

PERTANGGUNGJAWABAN PIDANA ATAS PENGGUNAAN DATA PRIBADI SECARA MELAWAN HUKUM: ANALISIS YURIDIS TERHADAP UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Criminal Liability for the Unlawful Use of Personal Data: A Juridical Analysis of Law Number 27 of 2022 on Personal Data Protection

Santika Aprilia^{1*}

Siti Marwiyah²

Dedi Wardana Nasution³

Muhammad Yustino
Aribawa⁴

*1-4 Fakultas Hukum, Universitas Dr.
Soetomo Surabaya, Indonesia

*email:

authorsantikaaprilia904@gmail.com

Lisensi:CC-BY



Abstrak

Perkembangan teknologi informasi dan juga komunikasi sudah meningkatkan pemanfaatan data pribadi didalam bermacam layanan digital, namun juga meningkatkan risiko penyalahgunaan dan juga bocornya data pribadi. Kondisi itu memberi dorongan terbentuknya Undang-Undang Nomor 27 Tahun 2022 terkait Perlindungan Data Pribadi selaku dasar hukum yang mengelola perlindungan data pribadi, termasuk pemakaian data pribadi dengan menentang hukum dan pertanggungjawabannya pidana terhadap pelakunya. Tujuan penelitian yakni guna melaksanakan analisis kualifikasi yuridis tindakan pidana pemakaian data pribadi dengan menentang hukum berdasarkan Undang-Undang Nomor 27 Tahun 2022 terkait Perlindungan Data Pribadi serta melaksanakan analisis permintaan tanggungjawab pidana terhadap pelaku tindakan pidana tersebut. Metode penelitian yang dipakai yakni penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan juga pendekatan konseptual (*conceptual approach*), yang dilaksanakan analisis dengan deskriptif-analitis. Hasil dari penelitian mengungkapkan bahwasanya penggunaan data pribadi secara melawan hukum dikualifikasikan sebagai tindak pidana melalui Pasal 65 dan juga Pasal 66 dengan ancaman pidana dalam Pasal 67 serta pidana tambahan dalam Pasal 68. Pertanggungjawaban pidana dilandasi dengan asas *geen straf zonder schuld*, sehingga pembedaan hanya bisa dilakukan jikalau terbukti adanya perbuatan pidana, kesalahan, kemampuan bertanggungjawab, dan juga tidak ada alasan pembenar maupun alasan pemaaf. Pertanggungjawaban pidana dapat dikenakan terhadap orang perseorangan maupun korporasi selaras dengan ketentuan peraturan perundang-undangan yang ada.

Kata Kunci:

Perlindungan Data Pribadi,
Pertanggungjawaban Pidana,
Tindak Pidana,
Data Pribadi,
Penyelenggara Sistem Elektronik.

Keywords:

Personal Data Protection,
Criminal Liability,
Crime,
Personal Data,
Electronic System Operators.

Abstract

The development of information and communication technology has increased the use of personal data in various digital services, but also increases the risk of misuse and leakage of personal data. This situation led to the enactment of Law Number 27 of 2022 concerning Personal Data Protection as the legal basis governing personal data protection, including the unlawful use of personal data and the criminal liability of perpetrators. This study aims to analyze the legal qualifications of the crime of unlawful use of personal data under Law Number 27 of 2022 concerning Personal Data Protection and analyze the criminal liability of perpetrators of such crimes. The research method used is normative legal research with a statutory approach and a conceptual approach, analyzed descriptively and analytically. The research results show that the unlawful use of personal data is classified as a criminal offense under Articles 65 and 66, with penalties under Article 67 and additional penalties under Article 68. Criminal liability is based on the principle of "*geen straf zonder schuld*," meaning that punishment can only be imposed if there is evidence of a criminal act, fault, capacity to take responsibility, and the absence of justification or excuse. Criminal liability can be imposed on individuals and corporations in accordance with applicable laws and regulations.

PENDAHULUAN

Transformasi digital telah mengubah cara masyarakat Indonesia bertransaksi, berkomunikasi, dan mengakses layanan publik. Perbankan, perdagangan elektronik, layanan kesehatan, hingga administrasi kependudukan kini bertumpu pada pengumpulan dan pengolahan data pribadi didalam skala besar. Pergeseran ini menempatkan data pribadi jadi aset yang bernilai ekonomi tinggi sekaligus objek yang rentan disalahgunakan. Dalam beberapa tahun terakhir, publik Indonesia dihadapkan pada rentetan insiden kebocoran data yang melibatkan sektor privat maupun instansi pemerintah, mulai dari dugaan kebocoran data pengguna platform perdagangan elektronik, data peserta jaminan sosial kesehatan, data pemilih pada penyelenggara pemilihan umum, hingga insiden pada Pusat Data Nasional yang berdampak luas terhadap layanan publik (Sugiantari et al., 2024). Rangkaian peristiwa tersebut menegaskan bahwa kerentanan data pribadi bukan lagi terkait teknis semata, bahkan sudah jadi persoalan hukum yang menuntut kejelasan mengenai siapa yang dapat dimintai pertanggungjawaban dan dalam bentuk apa pertanggungjawaban tersebut dibebankan.

Fenomena tersebut tidak berdiri sendiri di Indonesia. Secara global, negara-negara maju maupun berkembang telah lebih dahulu menghadapi persoalan serupa dan meresponsnya melalui kerangka hukum yang komprehensif. Uni Eropa melalui *General Data Protection Regulation* (GDPR) menempatkan prinsip akuntabilitas dan sanksi administratif yang berat sebagai instrumen utama, sementara sejumlah yurisdiksi Asia seperti Singapura melalui *Personal Data Protection Act* telah menerapkan rezim perlindungan data sejak lebih dari satu dekade lalu (Sudarwanto & Kharisma, 2021). Kajian komparatif membuktikan bahwasanya UU PDP Indonesia banyak mengambil struktur dan prinsip GDPR, terutama menyangkut hak subjek data dan kewajiban pengendali data, meskipun implementasi teknis atas sanksi administratif dan pidana di Indonesia belum sepenuhnya terstruktur secara jelas dibandingkan model Eropa tersebut (Kurniawan et al., 2023). Karakteristik kejahatan data pribadi yang bersifat lintas batas turut menambah kerumitan penegakan hukum, karena pelaku dapat memanfaatkan infrastruktur digital di luar yurisdiksi Indonesia sehingga penegakan hukum pidana domestik menghadapi keterbatasan instrumen kerja sama internasional. Dengan demikian, persoalan yang dihadapi Indonesia bukan sekadar menyusun norma pidana, melainkan juga menyelaraskan norma tersebut dengan realitas kejahatan siber yang berkarakter transnasional.

Urgensi perlindungan data pribadi di Indonesia makin kuat mengingat data pribadi berhubungan erat dengan hak privasi yang dijamin sebagai hak konstitusional melewati Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Sebelum adanya UU PDP, pengaturan terkait data pribadi terdistribusi di bermacam peraturan sektoral, contohnya Undang-Undang Informasi dan Transaksi Elektronik, tanpa satu kerangka hukum yang secara khusus mengatur pertanggungjawaban pidana atas penyalahgunaan data pribadi (Hisbulloh, 2021). Kekosongan tersebut menimbulkan ketidakpastian hukum, karena korban penyalahgunaan data pribadi kerap kesulitan menentukan dasar hukum pidana yang tepat untuk menjerat pelaku, sementara aparat penegak hukum juga menghadapi kendala dalam menafsirkan unsur-unsur delik yang relevan. Kehadiran UU PDP, khususnya Pasal 65 hingga Pasal 70, dimaksudkan untuk mengisi kekosongan tersebut dengan merumuskan secara khusus perbuatan mendapat, mengatakan, memakai, dan memalsukan data pribadi dengan menentang hukum sebagai tindak pidana, sekaligus menegaskan kemungkinan pidana terhadap korporasi sebagai penyelenggara sistem elektronik.

Kajian akademik mengenai UU PDP telah berkembang cukup pesat sejak undang-undang tersebut disahkan. Sebagian penelitian memfokuskan pembahasan pada pertanggungjawaban penyelenggara sistem elektronik didalam kasus kebocoran data yang bersumber dari kelalaian administratif, dengan menyoroti ketidakjelasan pengaturan pertanggungjawaban pidana pada Pasal 46 UU PDP yang cenderung menempatkan kegagalan perlindungan data semata-mata sebagai objek sanksi administratif (Husri et al., 2026). Penelitian lain menitikberatkan pada bentuk larangan dan juga

sanksi pidana terhadap pendapatan dan juga pemakaian data pribadi dengan menentang hukum, namun cenderung berhenti pada pemaparan norma tanpa menguraikan secara mendalam konstruksi unsur objektif dan subjektif yang membedakan setiap ayat dalam Pasal 65 (Mamadoa et al., 2025). Sejumlah kajian lain berfokus pada aspek kepastian hukum bagi korban dan kelembagaan pengawasan (Solihin, 2023; Manurung & Thalib, 2022), pada rekonstruksi tanggung jawab korporasi publik semata (Darmadi & Dananjaya, 2023; Sugiantari et al., 2024), atau pada perbandingan norma UU PDP dengan GDPR dari sudut pandang kepatuhan korporasi (Utama & Yulistiyani, 2026). Dari penelusuran tersebut tampak bahwa kajian terdahulu pada umumnya membahas pertanggungjawaban pidana secara parsial, baik hanya dari sisi kelalaian penyelenggara sistem elektronik, hanya dari sisi normatif larangan dan sanksi, maupun hanya dari sudut pandang perbandingan hukum, tanpa menghubungkan secara sistematis kualifikasi yuridis unsur delik pada Pasal 65 dan Pasal 66 dengan konstruksi pertanggungjawaban pidana yang membedakan orang perseorangan dan korporasi sekaligus mengujinya terhadap batas antara kesengajaan dan kelalaian.

Celah tersebut menjadi dasar novelty artikel ini. Mempunyai perbedaan dengan penelitian terdahulu yang condong memberi pemisah antara pembahasan kualifikasi delik dan juga pertanggungjawaban pidana, artikel ini menawarkan pembacaan yang menghubungkan keduanya secara sistematis: bahwa konstruksi delik berlapis didalam Pasal 65 dan juga Pasal 66 UU PDP hanya dapat dipahami secara utuh apabila dikaitkan dengan batas pertanggungjawaban pidana yang secara konsisten mensyaratkan pembuktian kesengajaan, sehingga kegagalan sistem yang murni bersifat kelalaian administratif berada di luar jangkauan pidana UU PDP dan harus diselesaikan melalui jalur sanksi administratif atau perdata. Novelty ini lahir bukan dari asumsi awal, melainkan dari hasil analisis terhadap rumusan pasal itu sendiri, yang secara konsisten merumuskan unsur "dengan sengaja" pada setiap delik tanpa merumuskan padanan delik kealpaan, sebuah pilihan kebijakan kriminal yang belum banyak diuraikan secara eksplisit dalam literatur terdahulu, khususnya dalam kaitannya dengan kriteria atribusi kesalahan korporasi berdasarkan doktrin identifikasi yang dianut Pasal 70 UU PDP.

Sesuai dengan uraian tadi, penelitian ini merumuskan dua permasalahan: pertama, bagaimana kualifikasi yuridis tindak pidana penggunaan data pribadi secara melawan hukum dalam UU PDP; dan kedua, bagaimana bentuk pertanggungjawaban pidana pada pelaku tindakan pidana tersebut, baik yang berstatus orang perseorangan maupun korporasi. Selaras dengan rumusan masalah itu, artikel ini mempunyai tujuan guna melaksanakan analisis kualifikasi yuridis tindakan pidana penggunaan data pribadi dengan menentang hukum sesuai UU PDP serta menganalisis konstruksi pertanggungjawaban pidana yang dapat dibebankan kepada pelakunya, sekaligus mengidentifikasi tantangan penerapannya didalam praktik penegakan hukum di Indonesia.

METODE PENELITIAN

Penelitian ini memakai metode penelitian hukum normatif (yuridis normatif), yakni penelitian yang dilaksanakan dengan mengkaji norma hukum, peraturan perundang-undangan, doktrin, dan juga teori hukum yang berkaitan dengan pertanggungjawaban pidana atas pemakaian data pribadi dengan menentang hukum. Penelitian berfokus pada norma yang mengelola larangan pemakaian data pribadi dengan menentang hukum serta konsekuensi pidana bagi pelakunya sebagaimana diatur dalam UU PDP. Dua pendekatannya digunakan dengan bersamaan. Pendekatan perundang-undangan (*statute approach*) diterapkan dengan menelaah UU PDP, Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan juga Transaksi Elektronik, dan juga Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 selaku kerangka konstitusional. Pendekatan konseptual (*conceptual approach*) diterapkan dengan mengkaji doktrin pertanggungjawaban pidana, teori tindakan pidana, serta konsep informational self-determination guna memahami hakikat kepentingan hukum yang dilindungi UU PDP.

Bahan hukum didalam penelitian ini diantaranya ada tiga jenis. Bahan hukum primer yakni UUD NRI Tahun 1945, KUHP, UU PDP, dan juga Undang-Undang Informasi dan Transaksi Elektronik. Bahan hukum sekunder meliputi buku-buku hukum pidana dan juga hukum perlindungan data pribadi, artikel jurnal ilmiah nasional dan internasional yang terbit dalam rentang tahun 2021 hingga 2026, hasil dari penelitian sebelumnya, serta dari pendapatnya ahli hukum. Bahan hukum tersier yakni kamus hukum, Kamus Besar Bahasa Indonesia, dan juga sumber pendukung lainnya yang relevan. Prosedur pengumpulan bahan hukum dilaksanakan melewati studi kepustakaan (*library research*) dengan menelusuri, mengidentifikasi, dan juga menginventarisasi bahan hukum yang relevan, yang selanjutnya diklasifikasikan berdasarkan hierarki dan sistematika rumusan masalah untuk memudahkan proses interpretasi. Analisis bahan hukum dilaksanakan dengan kualitatif memakai metode deskriptif-analitis, yakni penguraian, menginterpretasikan, dan juga menghubungkan ketentuan peraturan perundang-undangan, teori hukum, dan juga pendapatnya para ahli guna menjawab rumusan masalah, dilengkapi dengan kajian atas beberapa kasus kebocoran data pribadi yang sudah jadi perhatian publik sebagai ilustrasi penerapan norma.

HASIL DAN PEMBAHASAN

I. Kualifikasi Yuridis Tindak Pidana Penggunaan Data Pribadi Secara Melawan Hukum

Kualifikasi tindak pidana pada hakikatnya merupakan proses menilai apakah suatu perbuatan konkret memenuhi seluruh unsur delik yang dirumuskan pembentuk undang-undang, bukan sekadar penilaian moral atas pantas-tidaknya perbuatan tersebut dihukum. Prinsip ini bertumpu pada asas legalitas (*nullum crimen, nulla poena sine lege*) yang menempatkan rumusan undang-undang, bukan rasa keadilan semata, sebagai batu uji pertama. Oleh karena itu, sebelum menilai apakah suatu perbuatan penggunaan data pribadi merupakan kejahatan, kerangka norma harus ditegakkan terlebih dahulu melalui Pasal 65 sampai dengan Pasal 68 UU PDP, kemudian pendapat ahli dan contoh kasus ditempatkan sebagai alat uji terhadap kerangka tersebut.

Norma dasar yang menopang seluruh delik dalam UU PDP adalah unsur "secara melawan hukum". Unsur ini berfungsi sebagai saringan pertama yang memisahkan pemrosesan data pribadi yang sah dari pemrosesan yang dapat dipidana; tidak setiap pengumpulan, pengungkapan, atau penggunaan data pribadi dapat dipidana, melainkan hanya perbuatan yang bertentangan dengan hukum objektif maupun hak subjektif pemilik data. Doktrin hukum pidana mengenal dua dimensi sifat menentang hukum (*wederrechtelijkheid*), yakni menentang hukum formal yang mensyaratkan pertentangan tegas dengan ketentuan tertulis, dan melawan hukum materiil yang menilai pertentangan perbuatan dengan nilai keadilan dan kepentingan hukum yang hendak dilindungi (Moeljatno, 2018; Prasetyo, 2022). Secara lebih khusus pada ranah data pribadi, kepentingan hukum tersebut dapat dimaknai sebagai kendali individu atas informasi pribadinya (*informational self-determination*), yaitu hak untuk menentukan bagaimana datanya dikumpulkan, digunakan, disimpan, dan diungkapkan (Rosadi, 2021). Ketiga pandangan tersebut, apabila dibaca secara sistematis, saling melengkapi: rumusan formal Pasal 65 sampai dengan Pasal 68 UU PDP memberikan kepastian hukum tentang perbuatan yang dilarang, sementara dimensi materiil dari sifat melawan hukum menjelaskan mengapa perbuatan tersebut layak dipidana, yaitu karena merampas kendali subjek data atas informasi pribadinya, yang merupakan wujud konkret hak konstitusional atas perlindungan diri pribadi seperti yang ada didalam Pasal 28G ayat (1) UUD NRI Tahun 1945.

Konsekuensi metodologis dari penempatan hak privasi sebagai kepentingan hukum yang dilindungi adalah bahwa setiap kali unsur "melawan hukum" hendak dibuktikan, aparat penegak hukum tidak boleh berhenti pada pertanyaan formal "apakah ada izin", melainkan harus menilai apakah tindakan tersebut menyerang kendali subjek data atas informasinya. Cara baca inilah yang digunakan secara konsisten pada analisis terhadap Pasal 65 dan Pasal 66 berikut ini.

Pasal 65 UU PDP merumuskan tiga bentuk perbuatan yang dilarang, yaitu mendapatkan ataupun menimbun data pribadi bukan miliknya (ayat 1), mengatakan data pribadi bukan miliknya (ayat 2), dan menggunakan data pribadi bukan miliknya (ayat 3), yang seluruhnya dilakukan dengan sengaja dan melawan hukum. Ketiga ayat tersebut bukan norma yang berdiri sendiri-sendiri, melainkan representasi tiga tahap dalam satu siklus pemrosesan data pribadi: penguasaan awal, penyebaran kepada pihak lain, dan pemanfaatan data untuk suatu tujuan. Ratio legis pemisahan ini memungkinkan hukum pidana menjangkau pelaku pada titik mana pun ia masuk ke dalam rantai penyalahgunaan data, tanpa harus menunggu pelaku menyelesaikan seluruh tahapan tersebut.

Unsur "setiap orang" pada ketiga ayat bersifat umum, mencakup baik pihak eksternal yang tidak ada hubungannya dengan data tersebut maupun pihak internal, seperti pegawai bank, tenaga kesehatan, atau pengelola sistem elektronik, yang semula memiliki akses sah namun menyalahgunakannya di luar tujuan pemrosesan yang telah disepakati. Keluasan cakupan subjek ini merupakan pilihan kebijakan kriminal yang tepat, sebab dalam praktik, kebocoran dan penyalahgunaan data pribadi lebih sering berasal dari penyalahgunaan akses oleh orang dalam (insider abuse) daripada peretasan murni dari luar sistem, sebagaimana tercermin pula pada kajian mengenai kebocoran data nasabah perbankan yang kerap melibatkan pihak internal (Rahmawati et al., 2023).

Unsur "dengan sengaja" (opzet) mensyaratkan bahwa pelaku mengetahui data yang diperoleh, diungkapkan, atau digunakan adalah milik orang lain dan menghendaki perbuatannya, sehingga kegagalan sistem yang murni bersifat teknis, tanpa kehendak untuk menguasai atau menyebarkan data, berada di luar jangkauan pasal ini dan harus diuji melalui bentuk kesalahan lain, seperti kealpaan, yang justru tidak dirumuskan sebagai delik dalam UU PDP. Ketidadaan rumusan delik kealpaan ini, apabila dikaitkan dengan asas legalitas, berimplikasi bahwa kebocoran data akibat kelalaian murni suatu penyelenggara sistem elektronik tidak dapat dipidana melalui Pasal 65, melainkan harus diselesaikan melalui jalur sanksi administratif sebagaimana diatur dalam bab tersendiri UU PDP atau melalui pertanggungjawaban perdata (Husri et al., 2026).

Secara khusus, Pasal 65 ayat (1) turut merumuskan unsur "dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian", yang menempatkan delik ini sebagai delik formil dengan unsur akibat potensial, bukan akibat nyata. Kasus dugaan kebocoran data pengguna pada salah satu platform perdagangan elektronik nasional memperlihatkan penerapan konstruksi ini secara jelas: begitu data pengguna diperoleh tanpa hak dan ditawarkan melalui forum daring, tindak pidana telah sempurna tanpa perlu menunggu pembuktian kerugian finansial nyata pada setiap korban, karena potensi kerugian berupa pencurian identitas dan penipuan sudah cukup memenuhi rumusan pasal (Utami et al., 2025). Ratio legis konstruksi delik formil semacam ini terletak pada karakteristik data pribadi yang sangat mudah digandakan dan disebarluaskan melalui sistem elektronik, sehingga penegakan hukum yang menunggu kerugian nyata justru akan datang terlambat untuk melindungi kepentingan hukum yang dimaksud.

Pasal 65 ayat (2) memindahkan fokus perlindungan pada tahap pengungkapan data yang telah berada dalam penguasaan seseorang, sehingga menjangkau modus penyalahgunaan akses oleh pihak internal, sebagaimana tampak dalam berbagai dugaan kebocoran data peserta pada lembaga penyelenggara jaminan sosial (Husri et al., 2026). Dalam kasus semacam itu, unsur "mengungkapkan" terpenuhi sejak data peserta ditawarkan atau disebarluaskan melalui forum digital, terlepas dari apakah kerugian finansial konkret telah dialami oleh seluruh pihak yang datanya tersebar. Karakter Pasal 65 ayat (2) sebagai delik formil menegaskan bahwa pembuktian cukup diarahkan pada perbuatan pengungkapan itu sendiri, bukan pada akibat yang benar-benar terjadi.

Adapun Pasal 66 UU PDP mengatur delik pemalsuan data pribadi, yaitu perbuatan membuat, menggunakan, atau menyebarkan data pribadi palsu dengan tujuan mencari untung dirinya sendiri ataupun orang lainnya yang bisa

menyebabkan kerugian. Berbeda dari Pasal 65 yang berpusat pada perlindungan kendali atas data yang benar-benar milik seseorang, Pasal 66 melindungi keaslian dan integritas informasi identitas yang beredar dalam sistem elektronik. Kedua pasal ini pada praktiknya kerap saling terkait, sebagaimana tampak pada modus pemalsuan identitas digital menggunakan Nomor Induk Kependudukan dan data kependudukan orang lain untuk membuka rekening, mengajukan pinjaman berbasis teknologi finansial, atau melakukan transaksi elektronik atas nama korban (Silalahi & Dameria, 2023). Perbuatan tersebut umumnya diawali dengan pelanggaran Pasal 65 berupa perolehan data secara melawan hukum, kemudian berlanjut pada pemalsuan sebagaimana diatur Pasal 66, sehingga berpotensi menimbulkan efek berantai berupa tindak pidana lanjutan, seperti penipuan atau pencucian uang berbasis identitas palsu. Oleh karena itu, Pasal 65 dan Pasal 66 semestinya dibaca sebagai dua sisi dari satu kepentingan hukum yang sama, yaitu integritas hubungan antara individu dan datanya, bukan sebagai dua delik yang terpisah secara substansial.

Pasal 67 dan Pasal 68 UU PDP merupakan norma pemidanaan (strafbepaling) yang melengkapi rumusan delik pada Pasal 65 dan Pasal 66. Pasal 67 mengatur ancaman pidana atas pelanggaran Pasal 65, yaitu pidana penjara paling panjang lima tahun dan/ataupun denda paling tinggi Rp5.000.000.000,00 untuk pelanggaran ayat (1) dan juga ayat (3), serta pidana penjara paling panjang empat tahun dan/ataupun denda paling tinggi Rp4.000.000.000,00 untuk pelanggaran ayat (2). Pasal 68 mengatur ancaman pidana atas pelanggaran Pasal 66, yaitu pidana penjara paling panjang enam tahun dan/ataupun denda paling tinggi Rp6.000.000.000,00. Perbedaan ancaman pidana antarayat pada Pasal 67 mencerminkan penerapan asas proporsionalitas yang konsisten dengan pembagian tahap siklus data: ancaman yang relatif lebih rendah pada ayat (2) dibandingkan ayat (1) dan juga ayat (3) menunjukkan penilaian pembentuk undang-undang bahwa perbuatan memperoleh dan memanfaatkan data secara aktif membawa potensi kerugian yang lebih besar daripada sekadar mengungkapkannya, meskipun ketiganya tetap dirumuskan sebagai delik formil. Ancaman pidana yang lebih tinggi pada Pasal 68 dibandingkan seluruh ayat Pasal 67 juga konsisten dengan penilaian bahwa pemalsuan data pribadi berpotensi menimbulkan efek berantai berupa tindak pidana lanjutan yang memanfaatkan identitas palsu tersebut.

Ancaman pidana didalam Pasal 67 dan juga Pasal 68 perlu dibaca bersama Pasal 69, yang memungkinkan penjatuhan pidana tambahan yakni perampasan keuntungan dan/ataupun harta kekayaan yang asalnya dari tindakan pidana dan juga pembayaran ganti kerugian. Ratio legis pidana tambahan itu adalah menghilangkan motif ekonomi yang pada umumnya melatarbelakangi tindak pidana data pribadi, sehingga sanksi tidak berhenti pada aspek pembalasan (retributive), tetapi juga menghilangkan manfaat ekonomi yang telah dinikmati pelaku. Apabila dibandingkan dengan ancaman pidana didalam Undang-Undang Informasi dan Transaksi Elektronik, misalnya ketentuan mengenai perubahan data elektronik tanpa hak dengan ancaman pidana penjaranya paling panjang delapan tahun, tampak bahwa kedua undang-undang menempatkan bobot yang relatif berat terhadap kejahatan berbasis data elektronik, meskipun titik berat kepentingan hukum yang dilindungi berbeda: UU ITE menitikberatkan pada integritas sistem elektronik, sedangkan UU PDP menitikberatkan pada hak individu atas datanya. Tumpang tindih ancaman pidana antara kedua undang-undang ini idealnya diselesaikan melalui penerapan asas *lex specialis* dengan konsisten dari aparat penegak hukum, agar tidak terjadi duplikasi penuntutan atas perbuatan yang secara substansial sama.

Apabila seluruh rumusan Pasal 65 dan Pasal 66 disarikan ke dalam struktur teori tindak pidana, tampak pemisahan yang konsisten antara unsur objektif (*actus reus*), berupa perbuatan memperoleh, mengungkapkan, menggunakan, membuat, atau memalsukan data pribadi, dan unsur subjektif (*mens rea*), berupa kesengajaan serta maksud menguntungkan diri sendiri ataupun orang lainnya. Dalam praktik pembuktian, unsur objektif umumnya dibuktikan melalui bukti elektronik dan hasil digital forensik, sedangkan unsur subjektif disimpulkan dari rangkaian perbuatan, pola akses, dan tujuan yang hendak dicapai pelaku, karena keadaan batin seseorang jarang dapat dibuktikan secara langsung.

Hubungan antara kedua unsur ini menegaskan bahwa UU PDP menganut asas *geen straf zonder schuld*: seseorang tidak bisa dipidana hanya karena secara objektif menguasai atau mengakses data pribadi punya orang lain, tanpa terbuktinya kesengajaan dan juga sifat menentang hukum. Konsistensi struktur delik semacam ini penting justru karena akses terhadap data pribadi dalam ekosistem digital modern sangat sulit dihindari sepenuhnya oleh siapa pun yang bekerja pada sistem elektronik; tanpa penekanan pada unsur subjektif, penerapan UU PDP berisiko menjerat pihak yang sekadar memiliki akses administratif tanpa kehendak jahat.

Berdasarkan keseluruhan analisis di atas, kualifikasi yuridis tindak pidana penggunaan data pribadi secara melawan hukum menurut UU PDP didirikan diatas tiga pilar yang saling berhubungan: konstruksi delik berlapis pada Pasal 65 yang mengikuti siklus perolehan, pengungkapan, dan penggunaan data; perlindungan terhadap keaslian dan integritas data melalui Pasal 66; dan sistem ancaman pidana proporsional pada Pasal 67 dan Pasal 68 yang menegakkan asas proporsionalitas sekaligus fungsi preventif hukum pidana. Ketiga pilar tersebut hanya dapat diterapkan apabila unsur objektif dan unsur subjektif terbukti secara kumulatif, sehingga penggunaan data pribadi secara melawan hukum bukanlah *strict liability offence*, melainkan delik yang mensyaratkan kesalahan (*offence based on fault*).

2. Pertanggungjawaban Pidana Terhadap Pelaku Penggunaan Data Pribadi Secara Melawan Hukum

Pertanggungjawaban pidana tidak lahir semata-mata karena tercukupinya unsur-unsur tindakan pidana, melainkan juga mensyaratkan ada kesalahan (*schuld*) yang bisa dipertanggungjawabkan kepada pelaku. Prinsip tersebut dikenal sebagai asas *geen straf zonder schuld* ataupun *nulla poena sine culpa*, yang mengandung makna bahwasanya seseorang hanya bisa dijatuhi pidana apabila terdapat bukti melakukan perbuatan yang dilarang undang-undang dan pada saat yang sama memiliki kesalahan yang secara hukum dapat dicela (Hiariej, 2021; Lamintang, 2019; Prasetyo, 2022). Pidanaan tidak hanya didasarkan pada hubungan antara pelaku dengan perbuatan pidana (*actus reus*), tetapi juga pada hubungan batin antara pelaku dengan perbuatan tersebut (*mens rea*). Asas ini merupakan salah satu prinsip fundamental hukum pidana modern karena berfungsi membatasi kewenangan negara dalam menjatuhkan pidana sekaligus menjamin bahwa pidanaan hanya dikenakan kepada pihak yang benar-benar layak dipersalahkan secara hukum (Chazawi, 2019). Simons merumuskan bahwa pertanggungjawaban pidana dibangun atas tiga komponen kumulatif, yaitu perbuatan yang menjawab rumusan delik, keahlian bertanggungjawab (*toerekeningsvatbaarheid*), dan kesalahan dalam bentuk kesengajaan maupun kealpaan (Lamintang, 2019). Dalam konteks UU PDP, unsur pertama diwujudkan melalui pembuktian perbuatan sebagaimana dirumuskan Pasal 65 sampai dengan Pasal 68, sedangkan unsur kedua dan juga ketiga berkaitan dengan kemampuan bertanggung jawab dan pembuktian kesengajaan pelaku.

Pilihan pembentuk undang-undang untuk merumuskan seluruh delik dalam UU PDP sebagai delik sengaja, bukan delik kealpaan, memiliki implikasi ganda: disatu sisi memberi kepastian hukum dan juga perlindungan terhadap tersangka dari pidanaan yang terlampau luas, tetapi di sisi lain menyisakan celah bagi penyelenggara sistem elektronik yang lalai menjaga keamanan data untuk lolos dari pertanggungjawaban pidana, sehingga kelalaian semacam itu hanya dapat dijangkau melalui sanksi administratif atau gugatan perdata, bukan melalui ketentuan pidana UU PDP. Dengan demikian, asas *geen straf zonder schuld* dalam konteks UU PDP berfungsi ganda: melindungi individu dari kriminalisasi berlebihan, sekaligus membatasi jangkauan hukum pidana hanya pada penyalahgunaan data yang benar-benar dikehendaki pelakunya.

Subjek hukum yang paling umum dalam penerapan ketentuan pidana UU PDP adalah orang perseorangan. Sebagai subjek hukum pidana, orang perseorangan bisa diminta tanggungjawab pidananya jika ada bukti melaksanakan perbuatan yang menjawab rumusan Pasal 65 sampai dengan Pasal 68 serta memenuhi syarat pertanggungjawaban pidana menurut doktrin hukum pidana. Seseorang tidak bisa dipidana hanya dikarenakan terlibat dalam sebuah peristiwa pidana,

melainkan harus terlebih dahulu dibuktikan bahwa ia mempunyai keahlian bertanggungjawab, melaksanakan perbuatan dengan kesengajaan, serta tidak terdapat alasan pembeda ataupun alasan pemaaf yang menghilangkan pertanggungjawaban pidananya (Moeljatno, 2018). Kemampuan bertanggung jawab menjadi aspek yang sangat penting dalam tindak pidana penggunaan data pribadi karena penyalahgunaan data umumnya dilakukan melalui tindakan yang memerlukan pengetahuan, perencanaan, dan pemanfaatan teknologi informasi, sehingga terdapat hubungan psikologis yang jelas antara pelaku dan perbuatannya (Hiariej, 2021).

Dalam praktik, penyalahgunaan data pribadi oleh orang perseorangan berkembang dalam berbagai modus seiring pesatnya transformasi digital, antara lain penggunaan identitas orang lain untuk membuka rekening bank, mengajukan pinjaman berbasis teknologi finansial, membuat akun media sosial palsu, melakukan phishing, membeli data hasil kebocoran untuk kepentingan komersial, hingga memanfaatkan data kependudukan yang diperoleh secara melawan hukum untuk memperoleh fasilitas keuangan (Widayanti, 2022; Edbert & Putra, 2023). Salah satu bentuk penyalahgunaan yang paling relevan dengan konstruksi Pasal 65 dan Pasal 66 secara bersamaan adalah pemalsuan identitas digital dengan memanfaatkan Nomor Induk Kependudukan atau foto identitas milik orang lainnya tanpa persetujuan pemilik data untuk membuka rekening atau memperoleh pinjaman daring atas nama korban. Perbuatan tersebut tidak hanya membentuk unsur penggunaan data pribadi dengan menentang hukum, tetapi juga berpotensi memenuhi unsur tindak pidana lain, seperti pemalsuan dokumen elektronik atau penipuan, sehingga penerapan UU PDP dalam praktik sering kali berjalan beriringan dengan penerapan ketentuan pidana umum dalam KUHP.

Karakteristik kejahatan data pribadi yang umumnya melibatkan struktur organisasi, sistem teknologi informasi, dan proses bisnis yang berada dalam kendali korporasi menuntut agar pertanggungjawaban pidana tidak berhenti pada pelaku individual, melainkan turut mempertimbangkan tanggung jawab korporasi sebagai entitas hukum yang memperoleh manfaat dari kegiatan tersebut (Arief, 2018). Secara normatif, Pasal 70 UU PDP menentukan bahwa apabila tindakan pidana seperti dijabarkan didalam Pasal 67 dan juga Pasal 68 dilaksanakan oleh korporasi, pidana bisa diberikan pada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat (beneficial owner), dan/ataupun korporasi itu sendiri. Ketentuan tersebut menunjukkan bahwa UU PDP menerapkan pertanggungjawaban pidana multipihak (multiple criminal liability) yang memungkinkan lebih dari satu subjek hukum dimintai pertanggungjawaban atas tindak pidana yang sama, sepanjang masing-masing memenuhi unsur pertanggungjawaban pidana. Terhadap korporasi juga bisa diberi pidana denda dengan jumlah paling tinggi sepuluh kali lipat dari ancaman pidana denda maksimum yang ditentukan dalam ketentuan pidana yang dilanggar.

Penerapan ketentuan tersebut dapat diuji melalui bermacam kasus dugaan kebocoran data pribadi yang menyeret penyelenggara sistem elektronik berskala besar (Sugiantari et al., 2024; Silalahi et al., 2025). Dalam konteks pertanggungjawaban pidana, fokus analisis tidak lagi diarahkan pada pemenuhan unsur tindak pidana sebagaimana telah dibahas pada bagian sebelumnya, melainkan pada penentuan pihak yang dengan hukum bisa dimintai pertanggungjawabannya atas terjadinya kebocoran tersebut, karena kebocoran data pribadi dalam praktik sering kali melibatkan berbagai pihak, mulai dari pelaku peretasan, pegawai internal, pengurus korporasi, hingga korporasi itu sendiri. Berdasarkan analisis terhadap konstruksi norma didalam UU PDP, pertanggungjawaban pidana korporasi dalam kasus kebocoran data seharusnya diuji melalui dua aspek yang berbeda. Pertama, apakah kebocoran data terjadi akibat kebijakan, perintah, pembiaran yang disengaja, atau kegagalan korporasi menerapkan standar perlindungan data yang secara nyata telah diketahui berpotensi menimbulkan risiko kebocoran; apabila terbukti korporasi secara sadar mengabaikan kewajiban hukumnya atau memperoleh keuntungan dari praktik pengelolaan data yang tidak sesuai ketentuan UU PDP, maka korporasi memiliki dasar untuk dimintai pertanggungjawaban pidana. Kedua, apakah kebocoran

data semata-mata merupakan akibat serangan siber dari pihak ketiga yang tidak dapat diprediksi dan berada di luar pengendalian yang wajar (*beyond reasonable control*), meskipun korporasi telah menerapkan standar keamanan informasi sesuai ketentuan; dalam kondisi demikian, penyelesaian hukum lebih tepat diarahkan melalui mekanisme pertanggungjawaban administratif daripada instrumen hukum pidana yang mensyaratkan adanya kesalahan (*schuld*) sebagai dasar (Djafar & Setiawan, 2020).

Pembedaan tersebut memiliki arti penting karena tidak setiap kebocoran data pribadi secara otomatis melahirkan pertanggungjawaban pidana bagi korporasi. Hukum pidana tetap mensyaratkan pembuktian mengenai hubungan antara tindakan atau kebijakan korporasi dengan terjadinya tindak pidana, sehingga keberadaan kerugian yang dialami subjek data pribadi tidak dapat dijadikan satu-satunya dasar untuk menjatuhkan pidana kepada korporasi apabila tidak ditemukan unsur kesalahan yang dapat dipertanggungjawabkan secara hukum. Pendekatan tersebut mencerminkan penerapan asas *geen straf zonder schuld* yang konsisten, yang menghendaki agar pemidanaan didasarkan pada adanya kesalahan yang dapat dicela, bukan semata-mata karena timbulnya akibat yang merugikan. Dalam doktrin hukum pidana Indonesia, perbuatan pengurus, direksi, pegawai, atau pihak lain yang bertindak didalam lingkup kewenangannya dan juga dilakukan guna keperluan korporasi dapat dipandang selaku perbuatan korporasi itu sendiri, karena korporasi sebagai badan hukum tidak memiliki kehendak secara fisik sehingga kehendaknya diwujudkan melalui tindakan organ-organ yang menjalankannya (Arief, 2018). Doktrin identifikasi semacam ini sejalan dengan pergeseran paradigma pertanggungjawaban korporasi yang lebih luas dalam KUHP nasional, yang juga menegaskan bahwa tindak pidana korporasi dapat lahir dari kebijakan struktural, bukan semata perbuatan individu yang berdiri sendiri (Fadhila, 2024; Hio, 2025).

Berdasarkan doktrin tersebut, korporasi bukan bisa melepaskan diri dari pertanggungjawabannya pidana hanya dengan menyatakan bahwasanya tindak pidana dilaksanakan oleh pegawai tertentu tanpa sepengetahuan manajemen. Apabila dapat dibuktikan bahwa tindakan pegawai tersebut merupakan konsekuensi kebijakan perusahaan, lemahnya sistem pengawasan internal, pembiaran terhadap praktik yang bertentangan dengan hukum, atau dilaksanakan hanya mencapai kepentingan korporasi, maka pertanggungjawaban pidana dapat dibebankan kepada korporasi bersamaan dengan pertanggungjawaban pidana individu yang terlibat. Sebaliknya, apabila tindakan tersebut merupakan perbuatan pribadi yang sepenuhnya berada di luar ruang lingkup pekerjaan, bertentangan dengan kebijakan perusahaan, serta tidak memberikan manfaat bagi korporasi, maka pembebanan pertanggungjawaban pidana kepada korporasi harus dinilai secara lebih hati-hati agar tidak bertentangan dengan asas kesalahan yang menjadi dasar hukum pidana Indonesia. Dengan begitu, pengaturan didalam Pasal 70 UU PDP tidak mencerminkan penerapan *strict liability*, melainkan tetap berlandaskan pada asas kesalahan (*culpability principle*) sebagai fondasi utama pertanggungjawaban pidana dalam sistem hukum pidana Indonesia (Utama & Yulistiyani, 2026).

Sistem pemidanaan UU PDP tidak berhenti pada pidana pokok berupa penjara dan juga denda seperti yang sudah diatur Pasal 67 dan Pasal 68. Pasal 69 UU PDP memungkinkan penjatuhan pidana tambahan berupa perampasan keuntungan dan/ataupun harta kekayaan yang didapat dari tindakan pidana dan juga pembayaran ganti kerugian pada korban, sedangkan terhadap korporasi, pidana tambahan bisa pula dalam bentuk pembekuan sebagian atau juga keseluruhan kegiatan usaha. Pengaturan pidana tambahan ini menunjukkan adanya perubahan orientasi kebijakan hukum pidana: pembentuk undang-undang bukan lagi menempatkan pidana penjara dan denda selaku satu-satunya instrumen penegakan hukum, melainkan melengkapinya dengan pidana yang diarahkan untuk menghilangkan manfaat ekonomi yang diperoleh pelaku serta memulihkan kerugian yang dialami subjek data pribadi. Dari perspektif hukum pidana, pidana tambahan berupa perampasan keuntungan merupakan implementasi prinsip bahwasanya tidak seorangpun diperbolehkan mendapatkan manfaat dari perbuatan menentang hukum (*nemo ex delicto meliorem suam conditionem*

facere potest), sedangkan pidana tambahan berupa ganti kerugian memiliki fungsi restoratif yang memberikan perlindungan lebih nyata terhadap kepentingan hukum subjek data pribadi. Kombinasi pidana pokok dan pidana tambahan tersebut menunjukkan bahwa kebijakan pemidanaan dalam UU PDP bukan semata-mata berorientasi pada pembalasan (retributive justice), tapi juga mengakomodasi tujuan pencegahan (deterrence), pemulihan kerugian korban (restorative justice), serta penghapusan keuntungan hasil tindak pidana (asset deprivation), suatu pendekatan yang lebih sesuai dengan karakteristik kejahatan di ruang digital.

Meskipun kerangka normatif pertanggungjawaban pidana dalam UU PDP relatif lengkap, penerapannya di lapangan menghadapi sejumlah tantangan nyata yang sekaligus menjadi kontribusi baru artikel ini terhadap diskursus yang telah ada. Pertama, pembuktian unsur kesengajaan dalam kejahatan siber lintas batas relatif kompleks karena pelaku sering menyembunyikan identitas dan menggunakan infrastruktur digital lintas yurisdiksi, sementara instrumen kerja sama hukum internasional Indonesia dalam penegakan pidana siber masih terbatas. Kedua, dalam kasus yang melibatkan korporasi, penegak hukum harus secara cermat membedakan antara kegagalan sistem yang bersifat administratif dan penyalahgunaan data yang memenuhi unsur kesengajaan, sebuah pembedaan yang menuntut kapasitas digital forensik yang belum menyeluruh disemua wilayah penegakan hukum di Indonesia. Ketiga, karena UU PDP relatif baru, belum banyak putusan pengadilan yang menguji penerapan pasal-pasalanya, sehingga sejumlah tafsir, termasuk batas antara pertanggungjawaban individu dan korporasi yang telah diuraikan di atas, masih akan terus berkembang melalui praktik peradilan. Oleh karena itu, penerapan pertanggungjawaban pidana berdasarkan UU PDP perlu dilakukan secara hati-hati dengan tetap berpegang pada asas legalitas, asas kesalahan, dan asas proporsionalitas, sembari mendorong penguatan kapasitas penyidikan digital forensik sebagai prasyarat teknis bagi tegaknya kepastian hukum yang dijanjikan undang-undang ini.

KESIMPULAN

Kualifikasi yuridis tindak pidana pemakaian data pribadi dengan melawan hukum berdasarkan Undang-Undang Nomor 27 Tahun 2022 terkait Perlindungan Data Pribadi dibangun melalui konstruksi delik yang sistematis sebagaimana dikelola didalam Pasal 65 sampai dengan Pasal 68. Pasal 65 mengelola larangan mendapatkan, mengutarakan, dan juga memakai data pribadi dengan melawan hukum sebagai rangkaian perbuatan yang mengikuti siklus pemrosesan data pribadi, sedangkan Pasal 66 memberikan perlindungan terhadap keaslian dan integritas data melalui larangan membuat atau memalsukan data pribadi. Seluruh rumusan delik tersebut merupakan delik sengaja (dolus) yang mensyaratkan terpenuhinya unsur objektif berupa adanya perbuatan sebagaimana dirumuskan undang-undang dan unsur subjektif berupa kesengajaan serta sifat melawan hukum. Dengan begitu, sebuah perbuatan baru bisa dikualifikasikan selaku tindakan pidana jikalau seluruh elemen delik terpenuhi secara kumulatif, sehingga perlindungan hukum yang diberikan UU PDP berorientasi pada perlindungan hak privasi dan kendali individu atas data pribadinya sebagai komponen dari hak konstitusional warga negaranya. Pertanggungjawaban pidana terhadap pelaku pemakaian data pribadi dengan melawan hukum didasarkan pada prinsip *geen straf zonder schuld* (tiada pidana tanpa kesalahan). Pemidanaan hanya bisa dijatuhkan jikalau terbukti adanya tindakan pidana, kemampuan bertanggung jawab pelaku, kesengajaan sebagai bentuk kesalahan, dan juga tidak ada alasan pembenar ataupun alasan pemaaf. UU PDP menganut sistem pertanggungjawaban pidana berbasis kesalahan (*fault-based liability*), sehingga tidak menerapkan pertanggungjawaban pidana secara mutlak (*strict liability*). Konsekuensinya, penyalahgunaan data pribadi yang dilakukan secara sengaja bisa dikenakan sanksi pidana yang sudah ditetapkan didalam Pasal 67 dan juga Pasal 68 UU PDP, sedangkan kebocoran data yang semata-mata terjadi karena kelalaian penyelenggara sistem elektronik belum dapat dijangkau melalui ketentuan pidana UU PDP dan lebih diarahkan

pada mekanisme sanksi administratif atau pertanggungjawaban perdata. Kondisi tersebut menunjukkan bahwa walaupun UU PDP telah memberi dasar hukum yang kuat didalam menanggulangi penyalahgunaan data pribadi, masih ada ruang penyempurnaan pengaturan agar perlindungan hukum terhadap subjek data menjadi lebih komprehensif dan mampu menjawab perkembangan kejahatan digital.

REFERENSI

- Arief, B. N. (2018). Bunga rampai kebijakan hukum pidana. Kencana.
- Chazawi, A. (2019). Pelajaran hukum pidana bagian I. PT RajaGrafindo Persada.
- Darmadi, A. A. N. O. Y., & Dananjaya, N. S. (2023). Perlindungan hukum terhadap korban kebocoran data pribadi (studi kasus di Kota Denpasar). *Jurnal Kertha Semaya*, 11(5), 1118–1130. <https://doi.org/10.24843/KS.2023.v11.i05.p13>
- Djafar, W., & Setiawan, M. Y. D. A. (2020). Perlindungan privasi dan data pribadi di Indonesia. ELSAM.
- Edbert, F., & Putra, M. R. S. (2023). Pertanggungjawaban hukum terhadap kebocoran data pribadi pada perusahaan pengelola jasa keuangan berbasis IT. *Unes Law Review*, 6(2), 5966–5977.
- Fadhila, K. W. (2024). Reformasi hukum pidana dan pertanggungjawaban korporasi dalam UU KUHP 2023. *Action Research Literate*, 8(3), 649–657.
- Hadi, A., & Guntara, B. (2022). Pembaharuan hukum nasional dalam upaya perlindungan data pribadi di era disrupsi kecerdasan buatan (artificial intelligence). *Jurnal Hukum Mimbar Justitia*, 8(1), 233–253. <https://doi.org/10.35194/jhmj.v8i1.2426>
- Hamzah, A. (2019). Asas-asas hukum pidana di Indonesia dan perkembangannya. Sofmedia.
- Hertianto, M. R. (2021). Sistem penegakan hukum terhadap kegagalan dalam perlindungan data pribadi di Indonesia. *Jurnal Kertha Patrika*, 43(1), 93–109.
- Hiariej, E. O. S. (2021). Prinsip-prinsip hukum pidana. Cahaya Atma Pustaka.
- Hio, Y. K. P. (2025). Politik hukum pidana: Penerapan asas tiada pidana tanpa kesalahan dalam pertanggungjawaban pidana korporasi kepada pemegang saham berdasarkan KUHP nasional. *Jurnal Media Hukum*, 13(2), 156–172.
- Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum*, 37(2), 119–133.
- Husri, H., Gurusi, L., & Samsul. (2026). Pertanggungjawaban pidana atas kebocoran data pribadi oleh penyelenggara sistem elektronik dalam perspektif UU Perlindungan Data Pribadi. *Progresif: Jurnal Hukum*, 20(1), 183–204.
- Ismaidar, I., & Ula, R. F. (2025). Pertanggungjawaban pidana korporasi terhadap kebocoran data pribadi konsumen dalam perspektif hukum pidana siber di Indonesia. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 2(2).
- Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R., Susilowati, I., Sopian, & Helfisar, D. (2023). Criminal sanctions and personal data protection in Indonesia. *Lex Publica*, 10(1).
- Lamintang, P. A. F. (2019). Dasar-dasar hukum pidana Indonesia. Citra Aditya Bakti.
- Mamadoa, F. P. C., Bawole, H. Y. A., & Simbala, Y. (2025). Larangan dan sanksi atas perolehan dan penggunaan data pribadi secara melawan hukum berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Lex Crimen*, 14(2).
- Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati*, 4(2), 139–148. <https://doi.org/10.36733/jhshs.v4i2>

- Marzuki, P. M. (2021). Penelitian hukum. Kencana.
- Moeljatno. (2018). Asas-asas hukum pidana (Rev. ed.). Rineka Cipta.
- Pakpahan, H., & Dwimaylando, C. M. (2021). Pertanggungjawaban pidana korporasi dalam cyber pornografi. *Jurnal Cakrawala Hukum*, 12(3), 274–283.
- 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>
- Prasetyo, T. (2022). Hukum pidana (Rev. ed.). Rajawali Pers.
- Rahmawati, I. N., Rahmadani, N., Heni, D. R., & Kevin, S. (2023). Pertanggungjawaban pihak bank terhadap kebocoran data diri nasabah. *Aufklarung: Jurnal Pendidikan, Sosial dan Humaniora*, 3(2), 208–215.
- Rosadi, S. D. (2021). Perlindungan data dan informasi pribadi di Indonesia. PT Refika Aditama.
- Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis yuridis terhadap mekanisme perlindungan data pribadi dalam sistem informasi elektronik berdasarkan perspektif hukum pidana di Indonesia. *Jurnal Minfo Polgan*, 14(1), 604–613. <https://doi.org/10.33395/jmp.v14i1.14810>
- Silalahi, P. H., & Dameria, F. A. (2023). Perlindungan data pribadi mengenai kebocoran data dalam lingkup cyber crime sebagai kejahatan transnasional. *Wajah Hukum*, 7(2), 614–627. <https://doi.org/10.33087/wjh.v7i2.1244>
- Solihin, F. (2023). Analisa cakupan hukum pengelolaan perlindungan hukum data pribadi di Indonesia. *JISPAR*, 12(1), 99–110.
- Sudarwanto, A. S., & Kharisma, D. B. (2021). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, 29(4).
- Sugiantari, A. A., Wiryawan, I. W. G., Hengki, I. G. B., Asrita, N. N. M. G., & Putra, I. K. A. A. (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.
- Utama, F. S., & Yulistyani, I. D. (2026). The urgency of compliance audit 5.0 through an approach to personal data protection law. *Perspektif Hukum*, 26, 1–32. <https://doi.org/10.30649/ph.v26i1.433>
- Utami, T. K., Putri, K. A., Suryanto, S. O., & Asriani, F. (2025). Personal data breach cases in Indonesia: Perspective of personal data protection law. *Journal Customary Law*, 2(2), 21. <https://doi.org/10.47134/jcl.v2i2.3742>
- Widayanti, P. W. (2022). Tindak pidana pencurian data nasabah dalam bidang perbankan sebagai cyber crime. *Legacy: Jurnal Hukum dan Perundang-Undangan*, 2(2), 1–21.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).
- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.