Verdict: Journal of Law Science
E-ISSN: 2985-3680
Journal Homepage:
https://www.ojs.wahanapublikasi.com/index.php/vjlaws

Implikasi Hukum dan Pertanggungjawaban Pidana dalam Kasus Kebocoran Data Pribadi

Natalina Prisilla Purba[1], Suhaila Zulkifli[2*],Tajuddin Noor[3]

[1,2] PUI PT Business Law, Fakultas Hukum, Universitas Prima Indonesia, Medan, Sumatera Utara, 20112, Indonesia
[3] Fakultas Hukum, Universitas Islam Sumatera Utara, Medan 20217, Indonesia

Legal Implications and Criminal Liability in Cases of Personal Data Breaches

ARTICLE INFO

Received:
11 April 2026

Accepted:
29 June 2026

Published:
05 August 2026

Keywords:

Criminal Liability, Data Breach, Law Enforcement, Personal Data Protection

ABSTRACT

Personal data leakage has become a serious legal issue in the digital era due to its increasing frequency and adverse impacts, including financial losses, identity theft, and privacy violations. Between 2019 and mid-2024, Indonesia experienced numerous personal data breach incidents, indicating that enforcement of personal data protection laws remains ineffective despite the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This study analyzes the legal framework governing criminal liability for perpetrators of personal data leakage and examines challenges in enforcing these regulations in Indonesia. This research employs normative legal methods using statutory, conceptual, and case approaches. Legal materials include primary sources, particularly the PDP Law, Electronic Information and Transactions Law (ITE Law), Criminal Code (KUHP), Civil Code (KUHPerdata), and related regulations, supported by secondary legal materials from books and scholarly literature. The findings indicate that Indonesia has established a comprehensive legal framework through the PDP Law as a *lex specialis*, supported by the ITE Law, Article 322 of the Criminal Code, and Article 1365 of the Civil Code. However, enforcement faces obstacles, including limited digital forensic capacity, insufficient law enforcement expertise, low public legal awareness, the absence of an effective independent data protection authority, and the complexity of cross-border cybercrime. This study recommends strengthening the independent data protection supervisory authority, digital forensic capacity, cybersecurity training, and public legal awareness to improve personal data protection and criminal law enforcement in Indonesia.

Copyright © 2026 The Author(s)
Published by CV Wahana Publikasi.
This article is an open access article under the CC BY-NC 4.0 License

* Corresponding Author: suhailazulkifli@unprimdn.ac.id
DOI: https://doi.org/10.59011/vjlaws.5.3.2026.684-693

1. Pendahuluan

Perkembangan terkonologi dan globalisasi yang sangat pesat membuat dampak ganda menjadi masyarakat yang modern. Di satu sisi, teknologi yang sering kita gunakan yaitu handpone mempermudah akses untuk bertukar informasi, tidak hanya di indonesia namun seluruh dunia dapat merasakan kemudahannya, kemajuan teknologi seperti internet yang terus menerus berkembang dapat juga membantu mempermuda aktivitas banyak orang. Tetapi di sisi lain memunculkan ancaman yang sangat serius terhadap keamaan data pribadi. Kini kasus pembocoran data pribadi menjadi isu yang kompleks karna tidak hanya merugikan pada finansial tetapi juga pada pencurian indetitas dan pelanggaran privasi yang berdampak langsung pada harkat dan martabat seseorang.[1]

Persoalan kebocoran data pribadi kini bukan lagi peristiwa yang terjadi sesekali, melainkan sudah menjadi masalah yang terus muncul. Di Indonesia, sejak tahun 2019 sampai pada pertengahan 2024, Kementrian Komunikasi dan Informatika (Kominfo) telah menangani tidak kurang dari 111 kasus kebocoran data pribadi, dan dengan setiap kasus berpotensi melibatkan ratusan juta data penduduk. Seperti kasus kebocoran data tokopedia pada tahun 2020 yang sangat berdampak pada data nama, alamat email, nomor telepon dan alamat pengirim penggunanya, serta pada tahun 2022 aksi hacker Bjorka yang membocorkan data pejabat pemerintah ke ruang publik digital, menjadi bukti nyata bahwa rentannya sistem perlindungan data pribadi di Indonesia.[2]

Secara yuridis, tindakan pembocoran data pribadi sesungguhnya telah memiliki landasan hukum yang dapat dijadikan dasar penuntutan. Kitab Undang-Undang Hukum Pidana (KUHP) serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah memuat sejumlah ketentuan yang berkaitan.[3] Akan tetapi, kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai babak baru dalam upaya perlindungan hukum yang lebih komprehensif. UU PDP secara tegas mengatur sanksi pidana dalam Pasal 67 hingga Pasal 71 bagi siapa pun yang dengan sengaja dan tanpa hak melakukan pembocoran data pribadi Meskipun demikian, adanya regulasi tersebut belum menjamin efektivitas penegakan hukum yang ada di lapangan. Pertanggungjawaban pidana dalam kasus pembocoran Perlindungan data pribadi masih dihadapkan pada berbagai kendala, mulai dari sulitnya pembuktian digital hingga terbatasnya kemampuan aparat penegak hukum dalam menangani kejahatan siber, hingga kurangnya kesadaran hukum masyarakat.[4] Hal ini diperkuat oleh pandangan Soerjono Soekanto yang menegaskan bahwa efektivitas tidak hanya bergantung pada substansi regulasi, melainkan struktur, budaya hukum, serta sarana dan prasarana yang tersedia.[5]

Kebocoran data pribadi merupakan permasalahan yang memerlukan perhatian serius serta penanganan yang komprehensif. Seiring dengan pesatnya perkembangan internet dan teknologi informasi, risiko terjadinya kejahatan siber, termasuk pembocoran data pribadi, terus meningkat.[6] Kondisi tersebut menuntut adanya kerangka hukum yang mampu

[1] Pranoto et al., "Pertanggungjawaban Pidana Pembocoran Data Pribadi."
[2] Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022."
[3] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 30 ayat (1) dan Pasal 32 ayat (1).
[4] Suharyanti and Sutrisni, "Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi Masyarakat."
[5] Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum.*
[6] Cross and Holt, "Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims."; Pool et al., "A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review."

memberikan perlindungan yang efektif terhadap hak privasi masyarakat sekaligus menjamin kepastian hukum dalam penegakannya. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis dua aspek utama, yaitu: (1) bagaimana regulasi yang berlaku mengatur pertanggungjawaban pidana terhadap pelaku pembocoran data pribadi; dan (2) apa saja tantangan yang dihadapi dalam penegakan hukum terhadap tindak pidana pembocoran data pribadi di Indonesia.

1.1 Konsep dan Teori

Penelitian ini didasarkan pada tiga landasan teoretis yang saling melengkapi dalam menganalisis pertanggungjawaban pidana atas kebocoran data pribadi di Indonesia. Pertama, teori perlindungan hukum yang dikemukakan oleh Satjipto Rahardjo menempatkan hukum sebagai instrumen untuk memberikan pengayoman, kepastian, dan keadilan bagi masyarakat, sehingga negara berkewajiban menjamin perlindungan terhadap hak-hak warga negara, termasuk hak atas data pribadi sebagai bagian dari hak asasi manusia.[7] Kedua, teori pertanggungjawaban pidana yang berlandaskan asas *geen straf zonder schuld* (tiada pidana tanpa kesalahan) menegaskan bahwa seseorang hanya dapat dimintai pertanggungjawaban pidana apabila terbukti melakukan perbuatan yang memenuhi unsur tindak pidana dan disertai adanya kesalahan, baik berupa kesengajaan (*dolus*) maupun kealpaan (*culpa*). Teori ini menjadi dasar dalam menilai pertanggungjawaban hukum terhadap pelaku kebocoran data pribadi.[8] Ketiga, teori hak privasi yang dikemukakan oleh Alan F. Westin memandang privasi sebagai hak individu untuk menentukan kapan, bagaimana, dan sejauh mana informasi mengenai dirinya dapat diakses atau disebarluaskan kepada pihak lain.[9] Dalam konteks perlindungan data pribadi, teori ini menegaskan bahwa setiap individu memiliki kendali atas informasi pribadinya sehingga setiap bentuk akses, penggunaan, atau pengungkapan tanpa persetujuan merupakan pelanggaran terhadap hak privasi. Ketiga teori tersebut digunakan secara terpadu sebagai kerangka analisis untuk mengkaji pengaturan pertanggungjawaban pidana dan tantangan penegakan hukum terhadap kebocoran data pribadi, sehingga dapat dirumuskan upaya penguatan kerangka hukum pidana yang lebih efektif dalam memberikan perlindungan hukum bagi masyarakat.

2. Metode dan Bahan Hukum

Metode penelitian yang digunakan dalam penulisan ini adalah penelitian yuridis normatif, yaitu penelitian yang berfokus pada pengkajian dan analisis terhadap norma-norma hukum tertulis, baik yang terdapat dalam peraturan perundang-undangan, doktrin, maupun asas-asas hukum yang berkaitan dengan pertanggungjawaban pidana dalam kasus kebocoran data pribadi. Penelitian ini sepenuhnya berbasis kajian pustaka dan tidak menggunakan metode empiris seperti wawancara maupun observasi lapangan. Pendekatan masalah yang digunakan dalam penelitian ini terdiri atas tiga jenis, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai regulasi yang berkaitan dengan perlindungan data pribadi dan pertanggungjawaban pidana. Sementara itu, pendekatan konseptual ditempuh melalui kajian terhadap doktrin serta teori-teori hukum yang relevan. Adapun pendekatan kasus

[7] Rahardjo, *Ilmu Hukum*.
[8] Moeljatno, *Asas-Asas Hukum Pidana*.
[9] Westin, *Privacy and Freedom*.

digunakan untuk memahami penerapan norma hukum dalam praktik peradilan.[10]

Sumber bahan hukum dalam penelitian ini dikelompokkan ke dalam dua kategori utama. Pertama, bahan hukum primer, yaitu peraturan perundang-undangan yang mengikat, meliputi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.[11] Kedua, bahan hukum sekunder, yaitu bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, meliputi buku-buku hukum, jurnal ilmiah, artikel, dan hasil penelitian terdahulu yang relevan dengan topik penelitian[12]

Teknik pengumpulan dilakukan melalui studi dokumentasi, yakni menelaah, mengidentifikasi, mengklasifikasi bahan tertulis yang relevan dengan permasalahan yang dikaji. Seluruh bahan hukum yang telah dikumpulkan kemudian dianalisis dengan menggunakan metode analisis normatif-deskriptif. Analisis ini dilakukan dengan cara menguraikan, membandingkan, dan menafsirkan norma-norma hukum yang berlaku, kemudian menghubungkannya dengan teori hukum yang dijadikan sebagai alat analisis, sehingga diperoleh gambaran yang utuh mengenai efektivitas pertanggungjawaban pidana dalam penanggulangan kebocoran data pribadi di Indonesia.[13]

3. Hasil dan Pembahasan

3.1 Regulasi yang Mengatur Pertanggungjawaban Pidana bagi Pelaku Pembocoran Data Pribadi

a. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Ditetapkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan peristiwa penting dalam sejarah perlindungan hukum data pribadi di Indonesia. Seperti yang dikatakan Satjipto Rahardjo, undang-undang ini melindungi masyarakat guna memastikan bahwa keadilan dan hukum ditegakkan dengan jelas. Dengan konteks ini, UU PDP hadir sebagai instrumen negara untuk melindungi hak subjek data dari segala bentuk penyalahgunaan, pengungkapan, maupun distribusi data tanpak hak.UU PDP juga memuat pengaturan yang cukup rinci mengenai pertanggungjawaban pidana dalam Pasal 67 sampai dengan Pasal 71. Pada Pasal 67 ayat (1), misalnya, ditegaskan bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi milik orang lain dengan maksud menguntungkan diri sendiri atau pihak lain, sehingga dapat merugikan subjek data, dapat dipidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5.000.000.000,00. Sementara itu, Pasal 67 ayat (2) mengatur sanksi pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4.000.000.000,00 bagi siapa pun yang mengungkapkan data pribadi orang lain tanpa hak.Sementara itu, di Pasal 68 hingga Pasal 71 mengatur bentuk-bentuk pelanggaran lain beserta ancaman pidananya, termasuk penggunaan data pribadi yang tidak sesuai tujuan perolehan dan pemrosesan data pribadi anak tanpa

[10] Marzuki, *Penelitian Hukum.*

[11] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Peraturan Pemerintah Nomor 71 Tahun 2019; Peraturan Menteri Kominfo Nomor 20 Tahun 2016.

[12] Mirna, Judhariksawan, and Maskum, "Analisis Pengaturan Keamanan Data Pribadi di Indonesia."

[13] Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum.*

persetujuan orang tua.[14]

Dalam UU PDP, implikasi pidana menunjukkan berlakunya asas *geen straf zonder schuld*, yaitu tidak ada pidana tanpa adanya kesalahan. Artinya, seseorang hanya dapat dimintai pertanggungjawaban pidana apabila telah terbukti adanya perbuatan pidana, unsur kesalahan, serta kemampuan untuk bertanggung jawab.[15] Dengan demikian, pelaku pembocoran data pribadi yang terbukti salah dan bertindak dengan sengaja dan tanpa hak dapat dijatuhi sanksi pidana sesuai ketentuan UU PDP.

b. Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pengaturan mengenai perlindungan data pribadi di Indonesia masih bertumpu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (UU ITE). UU ITE menjadi dasar hukum utama untuk menindak pelaku kejahatan siber yang berkaitan dengan akses dan penyalahgunaan data pribadi. Pasal 30 ayat (1) UU ITE melarang setiap orang mengakses komputer dan/atau sistem elektronik milik orang lain tanpa hak atau melawan hukum. Selanjutnya, Pasal 32 ayat (1) mengatur larangan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, memindahtangankan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik orang lain tanpa hak.[16] Pelanggaran terhadap ketentuan tersebut dikenai sanksi pidana sebagaimana diatur dalam ketentuan pidana UU ITE, berupa pidana penjara paling lama 6 - 8 tahun serta denda hingga Rp800.000.000,00 bergantung pada jenis dan unsur tindak pidana yang dilakukan.

Meskipun UU ITE telah memberikan dasar hukum bagi penegakan hukum terhadap tindak pidana yang berkaitan dengan data elektronik, pengaturannya masih bersifat umum dan belum secara khusus mengatur perlindungan data pribadi sebagai objek hukum yang berdiri sendiri.[17] Akibatnya, perlindungan terhadap hak subjek data belum terlaksana secara optimal. Oleh karena itu, kehadiran UU PDP menjadi sangat penting sebagai *lex specialis* yang mengatur perlindungan data pribadi secara lebih komprehensif, mulai dari pemrosesan data, hak-hak subjek data, kewajiban pengendali dan prosesor data, hingga pengenaan sanksi administratif maupun pidana.[18] Dengan demikian, UU PDP melengkapi sekaligus memperkuat kerangka hukum nasional dalam memberikan kepastian hukum dan perlindungan yang lebih efektif terhadap data pribadi di Indonesia.

c. Kitab Undang-Undang Hukum Pidana dan KUH Perdata

Selain dari kedua hukum itu, Kitab Undand-Undang Hukum Pidana (KUHP) juga bisa dijadikan sebagai dasar hukum dalam kasus Kebocoran Data Pribadi. Tepat pada pasal 322

[14] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 67–71.

[15] Moeljatno, *Asas-Asas Hukum Pidana*.

[16] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 30 ayat (1) dan Pasal 32 ayat (1).

[17] Asmadi, Mansar, and Eddy, "Actualization of Criminal Liability for Personal Data Protection in the Use of Financial Technology: A Comparative Study of Law Number 11 of 2008 Concerning Information and Electronic Transactions and Law Number 27 of 2022 Concerning Protection of Personal Data"; Putra, Pratama, and Susilo, "Perlindungan Konsumen atas Data Pribadi dalam Transaksi E-Commerce Pasca Berlakunya Undang-Undang Nomor 1 Tahun 2024"; Rahmadani and Zela, "The Existence of Personal Data Protection in the Digital Era Based on Indonesia's Electronic Information and Transactions Law."

[18] Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022."

ayat 1 KUHP menegaskan adanya sanksi pidana bagi orang yang membocorkan rahasia yang seharusnya dijaga karena jabatan atau pekerjaannya. Dari sisi lain, dalam hukum perdata, Pasal 1365 KUH Perdata memberikan landasan bagi korban menuntut ganti rugi atas kerugian yang ditimbulkan akibat perbuatan melawan hukum. Dengan demikian, korban pembocoran data pribadi dapat pula menuntut ganti rugi secara perdata di samping penuntutan pidana.[19]

Dengan demikian, eksistensi kerangka regulasi mengenai pertanggungjawaban pidana dalam insiden kebocoran data pribadi di Indonesia saat ini telah terakomodasi melalui skema norma yang berlapis. Hal tersebut terefleksi dari kedudukan UU PDP sebagai lex specialis yang bersinergi seperti UU ITE, KUHP, KUH Perdata. Sejalan dengan doktrin Jimly Asshiddiqie, penguatan instrumen hukum ini merupakan manifestasi dari kewajiban konstitusional negara dalam menjamin perlindungan terhadap hak atas privasi setiap warga negara.

3.2 Tantangan dalam Penegakan Hukum Terkait Kasus Kebocoran Data Pribadi di Indonesia

a. Keterbatasan Kapasitas Aparat Penegak Hukum

Merujuk pada teori Soejono Soekanto, bahwa kunci dari keberhasilan penegakan hukum sangat bergantung pada aspek struktural, yakni kapasitas para aparat penegak hukum, bukan hanya dilihat pada kelengkapan regulasi.[20] Di sektor kejahatan siber dan kebocoran data pribadi, tantangan ini adalah kendala yang serius karna belum meratanya penguasaan teknis aparat dan terlihat dari minimnya literasi digital penegak hukum mengenai mekanisme dan sistem informasi dan bukti digital. Kesenjangan ini berpotensi mengakibatkan resiko kasus kebocoran data pribadi terhambat karna aparat hukum belum sepenuhnya siap menghadapi aspek teknis kejahatan tersebut dari tahap penyelidikan hingga tahap peradilan.[21]

b. Kesulitan Pembuktian Digital

Karakteristik dalam pembuktian pada kasus kebocoran data pribadi berbeda signifikan dengan tindak pidana umum. Sifat alat buktinya yang elektronik dan rentan dimanipulasi, di hapus atau di sembunyikan. Hal ini memerlukan kopetensi teknis yang mendalam dalam menjaga integritas bukti. Sejalan dengan teori Lawrence M. Friedman, keberhasilan sangat berpengaruh oleh budaya serta adaptabilitas sistem hukum terhadap dinamika sosial. Dalam konteks indonesia, sayangnya, efektifitas ini masih terhambat oleh keterbatasan infastruktur digital forensik karna masih menjadi kendala fundamental dalam proses penegakan hukum tersebut di tanah air.[22]

c. Kurangnya Kesadaran Hukum Masyarakat

Selain aspek teknis, tantangan ini tidak kalah penting karna rendahnya tingkat kesadaran hukum dari subjek maupun pengendali data menjadi kendala yang krusial. Minimnya pengetahuan masyarakat mengenai hak-hak yang dijamin oleh UU PDP mengakibatkan banyak pelanggaran mengenai insiden kebocoran berakhir tanpa pelaporan

[19] Kitab Undang-Undang Hukum Perdata, Pasal 1356

[20] Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum.*

[21] Wiarti, "Legality of Electronic Evidence in Cyber Crime Cases"; Prihatini, Sihombing, and Nuraeni, "Optimizing Digital Forensics for Effective Cybercrime Law Enforcement in Indonesia."

[22] Friedman, *The Legal System: A Social Science Perspective*.

ke otoritas terkait. Di sisi lain, para pengelola data sering kali belum menginternalisasi kewajiban hukum mereka dalam memproteksi data pribadi secara maksimal.[23] Akibatnya, banyak kasus kebocoran yang akhiirnya hilang begitu saja tanpa adanya tindak lanjut yuridis.

d. Belum Terbentuknya Lembaga Pengawas Perlindungan Data Pribadi

Meski UU PDP telah memberikan mandat untuk mendirikan Badan Pengawas Perlindungan Data Pribadi, tapi hingga saat ini eksistensi lembaga tersebut masih belum terealisasikan secara fungsional. Belum adanya otoritas pengawas yang independen menciptakan kekosongan hukum yang signifikan dalam sistem proteksi data nasional. Hal ini berakibat mekanisme penegakan hukum mulai dari penerimaan laporan masyarakat hingga pemberian sanksi administratif terhadap pelanggar menjadi tidak berjalan secara optimal.[24]

e. Dimensi Lintas Yurisdiksi

Tantangan penegakan hukum semakin kompleks ketika pelaku pembocoran data berada di luar yurisdiksi Indonesia atau menggunakan server mancanegara. Hal ini sulit dijangkau karena sistem hukum kita masih membutuhkan dukungan kerja sama internasional yang lebih kuat untuk menindak pelaku lintas batas.[25] Hanifan Nifari mencatat bahwa kekosongan hukum dalam aspek lintas batas yurisdiksi ini menjadi salah satu faktor yang masih kurang efektif.[26] Melihat berbagai tantangan tersebut, terlihat bahwa persoalan penegakan hukum dalam kasus ini bersifat multidimensional. Penegakan hukum terhadap kebocoran data dinilai belum efektif karena sanksi yang masih terbatas serta mekanisme pengawasan yang lemah. Karena itu, perlu adanya penguatan aturan teknis, peningkatan kemampuan aparat penegak hukum, serta pembentukan lembaga pengawas yang independen agar perlindungan hukum dapat berjalan lebih efektif.[27]

4. Kesimpulan

Berdasarkan hasil analisis dan pembahasan, penelitian ini menghasilkan dua kesimpulan utama. Pertama, Indonesia pada dasarnya telah memiliki kerangka regulasi yang berlapis dalam mengatur pertanggungjawaban pidana terhadap pelaku pembocoran data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan regulasi khusus (lex specialis) yang mengatur perlindungan data pribadi secara komprehensif, termasuk ketentuan mengenai sanksi pidana sebagaimana diatur dalam Pasal 67 sampai dengan Pasal 71, dengan ancaman pidana penjara paling lama 5 (lima) tahun dan pidana denda paling banyak Rp5.000.000.000,00. Pengaturan dalam UU PDP bersinergi dengan instrumen hukum lainnya, yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Pasal 322 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP), serta Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) yang memberikan dasar hukum bagi tuntutan ganti kerugian secara perdata. Keseluruhan pengaturan tersebut mencerminkan penerapan asas geen straf zonder schuld dalam pertanggungjawaban pidana sekaligus merefleksikan kewajiban konstitusional negara

[23] Suharyanti and Sutrisni, "Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi Masyarakat."
[24] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Penjelasan Umum.
[25] Muladi and Priyatno, *Pertanggungjawaban Pidana Korporasi*.
[26] Niffari, "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain)."
[27] Mirna, Judhariksawan, and Maskum, "Analisis Pengaturan Keamanan Data Pribadi di Indonesia."

untuk melindungi hak privasi warga negara sebagaimana dikemukakan oleh Jimly Asshiddiqie.

Kedua, meskipun kerangka regulasi yang mengatur perlindungan data pribadi telah relatif memadai, implementasi penegakan hukumnya masih menghadapi berbagai tantangan yang kompleks. Tantangan tersebut tidak hanya berkaitan dengan keterbatasan kapasitas dan literasi digital aparat penegak hukum, tetapi juga mencakup kesulitan pembuktian dalam perkara kejahatan siber akibat belum optimalnya infrastruktur dan kemampuan forensik digital. Selain itu, tingkat kesadaran hukum masyarakat, baik sebagai subjek data maupun pengendali data pribadi, masih relatif rendah. Kondisi tersebut semakin diperberat oleh belum berfungsinya secara optimal lembaga pengawas perlindungan data pribadi sebagaimana diamanatkan oleh UU PDP, serta kompleksitas penanganan perkara yang melibatkan pelaku lintas yurisdiksi. Temuan ini sejalan dengan teori efektivitas hukum yang dikemukakan oleh Soerjono Soekanto, yang menyatakan bahwa keberhasilan penegakan hukum tidak hanya ditentukan oleh kualitas substansi peraturan perundang-undangan, tetapi juga dipengaruhi oleh efektivitas struktur penegak hukum, sarana dan prasarana pendukung, serta budaya hukum masyarakat.

Berdasarkan kedua kesimpulan tersebut, penelitian ini merekomendasikan tiga langkah strategis. Pertama, pemerintah perlu segera membentuk Badan Pengawas Perlindungan Data Pribadi yang independen dan memiliki kewenangan yang efektif sebagaimana diamanatkan dalam UU PDP. Kedua, kapasitas aparat penegak hukum perlu ditingkatkan melalui pendidikan dan pelatihan yang berkelanjutan di bidang forensik digital, keamanan siber, dan penanganan tindak pidana berbasis teknologi informasi. Ketiga, perlu dilakukan penguatan edukasi dan literasi hukum kepada masyarakat mengenai hak dan kewajiban dalam perlindungan data pribadi berdasarkan UU PDP, sehingga masyarakat memiliki kesadaran yang lebih tinggi untuk menjaga data pribadinya serta berpartisipasi aktif dalam melaporkan setiap dugaan pelanggaran atau kebocoran data pribadi.

Funding
This research received no funding from any public, commercial, or not-for-profit funding agency.

Conflict of Interest
The authors declare that there are no conflicts of interest regarding the publication of this article.

Author Contributions
All authors made substantial contributions to the conception and design of the study, data analysis and interpretation, and the drafting and revision of the manuscript. All authors have read, approved, and accepted responsibility for the final version of the manuscript.

Use of Artificial Intelligence (AI)
The authors declare that no artificial intelligence (AI) tools or technologies were used in the research, writing, or preparation of this manuscript.

Referensi
Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana, 2025.

Mirna, Mirnayanti, Judhariksawan, and Maskum. "Analisis Pengaturan Keamanan Data Pribadi di Indonesia." *Jurnal Ilmiah Living Law* 15, no. 1 (2023): 16–30. https://doi.org/10.30997/jill.v15i1.4726.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2018.

Muladi, and Dwidja Priyatno. *Pertanggungjawaban Pidana Korporasi*. Edisi ke-3. Jakarta: Kencana, 2015.

Niffari, Hanifan. "Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain)." *Jurnal Yuridis* 7, no. 1 (2020): 105–119. https://doi.org/10.35586/jyur.v7i1.1846.

Kitab Undang-Undang Hukum Perdata.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Pranoto, Tri Wahyu, Markoni, I Made Kanthika, and Joko Widarto. "Pertanggungjawaban Pidana Pembocoran Data Pribadi." *Jurnal Cinta Nusantara (JCN)* 2, no. 2 (2024): 30–45. https://doi.org/10.63754/jcn.v2i02.43.

Rahardjo, Satjipto. *Ilmu Hukum*. Cet. IX. Bandung: PT Citra Aditya Bakti, 2021.

Saly, Jeane Neltje, Halena Artamevia, Kendelif Kheista, Barnabas Juni Saputra Gulo, Evellyn Abigael Rhemrev, and Michelle Christie. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022." *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145–153. https://doi.org/10.24912/jssh.v1i3.28615.

Soekanto, Soerjono. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Cet. 16. Depok: PT RajaGrafindo Persada, 2019.

Suharyanti, Ni Putu Noni, and Ni Komang Sutrisni. "Urgensi Perlindungan Data Pribadi dalam Menjamin Hak Privasi Masyarakat." In *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020: Urgensi dan Implikasi RUU Perlindungan Keamanan Kerahasiaan Data Diri Berbasis Digitalisasi*, 119–134. Denpasar: Fakultas Hukum Universitas Mahasaraswati Denpasar, 2021.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Westin, Alan F. *Privacy and Freedom*. New ed. New York: Ig Publishing, 2015.

Cross, Cassandra, and Thomas J. Holt. "Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims." *Journal of Crime and Justice* (2025). https://doi.org/10.1080/0735648X.2025.2535007.

Asmadi, Erwin, Adi Mansar, and Triono Eddy. "Actualization of Criminal Liability for Personal Data Protection in the Use of Financial Technology: A Comparative Study of Law Number 11 of 2008 Concerning Information and Electronic Transactions and Law Number 27 of 2022 Concerning Protection of Personal Data." *De Lega Lata: Jurnal Ilmu Hukum* 8, no. 2 (2023): 292–300. https://doi.org/10.30596/dll.v8i2.15252.

Putra, Fajri Jandika, Annisa Arif Pratama, and Fadilah Akbar Susilo. "Perlindungan Konsumen atas Data Pribadi dalam Transaksi E-Commerce Pasca Berlakunya Undang-Undang Nomor 1 Tahun 2024." *Jurnal Jurisprudentia* 7, no. 2 (2024).

Rahmadani, Gema, and Yovani Zela. "The Existence of Personal Data Protection in the Digital Era Based on Indonesia's Electronic Information and Transactions Law." *AT-TAFAHUM: Journal of Law* 3, no. 2 (2019): 117–124. https://doi.org/10.47006/attafahum.v3i2.29107.

Wiarti, July. "Legality of Electronic Evidence in Cyber Crime Cases." *Ahmad Dahlan Indonesian Law Journal* 1, no. 2 (2023/2024): 11–19. https://doi.org/10.12928/adil.v1i1.572.

Prihatini, Lilik, Lasmin Alfies Sihombing, and Yeni Nuraeni. "Optimizing Digital Forensics for Effective Cybercrime Law Enforcement in Indonesia." *Law Development Journal* 8, no. 2 (2026): 443–457. https://doi.org/10.30659/ldj.8.2.443-457.