Journal of Law and Legal System
Publisher: CV. Doki Course and Training
Vol. 2 No. 1 2026, 183-193
https://jurnal.dokicti.org/index.php/JLLS/index

Pertanggungjawaban Pidana atas Penyalahgunaan Data Pribadi dalam Kejahatan Siber

Dilla Septiani[1], Holijah[2], Nengsih Ari Saputri[3], Tiara Monika[4], Rahma Aulia Riski[5], Ahmad Fauzan[6]
[1,2,3,4,5,6]Universitas Islam Negeri Raden Fatah Palembang;
e-mail: dillasep099@gmail.com

ABSTRAK

Perkembangan teknologi informasi tlah meningkatkan risiko penyalahgunaan data pribadi dalam berbagai bentuk kejahatan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dalam kejahatan siber serta mengkaji integrasi antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai dasar penegakan hukum di Indonesia. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Bahan hukum diperoleh dari peraturan perundang-undangan, buku, artikel ilmiah, dan sumber hukum lain yang relevan. Hasil penelitian menunjukkan bahwa penyalahgunaan data pribadi dalam kejahatan siber dapat berupa perolehan data tanpa hak, penggunaan dan pengungkapan data secara melawan hukum, pemalsuan identitas, pengambilalihan akun, serta pemanfaatan data untuk transaksi ilegal. Pertanggungjawaban pidana dapat dibebankan kepada pelaku perorangan maupun korporasi sepanjang unsur perbuatan, kesalahan, dan pembuktian elektronik dapat dipenuhi secara sah. Kontribusi penelitian ini terletak pada analisis terpadu antara rezim pelindungan data pribadi dan rezim hukum siber dalam menentukan mekanisme pertanggungjawaban pidana. Penelitian ini menyimpulkan bahwa harmonisasi penerapan UU Pelindungan Data Pribadi dan UU Informasi dan Transaksi Elektronik diperlukan untuk mewujudkan kepastian hukum dan perlindungan yang lebih efektif terhadap subjek data pribadi.

Kata Kunci**:** Data Pribadi, Kejahatan Siber, Pelindungan Data Pribadi, Pertanggungjawaban Pidana

ABSTRACT

The rapid development of information technology has increased the risk of personal data misuse in increasingly complex forms of cybercrime. This study aims to analyze criminal liability for personal data misuse in cybercrime and examine the integration of Law Number 27 of 2022 concerning Personal Data Protection and Law Number 1 of 2024 concerning Electronic Information and Transactions as the legal basis for law enforcement in Indonesia. This research employs a normative juridical method using statutory and conceptual approaches. Legal materials were obtained from legislation, books, scientific articles, and other relevant legal sources. The findings indicate that personal data misuse in cybercrime includes unlawful acquisition of personal data, unauthorized use and disclosure of data, identity falsification, account takeover, and the use of personal data for illegal transactions. Criminal liability may be imposed on both individuals and corporations, provided that the elements of unlawful conduct, fault, and electronic evidence are legally established. The contribution of this study lies in its integrated analysis of the personal data protection regime and cyber law regime in determining criminal liability mechanisms. The study concludes that harmonizing the implementation of the Personal Data Protection Law and the Electronic Information and Transactions Law is necessary to ensure legal certainty and provide more effective protection for personal data subjects.

Keywords: Cybercrime; Criminal Liability; Personal Data; Personal Data Protection.

PENDAHULUAN

Penyalahgunaan data pribadi tidak hanya menimbulkan kerugian dalam bentuk kehilangan data atau kebocoran informasi, tetapi juga berdampak langsung terhadap kehidupan

sosial dan psikologis korban. Data pribadi yang jatuh ke tangan pihak yang tidak berwenang dapat digunakan untuk pencurian identitas, pengajuan pinjaman tanpa persetujuan, penipuan daring, maupun penyebaran informasi pribadi yang merugikan reputasi seseorang.

Pada konteks masyarakat digital, identitas elektronik telah menjadi bagian penting dari aktivitas ekonomi, sosial, dan administratif sehingga penyalahgunaannya dapat menimbulkan kerugian yang bersifat berkelanjutan. Oleh karena itu, pelindungan data pribadi tidak lagi dipandang sekadar sebagai persoalan teknis keamanan informasi, tetapi juga sebagai bagian dari upaya melindungi hak privasi dan keamanan warga negara di ruang digital.

Beberapa penelitian terdahulu telah membahas pelindungan data pribadi dari berbagai perspektif. Sinaga dan Putri (2020) mengkaji formulasi legislasi pelindungan data pribadi sebelum lahirnya Undang-Undang Pelindungan Data Pribadi dan menemukan bahwa pengaturannya masih tersebar dalam berbagai regulasi sektoral. Fauzy dan Shandy (2023) menelaah hak atas privasi serta politik hukum pembentukan UU PDP sebagai instrumen perlindungan hak konstitusional warga negara di era digital. Sementara itu, Nababan et al. (2023) memfokuskan kajiannya pada pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dalam tindak pidana dunia maya dan menunjukkan masih adanya ketidakjelasan mengenai bentuk pertanggungjawaban pidana yang dapat diterapkan terhadap pelaku.

Meskipun penelitian-penelitian tersebut memberikan kontribusi penting dalam pengembangan kajian pelindungan data pribadi, sebagian besar masih membahas aspek regulasi, hak privasi, atau pertanggungjawaban pidana secara terpisah. Penelitian terdahulu juga belum secara khusus mengkaji hubungan antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dalam menentukan konstruksi pertanggungjawaban pidana terhadap penyalahgunaan data pribadi sebagai bagian dari kejahatan siber.

Berdasarkan kondisi tersebut, penelitian ini memiliki kebaruan (state of the art) berupa analisis integratif antara rezim pelindungan data pribadi dan rezim hukum siber melalui pengkajian terpadu terhadap UU PDP dan UU ITE. Penelitian ini tidak hanya menelaah bentuk penyalahgunaan data pribadi sebagai pelanggaran privasi, tetapi juga menganalisis bagaimana kedua regulasi tersebut digunakan sebagai dasar penentuan pertanggungjawaban pidana terhadap pelaku, baik perorangan maupun korporasi, dalam kejahatan siber.

Penguatan argumentasi mengenai pertanggungjawaban pidana juga dapat dilihat melalui praktik peradilan yang menempatkan informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana berbasis teknologi informasi. Dalam berbagai putusan perkara yang berkaitan dengan tindak pidana elektronik, hakim menilai bahwa jejak digital, data elektronik, dan aktivitas dalam sistem elektronik dapat digunakan untuk membuktikan unsur perbuatan maupun keterlibatan pelaku. Kecenderungan tersebut menunjukkan bahwa perkembangan hukum pembuktian di Indonesia telah memberikan ruang yang lebih luas bagi penggunaan alat bukti elektronik dalam mengungkap tindak pidana siber, termasuk penyalahgunaan data pribadi yang dilakukan melalui sistem elektronik.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis bentuk pertanggungjawaban hukum pidana terhadap penyalahgunaan data pribadi dalam kejahatan siber serta menelaah dasar hukum yang digunakan dalam penegakannya.

METODE

Penelitian ini menggunakan metode studi literatur dengan jenis penelitian yuridis normatif. Penelitian yuridis normatif menempatkan hukum sebagai norma yang tertuang dalam peraturan perundang-undangan, putusan, dan doktrin hukum yang digunakan untuk

menganalisis pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dalam kejahatan siber. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan digunakan untuk menelaah berbagai regulasi yang berkaitan dengan pelindungan data pribadi dan kejahatan siber, sedangkan pendekatan konseptual digunakan untuk menganalisis konsep pertanggungjawaban pidana, hak atas privasi, dan pelindungan data pribadi.

Bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Kitab Undang-Undang Hukum Pidana, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi. Bahan hukum sekunder diperoleh dari buku, artikel jurnal ilmiah, hasil penelitian, dan dokumen akademik lain yang relevan dengan topik penelitian.

Pengumpulan bahan hukum dilakukan melalui penelusuran literatur secara sistematis pada Google Scholar, SINTA, GARUDA, portal jurnal perguruan tinggi, dan laman resmi pemerintah dengan menggunakan kata kunci "pelindungan data pribadi", "penyalahgunaan data pribadi", "kejahatan siber", "cybercrime", dan "pertanggungjawaban pidana". Sumber literatur dipilih berdasarkan relevansi dengan fokus penelitian, kredibilitas penerbit, serta keterbaruan publikasi yang diprioritaskan pada rentang tahun 2020–2025, kecuali peraturan perundang-undangan dan referensi dasar yang masih memiliki relevansi konseptual.

Analisis bahan hukum dilakukan secara kualitatif melalui empat tahapan, yaitu inventarisasi, klasifikasi, interpretasi, dan sistematisasi bahan hukum. Tahap inventarisasi dilakukan dengan mengumpulkan seluruh bahan hukum yang relevan. Tahap klasifikasi dilakukan dengan mengelompokkan bahan hukum berdasarkan tema pelindungan data pribadi, kejahatan siber, dan pertanggungjawaban pidana. Tahap interpretasi dilakukan untuk menafsirkan norma hukum yang terdapat dalam peraturan perundang-undangan serta menghubungkannya dengan teori hukum pidana dan hasil penelitian terdahulu. Selanjutnya, tahap sistematisasi dilakukan dengan menyusun hubungan antara norma hukum, bentuk penyalahgunaan data pribadi, dan mekanisme pertanggungjawaban pidana sehingga diperoleh pemahaman yang komprehensif mengenai penegakan hukum terhadap penyalahgunaan data pribadi dalam kejahatan siber. Hasil analisis kemudian disajikan secara deskriptif-analitis untuk menjawab tujuan penelitian.

HASIL DAN PEMBAHASAN

Bagian ini membahas hasil analisis mengenai dasar hukum yang mengatur pelindungan data pribadi dan kejahatan siber di Indonesia, bentuk penyalahgunaan data pribadi dalam ruang digital, serta pertanggungjawaban pidana terhadap pelaku berdasarkan ketentuan peraturan perundang-undangan yang berlaku.

Pembahasan disusun untuk menunjukkan hubungan antara dasar hukum, bentuk penyalahgunaan data pribadi, dan mekanisme pertanggungjawaban pidana dalam kejahatan siber. Melalui pembahasan tersebut dapat diketahui bagaimana integrasi antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dalam memberikan dasar hukum dan kepastian hukum terhadap penanganan penyalahgunaan data pribadi di ruang digital.

Journal of Law and Legal System
Publisher: CV. Doki Course and Training
Vol. 2 No. 1 2026, 183-193
https://jurnal.dokicti.org/index.php/JLLS/index

Dasar Hukum Pelindungan Data Pribadi dan Kejahatan Siber di Indonesia

Pelindungan data pribadi di Indonesia bertumpu pada pengakuan hak atas privasi sebagai bagian dari hak konstitusional warga negara, yang kemudian diterjemahkan ke dalam pengaturan sektoral sebelum lahirnya undang-undang khusus. Fauzy dan Shandy (2023) memandang hak atas privasi sebagai landasan utama pembentukan rezim pelindungan data pribadi, sedangkan Sinaga dan Putri (2020) menegaskan bahwa pengaturannya pada masa sebelum Undang-Undang Nomor 27 Tahun 2022 masih tersebar dan parsial.

Wantania (2025) juga menunjukkan bahwa perkembangan pelindungan hukum terhadap keamanan data pribadi di era digital menuntut aturan yang mampu mengikuti perubahan teknologi dan kesadaran hukum masyarakat. Penelitian ini sejalan dengan kajian tersebut karena sebelum hadirnya UU PDP, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 memang telah memberikan dasar perlindungan data pribadi dalam sistem elektronik, tetapi pengaturannya belum membentuk kerangka nasional yang utuh untuk menjawab persoalan penyalahgunaan data pribadi dalam kejahatan siber.

Undang-Undang Nomor 27 Tahun 2022 kemudian menjadi titik penting karena untuk pertama kalinya data pribadi didefinisikan secara tegas sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, sedangkan pelindungan data pribadi dipahami sebagai upaya untuk menjamin hak konstitusional subjek data pribadi. Penguatan itu tidak berhenti pada definisi, sebab undang-undang tersebut juga mewajibkan Pengendali Data Pribadi untuk melindungi dan memastikan keamanan data yang diproses serta menghapus data dalam keadaan tertentu.

Fauzy dan Shandy (2023) melihat UU PDP sebagai bentuk politik hukum yang responsif, penelitian Sinaga dan Putri (2020) sejak awal telah menuntut undang-undang khusus, sedangkan Firdaus (2024) menilai kehadiran UU PDP memberi harapan baru bagi kepastian hukum meskipun masih memerlukan penguatan implementasi. Dengan hal tersebut, UU PDP merupakan fondasi utama pelindungan data pribadi, tetapi tulisan ini menambahkan bahwa arti pentingnya terletak pula pada pemisahan yang lebih jelas antara pengelolaan data yang sah, kelalaian tata kelola, dan penyalahgunaan data yang dapat bergeser ke ranah pidana.

Dasar hukum penyalahgunaan data pribadi dalam kejahatan siber tidak dapat dipahami hanya berdasarkan UU PDP. Hal ini karena peristiwa hukumnya berlangsung melalui sistem elektronik yang juga diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

Penelitian terdahulu Nababan dan rekan-rekannya (2023) menekankan bahwa penyalahgunaan data pribadi pada tindak pidana dunia maya harus dianalisis bersama rezim hukum siber, sedangkan Sabadina (2022) lebih dahulu menunjukkan bahwa kebocoran data pribadi oleh korporasi berbasis online menuntut politik hukum pidana yang lebih tegas. Pandangan kedua penelitian itu pada dasarnya sejalan karena sama-sama menempatkan data pribadi sebagai objek yang rentan disalahgunakan melalui teknologi informasi, meskipun titik tekannya berbeda, yakni Nababan et al. (2023) lebih dekat pada pertanggungjawaban pidana pelaku, sedangkan Sabadina (2022) menyoroti arah kebijakan hukum pidana terhadap kejahatan teknologi informasi. Penelitian ini mengambil posisi bahwa UU PDP merupakan pengatur khusus mengenai data pribadi, sementara PP PSTE dan UU ITE berfungsi melengkapi pengaturan mengenai penyelenggara sistem elektronik, akses terhadap informasi elektronik, serta kewenangan penyidikan, sehingga pembacaan dasarnya harus dilakukan secara terpadu.

Kekuatan dasar hukum tersebut tampak lebih nyata setelah UU PDP merumuskan larangan dan ancaman pidana secara spesifik terhadap perolehan atau pengumpulan data pribadi secara melawan hukum, pengungkapan data pribadi yang bukan miliknya, penggunaan data

pribadi yang bukan miliknya, serta pembuatan atau pemalsuan data pribadi. Pengaturan tersebut menunjukkan bahwa perlindungan data pribadi tidak lagi hanya berada pada ranah administratif, tetapi telah memperoleh dasar penegakan hukum pidana yang lebih jelas.

Selain itu, UU PDP juga mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti dalam proses penegakan hukum. Ketentuan ini memperlihatkan adanya keterkaitan yang erat antara rezim pelindungan data pribadi dan rezim hukum siber. Oleh karena itu, analisis pertanggungjawaban pidana terhadap penyalahgunaan data pribadi perlu dilakukan secara terpadu dengan memperhatikan ketentuan dalam UU PDP, UU ITE, dan PP PSTE.

Meskipun UU PDP dan UU ITE sama-sama berfungsi sebagai instrumen perlindungan dalam ruang digital, hubungan keduanya masih menyisakan potensi tumpang tindih norma dalam praktik penegakan hukum. UU PDP secara khusus mengatur hak subjek data pribadi, kewajiban pengendali data, larangan penyalahgunaan data pribadi, dan ancaman pidana terhadap pelanggaran yang berkaitan dengan data pribadi. Sebaliknya, UU ITE memiliki cakupan yang lebih luas karena mengatur berbagai perbuatan melawan hukum yang dilakukan melalui sistem elektronik, termasuk akses tanpa hak, manipulasi informasi elektronik, dan gangguan terhadap sistem elektronik.

Dalam praktiknya, suatu perbuatan dapat memenuhi unsur tindak pidana dalam kedua undang-undang sekaligus. Sebagai contoh, tindakan mengakses sistem elektronik tanpa hak untuk memperoleh data pribadi dapat diproses menggunakan ketentuan akses ilegal dalam UU ITE maupun ketentuan perolehan data pribadi secara melawan hukum dalam UU PDP. Situasi ini berpotensi menimbulkan perbedaan penafsiran dan penerapan pasal oleh aparat penegak hukum apabila tidak terdapat pedoman yang jelas mengenai hubungan antara kedua rezim hukum tersebut. Oleh karena itu, diperlukan pendekatan interpretasi yang menempatkan UU PDP sebagai lex specialis dalam perkara yang secara langsung berkaitan dengan pelanggaran terhadap data pribadi, sedangkan UU ITE berfungsi sebagai instrumen pendukung yang mengatur aspek teknis dan sarana elektronik yang digunakan dalam terjadinya tindak pidana.

Selain persoalan harmonisasi nasional, perkembangan hukum pelindungan data pribadi di Indonesia juga perlu ditempatkan dalam konteks perkembangan standar internasional. Salah satu instrumen yang paling berpengaruh adalah General Data Protection Regulation (GDPR) Uni Eropa yang menempatkan pelindungan data pribadi sebagai bagian dari hak fundamental setiap individu.

GDPR mengembangkan prinsip-prinsip penting seperti lawfulness, fairness, transparency, purpose limitation, data minimization, accountability, dan data security. Jika dibandingkan dengan ketentuan dalam UU PDP, terdapat sejumlah kesamaan, terutama terkait pengakuan hak subjek data, kewajiban pengendali data, mekanisme persetujuan (consent), serta kewajiban menjaga keamanan data pribadi.

Namun demikian, efektivitas perlindungan data pribadi tidak hanya ditentukan oleh keberadaan regulasi, melainkan juga oleh kapasitas lembaga pengawas, mekanisme penegakan hukum, dan tingkat kepatuhan penyelenggara sistem elektronik. Dalam hal ini, Indonesia masih menghadapi tantangan berupa keterbatasan pengawasan, rendahnya kesadaran sebagian masyarakat mengenai hak atas data pribadi, serta belum meratanya kesiapan penyelenggara sistem elektronik dalam menerapkan standar keamanan data yang memadai. Kondisi tersebut menunjukkan bahwa keberhasilan implementasi UU PDP tidak hanya bergantung pada kelengkapan norma hukum, tetapi juga pada kemampuan negara membangun ekosistem perlindungan data pribadi yang efektif dan berkelanjutan.

Berikut yang menunjukkan beberapa regulasi utama yang berkaitan dengan pelindungan data pribadi dan kejahatan siber di Indonesia.

Tabel 1 Regulasi Pelindungan Data Pribadi dan Kejahatan Siber di Indonesia

No	Regulasi	Ruang Lingkup	Relevansi terhadap Penelitian
1	UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi	Perlindungan data pribadi dan sanksi pidana	Menjadi dasar utama penentuan unsur tindak pidana penyalahgunaan data pribadi
2	UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik	Tindak pidana berbasis sistem elektronik	Mengatur sarana, media, dan pembuktian elektronik dalam kejahatan siber
3	PP No. 71 Tahun 2019 tentang PSTE	Penyelenggaraan sistem elektronik	Mengatur kewajiban penyelenggara sistem elektronik dalam pengelolaan data
4	PERMA No. 13 Tahun 2016	Pertanggungjawaban pidana korporasi	Menjadi dasar pemidanaan korporasi dalam tindak pidana penyalahgunaan data pribadi

Sumber: Hasil Analisis dari berbagai peraturan perundang-undangan 2026.

Walaupun pengaturan hukum sudah semakin lengkap, implementasi pelindungan data pribadi masih menghadapi berbagai kendala. Salah satu kelemahan regulasi terletak pada belum optimalnya pengawasan terhadap penyelenggara sistem elektronik. Selain itu, belum semua masyarakat memahami hak-hak mereka sebagai subjek data pribadi sehingga kasus kebocoran data sering tidak dilaporkan secara hukum.

Bentuk Penyalahgunaan Data Pribadi dalam Kejahatan Siber

Bentuk penyalahgunaan data pribadi dalam kejahatan siber pada dasarnya dapat ditelusuri dari perbuatan yang dilarang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yaitu memperoleh atau mengumpulkan data pribadi secara melawan hukum, mengungkapkan data pribadi yang bukan miliknya, menggunakan data pribadi yang bukan miliknya, serta membuat atau memalsukan data pribadi untuk menguntungkan diri sendiri atau orang lain (Republik Indonesia, 2022).

Perbuatan tersebut menunjukkan bahwa penyalahgunaan data pribadi tidak hanya berbentuk pencurian data dalam arti mengambil data dari suatu sistem, tetapi juga mencakup penguasaan, pemindahan, penyebaran, dan pemanfaatan data tanpa dasar hak yang sah dalam ruang elektronik yang diatur pula dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (Republik Indonesia, 2024). Nababan et al. (2023) menempatkan penyalahgunaan data pribadi sebagai bagian dari tindak pidana dunia maya yang harus dibaca bersama perkembangan kejahatan digital yang semakin kompleks.

Penyalahgunaan data pribadi dalam praktik kejahatan siber tidak selalu dilakukan melalui peretasan sistem elektronik. Dalam banyak kasus, pelaku memanfaatkan rekayasa sosial (social engineering) untuk memperoleh data korban secara tidak langsung.

Salah satu modus yang sering digunakan adalah smishing, yaitu pengiriman pesan singkat yang berisi tautan palsu atau lampiran berbahaya yang bertujuan memperoleh data pribadi dan kredensial akun korban. Selain itu, phishing juga banyak dilakukan melalui surat elektronik palsu yang mengatasnamakan lembaga resmi atau penyedia layanan tertentu untuk meyakinkan korban agar memberikan informasi pribadi.

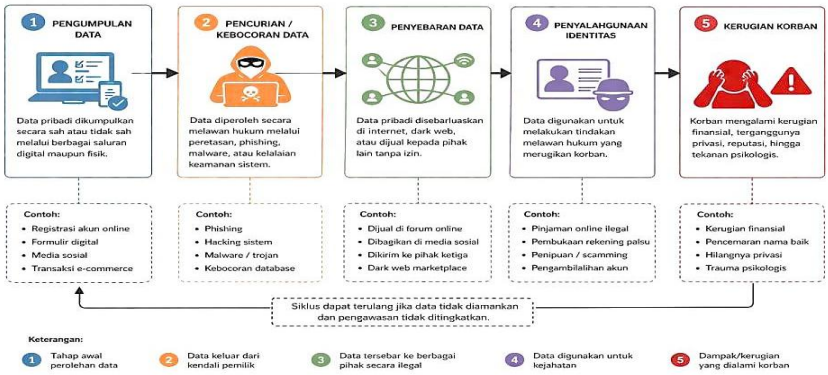
Bentuk penyalahgunaan lain yang saat ini sering terjadi adalah pencurian identitas, pengambilalihan akun, dan pemanfaatan data pribadi untuk layanan keuangan ilegal. Otoritas Jasa Keuangan menegaskan bahwa penyelenggara fintech lending tidak boleh mengakses kontak dan gambar pada telepon seluler pengguna, sedangkan pinjaman online ilegal justru

Journal of Law and Legal System
Publisher: CV. Doki Course and Training
Vol. 2 No. 1 2026, 183-193
https://jurnal.dokicti.org/index.php/JLLS/index

dikenal meminta akses terhadap data pribadi dan bahkan menggunakan ancaman penyebaran data sebagai sarana penagihan (Otoritas Jasa Keuangan, 2023).

Otoritas Jasa Keuangan juga mengingatkan bahwa apabila data pribadi seseorang disalahgunakan untuk mengajukan pinjaman, korban dapat melaporkannya kepada kepolisian, asosiasi penyelenggara, atau OJK, yang berarti data pribadi dapat dipakai secara langsung untuk membangun identitas keuangan palsu. Temuan Wijayanto (2020) memperlihatkan bahwa aplikasi fintech ilegal berpotensi mengakses data keluarga, data kontak, data pekerjaan, data perbankan, dan data media sosial, sehingga ruang penyalahgunaannya jauh melampaui kebutuhan verifikasi yang wajar. Keadaan tersebut menunjukkan bahwa penyalahgunaan data pribadi tidak berhenti pada pengambilan data, tetapi berkembang menjadi pemakaian data untuk intimidasi, pembentukan identitas palsu, pengajuan pinjaman tanpa hak, dan pengambilalihan akses terhadap akun digital korban.

Fenomena penyalahgunaan dan kebocoran data pribadi juga tercermin dalam sejumlah kasus yang terjadi di Indonesia. Salah satu kasus yang banyak mendapat perhatian publik adalah dugaan kebocoran data peserta BPJS Kesehatan yang melibatkan jutaan data warga negara. Selain itu, dugaan kebocoran data paspor dan berbagai insiden kebocoran data pada platform digital menunjukkan bahwa data pribadi memiliki nilai ekonomi yang tinggi dan rentan dimanfaatkan oleh pihak yang tidak berwenang. Kasus-kasus tersebut memperlihatkan bahwa ancaman terhadap data pribadi tidak hanya bersumber dari tindakan individu, tetapi juga dapat terjadi akibat lemahnya tata kelola dan sistem keamanan data pada penyelenggara sistem elektronik.



Gambar 1 Skema Penyalahgunaan Data pribadi dalam Kejahatan Siber

Regulasi yang ada masih menghadapi konflik norma dalam praktik penegakan hukum. UU PDP mengatur perlindungan data pribadi secara khusus, sedangkan UU ITE lebih menitikberatkan pada tindak pidana elektronik secara umum. Perbedaan ruang lingkup tersebut terkadang menyebabkan penegak hukum menggunakan pasal yang berbeda terhadap kasus yang serupa. Akibatnya, penerapan hukum dapat menimbulkan ketidakseragaman dalam proses penyidikan maupun pemidanaan.

Dari perspektif viktimologi, penyalahgunaan data pribadi dalam kejahatan siber tidak hanya menimbulkan kerugian ekonomi, tetapi juga berdampak pada kondisi psikologis dan sosial korban. Korban yang identitasnya disalahgunakan sering kali mengalami kehilangan rasa aman dalam menggunakan layanan digital karena khawatir data pribadinya kembali dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain itu, penyalahgunaan data pribadi dapat menyebabkan kerusakan reputasi, munculnya tekanan psikologis, serta terganggunya aktivitas sosial dan profesional korban.

Pada kasus pinjaman online ilegal, misalnya, korban tidak hanya menghadapi risiko kerugian finansial, tetapi juga ancaman penyebaran data pribadi kepada keluarga, rekan kerja, dan pihak lain yang terdapat dalam daftar kontaknya. Dampak tersebut menunjukkan bahwa kejahatan terhadap data pribadi pada hakikatnya merupakan kejahatan yang menyerang identitas dan privasi seseorang, sehingga konsekuensinya dapat berlangsung lebih lama dibandingkan kerugian materiil yang ditimbulkan.

Lebih lanjut, posisi korban dalam perkara penyalahgunaan data pribadi sering kali berada pada kondisi yang kurang menguntungkan karena korban harus membuktikan bahwa tindakan tertentu bukan dilakukan oleh dirinya. Ketika data pribadi digunakan untuk membuat akun palsu, melakukan transaksi elektronik, atau mengajukan pinjaman tanpa persetujuan pemilik data, korban kerap menghadapi kesulitan dalam proses pemulihan haknya.

Oleh karena itu, perlindungan hukum terhadap korban tidak cukup diwujudkan melalui pemidanaan pelaku semata, tetapi juga memerlukan mekanisme pemulihan yang efektif, termasuk pemulihan identitas digital, penghapusan data yang disalahgunakan, serta jaminan keamanan terhadap data pribadi di masa mendatang. Dengan demikian, pendekatan viktimologi menjadi penting dalam memahami bahwa penyalahgunaan data pribadi bukan hanya persoalan pelanggaran hukum, tetapi juga persoalan perlindungan hak asasi dan martabat individu di ruang digital.

Kebocoran data pribadi oleh korporasi atau penyelenggara sistem elektronik juga merupakan bentuk penyalahgunaan yang sangat relevan dalam kejahatan siber karena data yang bocor dapat diperdagangkan, dipindahkan, atau dipakai untuk tindak pidana lanjutan. Komdigi pada 2025 membekukan izin layanan Worldcoin dan WorldID serta memeriksa kepatuhan hukumnya sebagai langkah perlindungan terhadap privasi dan data pribadi warga, yang menunjukkan bahwa pengumpulan data biometrik dalam layanan digital dapat menimbulkan risiko hukum yang serius apabila tata kelolanya tidak jelas (Kementerian Komunikasi dan Digital, 2025).

Komdigi juga menegaskan bahwa pencurian data pribadi merupakan pelanggaran serius dan setiap pengungkapan data pribadi yang bukan miliknya dapat dikenai sanksi pidana berdasarkan UU PDP, sehingga kebocoran data tidak dapat dipandang hanya sebagai gangguan teknis biasa (Kementerian Komunikasi dan Digital, 2024). Sabadina (2022) telah menyoroti bahwa kebocoran data pribadi oleh korporasi berbasis online membuka peluang penggunaan data oleh pihak yang tidak berhak dan memperbesar risiko kejahatan teknologi informasi. Uraian tersebut menunjukkan bahwa bentuk penyalahgunaan data pribadi dalam kejahatan siber meliputi pengambilan data tanpa hak, penyerahan data melalui tipu daya, pemakaian data untuk identitas dan transaksi palsu, serta kebocoran data yang kemudian dipakai kembali untuk kepentingan melawan hukum.

Pertanggungjawaban Hukum Pidana terhadap Pelaku Penyalahgunaan Data Pribadi dalam Kejahatan Siber

Pertanggungjawaban hukum pidana terhadap pelaku penyalahgunaan data pribadi dalam kejahatan siber pada dasarnya lahir ketika unsur perbuatan yang dilarang dapat dibuktikan secara sah menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Bentuk perbuatan tersebut meliputi memperoleh atau mengumpulkan data pribadi secara melawan hukum, mengungkapkan data pribadi yang bukan miliknya, menggunakan data pribadi yang bukan miliknya, serta membuat atau memalsukan data pribadi untuk keuntungan diri sendiri atau orang lain.

Nababan et al. (2023) menjelaskan bahwa penyalahgunaan data pribadi dalam tindak pidana dunia maya telah memiliki dasar pemidanaan yang nyata dan tidak lagi dapat dipandang

sekadar sebagai pelanggaran etika digital. Pemidanaan karena itu tidak timbul hanya karena terjadi gangguan terhadap data pribadi, melainkan harus dibuktikan adanya unsur melawan hukum, kesalahan, dan hubungan antara perbuatan pelaku dengan kerugian yang timbul pada subjek data pribadi.

Pertanggungjawaban pidana dalam perkara penyalahgunaan data pribadi tidak hanya dapat dibebankan kepada orang perorangan, tetapi juga dapat diarahkan kepada korporasi apabila tindak pidana dilakukan untuk kepentingan korporasi atau dibiarkan terjadi dalam kegiatan usahanya. Undang-Undang Pelindungan Data Pribadi memberi ruang pemidanaan terhadap pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan korporasi, sedangkan terhadap korporasi pidana pokok yang dapat dijatuhkan berupa pidana denda dengan pemberatan tertentu (Republik Indonesia, 2022).

Pedoman mengenai pertanggungjawaban pidana korporasi juga telah ditegaskan dalam Peraturan Mahkamah Agung Nomor 13 Tahun 2016, terutama ketika korporasi memperoleh keuntungan dari tindak pidana, membiarkan tindak pidana terjadi, atau tidak menjalankan langkah pencegahan dan kepatuhan hukum yang semestinya. Firdaus (2024) juga menekankan pentingnya kepastian hukum bagi pengendali data pribadi, sehingga tanggung jawab pidana tidak seharusnya berhenti pada pelaku lapangan, tetapi juga harus menjangkau struktur pengendalian yang menikmati manfaat atau lalai memenuhi kewajiban perlindungan data.

Pembebanan pertanggungjawaban pidana dalam perkara penyalahgunaan data pribadi sangat bergantung pada proses pembuktian. Hal ini disebabkan karena sebagian besar perbuatan dilakukan melalui sistem elektronik, akun digital, jaringan komunikasi, dan jejak data yang tidak selalu terlihat secara fisik.

Oleh karena itu, informasi elektronik dan dokumen elektronik memiliki peranan yang sangat penting dalam proses penyidikan maupun persidangan. Pengakuan terhadap alat bukti elektronik tersebut telah diatur dalam UU ITE dan diperkuat oleh ketentuan dalam UU PDP.

Pentingnya pertanggungjawaban pidana terhadap penyalahgunaan data pribadi dapat dilihat dari berbagai kasus kebocoran data yang pernah terjadi di Indonesia dalam beberapa tahun terakhir. Kebocoran data yang melibatkan jutaan data pengguna layanan digital menunjukkan bahwa penyalahgunaan data pribadi tidak lagi berdampak pada individu tertentu saja, melainkan dapat menimbulkan risiko yang luas terhadap keamanan informasi, kepercayaan publik, dan stabilitas aktivitas ekonomi digital. Dalam konteks tersebut, pertanggungjawaban pidana memiliki fungsi strategis sebagai instrumen perlindungan hukum sekaligus sarana pencegahan agar pengendali data dan penyelenggara sistem elektronik menjalankan kewajiban perlindungan data secara lebih serius. Kehadiran sanksi pidana juga menunjukkan bahwa pelanggaran terhadap data pribadi bukan sekadar pelanggaran administratif, tetapi merupakan perbuatan yang dapat menimbulkan konsekuensi hukum yang serius apabila mengakibatkan kerugian bagi subjek data pribadi.

Di sisi lain, implementasi pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi masih menghadapi berbagai hambatan praktis. Karakteristik kejahatan siber yang memanfaatkan teknologi informasi menyebabkan proses identifikasi pelaku sering kali lebih kompleks dibandingkan tindak pidana konvensional. Pelaku dapat menggunakan identitas palsu, jaringan virtual, atau server yang berada di luar wilayah hukum Indonesia sehingga menyulitkan proses pelacakan.

Selain itu, proses pembuktian memerlukan dukungan forensik digital yang memadai untuk memastikan keaslian dan integritas alat bukti elektronik yang diajukan di persidangan. Keterbatasan sumber daya manusia yang memiliki kompetensi khusus di bidang keamanan siber dan forensik digital juga menjadi tantangan tersendiri bagi aparat penegak hukum. Tidak jarang penanganan perkara membutuhkan koordinasi antara kepolisian, kementerian terkait,

penyelenggara sistem elektronik, dan bahkan otoritas di negara lain apabila kejahatan dilakukan secara lintas batas. Oleh karena itu, efektivitas pertanggungjawaban pidana terhadap penyalahgunaan data pribadi tidak hanya ditentukan oleh keberadaan norma hukum, tetapi juga oleh kapasitas kelembagaan, kualitas sumber daya manusia, serta kerja sama antarinstansi dalam proses penegakan hukum.

Tabel 2 Hambatan Penegakan Hukum Penyalahgunaan Data Pribadi

No	Hambatan	Dampak
1	Rendahnya literasi digital masyarakat	Korban mudah tertipu phishing/smishing
2	Keterbatasan forensik digital	Pembuktian elektronik menjadi sulit
3	Lemahnya pengawasan sistem elektronik	Risiko kebocoran data meningkat
4	Tumpang tindih regulasi	Penegakan hukum kurang konsisten

Sumber: Hasil analisis penulis, 2026.

Selain hambatan teknis, terdapat pula kelemahan implementasi dalam bentuk belum optimalnya koordinasi antar lembaga penegak hukum. Penanganan kasus data pribadi sering melibatkan kepolisian, kementerian terkait, dan penyelenggara sistem elektronik sehingga proses penegakannya membutuhkan sinkronisasi yang baik. Kurangnya koordinasi dapat menyebabkan lambatnya penanganan perkara dan rendahnya efektivitas perlindungan hukum terhadap korban.

Dengan demikian, pertanggungjawaban pidana terhadap penyalahgunaan data pribadi harus dipahami sebagai bagian dari penegakan hukum siber yang terpadu. Penegakan hukum tidak cukup hanya melalui pemidanaan pelaku, tetapi juga memerlukan penguatan pengawasan sistem elektronik, peningkatan literasi digital masyarakat, dan harmonisasi regulasi agar perlindungan data pribadi dapat berjalan lebih efektif.

KESIMPULAN

Penyalahgunaan data pribadi dalam kejahatan siber merupakan bentuk pelanggaran hukum yang tidak hanya mengancam hak privasi individu, tetapi juga berpotensi menimbulkan kerugian ekonomi, sosial, dan hukum bagi korban. Hasil penelitian menunjukkan bahwa dasar hukum pertanggungjawaban pidana terhadap penyalahgunaan data pribadi di Indonesia bertumpu pada 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). Kedua regulasi tersebut memiliki hubungan yang saling melengkapi, di mana UU PDP mengatur secara khusus perlindungan dan larangan penyalahgunaan data pribadi, sedangkan UU ITE memberikan dasar hukum terkait tindak pidana yang dilakukan melalui sistem elektronik.

Penelitian ini menemukan bahwa pertanggungjawaban pidana dapat dibebankan baik kepada pelaku perorangan maupun korporasi apabila terbukti memenuhi unsur perbuatan melawan hukum, kesalahan, dan pembuktian yang sah berdasarkan ketentuan hukum yang berlaku. Kebaruan penelitian ini terletak pada analisis integratif antara UU PDP dan UU ITE dalam menilai konstruksi pertanggungjawaban pidana terhadap penyalahgunaan data pribadi sebagai bagian dari kejahatan siber.

Meskipun demikian, efektivitas penegakan hukum masih menghadapi berbagai hambatan, antara lain potensi tumpang tindih penerapan norma antara UU PDP dan UU ITE, keterbatasan kemampuan teknis dalam pembuktian elektronik, serta rendahnya kesadaran masyarakat terhadap pentingnya perlindungan data pribadi. Penelitian ini juga masih terbatas pada pendekatan yuridis normatif sehingga belum mengkaji secara empiris praktik penegakan hukum yang terjadi di lapangan.

Oleh karena itu, penelitian selanjutnya disarankan untuk mengkaji implementasi pertanggungjawaban pidana dalam kasus-kasus konkret penyalahgunaan data pribadi melalui pendekatan empiris maupun studi kasus, sehingga dapat memberikan gambaran yang lebih komprehensif mengenai efektivitas penegakan hukum pelindungan data pribadi di Indonesia.

REFERENSI

Dewantoro, Dwi. 2024. "Autentikasi Alat Bukti Elektronik dalam Memperlancar Pembuktian di Persidangan pada Era Disrupsi." Jurnal Hukum Progresif 12 (2): 135–51. https://doi.org/10.14710/jhp.12.2.135-151.

Digital, JDIH Kementerian Komunikasi dan. 2024. "Pencurian Data Pribadi."

Digital, Kementerian Komunikasi dan. 2024. "Menkominfo: Tidak Ada Toleransi untuk Pencurian Data Pribadi."

———. 2025. "Kemkomdigi Periksa Aspek Kepatuhan Hukum PSE World Coin dan World ID."

———. 2026. "Waspada Smishing: Ancaman Penipuan Lewat SMS yang Perlu Diwaspadai."

Fauzy, Eko, dan Nanda Ayu Rizky Shandy. 2023. "Hak atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." Lex Renaissance 7 (3): 445–61. https://doi.org/10.20885/JLR.vol7.iss3.art1.

Firdaus, Fajar Hidayat. 2024. "Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan." Masalah-Masalah Hukum 53 (2): 135–44. https://doi.org/10.14710/mmh.53.2.2024.135-144.

Fitriati, Fitria, Ika Faniyah, dan Nur Rahmad. 2022. "Hambatan Teknis Penyidikan Tindak Pidana Manipulasi Informasi Elektronik pada Polda Sumatera Barat." Masalah-Masalah Hukum 51 (4). https://doi.org/10.14710/mmh.51.4.2022.390-400.

Indonesia, Asosiasi Penyelenggara Jasa Internet. 2024. "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang."

Indonesia, Mahkamah Agung Republik. 2016. Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi. Mahkamah Agung RI.

Indonesia, Pusat Informasi Kriminal Nasional Kepolisian Negara Republik. 2025. "Kasus Kejahatan Manipulasi Data secara ITE Meningkat."

Indonesia, Republik. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Sekretariat Negara.

———. 2024. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sekretariat Negara.

Informatika, Direktorat Jenderal Penyelenggaraan Pos dan. 2024. "Waspada terhadap Tindak Kejahatan SIM Swap."

Informatika, Kementerian Komunikasi dan. 2023. "Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia."

Keuangan, Otoritas Jasa. 2023. "OJK Minta Bank Blokir 85 Rekening Pinjol Ilegal."

Nababan, Dedi Murni Budi, Sabar Lasmadi, dan Erwin. 2023. "Pertanggungjawaban Pidana terhadap Penyalahgunaan Data Pribadi pada Tindak Pidana Dunia Maya." PAMPAS: Journal of Criminal Law 4 (2): 232–51.

Sabadina, Siti. 2022. "Politik Hukum Pidana terhadap Kejahatan Teknologi Informasi Kebocoran Data Pribadi oleh Korporasi Berbasis Online." Jurnal Pengembangan Hukum Indonesia.

Sinaga, Elfrida Maria Christina, dan Melisa Citra Putri. 2020. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0." Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional 9 (2): 237–56. https://doi.org/10.33331/rechtsvinding.v9i2.428.

Wantania, Maria. 2025. "Perkembangan Perlindungan Hukum terhadap Keamanan Data Pribadi di Era Digital." Jurnal Hukum dan Pembangunan.

Widayanti, Tri Fajar, Ahmad Dwi Rohman, Ahmad Nur Zaki Haris, Eko Muhammad Djafar, dan Muhammad Zainul Hakim. 2025. "Enhancing Cybersecurity and Legal Integration: Reforming Indonesia's Cyber Law to Foster Sustainable Growth in the Digital Economy." Diponegoro Law Review 10 (1): 105–19. https://doi.org/10.14710/dilrev.10.1.2025.105-119.