain faktor kelembagaan dan sumber daya manusia, penelitian ini juga menemukan bahwa **rendahnya kesadaran hukum masyarakat** menjadi salah satu penyebab tingginya angka penyalahgunaan data pribadi. Sebagian besar masyarakat masih dengan mudah memberikan data pribadi kepada berbagai platform digital tanpa memahami risiko hukum maupun risiko keamanan informasi yang mungkin timbul. Di sisi lain, banyak korban yang tidak melaporkan penyalahgunaan data pribadi karena tidak mengetahui mekanisme pengaduan, menganggap kerugian yang dialami tidak signifikan, atau meragukan efektivitas proses penegakan hukum. Rendahnya literasi digital tersebut menyebabkan upaya perlindungan data pribadi belum dapat berjalan secara maksimal (Solove, 2021).

Penelitian ini juga menemukan adanya **tantangan yang bersifat lintas negara (*cross-border cybercrime*)**. Penyalahgunaan data pribadi sering dilakukan oleh pelaku yang berada di luar yurisdiksi Indonesia atau menggunakan infrastruktur digital yang berlokasi di negara lain. Keadaan tersebut menghambat proses penyidikan karena memerlukan kerja sama internasional dalam pertukaran informasi, pelacakan pelaku, maupun pengumpulan alat bukti elektronik. Perbedaan sistem hukum antarnegara juga menjadi hambatan tersendiri dalam pelaksanaan ekstradisi maupun bantuan hukum timbal balik (*mutual legal assistance*) sehingga proses penegakan hukum menjadi lebih kompleks.

Untuk memberikan gambaran mengenai berbagai kendala tersebut, hasil penelitian disajikan pada Tabel 3 berikut.

Tabel 3. Kendala Penegakan Hukum terhadap Penyalahgunaan Data Pribadi dalam Transaksi Elektronik

No	Kendala	Dampak terhadap Penegakan Hukum	Upaya Penyelesaian
1	Tumpang tindih pengaturan UU ITE dan UU PDP	Menimbulkan perbedaan penafsiran dan ketidakpastian hukum	Harmonisasi regulasi dan pedoman penerapan asas *lex specialis*.
2	Kelembagaan pelindungan data pribadi belum optimal	Pengawasan dan penegakan hukum belum berjalan efektif	Penguatan lembaga pelindungan data pribadi dan koordinasi antarlembaga.
3	Kesulitan pembuktian digital	Penyidikan dan pembuktian memerlukan waktu lebih lama	Pengembangan laboratorium forensik digital dan teknologi investigasi.
4	Kompetensi aparat penegak hukum masih terbatas	Penanganan perkara belum optimal	Pendidikan dan pelatihan hukum siber serta forensik digital.
5	Rendahnya literasi digital masyarakat	Banyak korban tidak melapor dan mudah menjadi korban	Edukasi publik mengenai pelindungan data pribadi.
6	Kejahatan lintas negara	Sulit mengidentifikasi dan menangkap pelaku	Peningkatan kerja sama internasional dan *mutual legal assistance*.

Sumber: Hasil analisis penulis berdasarkan studi kepustakaan (2026).

Berdasarkan Tabel 3 terlihat bahwa kendala penegakan hukum terhadap penyalahgunaan data pribadi bersifat multidimensional, mencakup aspek regulasi, kelembagaan, sumber daya manusia, teknologi, dan budaya hukum masyarakat. Oleh karena itu, penyelesaian permasalahan tersebut tidak dapat dilakukan hanya melalui pembentukan peraturan perundang-undangan, tetapi juga memerlukan penguatan kapasitas aparat penegak hukum, peningkatan literasi digital masyarakat, pengembangan teknologi forensik digital, serta penguatan kerja sama internasional dalam penanganan kejahatan siber. Dengan demikian, perlindungan terhadap data pribadi dalam transaksi elektronik dapat diwujudkan secara lebih efektif, memberikan kepastian hukum, sekaligus meningkatkan kepercayaan masyarakat terhadap sistem digital di Indonesia.

PEMBAHASAN

4.1 Analisis Yuridis Pertanggungjawaban Pidana terhadap Pelaku Penyalahgunaan Data Pribadi dalam Transaksi Elektronik

Hasil penelitian menunjukkan bahwa pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi elektronik pada dasarnya telah memiliki dasar hukum yang kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kedua regulasi tersebut mengatur larangan terhadap setiap orang yang secara melawan hukum memperoleh, menggunakan, mengungkapkan, memindahkan, maupun memanfaatkan data pribadi tanpa persetujuan pemilik data. Dengan demikian, sistem hukum Indonesia telah mengakui bahwa data pribadi merupakan objek perlindungan hukum yang memiliki nilai strategis sehingga penyalahgunaannya dapat dikenakan sanksi pidana.

Apabila dianalisis menggunakan **Teori Pertanggungjawaban Pidana** yang dikemukakan oleh **Moeljatno (2008)**, pemidanaan terhadap pelaku hanya dapat dilakukan apabila terpenuhi seluruh unsur pertanggungjawaban pidana, yaitu adanya perbuatan pidana (*actus reus*), adanya kesalahan (*mens rea*), kemampuan bertanggung jawab, serta tidak adanya alasan pembenar maupun alasan pemaaf. Dalam konteks penyalahgunaan data pribadi, unsur *actus reus* diwujudkan melalui tindakan memperoleh, mengakses, mengungkapkan, atau menggunakan data pribadi secara melawan hukum. Sementara itu, unsur *mens rea* tercermin dari adanya kesengajaan pelaku untuk memanfaatkan data

pribadi demi memperoleh keuntungan ekonomi atau tujuan lain yang bertentangan dengan hukum. Dengan demikian, keberadaan unsur kesalahan tetap menjadi syarat utama dalam menjatuhkan pidana sesuai asas **geen straf zonder schuld**.

Hasil penelitian juga menunjukkan bahwa pertanggungjawaban pidana tidak hanya dapat dibebankan kepada pelaku perseorangan, tetapi juga kepada korporasi. Pengakuan korporasi sebagai subjek hukum pidana merupakan perkembangan penting dalam hukum pidana modern karena sebagian besar aktivitas pemrosesan data pribadi dilakukan oleh badan usaha sebagai penyelenggara sistem elektronik. Korporasi yang dengan sengaja membiarkan terjadinya kebocoran data, tidak menerapkan standar keamanan informasi, atau menyalahgunakan data pelanggan dapat dimintai pertanggungjawaban pidana sesuai ketentuan UU PDP. Temuan ini sejalan dengan penelitian **Azhar dan Mahyani (2023)** yang menyatakan bahwa korporasi memiliki kewajiban hukum untuk menjamin keamanan data pribadi konsumen sehingga kegagalan memenuhi kewajiban tersebut dapat menimbulkan pertanggungjawaban pidana maupun administratif.

Dari perspektif hukum pidana, penelitian ini juga menemukan bahwa sistem pertanggungjawaban pidana dalam UU PDP telah mengadopsi konsep **perlindungan hukum preventif dan represif**. Perlindungan preventif diwujudkan melalui kewajiban memperoleh persetujuan subjek data, penerapan prinsip keamanan informasi, serta kewajiban melaporkan kebocoran data pribadi. Adapun perlindungan represif diwujudkan melalui pemberian sanksi pidana kepada pelaku penyalahgunaan data pribadi. Menurut **Philipus M. Hadjon (1987)**, kedua bentuk perlindungan hukum tersebut harus berjalan secara seimbang agar tujuan hukum dapat tercapai secara optimal. Hasil penelitian memperlihatkan bahwa aspek represif telah memiliki dasar hukum yang relatif kuat, sedangkan aspek preventif masih memerlukan penguatan melalui peningkatan pengawasan dan kepatuhan penyelenggara sistem elektronik.

4.2 Analisis Kepastian Hukum dalam Penerapan UU PDP dan UU ITE

Berdasarkan hasil penelitian, salah satu persoalan utama dalam penegakan hukum penyalahgunaan data pribadi adalah adanya potensi tumpang tindih pengaturan antara UU ITE dan UU PDP. Kedua regulasi tersebut memiliki objek pengaturan yang saling berkaitan sehingga dalam praktik sering ditemukan satu perbuatan yang memenuhi unsur pidana pada kedua undang-undang sekaligus. Kondisi tersebut berpotensi menimbulkan ketidakpastian hukum apabila aparat penegak hukum tidak memiliki pedoman yang jelas dalam menentukan dasar hukum yang digunakan.

Perspektif **Teori Kepastian Hukum** yang dikemukakan oleh **Gustav Radbruch** menegaskan bahwa hukum harus memberikan kepastian, keadilan, dan kemanfaatan secara seimbang. Kepastian hukum menghendaki adanya aturan yang jelas, tidak multitafsir, dan dapat diterapkan secara konsisten terhadap setiap perkara. Hasil penelitian menunjukkan bahwa secara normatif UU PDP telah memberikan pengaturan yang lebih spesifik mengenai pelindungan data pribadi dibandingkan UU ITE. Oleh karena itu, penerapan asas **lex specialis derogat legi generali** menjadi penting agar tidak terjadi konflik norma dalam praktik penegakan hukum.

Pendapat **Sudikno Mertokusumo (2005)** menyatakan bahwa kepastian hukum tidak hanya ditentukan oleh kejelasan rumusan norma, tetapi juga oleh konsistensi penerapan hukum oleh aparat penegak hukum. Berdasarkan hasil penelitian, masih ditemukan variasi penerapan pasal dalam perkara penyalahgunaan data pribadi sehingga menimbulkan disparitas putusan. Kondisi tersebut menunjukkan bahwa kepastian hukum belum sepenuhnya tercapai meskipun regulasi telah tersedia. Oleh sebab itu, diperlukan pedoman teknis yang mampu mengintegrasikan penerapan UU PDP dan UU ITE dalam proses penyidikan, penuntutan, maupun pemeriksaan di pengadilan.

Selain itu, penelitian ini menemukan bahwa keberadaan UU PDP tidak menghapus fungsi UU ITE. Kedua regulasi tersebut memiliki hubungan yang saling melengkapi (*complementary regulation*). UU ITE memberikan perlindungan terhadap keamanan sistem elektronik, sedangkan UU PDP berfokus pada perlindungan hak subjek data pribadi. Oleh karena itu, penerapan kedua regulasi harus mempertimbangkan karakteristik tindak pidana yang terjadi sehingga mampu memberikan kepastian hukum tanpa mengurangi efektivitas penegakan hukum.

4.3 Analisis Perlindungan Hukum terhadap Korban Penyalahgunaan Data Pribadi

Hasil penelitian memperlihatkan bahwa perlindungan hukum terhadap korban penyalahgunaan data pribadi masih menghadapi berbagai tantangan. Meskipun korban memiliki hak untuk memperoleh perlindungan hukum, meminta ganti rugi, serta melaporkan pelaku kepada aparat penegak hukum, pelaksanaan hak-hak tersebut belum sepenuhnya berjalan efektif. Banyak korban yang tidak mengetahui mekanisme pengaduan maupun prosedur pemulihan akibat penyalahgunaan data pribadi. Menurut **Philipus M. Hadjon (1987)**, perlindungan hukum harus diwujudkan melalui dua pendekatan, yaitu perlindungan preventif dan perlindungan represif. Berdasarkan hasil penelitian, perlindungan preventif masih menjadi titik lemah dalam sistem pelindungan data pribadi di Indonesia. Hal tersebut terlihat dari masih tingginya angka kebocoran data pribadi yang disebabkan oleh lemahnya sistem keamanan informasi maupun rendahnya kepatuhan penyelenggara sistem elektronik terhadap prinsip-prinsip pelindungan data pribadi.

Sementara itu, perlindungan represif telah mengalami perkembangan melalui pemberian sanksi pidana yang lebih tegas dalam UU PDP. Namun demikian, efektivitas perlindungan represif masih dipengaruhi oleh kemampuan aparat penegak hukum dalam melakukan pembuktian digital, mengidentifikasi pelaku, serta menindak kejahatan lintas negara. Oleh karena itu, penelitian ini menilai bahwa perlindungan hukum terhadap korban akan lebih efektif apabila diikuti dengan peningkatan kapasitas lembaga pelindungan data pribadi, penguatan forensik digital, serta peningkatan literasi digital masyarakat.

4.4 Konsep Ideal Penguatan Pertanggungjawaban Pidana terhadap Penyalahgunaan Data Pribadi dalam Transaksi Elektronik

Berdasarkan hasil penelitian dan analisis teoritis, konsep ideal pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi di Indonesia harus dibangun melalui pendekatan yang bersifat integratif antara aspek regulasi, kelembagaan, teknologi, dan budaya hukum masyarakat. Pendekatan tersebut diperlukan karena penyalahgunaan data pribadi merupakan bentuk kejahatan siber yang terus berkembang mengikuti perkembangan teknologi informasi.

Pertama, diperlukan **harmonisasi regulasi** antara UU PDP, UU ITE, KUHP, serta berbagai peraturan pelaksana sehingga tidak terdapat lagi konflik norma dalam praktik penegakan hukum. Harmonisasi tersebut harus disertai penyusunan pedoman teknis mengenai penerapan asas **lex specialis derogat legi generali** agar aparat penegak hukum memiliki standar yang sama dalam menentukan dasar hukum setiap perkara.

Kedua, pemerintah perlu memperkuat **kelembagaan pelindungan data pribadi** melalui pembentukan otoritas yang independen, memiliki kewenangan pengawasan, investigasi, serta pemberian sanksi administratif. Penguatan kelembagaan akan meningkatkan efektivitas pengawasan terhadap pengendali data maupun pemroses data sehingga mampu mencegah terjadinya penyalahgunaan data pribadi sejak tahap awal.

Ketiga, peningkatan kualitas **sumber daya manusia aparat penegak hukum** menjadi kebutuhan yang mendesak. Penyidik, penuntut umum, maupun hakim perlu memperoleh pelatihan berkelanjutan mengenai hukum siber, kecerdasan buatan, forensik digital, serta teknik pembuktian elektronik agar mampu mengikuti perkembangan modus operandi kejahatan digital.

Keempat, penelitian ini menekankan pentingnya **peningkatan literasi digital masyarakat**. Perlindungan data pribadi tidak hanya menjadi tanggung jawab negara, tetapi juga memerlukan partisipasi aktif masyarakat sebagai pemilik data. Edukasi mengenai keamanan data, perlindungan identitas digital, serta hak-hak subjek data perlu dilakukan secara berkelanjutan agar masyarakat lebih berhati-hati dalam memberikan maupun menggunakan data pribadi pada berbagai platform digital.

Dengan demikian, konsep ideal pertanggungjawaban pidana terhadap penyalahgunaan data pribadi tidak hanya bertujuan memberikan efek jera kepada pelaku, tetapi juga membangun sistem pelindungan data pribadi yang mampu menjamin **kepastian hukum, keadilan, dan kemanfaatan hukum** secara seimbang sesuai dengan tujuan hukum yang dikemukakan oleh Gustav Radbruch. Pendekatan tersebut diharapkan mampu meningkatkan kepercayaan masyarakat terhadap ekosistem transaksi elektronik sekaligus mendukung transformasi digital Indonesia yang aman, bertanggung jawab, dan berkelanjutan.

KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa pengaturan mengenai pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi elektronik di Indonesia telah mengalami perkembangan yang signifikan dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang melengkapi pengaturan sebelumnya dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kedua regulasi tersebut memberikan dasar hukum bagi penegakan pidana terhadap setiap orang maupun korporasi yang secara melawan hukum memperoleh, menggunakan, mengungkapkan, memindahkan, atau memanfaatkan data pribadi tanpa persetujuan pemilik data. Dari perspektif teori pertanggungjawaban pidana, pemidanaan terhadap pelaku harus memenuhi unsur adanya perbuatan melawan hukum (*actus reus*), unsur kesalahan (*mens rea*), kemampuan bertanggung jawab, serta tidak adanya alasan pembenar maupun alasan pemaaf. Hal tersebut menunjukkan bahwa sistem hukum pidana Indonesia tetap berpegang pada asas **geen straf zonder schuld** sebagai prinsip fundamental dalam menjatuhkan pidana.

Penelitian ini juga menemukan bahwa penerapan asas **lex specialis derogat legi generali** menjadi aspek penting dalam penyelesaian perkara penyalahgunaan data pribadi karena terdapat irisan pengaturan antara UU PDP dan UU ITE. UU PDP memiliki karakter sebagai peraturan yang lebih khusus dalam mengatur perlindungan data pribadi, sedangkan UU ITE memberikan perlindungan terhadap keamanan sistem elektronik sebagai media berlangsungnya transaksi digital. Namun demikian, implementasi kedua regulasi tersebut masih menghadapi berbagai kendala berupa belum optimalnya harmonisasi regulasi, keterbatasan kapasitas aparat penegak hukum dalam menangani pembuktian digital, belum optimalnya kelembagaan pelindungan data pribadi, rendahnya literasi digital masyarakat, serta meningkatnya karakter kejahatan siber yang bersifat lintas negara. Kondisi tersebut menyebabkan efektivitas penegakan hukum belum sepenuhnya mampu memberikan kepastian hukum dan perlindungan yang optimal bagi korban penyalahgunaan data pribadi.

Berdasarkan hasil penelitian tersebut, disarankan agar pemerintah melakukan harmonisasi lebih lanjut terhadap ketentuan dalam UU PDP dan UU ITE melalui penyusunan pedoman teknis mengenai penerapan asas **lex specialis derogat legi generali** sehingga terdapat keseragaman dalam proses penyidikan, penuntutan, maupun pemeriksaan di pengadilan. Selain itu, perlu dilakukan penguatan kelembagaan pelindungan data pribadi yang independen, peningkatan kompetensi aparat penegak hukum di bidang hukum siber dan forensik digital, pengembangan kerja sama internasional dalam penanganan kejahatan siber lintas negara, serta peningkatan literasi digital masyarakat mengenai pentingnya menjaga keamanan data pribadi. Dengan demikian, sistem pertanggungjawaban pidana terhadap penyalahgunaan data pribadi di Indonesia diharapkan mampu mewujudkan kepastian hukum, keadilan, kemanfaatan hukum, sekaligus memperkuat kepercayaan masyarakat terhadap penyelenggaraan transaksi elektronik yang aman dan berkelanjutan.

REFERENSI

Achmad Ali. (2017). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence) Termasuk Interpretasi Undang-Undang (Legisprudence)*. Jakarta: Kencana.

Azhar, D. P., & Mahyani, A. (2023). Pertanggungjawaban pidana korporasi sebagai pelaku tindak pidana penyebaran data pribadi konsumen. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(2), 1124–1138.

Brenner, S. W. (2018). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston: Northeastern University Press.

Greenleaf, G. (2023). Global data privacy laws 2023: Despite challenges, 162 laws show GDPR dominance. *Privacy Laws & Business International Report*, 183, 10–15.

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: Bina Ilmu.

Kurniawan, K. D. (2024). Criminal sanctions and personal data protection in Indonesia. *Lex Publica*, 11(2), 155–170.

Lutrianto, I. (2025). Legal problems of personal data protection in the digital era: Juridical analysis of Indonesia's Personal Data Protection Law. *Global International Journal of Law and Social Sciences*, 3(1), 25–38.
Marzuki, P. M. (2021). *Penelitian Hukum* (Edisi Revisi). Jakarta: Kencana.
Mertokusumo, S. (2005). *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Liberty.
Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
Palit, S. M. L. (2025). Legal perspective on data privacy protection as a human right in Indonesia. *East Asian Journal of Law and Human Rights*, 2(1), 44–59.
Putra, R. K., & Idris, M. F. (2024). Perlindungan data pribadi dalam era big data: Implikasi hukum di Indonesia. *Jurnal Jaksa*, 2(4), 178–193. https://doi.org/10.51903/jaksa.v2i4.2260
Razi, F., Tuasikal, H., & Markus, D. P. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285
Republik Indonesia. Kitab Undang-Undang Hukum Pidana.
Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
Simanjuntak, P. H. (2024). Perlindungan hukum terhadap data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Jurnal Esensi Hukum*, 6(2), 145–163.
Soekanto, S., & Mamudji, S. (2019). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada.
Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review*, 89(1), 1–51.
Wall, D. S. (2021). *Cybercrime: The Transformation of Crime in the Information Age* (3rd ed.). Cambridge: Polity Press.
Zainuddin Ali. (2021). *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.