LEXARA
Journal of Law and Legal Studies
Lexara: Journal of Law and Legal Studies
Vol. 1 No. 3 2026
E-ISSN: 3164-5763
punggawajournal.com/lexara

Pertanggungjawaban Pidana Pelaku Akses Ilegal terhadap Data Pribadi Melalui Serangan *Malware* Menurut Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Pelindungan Data Pribadi

Cicilia Winda Prastia Ningtias[1], Muchamad Iksan[2]
[1,2] Fakultas Ilmu Hukum & Politik, Universitas Muhammadiyah Surakarta, Indonesia
Korespondensi: cwp53106@student.ums.ac.id

Informasi Artikel
Riwayat artikel:
Received Oct 1th, 2026
Revised Nov 9th, 2026
Accepted Nov 17th, 2026

Keyword:
Malware; Pertanggungjawaban pidana; Data pribadi; UU ITE; UU PDP.

ABSTRAK
Kemajuan teknologi informasi diikuti oleh meningkatnya kejahatan siber, salah satunya serangan *malware* terhadap data pribadi berupa *ransomware*, *spyware*, *trojan horse*, dan *keylogger*. Pelaku bertindak secara tersembunyi, memalsukan identitas, memanfaatkan sistem otomatis, serta kerap berada di luar negeri, sehingga pembuktian unsur kesengajaan dan sifat melawan hukum di persidangan menjadi sulit. Di sisi lain, hukum positif Indonesia belum mengatur *malware* secara eksplisit dan masih terdapat ketidaksinkronan norma antara Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dengan Undang-Undang Pelindungan Data Pribadi (UU PDP). Penelitian ini bertujuan untuk menganalisis kualifikasi serangan *malware* terhadap data pribadi sebagai tindak pidana menurut UU ITE serta mengkaji mekanisme pertanggungjawaban pidana pelakunya. Metode yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Hasil penelitian menunjukkan bahwa serangan *malware* dapat dikualifikasikan sebagai tindak pidana melalui ketentuan akses ilegal dan perusakan sistem/informasi elektronik dalam UU ITE karena memenuhi unsur kesengajaan, tanpa hak, dan melawan hukum, meskipun belum ada definisi eksplisit mengenai *malware*. Pertanggungjawaban pidana pelaku berlandaskan asas *geen straf zonder schuld*, namun penegakannya terkendala hambatan pembuktian elektronik, yurisdiksi transnasional, dan potensi disparitas pemidanaan akibat konkurensi norma antara UU ITE dan UU PDP. Diperlukan harmonisasi regulasi kedua undang-undang, perumusan norma eksplisit mengenai *malware*, serta penguatan kapasitas digital forensik aparat penegak hukum

© 2026 The Authors. Published by Punggawa Legacy Center. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang ditopang oleh konektivitas internet telah membawa transformasi fundamental dalam berbagai aspek kehidupan masyarakat modern (Budhijanto, 2024). Kemajuan ini menciptakan efisiensi dalam pertukaran data, transaksi ekonomi, maupun layanan publik. Namun, di balik manfaatnya, ruang siber juga menghadirkan kerentanan baru berupa penyalahgunaan teknologi untuk melakukan perbuatan melawan hukum atau kejahatan siber (*cybercrime*)(Yurizal, 2018). Salah satu bentuk ancaman kejahatan siber yang paling destruktif dan terus meningkat eskalasinya di Indonesia adalah serangan perangkat lunak berbahaya (*malicious software* atau *malware*) yang menyasar data pribadi (Nurjanah & Liyus, 2025)

Secara teknis dan yuridis, *malware* merupakan program komputer yang dirancang secara sengaja untuk menyusup, merusak, mengambil alih kendali, atau mencuri informasi dari suatu sistem elektronik tanpa persetujuan pemilik yang sah ((Sangalang & Farina, 2024)(Nurjanah & Liyus, 2025). Dalam

praktiknya, serangan *malware* yang menargetkan data pribadi seperti Nomor Induk Kependudukan (NIK), kredensial perbankan, kata sandi (*password*), hingga data biometrik bermanifestasi dalam beragam varian. Pertama, *ransomware*, yakni *malware* yang mengenkripsi seluruh data korban dan menuntut uang tebusan untuk memulihkan akses, sebagaimana tercermin dalam insiden serangan *LockBit 3.0* terhadap PT Bank Syariah Indonesia Tbk (BSI) pada tahun 2023 ((M. Arief & Darmawan, 2024);(Simorangkir, 2024)). Kedua, *spyware*, yang bekerja secara diam-diam memantau aktivitas perangkat untuk memanen data sensitif. Ketiga, *trojan horse*, yang menyamar sebagai aplikasi resmi—seperti modus pengiriman berkas aplikasi (*Android Package Kit*/APK) undangan pernikahan atau aplikasi layanan publik palsu melalui pesan instan WhatsApp untuk menipu korban agar menginstalnya (D. P. Sari & Pratama, 2023). Keempat, *keylogger*, yang merekam setiap ketikan papan ketik (*keyboard*) korban guna memperoleh kredensial akses secara ilegal.

Modus operandi kejahatan *malware* memiliki karakteristik yang jauh lebih kompleks dibandingkan kejahatan konvensional. Dalam tipologi kejahatan siber modern, serangan *malware* menggabungkan dua dimensi kejahatan secara simultan, yakni komputer sebagai alat bantu kejahatan (*computer as a tool*) sekaligus komputer sebagai sasaran serangan (*computer as a target*) (Sangalang & Farina, 2024). Pelaku menciptakan dan menyebarkan kode berbahaya dari jarak jauh (*remote server*), menyamarkan identitas digital melalui anonimitas jaringan, memanfaatkan otomatisasi bot, serta sering kali beroperasi melintasi batas teritorial negara (*transnational crime*) (Suseno, 2022). Karakteristik tersebut memunculkan problematika yuridis yang serius dalam hukum pidana Indonesia, khususnya terkait pembuktian unsur kesalahan (*mens rea*), sifat melawan hukum (*wederrechtelijkheid*), serta penentuan yurisdiksi penegakan hukum (Pansariadi & Soekorini, 2023).

Secara normatif, Indonesia telah memiliki instrumen hukum khusus (*lex specialis*) untuk menanggulangi kejahatan siber melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (selanjutnya disebut UU ITE). Selain itu, perlindungan hukum atas privasi warga negara telah diperkuat melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) (Rosadi, 2023). Kendati demikian, baik UU ITE maupun UU PDP belum merumuskan definisi yuridis dan klasifikasi eksplisit mengenai tindak pidana berbasis *malware*. Kekaburan norma ini diperumit oleh potensi tumpang tindih (*overlapping*) dan ketidaksinkronan ancaman sanksi pidana antara ketentuan akses ilegal dalam UU ITE dan perolehan data pribadi secara melawan hukum dalam UU PDP (Djafar, 2023);(Amirulloh, 2025).

Berdasarkan uraian latar belakang tersebut, artikel ini merumuskan dua permasalahan utama: (1) bagaimana kualifikasi yuridis serangan *malware* terhadap data pribadi sebagai tindak pidana menurut ketentuan UU ITE; dan (2) bagaimana konstruksi pertanggungjawaban pidana serta problematika penegakan hukum bagi pelaku serangan *malware* ditinjau dari perspektif UU ITE dan UU PDP. Penelitian ini diharapkan memberikan kontribusi teoretis bagi pengembangan doktrin hukum pidana siber di Indonesia serta menjadi rekomendasi kebijakan bagi pembentuk undang-undang dan aparat penegak hukum dalam mengharmonisasikan regulasi pelindungan data pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (*doctrinal legal research*), yaitu penelitian hukum yang meletakkan hukum sebagai sebuah bangunan sistem norma mengenai asas-asas, kaidah peraturan perundang-undangan, serta doktrin hukum yang relevan (Marzuki, 2017). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dengan menelaah secara komprehensif ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP), UU Nomor 11 Tahun 2008 jo. UU Nomor 1 Tahun 2024 tentang ITE, dan UU Nomor 27 Tahun 2022 tentang PDP, serta pendekatan konseptual (*conceptual approach*) dengan mengkaji doktrin pertanggungjawaban pidana, tindak pidana siber, dan konsep pelindungan data pribadi. Bahan hukum primer dan sekunder dianalisis secara deskriptif-analitis menggunakan penafsiran sistematis dan ekstensif guna menjawab isu hukum yang dirumuskan.

HASIL DAN PEMBAHASAN

1. Kualifikasi Yuridis Serangan *Malware* terhadap Data Pribadi dalam UU ITE

Dalam perspektif hukum pidana Indonesia, suatu perbuatan hanya dapat dipidana apabila telah dirumuskan terlebih dahulu dalam peraturan perundang-undangan sesuai asas legalitas (*nullum delictum nulla poena sine praevia lege poenali*) sebagaimana termaktub dalam Pasal 1 ayat (1) KUHP (Hiariej, 2016). Meskipun UU ITE tidak mencantumkan istilah "*malware*" secara tekstual, pembentuk undang-undang menggunakan perumusan delik yang bersifat netral teknologi (*technology-neutral*), sehingga unsur-unsur perbuatan (*actus reus*) dari penyebaran dan pengoperasian *malware* dapat dijangkau melalui penafsiran ekstensif terhadap pasal-pasal tindak pidana siber di dalamnya (Yurizal, 2018).

Secara umum, delik siber dalam UU ITE mensyaratkan tiga elemen objektif dan subjektif utama: (a) adanya unsur kesalahan berupa *"dengan sengaja"*; (b) sifat melawan hukum yang dirumuskan melalui frasa *"tanpa hak atau melawan hukum"*; serta (c) objek perbuatan berupa *"Sistem Elektronik"*, *"Informasi Elektronik"*, dan/atau *"Dokumen Elektronik"*. Dalam konteks serangan *malware* terhadap data pribadi, unsur *"tanpa hak"* terpenuhi ketika pelaku mengakses, memodifikasi, atau menyedot data dari perangkat korban tanpa otorisasi atau persetujuan pemilik sistem (Adinda, 2024).

Adapun pemetaan kualifikasi berbagai jenis serangan *malware* ke dalam rumusan delik UU ITE dapat dianalisis secara sistematis pada Tabel 1 berikut.

Tabel 1. Pemetaan Kualifikasi Tindak Pidana Serangan *Malware* dalam UU ITE

Varian *Malware*	Modus dan Perbuatan (*Actus Reus*)	Pasal UU ITE yang Relevan	Analisis Kualifikasi Yuridis
Spyware & Keylogger	Menyusup ke sistem perangkat korban secara diam-diam untuk memantau aktivitas, merekam ketikan papan ketik, dan mengambil kredensial *login* atau data pribadi.	**Pasal 30 ayat (1), (2), dan (3)** (Akses ilegal) serta **Pasal 31 ayat (1)** (Intersepsi/penyadapan).	Memenuhi unsur mengakses sistem elektronik milik orang lain dengan sengaja dan tanpa hak untuk memperoleh informasi elektronik (Pasal 30 ayat 2) dengan cara melanggar atau menjebol sistem pengamanan (Pasal 30 ayat 3). Perekaman data yang sedang ditransmisikan juga dapat dikualifikasikan sebagai intersepsi ilegal (Pasal 31).
Ransomware	Mengenkripsi berkas data pribadi atau sistem korban sehingga tidak dapat diakses, disertai ancaman/permintaan uang tebusan untuk membuka kunci enkripsi.	**Pasal 32 ayat (1)** (Mengubah/merusak informasi), **Pasal 33** (Gangguan sistem), dan **Pasal 27B UU No. 1/2024** (Pemerasan elektronik).	Tindakan mengenkripsi data korban secara paksa memenuhi unsur mengubah, merusak, atau membuat tidak dapat diaksesnya informasi elektronik secara tanpa hak (Pasal 32 ayat 1) sekaligus mengganggu bekerjanya sistem elektronik (Pasal 33). Tuntutan tebusan memenuhi unsur pemerasan/pengancaman elektronik (Pasal 27B).

Varian *Malware*	Modus dan Perbuatan (*Actus Reus*)	Pasal UU ITE yang Relevan	Analisis Kualifikasi Yuridis
Trojan Horse (APK Palsu)	Menyamar sebagai aplikasi sah/resmi (misalnya aplikasi perbankan, layanan pemerintah, atau undangan digital) untuk menipu korban agar mengunduh dan memasangnya.	**Pasal 35** (Manipulasi informasi elektronik) dan **Pasal 28 ayat (1)** (Informasi menyesatkan yang merugikan konsumen).	Penyamaran kode berbahaya seolah-olah merupakan dokumen atau aplikasi otentik memenuhi unsur manipulasi/penciptaan informasi elektronik agar dianggap seolah-olah data yang otentik (Pasal 35).
Pembuatan & Distribusi Malware	Merancang, memproduksi, menjual, atau mendistribusikan perangkat lunak/kode berbahaya yang ditujukan untuk memfasilitasi kejahatan siber.	**Pasal 34 ayat (1) huruf a** (Penyediaan perangkat keras/lunak untuk memfasilitasi tindak pidana siber).	Menjerat aktor intelektual atau pembuat *malware* (*malware developer*), meskipun yang bersangkutan tidak secara langsung melancarkan serangan ke perangkat korban akhir.

Sumber: Diolah dari UU Nomor 11 Tahun 2008 jo. UU Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

Berdasarkan pemetaan di atas, dapat ditegaskan bahwa secara fungsional seluruh tahapan serangan *malware*—mulai dari fase penciptaan kode (Pasal 34), penyamaran aplikasi (Pasal 35), penetrasi sistem (Pasal 30), pencurian data (Pasal 31), hingga penguncian data dan pemerasan (Pasal 32, Pasal 33, dan Pasal 27B) telah memiliki pijakan hukum dalam UU ITE dengan ancaman pidana penjara berkisar antara 6 hingga 12 tahun dan/atau denda miliaran rupiah sebagaimana diatur dalam Pasal 45 hingga Pasal 51 UU ITE. Namun demikian, ketiadaan definisi eksplisit mengenai *malware* dan kategorisasi jenis-jenisnya tetap menyisakan ruang kekaburan norma (*vague norm*), sehingga aparat penegak hukum sangat bergantung pada konstruksi penafsiran ahli digital forensik untuk membuktikan bahwa suatu skrip program memenuhi unsur pasal-pasal tersebut (Wahyono, 2023).

2. Pertanggungjawaban Pidana dan Konkurensi Norma antara UU ITE dan UU PDP

a. Konstruksi Pertanggungjawaban Pidana Pelaku Serangan Malware

Pertanggungjawaban pidana (*criminal liability*) merupakan mekanisme untuk menentukan apakah pembuat tindak pidana dapat dijatuhi pidana atas perbuatan yang dilakukannya (Putri & Lasmadi, 2021). Dalam doktrin hukum pidana Indonesia, pertanggungjawaban pidana bertumpu pada asas fundamental *geen straf zonder schuld* (tiada pidana tanpa kesalahan) (Hiariej, 2016). Seseorang hanya dapat dimintai pertanggungjawaban pidana apabila memenuhi tiga syarat kumulatif: (1) kemampuan bertanggung jawab (*toerekeningsvatbaarheid*), yakni kondisi akal sehat dan kecakapan hukum pelaku; (2) adanya bentuk kesalahan berupa kesengajaan (*dolus*) atau kealpaan (*culpa*); serta (3) tidak adanya alasan pembenar (*rechtvaardigingsgrond*) maupun alasan pemaaf (*schulduitsluitingsgrond*) (Hiariej, 2016);(Putri & Lasmadi, 2021).

Pada kejahatan serangan *malware* terhadap data pribadi, syarat kemampuan bertanggung jawab umumnya terpenuhi secara nyata karena merancang dan menyebarkan *malware* memerlukan kompetensi teknis tingkat tinggi di bidang pemrograman dan arsitektur jaringan komputer (Pansariadi & Soekorini, 2023). Lebih lanjut, bentuk kesalahan dalam serangan *malware* hampir selalu berupa kesengajaan (*dolus*), baik dalam corak kesengajaan sebagai maksud (*opzet als oogmerk*)—yakni pelaku memang menghendaki tercurinya data pribadi korban untuk keuntungan finansial—maupun kesengajaan sebagai kepastian (*opzet bij zekerheidsbewustzijn*), karena pelaku menyadari bahwa menyebarkan berkas APK terinfeksi pasti akan merusak atau membobol sistem perangkat korban (Sangalang & Farina, 2024).

Perlu diluruskan pula bahwa dalam hukum pidana, pembuktian pertanggungjawaban pelaku *malware* tidak dapat serta-merta mengganti asas kesalahan dengan doktrin *res ipsa loquitur* (fakta

berbicara sendiri) yang lazim dikenal dalam ranah pembuktian perdata (*tort law*). Hukum pidana tetap mewajibkan penuntut umum membuktikan hubungan kausalitas antara tindakan terdakwa dan akses ilegal yang terjadi berdasarkan alat bukti yang sah, sehingga asas praduga tak bersalah (*presumption of innocence*) tetap terjaga (Faqir et al., 2024).

b. Pertanggungjawaban Pidana Menurut UU PDP dan Konkurensi Norma (Concursus)

Apabila objek yang diserang oleh *malware* adalah Data Pribadi yang menurut Pasal 1 angka 1 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mencakup data pribadi umum (nama, jenis kelamin, kewarganegaraan) maupun data pribadi spesifik (data kesehatan, biometrik, genetika, dan data keuangan pribadi) sebagaimana diatur dalam Pasal 4 UU PDP maka perbuatan pelaku juga bersinggungan langsung dengan rezim hukum pelindungan data pribadi (Rosadi, 2023);(Nurbaiti, 2022).

Pasal 65 ayat (1) dan ayat (3) UU PDP secara tegas melarang setiap orang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi, serta melarang penggunaan data pribadi secara melawan hukum (Kharisma, 2022). Pelanggaran terhadap ketentuan tersebut diancam dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah) berdasarkan Pasal 67 ayat (1) dan ayat (3) UU PDP. Selain subjek hukum orang perseorangan, Pasal 70 UU PDP juga mengakomodasi pertanggungjawaban pidana korporasi apabila serangan *malware* atau penyalahgunaan data pribadi dilakukan oleh atau atas nama badan hukum, dengan sanksi denda hingga 10 (sepuluh) kali lipat dari maksimal pidana denda yang diancamkan (Rosadi, 2023).

Situasi hukum di mana satu perbuatan penyebaran *malware* untuk mencuri data pribadi melanggar ketentuan UU ITE (Pasal 30 ayat 2 jo. Pasal 46 ayat 2 dengan ancaman pidana 7 tahun penjara) sekaligus melanggar ketentuan UU PDP (Pasal 65 ayat 1 jo. Pasal 67 ayat 1 dengan ancaman pidana 5 tahun penjara) memunculkan persoalan konkurensi norma. Jika ditinjau dari asas *lex specialis derogat legi generali*, UU PDP merupakan aturan yang lebih khusus dari segi objek delik (*data pribadi*), sedangkan UU ITE lebih khusus dari segi sarana perbuatan (*sistem elektronik*) (Amirulloh, 2025). Namun, merujuk pada doktrin bersamaan peraturan (*concursus idealis*) sebagaimana diatur dalam Pasal 63 ayat (1) KUHP, apabila suatu perbuatan masuk dalam lebih dari satu aturan pidana, maka yang dikenakan hanyalah salah satu di antara aturan-aturan itu, dan jika berbeda-beda, yang dikenakan adalah yang memuat ancaman pidana pokok yang paling berat (Hiariej, 2016). Tanpa adanya pedoman pemidanaan atau sinkronisasi regulasi antara UU ITE dan UU PDP, perbedaan ancaman sanksi ini berpotensi menimbulkan disparitas putusan hakim serta ketidakpastian hukum dalam praktik penuntutan (Djafar, 2023);(Amirulloh, 2025).

c. Hambatan Pembuktian, Yurisdiksi, dan Akibat Hukum

Dalam tataran implementasi, penegakan pertanggungjawaban pidana terhadap pelaku *malware* menghadapi tiga kendala struktural utama:

Pertama, Anonimitas dan Pembuktian Digital: Pelaku kerap menggunakan jaringan terenkripsi (*Virtual Private Network*/VPN, jaringan *Tor*), alamat protokol internet (*IP address*) palsu, serta infrastruktur *Command and Control* (C2) berlapis untuk menyembunyikan jejak digital. Meskipun Pasal 5 ayat (1) UU ITE telah mengakui informasi dan/atau dokumen elektronik sebagai alat bukti hukum yang sah, pembuktian integritas dan autentisitas bukti digitalseperti *server log*, nilai *hash* berkas *malware*, dan analisis *memory dump* menuntut standar forensik digital yang ketat agar tidak terbantahkan di persidangan (Wahyono, 2023);(Faqir et al., 2024).

Kedua, Kendala Yurisdiksi Transnasional: Banyak serangan *malware* di Indonesia dikendalikan oleh sindikat peretas dari luar negeri. Meskipun Pasal 2 UU ITE dan Pasal 2 UU PDP telah menganut asas ekstrateritorial yang menjangkau setiap orang di luar wilayah hukum Indonesia sepanjang perbuatannya menimbulkan akibat hukum di Indonesia eksekusi penangkapan dan ekstradisi pelaku lintas negara tetap bergantung pada efektivitas perjanjian bantuan hukum timbal balik (*Mutual Legal Assistance*/MLA) dan ratifikasi instrumen kerja sama siber internasional seperti Konvensi Budapest (*Budapest Convention on Cybercrime*) (Suseno, 2022).

Ketiga, Akibat Hukum dan Perlindungan Korban: Selain sanksi pidana pokok berupa penjara dan denda bagi pelaku, akibat hukum dari serangan *malware* juga melahirkan hak subjek data pribadi untuk menggugat dan menerima ganti kerugian atas pelanggaran pemrosesan data pribadinya sesuai Pasal 12 ayat (1) UU PDP (I. P. Sari & Prihatiningtyas, 2023). Di sisi lain, bagi Penyelenggara Sistem Elektronik

(PSE) selaku pengendali data pribadi yang sistemnya dibobol oleh *malware*, Pasal 20 dan Pasal 46 UU PDP mewajibkan penerapan standar keamanan teknis (*security by design*) serta kewajiban menyampaikan pemberitahuan tertulis kebocoran data (*data breach notification*) paling lambat 3 x 24 jam kepada subjek data pribadi dan lembaga pengawas pelindungan data pribadi (Sugiantari, 2024);(Rosadi, 2025).

3. Urgensi Harmonisasi Regulasi dan Penguatan Kapasitas Penegakan Hukum

Temuan pada bagian sebelumnya memperlihatkan bahwa penanggulangan serangan *malware* di Indonesia masih mengalami disharmoni norma dan kesenjangan kapasitas teknis. Kekosongan definisi eksplisit mengenai *malware* dalam UU ITE, ditambah perbedaan struktur ancaman sanksi pidana dengan UU PDP, menuntut adanya pembaruan kebijakan hukum pidana (*penal policy*) yang terintegrasi (S. Arief, 2022).

Harmonisasi regulasi perlu diarahkan pada dua aspek strategis. Pertama, penyusunan peraturan pelaksana (Peraturan Pemerintah) dari UU PDP serta pedoman teknis penuntutan bersama antara Kejaksaan Agung dan Kepolisian Negara Republik Indonesia guna menyelaraskan penerapan pasal-pasal akses ilegal dalam UU ITE dengan delik perolehan data pribadi secara melawan hukum dalam UU PDP (Amirulloh, 2025). Kedua, penguatan kapasitas sumber daya manusia aparat penegak hukum di bidang digital forensik hingga tingkat wilayah (Polda), disertai perluasan kerja sama internasional guna mengatasi hambatan yurisdiksi pelaku kejahatan siber lintas negara (Pansariadi & Soekorini, 2023);(Bua & Idris, 2025).

KESIMPULAN

Pertama, serangan *malware* terhadap data pribadi baik dalam bentuk *ransomware*, *spyware*, *trojan horse*, maupun *keylogger* dapat dikualifikasikan sebagai tindak pidana siber menurut UU ITE karena memenuhi unsur perbuatan yang dilakukan dengan sengaja, tanpa hak, dan melawan hukum. Kualifikasi tersebut terdistribusi pada ketentuan akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), perusakan dan gangguan sistem elektronik (Pasal 32 dan Pasal 33), penyediaan perangkat lunak berbahaya (Pasal 34), manipulasi informasi elektronik (Pasal 35), serta pemerasan elektronik (Pasal 27B UU Nomor 1 Tahun 2024). Meskipun demikian, ketiadaan definisi dan kategorisasi eksplisit mengenai *malware* dalam undang-undang menjadikan penegakannya masih bergantung pada penafsiran ekstensif aparat penegak hukum.

Kedua, pertanggungjawaban pidana pelaku serangan *malware* berlandaskan asas *geen straf zonder schuld* yang mensyaratkan kemampuan bertanggung jawab, kesengajaan (*dolus*), dan ketiadaan alasan penghapus pidana. Dalam konteks pencurian data pribadi, perbuatan pelaku juga memenuhi unsur tindak pidana dalam Pasal 65 jo. Pasal 67 UU PDP, sehingga memunculkan konkurensi norma dengan UU ITE yang berpotensi menimbulkan disparitas pemidanaan. Selain itu, efektivitas penegakan hukum masih terkendala oleh anonimitas pelaku, kompleksitas pembuktian alat bukti elektronik, serta batas yurisdiksi transnasional.

DAFTAR PUSTAKA

Buku:

Arief, B. N. (2022). *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana.

Budhijanto, D. (2024). *Hukum Pelindungan Data Pribadi dan Data Nasional*. Bandung: Logoz Publishing.

Djafar, W. (2023). *Hukum Pelindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Pembaruan*. Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Hiariej, E. O. S. (2016). *Prinsip-Prinsip Hukum Pidana* (Edisi Revisi). Yogyakarta: Cahaya Atma Pustaka.

Marzuki, P. M. (2017). *Penelitian Hukum* (Edisi Revisi). Jakarta: Kencana Prenada Media Group.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika.

Sangalang, R. S., & Farina, T. (2024). *Hukum Pidana Cyber*. Malang: Media Penerbit Indonesia.

Suseno, S. (2022). *Yurisdiksi Tindak Pidana Siber: Teori dan Praktik Penegakan Hukum Transnasional*. Bandung: Refika Aditama.

Wahyono, T. (2023). *Digital Forensics: Panduan Praktis Investigasi Kejahatan Siber dan Pembuktian Hukum*. Yogyakarta: Andi Offset.

Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Malang: Media Nusa Creative.

Jurnal:

Adinda, L. S. (2024). Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia. *Jurnal Ilmu Sosial, Politik, Dan Hukum Al-Dalil*, *2*(2), 145–158.

Amirulloh, M. (2025). Sinkronisasi Hukum Pidana Siber: Analisis Tumpang Tindih Regulasi antara Rezim UU ITE dan Undang-Undang Pelindungan Data Pribadi. *Jurnal Hukum IUS QUIA IUSTUM*, *32*(2), 115–138.

Arief, M., & Darmawan, A. (2024). Tanggung Jawab Hukum Penyelenggara Sistem Elektronik atas Kebocoran Data Pribadi Akibat Serangan Ransomware (Studi Kasus Bank Syariah Indonesia). *Jurnal Hukum IUS QUIA IUSTUM*, *31*(1), 112–134. https://doi.org/10.20885/iustum.vol31.iss1.art6

Arief, S. (2022). *Model Sistem BAgi HAsil: Pada Sektor Pertanian di Jawa Timur*. books.google.com. https://books.google.com/books?hl=en%5C&lr=%5C&id=oBRkEAAAQBAJ%5C&oi=fnd%5C&pg=PA1%5C&dq=screening+produk+islami%5C&ots=PmQijoYmTh%5C&sig=HVJ7pdT0GeiCrJEVcWa5O1RezUo

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), 100–114.

Budhijanto, D. (2024). *Hukum Pelindungan Data Pribadi dan Data Nasional*. Logoz Publishing.

Djafar, W. (2023). *Hukum Pelindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Pembaruan*. Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Faqir, R. S. A., Al-Kafawin, A. M., & Al-Shawabkeh, M. (2024). Digital Evidence Extracted from Electronic Media: A Comparative Study. *International Journal of Cyber Criminology*, *18*(2), 224–242.

Hiariej, E. O. S. (2016). *Prinsip-Prinsip Hukum Pidana (Edisi Revisi)*. Cahaya Atma Pustaka.

Kharisma, D. B. (2022). A Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong, and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0199

Marzuki, P. M. (2017). *Penelitian Hukum (Edisi Revisi)*. Kencana Prenada Media Group.

Nurbaiti, S. (2022). Perlindungan Hukum Pemilik Data Pribadi dalam Transaksi Digital. *Jurnal Hukum IUS QUIA IUSTUM*, *29*(1), 45–67. https://doi.org/10.20885/iustum.vol29.iss1.art3

Nurjanah, A. A., & Liyus, H. (2025). Perlindungan Hukum Bagi Korban Penyalahgunaan Artificial Intelligence (AI) Terhadap Serangan Malware dalam Perspektif Peraturan Perundang-Undangan. *PAMPAS: Journal of Criminal Law*, *6*(2), 230–244.

Pansariadi, R. S. B., & Soekorini, N. (2023). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum*, *12*(2), 287–298. https://doi.org/10.37893/jbh.v12i2.605

Putri, N. N., & Lasmadi, S. (2021). Pertanggungjawaban Pidana Perusahaan Pers Terhadap Pemberitaan yang Mencemarkan Nama Baik Orang Lain Melalui Media Cetak Online. *PAMPAS: Journal of Criminal Law*, *2*(2), 123–139.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.

Rosadi, S. D. (2025). Konvergensi Standar Global Pelindungan Data Pribadi ke dalam Rezim Hukum Siber Indonesia Pasca-Pengundangan UU PDP. *Jurnal Hukum IUS QUIA IUSTUM*, *32*(1), 55–78.

Sangalang, R. S., & Farina, T. (2024). *Hukum Pidana Cyber*. Media Penerbit Indonesia.

Sari, D. P., & Pratama, R. A. (2023). Penegakan Hukum Pidana terhadap Modus Penipuan Phishing Berkedok Undangan Digital (APK) dalam Perspektif Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Pembangunan Hukum Indonesia*, *5*(3), 489–505. https://doi.org/10.14710/jphi.v5i3.489-505

Sari, I. P., & Prihatiningtyas, W. (2023). Tanggung Jawab Hukum Platform Fintech Lending atas

Penyalahgunaan Data Kontak Darurat. *Jurnal Penelitian Hukum De Jure*, *23*(2), 201–215. https://doi.org/10.30641/dejure.2023.V23.201-215

Simorangkir, H. P. (2024). Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum? *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, *2*(4), 426–434. https://doi.org/10.55606/eksekusi.v2i4.1823

Sugiantari, A. A. P. W. (2024). Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masyarakat Dari Pusat Data Nasional (PDN) Indonesia. *Jurnal Hukum Saraswati*, *6*(2), 728–741.

Suseno, S. (2022). *Yurisdiksi Tindak Pidana Siber: Teori dan Praktik Penegakan Hukum Transnasional*. Refika Aditama.

Wahyono, T. (2023). *Digital Forensics: Panduan Praktis Investigasi Kejahatan Siber dan Pembuktian Hukum*. Andi Offset.

Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia*. Media Nusa Creative.

Peraturan Perundang-Undangan:

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905).