Volume 4 Number 1 (2026)
January – June 2026
Page: 23-34

Journal of Creative Power and Ambition (JCPA)
https://edujavare.com/index.php/jcpa
E-ISSN: 3031-4054
DOI: 10.70610/jcpa.1389

Pertanggungjawaban Pidana Pelaku Penyebaran Data Pribadi Melalui Media Sosial

Alfian Bantara Sumarmo[1], Mohamad Tohari, Idul Hamzah Alid

Universitas Darul Ulum Islamic Centre Sudirman
*Coresponding Email: alfianbantarasumarmo@gmail.com

Article history Submitted: 2026/02/01; Revised: 2026/03/11; Accepted: 2026/06/11

Abstract

The proliferation of social media has created new avenues for the unauthorized dissemination of personal data. Such conduct not only infringes on individual privacy but may also produce serious harms ranging from reputational damage to threats against victims' safety. This study examines how Indonesian criminal law particularly Law Number 27 of 2022 on Personal Data Protection (UU PDP) and Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions (UU ITE) constructs criminal liability for perpetrators who disseminate personal data through social media. A normative juridical method is employed, drawing on statutory and conceptual approaches. The study also analyzes the criminal elements that must be established, the penal sanctions prescribed, and the evidentiary challenges encountered in practice. The findings indicate that the regulatory framework has become more comprehensive following the enactment of UU PDP; however, its implementation remains hampered by significant obstacles particularly in identifying anonymous perpetrators, establishing mens rea, and ensuring inter-agency coordination. The study concludes that the effectiveness of criminal accountability in personal data dissemination cases requires strengthened digital forensics capacity among law enforcement actors and clearer technical guidance on UU PDP implementation.

Keywords Personal Data Protection; Criminal Liability; Social Media; UU PDP; UU ITE

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license, https://creativecommons.org/licenses/by-sa/4.0/.

PENDAHULUAN

Dalam satu dekade terakhir, media sosial telah bertransformasi dari sekadar platform komunikasi menjadi ruang di mana hampir seluruh aspek kehidupan seseorang terekam dan dibagikan. Indonesia sendiri tercatat sebagai salah satu negara dengan pengguna media sosial terbesar di dunia. Laporan We Are Social tahun 2024 menempatkan jumlah pengguna aktif media sosial di Indonesia pada angka sekitar 167 juta orang, atau hampir 60 persen dari total populasi. Di balik

kemudahan yang ditawarkan, fenomena ini juga membawa risiko yang tidak sepele: data pribadi seseorang kini bisa tersebar ke jutaan pengguna hanya dalam hitungan detik, tanpa pernah ada izin dari pemiliknya.

Penyebaran data pribadi tanpa persetujuan melalui media sosial atau yang dalam diskursus akademis sering disebut sebagai doxing atau non-consensual data sharing bukan sekadar persoalan etika digital. Ketika perbuatan itu dilakukan dengan sengaja dan menimbulkan kerugian bagi orang lain, ia bersentuhan langsung dengan ranah hukum pidana. Korbannya bisa mengalami pencemaran nama baik, pelecehan daring, diskriminasi, bahkan ancaman fisik ketika alamat rumah atau informasi lokasi mereka disebarluaskan oleh pihak yang tidak bertanggung jawab.

Indonesia sebenarnya sudah memiliki instrumen hukum yang mengatur persoalan ini. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016 memuat beberapa ketentuan yang relevan, khususnya Pasal 26 yang mengatur hak atas informasi pribadi dalam sistem elektronik. Namun kehadiran regulasi yang lebih spesifik dan komprehensif baru terwujud pada akhir 2022 melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) undang-undang pertama di Indonesia yang secara khusus dan menyeluruh mengatur perlindungan data pribadi, termasuk sanksi pidananya.

Meskipun perhatian akademis terhadap perlindungan data pribadi dan kejahatan siber terus tumbuh, kajian yang secara spesifik menelaah pertanggungjawaban pidana dalam konteks penyebaran data pribadi melalui media sosial masih mengandung beberapa celah yang belum tertangani. Widodo (2011) merupakan salah satu peneliti awal yang mengkaji tindak pidana di bidang teknologi informasi secara komprehensif dalam konteks Indonesia, namun tulisannya berangkat dari era sebelum revisi UU ITE maupun sebelum lahirnya UU PDP, sehingga konstruksi pertanggungjawabannya belum dapat mengakomodasi perkembangan regulasi yang paling mutakhir. Maskun (2013) menganalisis kejahatan siber dalam perspektif hukum pidana dan memberikan kerangka konseptual yang berguna, tetapi fokusnya lebih pada kejahatan siber secara umum, peretasan, penipuan daring, pornografi siber tanpa mendalami secara khusus penyebaran data pribadi sebagai satu kategori tindak pidana yang berdiri sendiri.

Sebelum berbicara tentang pertanggungjawaban pidana, perlu dipahami lebih dahulu apa yang dimaksud dengan data pribadi dalam konteks hukum Indonesia. UU PDP mendefinisikan data pribadi sebagai setiap data tentang orang

perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Definisi ini luas dan inklusif, mencakup tidak hanya data yang secara tradisional dianggap sensitif seperti nomor identitas, data kesehatan, atau informasi keuangan tetapi juga data yang tampaknya tidak berbahaya namun dapat mengidentifikasi seseorang ketika digabungkan dengan informasi lain.

UU PDP membedakan antara data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Data umum mencakup nama lengkap, jenis kelamin, kewarganegaraan, dan agama. Informasi yang memang sering tersedia di ruang publik. Sementara data spesifik mencakup data kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya yang berpotensi lebih merugikan jika disebarluaskan tanpa izin. Pembedaan ini penting karena memengaruhi tingkat perlindungan hukum yang diberikan dan, pada akhirnya, ancaman pidana yang dapat dijatuhkan.

Dalam konteks media sosial, penyebaran data pribadi dapat terjadi dalam berbagai bentuk: mengunggah foto atau video seseorang tanpa persetujuan, mempublikasikan nomor telepon atau alamat rumah seseorang di kolom komentar, membocorkan percakapan privat, hingga menyebarkan tangkapan layar (screenshot) informasi pribadi yang diperoleh dari konteks percakapan terbatas. Dalam banyak kasus, pelakunya adalah orang yang sebelumnya memiliki hubungan dengan korban, mantan pasangan, rekan kerja, atau kenalan yang kemudian memanfaatkan akses terhadap informasi pribadi korban sebagai alat balas dendam atau intimidasi.

Perlindungan data pribadi dalam hukum Indonesia kini berpijak pada dua regulasi utama yang keduanya memuat ketentuan pidana. Pertama, UU ITE yang dalam Pasal 26 ayat (1) menetapkan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Pasal 45 UU ITE mengancam pelanggar dengan pidana penjara maksimal 12 tahun dan/atau denda maksimal Rp 12 miliar apabila penyebaran data dilakukan dengan tujuan memeras atau mengancam, atau pidana penjara 6 tahun dan/atau denda Rp 1 miliar untuk pelanggaran Pasal 26.

Kedua, UU PDP yang mulai berlaku efektif pada Oktober 2024 memberikan kerangka yang jauh lebih komprehensif. Pasal 67 UU PDP mengatur tiga kategori tindak pidana: (1) memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data diancam penjara maksimal 5 tahun dan/atau

denda maksimal Rp 5 miliar; (2) mengungkapkan data pribadi yang bukan miliknya—diancam penjara maksimal 4 tahun dan/atau denda maksimal Rp 4 miliar; dan (3) menggunakan data pribadi yang bukan miliknya diancam penjara maksimal 5 tahun dan/atau denda maksimal Rp 5 miliar. Sementara Pasal 68 mengatur pemidanaan terhadap orang yang dengan sengaja dan melawan hukum menempatkan data pribadi orang lain dalam profiling untuk kepentingan tertentu.

Tabel 1. Perbandingan Ketentuan Pidana UU PDP dan UU ITE dalam Kasus Penyebaran Data Pribadi

Aspek	**UU PDP (UU 27/2022)**	**UU ITE (UU 11/2008 jo. 19/2016)**
Pasal utama	Pasal 67–68	Pasal 26 jo. Pasal 45
Jenis perbuatan diatur	Memperoleh, mengungkapkan, menggunakan data	Penggunaan data tanpa persetujuan
Ancaman penjara	Maks. 4–5 tahun (per kategori)	Maks. 6–12 tahun (tergantung konteks)
Ancaman denda	Maks. Rp 4–5 miliar	Maks. Rp 1–12 miliar
Data spesifik (sensitif)	Diatur tersendiri, ancaman lebih berat	Tidak dibedakan secara eksplisit
Korporasi sebagai pelaku	Diatur (Pasal 69)	Tidak diatur secara spesifik

Sumber: UU No. 27 Tahun 2022 dan UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016

Pertanggungjawaban pidana (criminal liability) dalam doktrin hukum pidana mensyaratkan terpenuhinya dua elemen utama: actus reus (perbuatan melawan hukum) dan mens rea (kesalahan atau niat pelaku). Moeljatno (2008) menegaskan bahwa seseorang tidak dapat dimintai pertanggungjawaban pidana apabila pada dirinya tidak terdapat kesalahan, baik dalam bentuk kesengajaan (dolus) maupun kelalaian (culpa). Dalam konteks penyebaran data pribadi, actus reus terpenuhi ketika seseorang secara nyata mengungkapkan atau menyebarkan data pribadi orang lain di media sosial. Sementara mens rea khususnya unsur kesengajaan (opzet) menjadi elemen yang paling kritis dan paling sulit dibuktikan.

Roeslan Saleh (1983) dalam kajiannya tentang perbuatan pidana dan pertanggungjawaban pidana menegaskan bahwa pembuktian kesengajaan harus diarahkan pada kondisi batin pelaku pada saat melakukan perbuatan sebuah kondisi yang pada dasarnya bersifat internal dan tidak dapat diamati secara langsung, melainkan hanya dapat disimpulkan dari rangkaian fakta eksternal. Dalam kasus penyebaran data di media sosial, fakta eksternal yang relevan antara lain: apakah pelaku mengetahui bahwa data tersebut adalah milik orang teridentifikasi, apakah

pelaku menyadari bahwa penyebaran itu dilakukan tanpa persetujuan, dan apakah ada tujuan tertentu yang menyertai perbuatan tersebut.

Prasetio (2020) mengkaji perlindungan hukum atas data pribadi dalam transaksi elektronik dan menyimpulkan bahwa kerangka hukum yang ada saat itu belum memadai karena belum ada undang-undang khusus perlindungan data. Kajian ini sangat relevan sebagai potret kondisi hukum sebelum UU PDP, namun justru karena itu tidak dapat menjawab pertanyaan tentang bagaimana UU PDP mengisi kekosongan yang diidentifikasinya. Dewi (2021) meneliti aspek hukum perlindungan privasi di media sosial dan mengidentifikasi ketidakjelasan norma dalam UU ITE yang menyebabkan lemahnya penegakan hukum namun penelitian ini berakhir sebelum UU PDP disahkan dan tidak menganalisis dimensi pertanggungjawaban pidananya secara mendalam, melainkan lebih pada analisis hak privasi sebagai hak konstitusional.

Santoso (2023) mencoba menganalisis UU PDP yang baru disahkan dari perspektif hukum administrasi, dengan fokus pada kewajiban pengendali data dan sanksi administratif. Penelitian ini penting sebagai kajian awal atas UU PDP, tetapi membatasi dirinya pada dimensi administratif dan tidak membahas secara spesifik bagaimana ketentuan pidana dalam UU PDP berinteraksi dengan UU ITE dalam kasus penyebaran data pribadi melalui media sosial. Sejauh yang penulis telusuri, belum ada kajian yang secara terpadu menganalisis konstruksi pertanggungjawaban pidana pelaku penyebaran data pribadi melalui media sosial pasca-berlakunya UU PDP, dengan mempertimbangkan relasi normatif antara UU PDP dan UU ITE, tantangan pembuktian unsur-unsur pidananya, serta implikasi dari anonimitas pelaku di ruang digital.

Dari pemetaan literatur di atas, teridentifikasi tiga celah akademis yang menjadi dasar penelitian ini. Pertama, belum ada kajian yang menganalisis secara terintegrasi bagaimana UU PDP dan UU ITE saling melengkapi atau justru berpotensi tumpang tindih dalam mengatur pertanggungjawaban pidana kasus penyebaran data pribadi. Kedua, hampir semua kajian yang ada ditulis sebelum atau segera setelah pengesahan UU PDP sehingga belum dapat mengevaluasi implikasi praktis ketentuan pidananya. Ketiga, tidak ada penelitian yang secara eksplisit membahas tantangan pembuktian mens rea dalam kasus penyebaran data pribadi oleh akun anonim di media sosial sebuah persoalan teknis-yuridis yang sangat nyata dihadapi penyidik di lapangan.

Tulisan ini hadir untuk mengisi ketiga celah tersebut. Berbeda dari kajian-kajian sebelumnya yang umumnya bersifat parsial membahas salah satu regulasi

saja, atau mengkaji perlindungan data dari sudut pandang privasi semata. Tulisan ini mengadopsi kerangka analisis yang lebih menyeluruh: menelaah konstruksi delik penyebaran data pribadi dalam dua regulasi utama sekaligus (UU PDP dan UU ITE), menganalisis unsur-unsur pertanggungjawaban pidananya secara komparatif, dan secara khusus mendiskusikan tantangan pembuktian yang muncul dari karakteristik unik kejahatan ini di ruang media sosial. Dengan demikian, tulisan ini diharapkan dapat menjadi rujukan yang lebih aktual dan komprehensif bagi akademisi, praktisi hukum, maupun pengambil kebijakan.

METHODS

Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Bahan hukum primer mencakup UU PDP, UU ITE beserta perubahannya, KUHP, dan KUHAP. Bahan hukum sekunder meliputi literatur akademik, jurnal hukum, laporan lembaga terkait, serta putusan pengadilan yang relevan. Analisis dilakukan secara deskriptif-analitis untuk memahami konstruksi normatif pertanggungjawaban pidana sekaligus mengidentifikasi celah dan tantangan dalam implementasinya.

FINDINGS AND DISCUSSION

Konstruksi Unsur-Unsur Tindak Pidana Penyebaran Data Pribadi

Menganalisis pertanggungjawaban pidana dalam kasus penyebaran data pribadi melalui media sosial menuntut pemahaman yang cermat tentang unsur-unsur tindak pidana yang harus terpenuhi secara kumulatif. Berdasarkan ketentuan UU PDP, khususnya Pasal 67 ayat (2), tindak pidana pengungkapan data pribadi mensyaratkan terpenuhinya unsur-unsur berikut: (1) adanya perbuatan mengungkapkan; (2) objek perbuatan adalah data pribadi; (3) data pribadi tersebut bukan milik pelaku; (4) perbuatan dilakukan dengan sengaja (opzet); dan (5) perbuatan dilakukan secara melawan hukum.

Unsur pertama perbuatan mengungkapkan dalam konteks media sosial dapat berupa tindakan mengunggah, memposting, membagikan (share), meneruskan (forward), atau mempublikasikan dalam bentuk apapun. Yang menarik adalah bahwa UU PDP tidak membatasi medium pengungkapan pada media sosial saja, sehingga ketentuan ini berlaku untuk berbagai platform digital maupun non-digital. Namun dari sisi praktik, media sosial menjadi medium yang paling sering digunakan karena kemudahan penyebaran dan jangkauan audiens yang luas.

Unsur ketiga bahwa data tersebut bukan milik pelaku menghadirkan pertanyaan yuridis yang menarik: apa artinya 'memiliki' data pribadi? UU PDP memperkenalkan konsep subjek data (data subject) sebagai pihak yang datanya diproses, dan pengendali data (data controller) sebagai pihak yang menentukan tujuan dan cara pemrosesan. Dalam pandangan ini, data pribadi seseorang adalah 'milik' subjek data dalam artian bahwa subjek data memiliki hak untuk mengontrol bagaimana datanya digunakan. Seorang pelaku yang menyebarkan data pribadi orang lain bahkan jika ia memperoleh data tersebut secara sah sebelumnya, misalnya karena pernah berteman dekat tetap dapat dianggap menyebarkan data 'bukan miliknya' apabila penyebaran itu dilakukan di luar tujuan semula perolehan data.

Unsur kesengajaan (mens rea) adalah titik paling krusial sekaligus paling kontroversial. Dalam praktek penegakan hukum, penyidik harus mampu membuktikan bahwa pelaku mengetahui dan menghendaki akibat dari perbuatannya dalam hal ini, bahwa ia menyadari bahwa yang disebarkannya adalah data pribadi orang lain dan bahwa penyebaran itu dilakukan tanpa hak. Pembuktian ini menjadi sangat kompleks ketika pelaku berdalih tidak mengetahui bahwa informasi yang ia sebarkan adalah 'data pribadi' dalam pengertian hukum, atau ketika pelaku mengklaim hanya meneruskan konten yang sudah tersebar di tempat lain sehingga ia merasa tidak bertanggung jawab atas penyebaran awalnya.

Tantangan Pembuktian: Anonimitas dan Batas Yurisdiksi

Salah satu karakteristik paling unik dari kejahatan siber termasuk penyebaran data pribadi melalui media sosial adalah kemampuan pelaku untuk beroperasi secara anonim atau pseudonim. Seseorang dapat dengan mudah membuat akun media sosial menggunakan nama palsu, alamat surel sementara, dan alamat IP yang disamarkan melalui Virtual Private Network (VPN) atau jaringan Tor. Dalam situasi seperti ini, identifikasi pelaku menjadi tantangan teknis yang sangat nyata bagi penyidik.

Secara yuridis, pembuktian dalam hukum acara pidana Indonesia mensyaratkan minimal dua alat bukti yang sah (Pasal 183 KUHAP). Untuk kasus siber, Pasal 5 UU ITE mengakui keabsahan bukti elektronik sebagai alat bukti yang sah. Namun penggunaan bukti elektronik dalam praktik masih menghadapi beberapa kendala: belum semua penyidik terlatih dalam penanganan dan pemeliharaan integritas barang bukti digital (digital forensics), platform media sosial asing sering kali tidak kooperatif dalam memberikan data pengguna kepada aparat penegak hukum Indonesia, dan prosedur mutual legal assistance yang diperlukan

untuk mendapatkan data dari perusahaan platform yang berkedudukan di luar negeri memakan waktu sangat lama.

Tantangan yurisdiksi juga tidak kalah pelik. Ketika pelaku, korban, dan server platform media sosial berada di yurisdiksi yang berbeda, penerapan hukum pidana Indonesia menjadi lebih rumit. Asas teritorialitas dalam hukum pidana internasional memungkinkan Indonesia menuntut pelaku selama akibat kejahatannya dirasakan di wilayah Indonesia, namun eksekusi putusan terhadap pelaku yang berada di luar negeri tetap memerlukan perjanjian ekstradisi atau mekanisme kerja sama hukum internasional yang tidak selalu tersedia.

Relasi Normatif UU PDP dan UU ITE: Lex Specialis atau Kumulatif?

Kehadiran UU PDP sebagai regulasi baru menimbulkan pertanyaan penting tentang relasi normatifnya dengan UU ITE, khususnya dalam kasus penyebaran data pribadi. Apakah UU PDP sebagai lex specialis menggantikan ketentuan UU ITE, ataukah keduanya dapat diterapkan secara bersamaan? Secara teoritis, asas lex specialis derogat legi generali menghendaki bahwa norma yang lebih khusus mengesampingkan norma yang lebih umum. Karena UU PDP secara spesifik mengatur perlindungan data pribadi sementara UU ITE mengatur informasi dan transaksi elektronik secara lebih luas, maka untuk kasus penyebaran data pribadi di ranah elektronik, ketentuan UU PDP seharusnya diutamakan. Namun dalam praktik, penerapan asas ini tidak selalu sederhana karena UU ITE memuat ancaman pidana yang dalam beberapa konfigurasi justru lebih berat terutama jika penyebaran data disertai ancaman atau pemerasan (Pasal 45 UU ITE: penjara hingga 12 tahun).

Ketidakjelasan relasi normatif ini berpotensi menimbulkan disparitas dalam penuntutan: jaksa yang memilih untuk mendakwa berdasarkan UU ITE saja, berdasarkan UU PDP saja, atau menggunakan dakwaan kumulatif dengan kedua regulasi, akan menghasilkan tuntutan yang sangat berbeda. Ini merupakan salah satu celah regulasi yang perlu segera ditangani melalui pedoman teknis dari Kejaksaan Agung atau melalui revisi terhadap salah satu regulasi untuk mempertegas hubungan keduanya.

Kasus Ilustratif: Pola dan Karakteristik Perkara

Untuk memperoleh gambaran yang lebih konkret tentang bagaimana pertanggungjawaban pidana bekerja dalam praktik, berikut diuraikan dua pola kasus yang umum ditemukan dalam penanganan perkara penyebaran data pribadi melalui media sosial di Indonesia. Pola Pertama: Revenge Porn dan Data Pribadi Intim. Kasus-kasus yang melibatkan penyebaran foto atau video intim mantan pasangan (revenge porn) merupakan salah satu bentuk penyebaran data pribadi

yang paling sering dilaporkan. Dalam pola ini, pelaku umumnya adalah mantan kekasih atau suami/istri yang menyebarkan konten intim korban sebagai bentuk balas dendam pasca-perpisahan. Sebelum UU PDP, kasus semacam ini ditangani menggunakan Pasal 27 ayat (1) UU ITE tentang konten asusila. Dengan berlakunya UU PDP, data biometrik dan data kesehatan dikategorikan sebagai data pribadi spesifik yang mendapatkan perlindungan lebih ketat membuka kemungkinan dakwaan yang lebih terstruktur.

Pola Kedua: Doxing Bermotif Kebencian atau Intimidasi. Pola kedua melibatkan publikasi data pribadi seseorang alamat rumah, tempat kerja, nomor telepon, atau foto wajah oleh akun anonim di media sosial dengan tujuan mengundang massa untuk melakukan pelecehan atau intimidasi terhadap korban. Pola ini sering terjadi dalam konteks konflik daring, perselisihan opini, atau persekusi berbasis perbedaan pandangan. Dari sisi pembuktian, pola ini paling menantang karena pelaku hampir selalu menggunakan identitas anonim dan platform yang berbeda-beda untuk menghapus jejak digital.

Tabel 2. Rangkuman Tantangan Hukum dalam Penanganan Kasus Penyebaran Data Pribadi melalui Media Sosial

Aspek Tantangan	Uraian Permasalahan	Kebutuhan Solusi
Identifikasi pelaku anonim	VPN dan akun palsu mempersulit penelusuran IP dan identitas nyata pelaku	Kapasitas digital forensik dan kerja sama dengan platform
Pembuktian mens rea	Sulit membuktikan kesengajaan pelaku yang berdalih tidak tahu atau sekadar meneruskan konten	Pedoman pembuktian khusus kejahatan siber
Kerja sama platform asing	Perusahaan media sosial asing sering lambat atau menolak memberikan data pengguna	Perjanjian bilateral dan tekanan regulasi
Relasi UU PDP–UU ITE	Ketidakjelasan tentang regulasi mana yang diutamakan menimbulkan disparitas penuntutan	Pedoman teknis Kejaksaan Agung atau revisi regulasi
Batas yurisdiksi	Pelaku atau server di luar negeri membatasi jangkauan hukum pidana Indonesia	Penguatan kerja sama hukum internasional

Sumber: Analisis penulis berdasarkan UU PDP, UU ITE, dan literatur terkait (2025)

Sanksi Pidana: Antara Deterensi dan Proporsionalitas

Ancaman sanksi pidana dalam UU PDP dan UU ITE sudah cukup berat di atas kertas. Namun efektivitas sanksi sebagai instrumen deterensi tidak hanya bergantung pada beratnya ancaman, tetapi juga pada kepastian penegakan

hukumnya. Dalam konteks kejahatan siber, penelitian kriminologi menunjukkan bahwa persepsi pelaku tentang kemungkinan tertangkap (certainty of detection) jauh lebih berpengaruh terhadap perilaku dibandingkan persepsi tentang beratnya hukuman (severity of punishment). Selama pelaku masih merasa dapat bersembunyi di balik anonimitas digital tanpa risiko teridentifikasi, ancaman pidana seberat apapun tidak akan menjadi faktor pencegah yang efektif.

Dari perspektif proporsionalitas, perlu dicermati apakah ancaman pidana dalam UU PDP sudah proporsional terhadap tingkat kerugian yang ditimbulkan. Penyebaran data pribadi yang 'ringan' misalnya menyebarkan nomor telepon seseorang tanpa izin dengan penyebaran data yang menimbulkan kerugian besar seperti mempublikasikan data medis atau foto intim seseorang sejatinya memiliki derajat keseriusan yang sangat berbeda. UU PDP mencoba mengakomodasi perbedaan ini dengan membedakan data pribadi umum dan data pribadi spesifik, serta dengan merumuskan ancaman pidana yang berbeda per kategori perbuatan. Namun dalam praktik, penentuan batas antara 'data umum' dan 'data spesifik' tidak selalu mudah dan berpotensi menjadi arena perdebatan hukum yang panjang.

CONCLUSION

Penyebaran data pribadi melalui media sosial adalah tindak pidana yang terus berkembang dalam pola dan kompleksitasnya, seiring dengan perluasan penggunaan platform digital di Indonesia. Kerangka hukum pidana yang mengaturnya kini berpijak pada dua regulasi utama UU PDP dan UU ITE yang masing-masing memberikan kontribusi normatif yang penting namun juga menyisakan ketidakjelasan dalam hal relasi dan prioritas penerapannya. UU PDP yang mulai berlaku efektif pada 2024 merupakan langkah maju yang signifikan dalam memperkuat kerangka pertanggungjawaban pidana. Ketentuan pidananya lebih terstruktur, membedakan jenis perbuatan dan kategori data yang dilanggar, serta secara eksplisit mengakomodasi korporasi sebagai subjek pidana. Namun kelebihannya dalam tataran normatif belum sepenuhnya diimbangi oleh kesiapan infrastruktur penegakan hukumnya terutama dari sisi kapasitas digital forensik penyidik, mekanisme kerja sama dengan platform media sosial asing, dan panduan teknis penuntutan. Tiga tantangan utama yang masih perlu diatasi adalah: (1) keterbatasan kemampuan teknis aparat dalam mengidentifikasi pelaku yang beroperasi secara anonim; (2) ketidakjelasan relasi normatif antara UU PDP dan UU ITE yang berpotensi menimbulkan disparitas penuntutan; dan (3) kompleksitas pembuktian unsur kesengajaan dalam konteks penyebaran konten digital yang sering kali melibatkan rantai penyebar yang panjang.

REFERENCES

Ali, M. (2015). Hukum pidana Indonesia: Perkembangan dan pembaharuan. Sinar Grafika.

Arief, B. N. (2016). Bunga rampai kebijakan hukum pidana: Perkembangan penyusunan konsep KUHP baru (Cet. ke-5). Kencana Prenada Media.

Hamzah, A. (2010). Asas-asas hukum pidana (Ed. revisi). Rineka Cipta.

Marzuki, P. M. (2016). Penelitian hukum (Ed. revisi). Kencana Prenada Media.

Maskun. (2013). Kejahatan siber (cybercrime): Suatu pengantar. Kencana Prenada Media.

Moeljatno. (2008). Asas-asas hukum pidana (Ed. ke-8). Rineka Cipta.

Saleh, R. (1983). Perbuatan pidana dan pertanggungjawaban pidana: Dua pengertian dasar dalam hukum pidana. Aksara Baru.

Soekanto, S. (2012). Faktor-faktor yang memengaruhi penegakan hukum (Ed. ke-11). PT Raja Grafindo Persada.

Widodo. (2011). Hukum pidana di bidang teknologi informasi: Cybercrime law sebagai tindak pidana khusus. Aswaja Pressindo.

Ariyanti, V. (2019). Kebijakan penegakan hukum dalam sistem peradilan pidana Indonesia. Jurnal Yuridis, 6(2), 33–54.

Dewi, S. (2021). Perlindungan privasi dan data pribadi dalam perspektif regulasi teknologi informasi. Jurnal Hukum dan Teknologi, 1(1), 1–16.

Fahrojih, I. (2023). Analisis yuridis tindak pidana penyebaran data pribadi dalam perspektif UU ITE. Jurnal Ilmu Hukum, 19(2), 215–234.

Prasetio, R. B. (2020). Perlindungan hukum atas data pribadi konsumen dalam transaksi elektronik. Jurnal Hukum Bisnis Bonum Commune, 3(2), 214–226.

Ramadhan, A. F. (2022). Pertanggungjawaban pidana pelaku penyebaran konten asusila melalui media sosial. Jurnal Penelitian Hukum De Jure, 22(1), 87–104.

Santoso, A. P. (2023). Tinjauan hukum administrasi terhadap Undang-Undang Perlindungan Data Pribadi. Jurnal Hukum Tata Negara, 8(1), 45–62.

Sulistyaningsih, E. (2020). Kebijakan kriminalisasi terhadap kejahatan siber di Indonesia: Pendekatan komparatif. Masalah-Masalah Hukum, 49(3), 241–256.

Wahyuni, F. (2022). Tantangan penegakan hukum kejahatan siber lintas batas negara dalam perspektif hukum internasional. Padjadjaran Jurnal Ilmu Hukum, 9(2), 135–153.

Wibowo, A. (2021). Doxing sebagai bentuk kejahatan siber dan respons hukum pidana Indonesia. Jurnal Hukum IUS QUIA IUSTUM, 28(3), 487–508.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11

Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1.

Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2017 tentang Perubahan atas Undang-Undang Nomor 17 Tahun 2013 tentang Organisasi Kemasyarakatan.

We Are Social & Meltwater. (2024). Digital 2024: Indonesia. We Are Social.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Laporan tahunan penanganan konten negatif dan pelanggaran ruang digital 2022. Kemenkominfo RI.