Cerdika: Jurnal Ilmiah Indonesia, 6 (3), 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534
Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

PENYALAHGUNAAN DATA PRIBADI SEBAGAI KEJAHATAN CYBERCRIME DITINJAU DARI HUKUM PIDANA INDONESIA

Indira Hertha Wibowo* , Jingga Aura Cinta, Nadia Herdiana Putri, Cecilia Chrysilla Liem
Universitas Pelita Harapan, Indonesia
Email: sallyroyaltycrowny@gmail.com* , auracintajingga@gmail.com, herdiananadia05@gmail.com, cecilialiem6@gmail.com

Keywords:
personal data misuse; cybercrime; Indonesian criminal law; Personal Data Protection Law; corporate liability

Abstract

The rise of cybercrime targeting personal data is reflected in the APJII report which recorded a surge in victims of personal data theft from 7.9 percent in 2023 to 20.9 percent in 2024, as well as 2,597 police reports at the Jakarta Metropolitan Police with losses of IDR 24.3 billion from January to August 2025. This study analyzes the misuse of personal data as a cybercrime from the perspective of Indonesian criminal law. This study uses a normative legal method with a statutory and conceptual approach, sourced from primary, secondary, and tertiary legal materials analyzed descriptively and analytically. The results of the study indicate that criminal law regulations have a strong foundation through the PDP Law and the ITE Law. The PDP Law, Articles 65-73, regulates criminal offenses with a maximum prison sentence of 6 years and a fine of IDR 6 billion, and has been implemented in the Karanganyar District Court Decision Number 5/Pid.Sus/2023/PN Krg. The crime typology includes carding, doxing, social engineering, data-based extortion, and identity theft for illegal online lending, characterized by cross-border activity, anonymous perpetrators, and volatile evidence. Criminal liability extends not only to individuals but also to corporations through Articles 69-70 of the Personal Data Protection Law, which carries a fine of up to IDR 60 billion. However, implementation still faces challenges, including the lack of a Personal Data Protection Supervisory Agency and the complexity of the evidentiary process.

Kata Kunci:
penyalahgunaan data pribadi; cybercrime; hukum pidana Indonesia; UU PDP; pertanggungjawaban korporasi

Abstrak

Maraknya kejahatan siber yang menyasar data pribadi tercermin dari laporan APJII yang mencatat lonjakan korban pencurian data pribadi dari 7,9 persen pada tahun 2023 menjadi 20,9 persen pada tahun 2024, serta 2.597 laporan polisi di Polda Metro Jaya dengan kerugian Rp24,3 miliar sepanjang Januari-Agustus 2025. Penelitian ini menganalisis penyalahgunaan data pribadi sebagai kejahatan cybercrime dalam perspektif hukum pidana Indonesia. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual, bersumber pada bahan hukum primer, sekunder, dan tersier yang dianalisis secara deskriptif-analitis. Hasil penelitian menunjukkan bahwa pengaturan hukum pidana telah memiliki landasan kuat melalui UU PDP dan UU ITE. UU PDP Pasal 65-73 mengatur delik pidana dengan ancaman penjara maksimal 6 tahun dan denda Rp6 miliar, serta telah diterapkan dalam Putusan PN Karanganyar Nomor 5/Pid.Sus/2023/PN Krg. Tipologi kejahatan meliputi carding, doxing, social engineering, pemerasan berbasis data, dan penyalahgunaan identitas untuk pinjaman online ilegal, dengan karakteristik lintas batas, pelaku anonim, dan bukti volatil. Pertanggungjawaban pidana tidak hanya menjangkau individu tetapi juga korporasi melalui Pasal 69-70 UU PDP dengan ancaman denda hingga Rp60 miliar. Meskipun demikian, implementasi masih menghadapi tantangan berupa belum terbentuknya Badan Pengawas PDP dan kompleksitas pembuktian.

PENDAHULUAN

Era digital telah mengubah lanskap kehidupan masyarakat Indonesia secara fundamental. Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia mencapai 212 juta jiwa pada tahun 2024, atau sekitar 74,6 persen dari total populasi (APJII, 2024). Kemajuan ini tentu membawa kemudahan dalam berbagai aspek kehidupan, mulai dari transaksi keuangan, layanan kesehatan, hingga interaksi sosial. Namun, di balik kemudahan tersebut, muncul ancaman baru yang tak kalah serius, yakni kejahatan siber yang menyasar data pribadi. Data pribadi saat ini telah menjelma menjadi komoditas berharga sekaligus rentan untuk disalahgunakan, baik melalui pencurian identitas, penipuan daring, maupun perdagangan ilegal di forum-forum gelap (dark forum). Fenomena ini menempatkan penyalahgunaan data pribadi sebagai salah satu tantangan terbesar dalam penegakan hukum pidana di Indonesia (Kurnianingrum, 2020).

Maraknya penyalahgunaan data pribadi tercermin dari berbagai data dan laporan kejahatan siber (Firdaus, 2022; Pratiwi & Miarsa, 2025). Laporan APJII mencatat lonjakan signifikan korban pencurian data pribadi dari 7,9 persen pada tahun 2023 menjadi 20,9 persen pada tahun 2024. Direktorat Reserse Siber Polda Metro Jaya bahkan menangani 2.597 laporan polisi terkait tindak pidana siber dengan total kerugian mencapai Rp24,3 miliar sepanjang Januari hingga Agustus 2025, dengan modus dominan berupa penipuan daring (online scam), phishing, dan pinjaman online illegal (Azhar, 2025). Dalam skala yang lebih luas, Kementerian Komunikasi dan Digital menerima lebih dari 1,2 juta laporan penipuan digital hingga pertengahan tahun 2025. Southeast Asia Freedom of Expression Network (SAFEnet) juga mencatat setidaknya 299 serangan digital pada kuartal III-2025, yang menjadi periode terburuk sepanjang tahun tersebut dengan korban terbanyak adalah warga sipil dan pelajar (Safenet, 2025). Data-data ini mengonfirmasi bahwa ruang digital Indonesia telah menjadi ladang subur bagi perburuan dan eksploitasi data pribadi secara ilegal.

Sebagai respons atas darurat perlindungan data pribadi, Pemerintah Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mulai berlaku penuh sejak Oktober 2024. UU ini menjadi instrumen hukum utama yang mengatur secara komprehensif mengenai hak pemilik data, kewajiban pengelola data, serta sanksi pidana bagi pelaku penyalahgunaan. Dalam UU PDP, ancaman pidana bagi pelaku pengungkapan data pribadi secara melawan hukum diatur dalam Pasal 67 ayat (2) dengan pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4 miliar. Selain itu, korban juga memiliki mekanisme untuk mendapatkan ganti rugi melalui jalur pidana, administrasi, maupun perdata. Namun, meskipun payung hukum telah tersedia, implementasinya masih menghadapi berbagai tantangan, termasuk belum terbentuknya (Rizqiyanto, Rohman, & Raya, 2024). Badan Pengawas Perlindungan Data Pribadi dan perlunya tafsir yang ketat terhadap pasal-pasal pidana agar tidak menimbulkan kriminalisasi yang keliru.

Tantangan lainnya terletak pada kompleksitas modus operandi kejahatan dan keragaman pemahaman masyarakat. Pelaku kejahatan siber kini menggunakan teknologi canggih seperti deepfake berbasis kecerdasan buatan, malware, serta memanfaatkan platform seperti WhatsApp (486 kasus), Instagram (98 kasus), dan Facebook (66 kasus) untuk menjalankan aksinya (Azhar, 2025). Bahkan, jaringan kejahatan ini telah bersifat lintas negara dengan pelaku yang terorganisir dari Indonesia, Malaysia, hingga Kamboja. Di sisi lain, kesadaran masyarakat dalam melindungi data pribadinya masih rendah, ditandai dengan budaya "klik

setuju" tanpa membaca syarat dan ketentuan, serta mudahnya membagikan data sensitif seperti KTP di aplikasi yang tidak jelas. Berdasarkan latar belakang tersebut, artikel ini akan mengkaji secara mendalam mengenai penyalahgunaan data pribadi sebagai kejahatan cybercrime dalam perspektif hukum pidana Indonesia, dengan fokus pada analisis ketentuan UU PDP, efektivitas penegakannya, serta tantangan yang dihadapi dalam melindungi hak konstitusional warga negara atas perlindungan data pribadi.

Kesenjangan penelitian (research gap) yang diidentifikasi adalah belum adanya kajian komprehensif yang mengintegrasikan tiga aspek sekaligus: analisis normatif terhadap ketentuan pidana dalam UU PDP pasca pemberlakuannya, pemetaan tipologi penyalahgunaan data pribadi terkini dengan data empiris, dan evaluasi terhadap implementasi pertanggungjawaban pidana baik individu maupun korporasi. Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan menawarkan analisis yang holistik dan mutakhir, mengingat UU PDP baru berlaku penuh pada Oktober 2024 dan berbagai kasus serta putusan pengadilan mulai bermunculan.

Kebaruan (novelty) penelitian ini terletak pada beberapa aspek. Pertama, penelitian ini menganalisis ketentuan pidana dalam UU PDP yang relatif baru dan belum banyak dikaji secara mendalam. Kedua, penelitian ini mengintegrasikan data terkini mengenai kasus-kasus penyalahgunaan data pribadi, termasuk putusan pengadilan yang telah menerapkan UU PDP seperti Putusan PN Karanganyar Nomor 5/Pid.Sus/2023/PN Krg. Ketiga, penelitian ini secara khusus membahas pertanggungjawaban pidana korporasi yang merupakan terobosan penting dalam sistem hukum pidana Indonesia. Keempat, penelitian ini memetakan tipologi kejahatan penyalahgunaan data pribadi yang terus berkembang seiring kemajuan teknologi.

Tujuan penelitian ini adalah untuk menganalisis secara mendalam pengaturan hukum pidana terhadap penyalahgunaan data pribadi sebagai kejahatan cybercrime di Indonesia, dengan fokus pada tiga hal utama: (1) pengaturan hukum pidana dalam UU PDP dan UU ITE; (2) tipologi dan karakteristik penyalahgunaan data pribadi di ruang siber; dan (3) pertanggungjawaban pidana bagi pelaku, baik individu maupun korporasi. Penelitian ini diharapkan dapat memberikan kontribusi teoretis bagi pengembangan kajian hukum pidana, khususnya dalam bidang kejahatan siber dan perlindungan data pribadi. Secara praktis, penelitian ini bermanfaat sebagai bahan masukan bagi pembuat kebijakan dalam mengevaluasi implementasi UU PDP, bagi aparat penegak hukum dalam menangani kasus-kasus penyalahgunaan data pribadi, serta bagi masyarakat umum dalam meningkatkan kesadaran akan pentingnya melindungi data pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif atau studi kepustakaan (library research). Penelitian hukum normatif dipilih karena fokus kajiannya adalah untuk meneliti dan menganalisis norma-norma hukum yang terkait dengan penyalahgunaan data pribadi sebagai kejahatan cybercrime dalam perspektif hukum pidana Indonesia. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah seluruh regulasi yang relevan dengan isu hukum yang diteliti, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan peraturan

perundang-undangan lain yang terkait dengan kejahatan siber. Sementara itu, pendekatan konseptual digunakan untuk memahami konsep-konsep hukum seperti kejahatan cybercrime, perlindungan data pribadi, dan pertanggungjawaban pidana dari perspektif doktrin para ahli hukum.

Sumber bahan hukum yang digunakan dalam penelitian ini terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Kitab Undang-Undang Hukum Pidana. Bahan hukum sekunder diperoleh dari literatur hukum, jurnal ilmiah, hasil penelitian terdahulu, artikel dari media massa terpercaya, serta pendapat para ahli yang relevan dengan topik penelitian. Adapun bahan hukum tersier mencakup kamus hukum dan ensiklopedia untuk melengkapi pemahaman terhadap istilah-istilah teknis.

Pengumpulan bahan hukum dilakukan melalui teknik dokumentasi atau studi pustaka, yaitu dengan menelusuri, menginventarisasi, dan mengkaji berbagai dokumen hukum serta literatur yang relevan (Benuf & Azhar, 2020). Seluruh bahan hukum yang terkumpul kemudian dianalisis secara kualitatif dengan menggunakan metode interpretasi hukum, yaitu menafsirkan teks peraturan perundang-undangan dan menghubungkannya dengan konsep-konsep teoritis yang relevan. Analisis dilakukan secara deskriptif-analitis, yang bertujuan untuk memberikan gambaran secara sistematis dan mendalam mengenai pengaturan hukum pidana terhadap penyalahgunaan data pribadi sebagai kejahatan cybercrime di Indonesia, serta menganalisis efektivitas dan tantangan dalam implementasinya.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Pidana Terhadap Penyalahgunaan Data Pribadi di Indonesia

Pengaturan hukum pidana terhadap penyalahgunaan data pribadi di Indonesia saat ini memiliki landasan normatif yang kuat dan bersifat ganda (double-track system), yakni bersumber dari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Sebelum UU PDP diundangkan, perlindungan data pribadi lebih banyak mengacu pada UU ITE. Pasal 26 ayat (1) UU ITE menegaskan bahwa penggunaan data pribadi melalui media elektronik harus mendapatkan persetujuan dari pemilik data. Ketentuan ini bersifat preventif, namun jika terjadi pelanggaran, UU ITE menyediakan sanksi pidana melalui Pasal 32 jo Pasal 48 (Watkat, Ingratubun, & Apriyanti, 2024). Pasal 32 melarang perbuatan mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik milik orang lain tanpa hak. Ancaman pidananya bervariasi: pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar untuk pelanggaran ayat (1); 9 tahun dan/atau denda Rp3 miliar untuk pelanggaran ayat (2); serta 10 tahun dan/atau denda Rp5 miliar jika perbuatan tersebut mengakibatkan terbukanya data rahasia ke publik (Ayustin, 2022).

Era baru pengaturan pidana data pribadi dimulai dengan berlakunya UU PDP pada 17 Oktober 2022. Undang-undang ini secara khusus dan komprehensif mengatur delik pidana penyalahgunaan data pribadi dalam Bab XI (Pasal 65-73). Ketentuan pidana dalam UU PDP langsung berlaku efektif meskipun lembaga pengawasnya belum terbentuk, berbeda dengan

sanksi administratif yang memerlukan kelembagaan tersebut. Pasal 65 UU PDP merumuskan tiga kategori perbuatan yang dilarang: (1) memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian; (2) mengungkapkan data pribadi yang bukan miliknya; dan (3) menggunakan data pribadi yang bukan miliknya. Sanksi pidananya diatur dalam Pasal 67, yaitu pidana penjara paling lama 5 tahun dan/atau denda Rp5 miliar untuk pemerolehan ilegal (ayat 1), penjara paling lama 4 tahun dan/atau denda Rp4 miliar untuk pengungkapan ilegal (ayat 2), serta penjara paling lama 5 tahun dan/atau denda Rp5 miliar untuk penggunaan ilegal (ayat 3). Selain itu, Pasal 68 secara khusus mengatur delik pencurian identitas (identity theft) dengan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar (Adcovates, 2024).

Praktik penegakan hukum telah menunjukkan penerapan pasal-pasal tersebut. Putusan Pengadilan Negeri Karanganyar Nomor 5/Pid.Sus/2023/PN Krg menjadi tonggak pertama penerapan sanksi pidana UU PDP, di mana pelaku pencurian identitas dengan menyamar sebagai petugas polisi dijatuhi hukuman 5 tahun penjara dan denda Rp1 miliar berdasarkan Pasal 68 UU PDP. Kasus lainnya melibatkan supervisor sales perusahaan telekomunikasi yang menggunakan NIK curian untuk aktivasi kartu SIM, dihukum 1,5 tahun penjara berdasarkan Pasal 67 ayat (3) UU PDP (Adcovates, 2024).

Pengaturan yang bersumber dari dua undang-undang ini menciptakan kompleksitas tersendiri. Tindak pidana penyalahgunaan data pribadi dapat dijerat baik dengan UU ITE maupun UU PDP, yang memiliki perbedaan ancaman pidana dan konstruksi delik. UU ITE lebih fokus pada perlindungan informasi dan dokumen elektronik secara umum, sementara UU PDP secara spesifik melindungi data pribadi sebagai entitas hukum tersendiri. Selain itu, KUHP baru yang berlaku 2 Januari 2026 juga turut memperkuat perlindungan privasi digital melalui Pasal 258 yang melarang penyadapan komunikasi elektronik secara melawan hukum dengan ancaman pidana penjara paling lama 10 tahun (Ramli, 2026). Mahkamah Konstitusi melalui Putusan Nomor 151/PUU-XXII/2024 juga menegaskan bahwa perlindungan data pribadi merupakan bagian tidak terpisahkan dari hak konstitusional atas perlindungan diri pribadi sebagaimana dijamin Pasal 28G ayat (1) UUD 1945.

Tipologi dan Karakteristik Penyalahgunaan Data Pribadi dalam Ruang Siber

Penyalahgunaan data pribadi di ruang siber hadir dalam berbagai tipologi dengan karakteristik khas yang membedakannya dari kejahatan konvensional. Berdasarkan tipologinya, kejahatan ini dapat diklasifikasikan ke dalam beberapa bentuk utama. Pertama, *carding* merupakan kejahatan yang menggunakan data kartu kredit atau debit milik orang lain untuk melakukan transaksi ilegal. Pelaku biasanya memperoleh data tersebut melalui skimming pada mesin ATM atau EDC, maupun dari kebocoran database merchant (Suhaemin & Muslih, 2021). Data yang dicuri kemudian digunakan untuk berbelanja daring atau bahkan dijual di forum-forum bawah tanah dengan harga bervariasi tergantung kelengkapan informasi. Kedua, *doxing* adalah tindakan mengumpulkan dan mempublikasikan data pribadi seseorang ke publik tanpa izin dengan tujuan mengintimidasi atau mempermalukan korban. Praktik ini marak terjadi dalam konflik daring, di mana identitas seperti alamat rumah, nomor telepon, tempat kerja, hingga foto pribadi disebarluaskan di media sosial (Tim Hukum Online, 2023).

Ketiga, *social engineering* menjadi metode yang cukup efektif karena mengeksploitasi faktor manusia sebagai mata rantai terlemah dalam keamanan siber. Pelaku memanipulasi psikologis korban agar membocorkan data rahasia atau melakukan tindakan tertentu, misalnya dengan berpura-pura menjadi petugas bank, customer service, atau bahkan kerabat dekat korban. Keempat, pemerasan berbasis data (*sextortion* atau *ransomware*) dilakukan setelah pelaku berhasil menguasai data pribadi korban (Universitas Medan Area, 2023). Data tersebut kemudian dijadikan alat pemerasan, misalnya dengan ancaman akan menyebarkan foto atau video pribadi, atau mengenkripsi seluruh data korban dan meminta tebusan untuk membukanya kembali.

Kelima, pendaftaran SIM card dan pinjaman online ilegal menggunakan identitas orang lain. Praktik ini marak terjadi di masyarakat karena registrasi kartu SIM prabayar yang seharusnya menggunakan data KTP sering kali diabaikan oleh oknum penjual. Akibatnya, data ribuan orang dapat digunakan untuk mendaftarkan kartu SIM yang kemudian dimanfaatkan untuk tindak pidana. Demikian pula dengan maraknya pinjaman online ilegal yang menggunakan data KTP korban tanpa sepengetahuan untuk mengajukan pinjaman, yang kemudian menagih korban yang sama sekali tidak pernah meminjam. Komisi I DPR RI mencatat temuan sekitar 4,5 juta data pinjaman online yang diduga bocor dan diperjualbelikan, sementara Kementerian Komunikasi dan Informatika telah memblokir ribuan fintech peer-to-peer lending ilegal yang melakukan praktik penagihan tidak beretika dengan menyebarkan data pribadi peminjam (Tempo, 2025).

Karakteristik penyalahgunaan data pribadi di ruang siber sangat khas. Pertama, bersifat lintas batas negara (cross-border), pelaku dapat berada di luar negeri sementara korban di Indonesia, atau sebaliknya. Kedua, pelaku dapat beroperasi secara anonim dengan memanfaatkan jaringan privat virtual (VPN), proxy server, atau dark web untuk menyembunyikan identitas asli. Ketiga, bukti elektronik bersifat volatil atau mudah hilang, sehingga penegak hukum harus bergerak cepat dalam melakukan penyitaan dan preservasi digital evidence. Keempat, dampak kejahatan dapat meluas secara massal dalam waktu singkat karena kecepatan penyebaran informasi di internet. Kelima, modus operandi terus berevolusi mengikuti perkembangan teknologi, misalnya penggunaan deepfake berbasis kecerdasan buatan untuk membuat konten palsu yang meyakinkan atau serangan siber yang mengeksploitasi kerentanan aplikasi Identitas Kependudukan Digital (Fachri, 2024). Motif pelaku umumnya didominasi keuntungan finansial, namun tidak sedikit pula yang bermotif non-ekonomi seperti balas dendam, uji kemampuan, atau bahkan kepentingan politik.

Pertanggungjawaban Pidana bagi Pelaku Penyalahgunaan Data Pribadi

Pertanggungjawaban pidana dalam kasus penyalahgunaan data pribadi di Indonesia tidak hanya membebankan tanggung jawab kepada individu pelaku, tetapi juga menjangkau korporasi sebagai subjek hukum yang dapat dimintai pertanggungjawaban secara mandiri. Hal ini merupakan perkembangan penting dalam sistem hukum pidana Indonesia yang selama ini lebih berorientasi pada pertanggungjawaban individu. UU PDP secara tegas mengatur pertanggungjawaban korporasi dalam Pasal 69 yang menyatakan bahwa jika tindak pidana sebagaimana dimaksud dalam UU ini dilakukan oleh korporasi, maka pertanggungjawaban pidana dikenakan terhadap korporasi, pengurus, pemberi perintah, pemegang kendali, atau pemilik manfaat korporasi (Primanta, 2020). Ketentuan ini menegaskan prinsip bahwa

korporasi tidak dapat berlindung di balik struktur organisasinya ketika terjadi pelanggaran data pribadi yang merugikan masyarakat.

Sanksi pidana bagi korporasi diatur secara khusus dalam Pasal 70 UU PDP dengan ancaman yang jauh lebih berat dibandingkan pelaku individu. Korporasi yang terbukti melakukan tindak pidana penyalahgunaan data pribadi dapat dijatuhi pidana denda paling banyak 10 kali dari maksimum pidana denda yang diancamkan, yang berarti dapat mencapai Rp60 miliar untuk pelanggaran Pasal 68. Selain pidana denda, Pasal 70 ayat (2) memberikan kewenangan kepada hakim untuk menjatuhkan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh usaha korporasi, hingga pencabutan izin usaha dan pembubaran korporasi (Elnizar, 2023). Pidana tambahan ini bersifat progresif karena dapat melumpuhkan bisnis korporasi yang terbukti menjadikan data pribadi sebagai komoditas ilegal.

Konstruksi pertanggungjawaban pidana korporasi dalam UU PDP menganut sistem pertanggungjawaban yang ketat (strict liability) dalam konteks tertentu. Artinya, korporasi dapat dimintai pertanggungjawaban meskipun tidak dibuktikan adanya unsur kesalahan (mens rea) pada pengurusnya, terutama dalam hal kelalaian menjaga keamanan data pribadi yang menjadi tanggung jawabnya. Hal ini sejalan dengan ketentuan Pasal 20 UU PDP yang mewajibkan pengendali data pribadi untuk melindungi dan menjamin keamanan data pribadi yang diprosesnya (Kurniawan & D, 2014). Kegagalan memenuhi kewajiban ini dapat berimplikasi pada pertanggungjawaban pidana jika mengakibatkan kerugian bagi subjek data pribadi.

Dalam praktik penegakan hukum, pertanggungjawaban pidana korporasi atas kasus kebocoran data pribadi mulai menjadi perhatian otoritas. Kementerian Komunikasi dan Informatika telah beberapa kali menjatuhkan sanksi administratif kepada platform digital yang mengalami kebocoran data pengguna, namun untuk penjatuhan sanksi pidana masih menghadapi tantangan pembuktian terkait hubungan kausal antara kelalaian korporasi dengan kebocoran data yang terjadi. Meskipun demikian, Pasal 69 ayat (2) UU PDP memberikan panduan bahwa jika tuntutan pidana dilakukan terhadap korporasi, maka korporasi diwakili oleh pengurus yang berwenang mewakili korporasi dalam berperkara, dan pengurus yang mewakili korporasi dapat dibebani kewajiban membayar pidana denda apabila korporasi tidak mampu membayarnya.

Selain korporasi, UU PDP juga mengatur pertanggungjawaban pidana bagi setiap orang yang dengan sengaja melawan hukum membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain. Ketentuan ini dalam Pasal 68 dirumuskan secara berbeda dari Pasal 65, karena secara spesifik mengatur delik pemalsuan data pribadi yang merupakan bentuk khusus dari penyalahgunaan data. Ancaman pidananya juga lebih berat, yaitu penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar (Salsabila & Wiraguna, 2025). Hal ini menunjukkan keseriusan pembentuk undang-undang dalam menangani kejahatan identitas yang selama ini marak terjadi dalam berbagai modus seperti pembuatan KTP palsu, ijazah palsu, atau dokumen kependudukan palsu untuk kepentingan fraud. Dengan sistem pertanggungjawaban pidana yang menjangkau korporasi dan mengatur delik khusus pemalsuan data, UU PDP memberikan landasan kuat bagi penegakan hukum yang lebih efektif.

KESIMPULAN

Berdasarkan pembahasan mengenai penyalahgunaan data pribadi sebagai kejahatan cybercrime ditinjau dari hukum pidana Indonesia, dapat disimpulkan beberapa hal sebagai berikut. Pertama, pengaturan hukum pidana terhadap penyalahgunaan data pribadi di Indonesia telah memiliki landasan normatif yang kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang melengkapi ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU PDP mengatur secara komprehensif delik pidana dalam Pasal 65 hingga 73 dengan ancaman pidana penjara maksimal 6 tahun dan denda hingga Rp6 miliar, serta telah diterapkan dalam putusan pengadilan seperti PN Karanganyar dan PN Tangerang. Kedua, tipologi penyalahgunaan data pribadi di ruang siber sangat beragam, meliputi carding, doxing, social engineering, pemerasan berbasis data (sextortion/ransomware), serta penyalahgunaan identitas untuk pendaftaran SIM card dan pinjaman online ilegal. Karakteristik kejahatan ini bersifat lintas batas negara, pelaku anonim, bukti elektronik volatil, serta modus operandi yang terus berevolusi mengikuti perkembangan teknologi seperti penggunaan deepfake dan malware canggih. Ketiga, pertanggungjawaban pidana tidak hanya dibebankan kepada individu pelaku, tetapi juga menjangkau korporasi sebagai subjek hukum. UU PDP mengatur pertanggungjawaban korporasi dalam Pasal 69 dengan sanksi pidana denda hingga sepuluh kali lipat (maksimal Rp60 miliar) serta pidana tambahan berupa pembekuan usaha hingga pencabutan izin. Konstruksi strict liability diterapkan terutama dalam hal kelalaian korporasi menjaga keamanan data pribadi.

DAFTAR PUSTAKA

Adcovates, K. (2024). Kasus-Kasus Awal dari Implementasi Sanksi Pidana dalam UU PDP.

APJII. (2024). *Jumlah pengguna internet Indonesia tembus 221 juta orang*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Ayustin, L. Z. (2022). Perbuatan pidana mengakses tanpa hak ke sistem elektronik orang lain menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Jurnal Ilmiah Mahasiswa Hukum (JIMHUM)*, *2*(11), 1–9.

Azhar, M. S. (2025). *Polda Metro menangani 2.597 laporan kejahatan siber dengan kerugian Rp24,3 miliar*. Metro TV News. https://www.metrotvnews.com/read/KdZCj5JX-polda-metro-menangani-2-597-laporan-kejahatan-siber-dengan-kerugian-rp24-3-miliar

Benuf, K., & Azhar, M. (2020). Metodologi penelitian hukum sebagai instrumen mengurai permasalahan hukum kontemporer. *Jurnal Gema Keadilan*, *7*, 20–33.

Elnizar, N. E. (2023). *Empat hal yang harus perusahaan perhatikan soal pelindungan data pribadi*. Hukum Online.

Fachri, F. K. (2024). *Deputi BSSN: Penyebab kebocoran data pribadi biasanya kepatuhan hukum yang kurang*. Hukum Online. https://www.hukumonline.com/berita/a/deputi-bssn--penyebab-kebocoran-data-pribadi-biasanya-kepatuhan-hukum-yang-kurang-lt6644ead0802f8/?page=all

Firdaus, I. (2022). Upaya perlindungan hukum hak privasi terhadap data pribadi dari kejahatan peretasan. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, *4*(2), 23–31.

Kurnianingrum, T. P. (2020). Urgensi pelindungan data pribadi konsumen di era ekonomi digital. *Kajian*, *25*(3), 197–216.

Kurniawan, R., & D, S. N. I. S. (2014). Pertanggungjawaban pidana korporasi berdasarkan asas strict liability (Studi pembaharuan hukum pidana lingkungan hidup). *Jurnal Yuridis, 1*(2), 153–168.

Primanta, A. I. (2020). Pertanggungjawaban pidana pada penyalahgunaan data pribadi. *Jurist-Diction*, *3*(4), 1431–1452. https://doi.org/10.20473/jd.v3i4.20214

Pratiwi, F. Y., & Miarsa, F. R. D. (2025). Urgensi edukasi publik dalam menangkal penyalahgunaan data pribadi. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(2), 1342–1349.

Ramli, A. M. (2026). *Ketentuan penyadapan dalam KUHP pengganti aturan UU ITE*. Kompas Nasional. https://nasional.kompas.com/read/2026/01/08/06100021/ketentuan-penyadapan-dalam-kuhp-pengganti-aturan-uu-ite

Rizqiyanto, N., Rohman, A. F., & Raya, F. A. M. (2024). Politik hukum pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, *2*(2), 1–14.

SAFEnet. (2025). *Polisi siber picu lonjakan pelanggaran hak digital selama triwulan III 2025*. https://safenet.or.id/id/2025/10/polisi-siber-picu-lonjakan-pelanggaran-hak-digital-selama-triwulan-iii-2025/

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2).

Suhaemin, A., & Muslih, M. (2021). Karakteristik cybercrime di Indonesia. *Edulaw: Journal of Islamic Law and Jurisprudence*, *2*(1), 15–26.

Tempo. (2025). *Polisi bongkar sindikat aktivasi SIM card pakai KTP dan KK orang lain*. https://www.tempo.co/hukum/polisi-bongkar-sindikat-aktivasi-sim-card-pakai-ktp-dan-kk-orang-lain-1215199

Tim Hukum Online. (2023). *Apa itu doxing dan bagaimana jerat hukumnya?* https://www.hukumonline.com/berita/a/jerat-hukum-pelaku-doxing-lt624d35e6c4f7a/

Universitas Medan Area. (2023). *Tindak pidana dalam era teknologi: Perlindungan data pribadi dan keamanan siber*. Fakultas Hukum Universitas Medan Area. https://hukum.uma.ac.id/tindak-pidana-dalam-era-teknologi-perlindungan-data-pribadi-dan-keamanan-siber/

Watkat, F. X., Ingratubun, M. T., & Apriyanti, A. (2024). Perlindungan data pribadi melalui penerapan sistem hukum pidana di Indonesia. *Jurnal Hukum Ius Publicum*, *5*(1).