



Analisis Hukum Pidana terhadap Praktik Pemerasan melalui Penyebaran Data Pribadi

Abyan Alimansyah¹, Rizki Mukhamad Firdaus²

^{1,2} Fakultas Hukum, Universitas Pamulang, Serang, Indonesia

Korespondensi: naybaila123@gmail.com¹, rizkirr21@gmail.com²

Informasi Artikel

Riwayat artikel:

Received Sept 5th, 2026

Revised Oct 2th, 2026

Accepted Oct 19th, 2026

Keyword:

Digital extortion; Personal data;
Criminal law; ITE Law; Personal
data protection.

ABSTRAK

Perkembangan teknologi informasi menghadirkan kemudahan dalam pengumpulan, penyimpanan, dan pertukaran informasi, tetapi sekaligus memperbesar risiko penyalahgunaan data pribadi. Salah satu bentuk penyalahgunaan yang berdampak serius ialah pemerasan dengan ancaman menyebarkan data pribadi, foto, percakapan, alamat, dokumen, atau informasi sensitif apabila korban tidak memenuhi tuntutan pelaku. Penelitian ini menganalisis konstruksi hukum pidana terhadap praktik tersebut, hubungan antara Undang-Undang Pelindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik, serta tantangan pembuktian dan perlindungan korban. Metode yang digunakan adalah penelitian hukum yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum primer ditelaah secara kualitatif dengan menguji unsur norma terhadap pola perbuatan yang lazim terjadi. Hasil kajian menunjukkan bahwa Pasal 27B ayat (2) UU ITE sebagaimana diubah dengan UU Nomor 1 Tahun 2024 relevan ketika informasi atau dokumen elektronik digunakan untuk memaksa seseorang melalui ancaman pencemaran atau pembukaan rahasia demi keuntungan melawan hukum. Sementara itu, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dapat menjangkau perolehan, pengungkapan, atau penggunaan data pribadi secara melawan hukum. Penerapan ketentuan harus memperhatikan unsur delik, asas legalitas, waktu terjadinya perbuatan, dan larangan penerapan pasal secara mekanis. Penegakan hukum yang efektif memerlukan pengamanan bukti elektronik, koordinasi lintas lembaga, pembatasan penyebaran ulang data, dan pemulihan korban.



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

PENDAHULUAN

Teknologi digital telah mengubah cara masyarakat berkomunikasi, bekerja, melakukan transaksi, dan menyimpan dokumen. Identitas seseorang kini tersebar dalam berbagai sistem, mulai dari akun media sosial, aplikasi percakapan, layanan keuangan, platform perdagangan, sampai basis data organisasi. Informasi yang tersimpan dapat berupa nama, alamat, nomor telepon, identitas kependudukan, data lokasi, foto, rekaman suara, riwayat komunikasi, dan informasi mengenai keluarga. Data tersebut mempunyai nilai bagi pemiliknya karena berkaitan dengan identitas, keamanan, kehormatan, serta kehidupan pribadi. Oleh karena itu, perlindungan terhadap data pribadi tidak hanya berhubungan dengan keamanan teknologi, tetapi juga dengan penghormatan terhadap hak asasi dan martabat manusia. Risiko muncul ketika pihak yang menguasai data menggunakannya untuk mengendalikan perilaku orang lain. Dalam pemerasan berbasis data pribadi, pelaku dapat mengancam akan mengirimkan percakapan pribadi kepada keluarga korban, mempublikasikan foto, menyebarkan alamat rumah, atau membuka informasi yang dapat mempermalukan korban. Ancaman tersebut kemudian dihubungkan dengan tuntutan tertentu, misalnya pembayaran uang, pengiriman barang, pemberian akses akun, penghapusan utang, pencabutan pengaduan, atau tindakan lain yang

menguntungkan pelaku. Korban menghadapi tekanan karena harus mempertimbangkan risiko apabila data benar-benar disebarkan.¹ Praktik tersebut berbeda dari kebocoran data yang tidak disertai tuntutan.

Kebocoran dapat terjadi akibat kelalaian, serangan siber, atau akses tanpa hak, sedangkan pemerasan mengandung penggunaan ancaman sebagai sarana untuk memaksa korban. Namun, kedua situasi dapat beririsan. Pelaku yang memperoleh data secara melawan hukum dapat menggunakannya untuk mengancam korban, kemudian menyebarkan data ketika korban menolak memenuhi tuntutan. Setiap tahap perlu diperiksa secara terpisah agar pertanggungjawaban pidana sesuai dengan fakta dan unsur delik yang terbukti. Dalam hukum Indonesia, kerangka perlindungan terhadap data pribadi antara lain diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. UU tersebut mengatur data pribadi, hak subjek data, kewajiban dalam pemrosesan, serta larangan dan sanksi pidana untuk tindakan tertentu. Di sisi lain, perubahan kedua UU Informasi dan Transaksi Elektronik melalui Undang-Undang Nomor 1 Tahun 2024 memasukkan Pasal 27B yang mengatur pemaksaan melalui informasi atau dokumen elektronik dalam keadaan tertentu. Hubungan kedua undang-undang itu harus dipahami secara sistematis, bukan dengan menganggap satu ketentuan otomatis menggantikan ketentuan lainnya. Penegak hukum perlu membuktikan setiap unsur perbuatan, kesengajaan, tujuan yang disyaratkan, bentuk ancaman, serta kaitan antara ancaman dan tuntutan. Istilah populer seperti doxing, revenge porn, kebocoran data, dan pemerasan digital dapat membantu menjelaskan modus, tetapi istilah tersebut tidak selalu merupakan nama delik dalam undang-undang. Penentuan pasal harus merujuk pada rumusan hukum positif dan waktu perbuatan dilakukan. Berangkat dari persoalan bahwa korban pemerasan digital kerap menghadapi lebih dari satu kerugian: kerugian uang, hilangnya kendali atas informasi pribadi, ancaman terhadap keselamatan, serta tekanan psikologis. Sementara itu, proses pembuktian membutuhkan pengamanan percakapan, tautan, akun, dan transaksi tanpa memperluas kembali penyebaran data sensitif. Dengan demikian, pembahasan hukum pidana perlu dipadukan dengan perhatian terhadap hak korban, ketepatan pembuktian, dan pemulihan setelah tindak pidana.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian yang berfokus pada norma hukum positif, asas hukum, dan konsep yang berhubungan dengan perbuatan pidana. Pendekatan perundang-undangan dilakukan dengan menelaah UUD 1945, UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, UU ITE sebagaimana diubah dengan UU Nomor 1 Tahun 2024, UU Nomor 1 Tahun 2023 tentang KUHP, serta peraturan terkait perlindungan saksi dan korban. Pendekatan konseptual digunakan untuk membahas pemerasan, data pribadi, kesengajaan, sifat melawan hukum, alat bukti elektronik, dan perlindungan korban. Bahan hukum primer berupa peraturan perundang-undangan. Bahan hukum sekunder meliputi buku hukum pidana dan literatur akademik yang relevan. Analisis dilakukan secara kualitatif dengan menguraikan unsur setiap norma, kemudian membandingkannya dengan pola perbuatan yang menjadi objek kajian. Penelitian ini tidak mengklaim melakukan wawancara, survei, atau pemeriksaan perkara lapangan. Oleh sebab itu, contoh yang digunakan bersifat ilustratif untuk menjelaskan penerapan norma, bukan pernyataan tentang perkara tertentu.

HASIL DAN PEMBAHASAN

A. Konsep Data Pribadi dan Karakteristik Pemerasan melalui Penyebaran Data Pribadi

Data pribadi merupakan informasi mengenai orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui kombinasi dengan informasi lainnya. Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, data pribadi mencakup setiap data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara tersendiri maupun dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun nonelektronik (Indonesia, UU No. 27 Tahun 2022, Pasal 1 angka 1). Pengertian tersebut menunjukkan bahwa identitas seseorang tidak selalu dapat dikenali hanya melalui satu jenis informasi. Kombinasi informasi berupa nama panggilan, foto, lokasi pekerjaan, nomor telepon, dan keterangan mengenai anggota keluarga dapat memungkinkan seseorang diidentifikasi secara lebih mudah. Oleh karena itu, penilaian terhadap perlindungan data pribadi perlu memperhatikan konteks penggunaan informasi dan kemungkinan

timbulnya risiko terhadap individu yang bersangkutan. Perlindungan data pribadi berkaitan erat dengan hak setiap orang untuk menjaga kehidupan pribadi, kehormatan, martabat, keamanan, serta kendali atas informasi mengenai dirinya. Dalam perspektif konstitusional, perlindungan tersebut memperoleh landasan melalui Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda (UUD NRI Tahun 1945, Pasal 28G ayat (1)). Dalam kehidupan digital, perlindungan terhadap kepentingan tersebut menghadapi tantangan karena informasi dapat disalin, disimpan, dan disebarluaskan dalam waktu singkat. Penghapusan suatu unggahan tidak selalu menjamin bahwa seluruh salinan informasi telah hilang dari ruang digital.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan kerangka hukum mengenai pemrosesan data pribadi, hak subjek data, serta kewajiban pihak yang melakukan pemrosesan. Legalitas pemrosesan data perlu dinilai berdasarkan dasar pemrosesan dan kewajiban yang ditentukan undang-undang. Penguasaan data yang semula diperoleh secara sah tidak serta-merta memberikan kewenangan kepada seseorang untuk mengungkapkan atau menggunakannya sebagai alat ancaman. Dalam hal ini, Pasal 65 UU PDP secara khusus melarang perbuatan memperoleh atau mengumpulkan, mengungkapkan, dan menggunakan data pribadi secara melawan hukum sesuai dengan unsur pada masing-masing ayat (Indonesia, UU No. 27 Tahun 2022, Pasal 65). Data pribadi yang digunakan dalam praktik pemerasan dapat berupa informasi identitas, seperti alamat tempat tinggal, nomor identitas, nomor telepon, dan tempat kerja; informasi komunikasi, seperti pesan pribadi dan surat elektronik; data visual atau audiovisual berupa foto dan video; informasi keuangan; serta data yang berpotensi mengancam keselamatan seseorang, seperti lokasi rumah dan aktivitas sehari-hari. Pengelompokan tersebut membantu menjelaskan bentuk risiko yang mungkin dialami korban, meskipun tidak dengan sendirinya menentukan klasifikasi tindak pidana. Tingkat sensitivitas suatu informasi juga perlu dinilai berdasarkan konteks penggunaannya. Praktik pemerasan melalui penyebaran data pribadi dapat dipahami sebagai perbuatan yang menggunakan ancaman pengungkapan informasi untuk memaksa seseorang memenuhi tuntutan tertentu. Perbuatan tersebut dapat berlangsung melalui beberapa tahapan, mulai dari penguasaan informasi, penyampaian ancaman, pengajuan tuntutan, hingga penyebaran data apabila korban tidak memenuhi permintaan pelaku. Namun, pola tersebut tidak selalu terjadi secara berurutan dalam setiap perkara. Oleh karena itu, karakteristik perbuatan harus ditentukan berdasarkan fakta konkret dan bukti yang tersedia, bukan semata-mata berdasarkan istilah yang digunakan untuk menggambarkan suatu modus kejahatan.

Salah satu aspek yang perlu diperhatikan ialah ketimpangan posisi antara pelaku dan korban. Ketika seseorang menguasai informasi pribadi yang dapat merugikan pihak lain, korban dapat mengalami tekanan karena tidak mengetahui kapan, kepada siapa, dan sejauh mana informasi tersebut akan disebar. Situasi ini dapat menimbulkan kecemasan, rasa malu, gangguan terhadap hubungan sosial, bahkan kekhawatiran terhadap keselamatan diri dan keluarga. Dengan demikian, praktik pemerasan melalui penyebaran data pribadi tidak hanya berkaitan dengan potensi kerugian materiil, tetapi juga menyangkut keamanan, kebebasan mengambil keputusan, dan kondisi psikologis korban. Modus pemerasan dapat terjadi dalam hubungan personal, transaksi daring, penipuan identitas, maupun penyalahgunaan akses terhadap akun elektronik. Dalam sejumlah kasus, pelaku menggunakan foto atau percakapan yang sebelumnya diberikan korban dalam hubungan yang bersifat pribadi. Dalam keadaan lain, informasi diperoleh melalui akses tanpa hak atau dari pihak ketiga. Cara memperoleh data tersebut perlu diperiksa karena dapat berkaitan dengan dugaan tindak pidana lainnya. Namun, asal-usul data harus dibedakan dari tindakan mengancam atau memeras, sebab masing-masing perbuatan mempunyai unsur hukum yang perlu dianalisis secara tersendiri. Tuntutan pelaku tidak selalu berupa uang. Pelaku dapat meminta barang, akses terhadap akun, penghapusan unggahan, penarikan laporan, atau tindakan tertentu. Akan tetapi, tidak seluruh bentuk tuntutan tersebut secara otomatis memenuhi unsur Pasal 27B ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik. Penerapan ketentuan pidana harus didasarkan pada jenis tuntutan dan unsur yang secara tegas dirumuskan dalam undang-undang (Indonesia, UU No. 1 Tahun 2024, Pasal 27B ayat (2)). Selain itu, penting untuk membedakan ancaman yang bertujuan melakukan pemerasan dari pemberitahuan mengenai tindakan yang sah. Pernyataan seseorang bahwa ia akan melaporkan dugaan pelanggaran kepada aparat penegak hukum tidak dengan sendirinya merupakan tindak pidana pemerasan. Penilaian hukum menjadi berbeda apabila ancaman digunakan untuk memaksa orang lain

menyerahkan sesuatu secara melawan hukum. Oleh sebab itu, isi komunikasi, konteks, tujuan, serta hubungan antara ancaman dan tuntutan harus diperiksa secara menyeluruh.

B. Analisis Hukum Pidana terhadap Pemerasan melalui Penyebaran Data Pribadi Berdasarkan UU ITE, UU PDP, dan KUHP Nasional

Analisis hukum pidana terhadap praktik pemerasan melalui penyebaran data pribadi perlu dimulai dengan mengidentifikasi ketentuan hukum yang relevan dan menghubungkannya dengan fakta yang dapat dibuktikan. Salah satu ketentuan yang dapat dikaji ialah Pasal 27B ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik. Ketentuan tersebut mengatur perbuatan yang dilakukan dengan sengaja dan tanpa hak untuk mendistribusikan dan/atau mentransmisikan informasi elektronik atau dokumen elektronik, dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, serta menggunakan ancaman pencemaran atau ancaman membuka rahasia untuk memaksa seseorang memberikan barang, memberi utang, membuat pengakuan utang, atau menghapuskan piutang (Indonesia, UU No. 1 Tahun 2024, Pasal 27B ayat (2)). Ketentuan pidananya diatur dalam Pasal 45 ayat (10) UU ITE, yang menetapkan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1.000.000.000,00. Pasal 45 ayat (11) juga menentukan bahwa tindak pidana sebagaimana dimaksud dalam Pasal 45 ayat (10) hanya dapat dituntut atas pengaduan korban (Indonesia, UU No. 1 Tahun 2024, Pasal 45 ayat (10) dan ayat (11)). Penerapan ketentuan tersebut mengharuskan penegak hukum membuktikan setiap unsur tindak pidana secara cermat. Unsur kesengajaan perlu dinilai berdasarkan tindakan dan keadaan yang menunjukkan adanya kehendak pelaku untuk melakukan perbuatan yang dilarang. Isi pesan, pola komunikasi, tindakan lanjutan, serta hubungan antara ancaman dan tuntutan dapat menjadi bahan penilaian. Perasaan takut yang dialami korban merupakan keadaan yang penting untuk dipahami, tetapi pembuktian unsur tindak pidana tetap harus didasarkan pada keseluruhan fakta dan alat bukti yang relevan. Unsur tanpa hak juga memerlukan pemeriksaan mengenai ada atau tidaknya dasar hukum yang membenarkan tindakan pelaku. Seseorang yang menguasai data pribadi tidak otomatis memiliki kewenangan untuk mengungkapkan atau menggunakannya sebagai alat pemaksaan. Oleh karena itu, perlu ditelusuri bagaimana data diperoleh, siapa yang mengendalikan akun, kepada siapa informasi dikirimkan, dan apa tujuan komunikasi tersebut.

Unsur mendistribusikan dan/atau mentransmisikan informasi elektronik harus dihubungkan dengan tindakan yang benar-benar terjadi. Pengiriman pesan, lampiran dokumen, atau unggahan digital dapat menjadi bagian dari pemeriksaan sepanjang memenuhi rumusan yang ditentukan undang-undang. Bukti elektronik yang digunakan dalam proses hukum juga perlu dinilai berdasarkan keaslian, integritas, dan konteksnya. UU ITE mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah sesuai dengan ketentuan Pasal 5 UU ITE (Indonesia, UU No. 11 Tahun 2008 sebagaimana telah diubah terakhir dengan UU No. 1 Tahun 2024, Pasal 5). Unsur maksud memperoleh keuntungan secara melawan hukum juga harus dibuktikan berdasarkan keadaan konkret. Permintaan uang yang disertai ancaman dapat menjadi petunjuk penting, tetapi hubungan antara ancaman, tuntutan, dan tujuan pelaku tetap perlu diperiksa. Konflik utang-piutang tidak serta-merta dapat dikategorikan sebagai pemerasan. Penilaian harus diarahkan pada ada atau tidaknya pemaksaan melalui ancaman yang memenuhi unsur tindak pidana sebagaimana dirumuskan dalam ketentuan yang diterapkan. Di samping UU ITE, UU PDP memberikan dasar hukum untuk menilai perolehan, pengungkapan, dan penggunaan data pribadi secara melawan hukum. Pasal 65 ayat (1) melarang perolehan atau pengumpulan data pribadi yang bukan milik pelaku secara melawan hukum dengan maksud menguntungkan diri sendiri atau orang lain dan yang dapat mengakibatkan kerugian bagi subjek data. Pasal 65 ayat (2) melarang pengungkapan data pribadi yang bukan miliknya secara melawan hukum, sedangkan Pasal 65 ayat (3) melarang penggunaan data pribadi yang bukan miliknya secara melawan hukum (Indonesia, UU No. 27 Tahun 2022, Pasal 65 ayat (1)–ayat (3)). Ancaman pidana terhadap perbuatan tersebut diatur dalam Pasal 67 UU PDP. Ketentuan tersebut membedakan ancaman pidana berdasarkan bentuk perbuatannya. Oleh karena itu, penerapan ancaman pidana harus disesuaikan dengan ayat yang relevan dan unsur yang terbukti dalam perkara, bukan hanya berdasarkan adanya penyebaran data pribadi (Indonesia, UU No. 27 Tahun 2022, Pasal 67 ayat (1)–ayat (3)). Dalam perkara pemerasan, perolehan data, pengungkapan data, dan penggunaan data perlu dibedakan agar analisis hukum tidak mencampuradukkan perbuatan yang mempunyai karakteristik berbeda. Seseorang mungkin memperoleh data melalui akses tanpa hak, kemudian menggunakannya untuk mengancam korban, dan akhirnya menyebarkannya kepada pihak lain. Setiap tindakan tersebut perlu diperiksa

berdasarkan unsur ketentuan yang sesuai. Penerapan beberapa pasal harus mempertimbangkan fakta yang terbukti, hubungan antara perbuatan, dan aturan mengenai perbarengan tindak pidana.

Hubungan antara UU ITE, UU PDP, dan Kitab Undang-Undang Hukum Pidana Nasional juga perlu diperhatikan. UU PDP berfokus pada perlindungan data pribadi, sedangkan UU ITE mengatur perbuatan tertentu yang dilakukan melalui sistem elektronik, termasuk pemaksaan dengan ancaman pencemaran atau membuka rahasia sebagaimana diatur dalam Pasal 27B ayat (2). Satu rangkaian kejadian dapat berkaitan dengan beberapa ketentuan hukum, tetapi hal tersebut tidak berarti seluruh pasal harus selalu diterapkan secara kumulatif. Untuk menentukan hubungan antarketentuan, perlu diperiksa apakah perbuatan yang didakwakan berbeda secara faktual, apakah satu tindakan memenuhi unsur lebih dari satu ketentuan, apakah terdapat aturan khusus yang relevan, serta bagaimana ketentuan mengenai perbarengan tindak pidana diterapkan. Analisis tersebut penting untuk menghindari pengulangan penghukuman terhadap perbuatan yang sama dan memastikan bahwa setiap dakwaan mempunyai dasar hukum yang jelas. KUHP Nasional berdasarkan Undang-Undang Nomor 1 Tahun 2023 mulai berlaku pada 2 Januari 2026. Oleh karena itu, penentuan dasar hukum terhadap perbuatan yang terjadi setelah tanggal tersebut perlu mempertimbangkan ketentuan KUHP Nasional dan peraturan penyesuaian pidana yang berlaku. Untuk perbuatan yang terjadi sebelumnya, perlu diperiksa hukum yang berlaku pada saat perbuatan dilakukan serta ketentuan mengenai perubahan peraturan pidana (Indonesia, UU No. 1 Tahun 2023, Pasal 624). Asas legalitas menghendaki agar seseorang hanya dapat dipidana berdasarkan ketentuan hukum yang berlaku dan apabila unsur tindak pidana yang didakwakan terbukti. Perkembangan teknologi dapat melahirkan modus kejahatan baru, tetapi keadaan tersebut tidak membenarkan penciptaan tindak pidana melalui analogi yang merugikan terdakwa. Penafsiran hukum harus tetap memperhatikan batas rumusan undang-undang, sekaligus mempertimbangkan tujuan perlindungan terhadap kepentingan hukum yang terancam. Pertanggungjawaban pidana juga perlu ditentukan berdasarkan peran dan keterlibatan setiap orang. Pihak yang membuat ancaman, memperoleh data, mengunggah informasi, atau meneruskan konten dapat memiliki tingkat pengetahuan dan kontribusi yang berbeda. Apabila penyebaran dilakukan melalui beberapa akun, penyidik perlu memastikan apakah akun-akun tersebut dikendalikan oleh satu orang, digunakan oleh beberapa orang yang bekerja sama, atau dioperasikan oleh pihak lain yang tidak mengetahui konteks perbuatan. Dengan demikian, penetapan pertanggungjawaban harus didasarkan pada bukti individual mengenai tindakan, kesalahan, dan unsur ketentuan pidana yang relevan.

C. Pembuktian, Tantangan Penegakan Hukum, Perlindungan Korban, dan Upaya Penguatan Penanganan Perkara

Pembuktian elektronik memiliki peranan penting dalam mengungkap praktik pemerasan melalui penyebaran data pribadi. Bukti yang relevan dapat berupa pesan langsung, percakapan melalui aplikasi, surat elektronik, rekaman panggilan, tautan unggahan, identitas akun, metadata, bukti transaksi, dan catatan akses. Bukti tersebut dapat membantu menjelaskan hubungan antara ancaman dan tuntutan, mengidentifikasi akun yang digunakan, serta menyusun urutan peristiwa. Penggunaan bukti elektronik dalam perkara perlindungan data pribadi juga memperoleh landasan dalam Pasal 64 ayat (3) UU PDP yang mengakui alat bukti menurut hukum acara dan alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan (Indonesia, UU No. 27 Tahun 2022, Pasal 64 ayat (3)). Tangkapan layar dapat menjadi dokumentasi awal, tetapi sebaiknya didukung oleh sumber asli apabila masih tersedia. Korban dapat menyimpan perangkat, mengeksplor percakapan, mencatat waktu kejadian, menyimpan tautan unggahan, dan mendokumentasikan nama akun yang digunakan. Berkas asli sebaiknya tidak diubah sebelum diserahkan kepada penyidik. Dalam perkara yang memuat informasi sensitif, penggandaan bukti perlu dilakukan secara terbatas agar proses pembuktian tidak justru memperluas penyebaran data yang merugikan korban. Pemeliharaan rantai penguasaan barang bukti atau *chain of custody* penting untuk memastikan bahwa proses akses, penyalinan, pemindahan, dan pemeriksaan bukti dapat ditelusuri. Dokumentasi yang baik membantu mengurangi keraguan mengenai perubahan atau manipulasi data. Dalam perkara yang melibatkan beberapa platform, bukti yang diperoleh korban dapat dikaitkan dengan informasi dari penyedia layanan melalui prosedur resmi. Keterangan korban tetap mempunyai arti penting, tetapi harus dinilai bersama alat bukti lainnya sesuai dengan ketentuan hukum yang berlaku. Identifikasi pelaku dapat menjadi lebih sulit apabila akun menggunakan nama samaran, nomor sementara, atau perangkat yang digunakan bersama. Oleh karena itu, penyidik perlu menghubungkan bukti komunikasi dengan informasi transaksi, pola penggunaan akun, keterangan saksi, dan data

elektronik lain yang diperoleh secara sah. Identitas pelaku tidak seharusnya disimpulkan hanya berdasarkan nama profil atau foto akun karena informasi tersebut dapat dipalsukan atau digunakan oleh orang lain. Dalam perkara yang melibatkan foto intim, informasi kesehatan, atau data anak, kerahasiaan bukti perlu dijaga secara khusus. Akses terhadap informasi harus dibatasi pada pihak yang berkepentingan dan berwenang. Penggandaan yang tidak diperlukan dapat menambah risiko penyebaran ulang dan memperbesar dampak yang dialami korban. Dengan demikian, pengelolaan bukti tidak hanya berkaitan dengan kepentingan pembuktian, tetapi juga merupakan bagian dari upaya melindungi martabat dan hak korban selama proses hukum berlangsung.

Salah satu hambatan dalam penegakan hukum ialah kekhawatiran korban untuk melaporkan peristiwa yang dialaminya. Ancaman penyebaran data dapat menimbulkan rasa malu, ketakutan terhadap reaksi keluarga atau lingkungan kerja, serta kekhawatiran akan terjadinya penyebaran yang lebih luas. Keadaan tersebut dapat membuat korban menunda pelaporan dan berpotensi menyebabkan hilangnya bukti elektronik. Oleh karena itu, diperlukan mekanisme pelaporan yang mudah diakses, menjaga kerahasiaan, dan memberikan ruang bagi korban untuk menyampaikan pengalamannya tanpa menghadapi perlakuan yang menyalahkan atau merendahkan. Perlindungan terhadap korban perlu ditempatkan sebagai bagian penting dalam penegakan hukum. Sejak tahap pelaporan, korban perlu memperoleh informasi yang jelas mengenai proses hukum, pilihan perlindungan, dan cara mengamankan bukti. Petugas juga perlu menjaga kerahasiaan data serta menghindari pertanyaan yang tidak relevan atau menyudutkan korban. Apabila terdapat ancaman terhadap keselamatan, kebutuhan untuk memperoleh tempat aman dan bantuan yang sesuai harus menjadi perhatian utama. Dampak pemerasan melalui penyebaran data pribadi tidak selalu berakhir setelah ancaman dihentikan atau pelaku diproses secara hukum. Korban dapat mengalami tekanan psikologis, gangguan hubungan sosial, kerugian ekonomi, atau kesulitan memulihkan reputasi. Oleh sebab itu, perlindungan perlu mencakup akses terhadap bantuan hukum, pendampingan psikologis, penanganan risiko pencurian identitas, dan dukungan untuk memulihkan kehidupan sosial korban. Bentuk pendampingan harus disesuaikan dengan kebutuhan masing-masing individu tanpa memaksa korban membuka informasi pribadi kepada pihak yang tidak berkepentingan. Penghapusan konten atau pembatasan akses juga dapat menjadi bagian dari pemulihan. Namun, penghapusan tidak selalu menjamin bahwa seluruh salinan informasi telah hilang. Oleh karena itu, penyimpanan bukti, pelaporan kepada platform, permintaan pembatasan distribusi ulang, dan pemantauan risiko perlu dipertimbangkan secara terkoordinasi. Dalam keadaan tertentu, bukti perlu diamankan terlebih dahulu sebelum konten dihapus atau tidak lagi dapat diakses.

Platform digital mempunyai peran praktis dalam mengurangi penyebaran data pribadi melalui penyediaan mekanisme pelaporan yang mudah dipahami, penanganan konten yang memuat informasi sensitif, dan prosedur untuk menjaga bukti yang relevan. Namun, pertanggungjawaban hukum platform tidak dapat disimpulkan secara otomatis hanya karena terjadi penyebaran data. Penilaiannya perlu memperhatikan ketentuan hukum, peran platform, kewajiban yang melekat padanya, serta tindakan yang dilakukan setelah menerima laporan. Organisasi yang mengumpulkan dan memproses data pribadi perlu menerapkan tata kelola keamanan yang memadai, seperti pembatasan akses, autentikasi yang kuat, pencatatan aktivitas, pelatihan pegawai, dan prosedur penanganan insiden. Apabila terjadi kebocoran data, organisasi perlu mengevaluasi penyebabnya dan memenuhi kewajiban yang ditetapkan oleh peraturan perundang-undangan. Tanggung jawab organisasi dalam menjaga keamanan data harus dibedakan dari pertanggungjawaban pidana individu yang menggunakan informasi sebagai alat pemerasan. Penerapan norma hukum dapat dijelaskan melalui ilustrasi. Apabila seseorang mengancam akan menyebarkan percakapan pribadi kepada keluarga korban apabila korban tidak mentransfer sejumlah uang, penegak hukum perlu memeriksa isi ancaman, tuntutan pembayaran, tujuan memperoleh keuntungan, media komunikasi yang digunakan, dan bukti yang menghubungkan akun dengan pelaku. Pasal 27B ayat (2) UU ITE dapat dipertimbangkan apabila seluruh unsur yang dirumuskan di dalamnya terbukti. Apabila pelaku juga mengungkapkan data pribadi secara melawan hukum, ketentuan UU PDP dapat dianalisis berdasarkan fakta dan unsur yang relevan. Dalam ilustrasi lain, seseorang mengancam akan mengirimkan informasi privat kepada pemberi kerja apabila korban tidak menarik laporan kepada aparat penegak hukum. Dalam keadaan tersebut, penilaian harus diarahkan pada sifat ancaman, tujuan pelaku, dan kesesuaian tuntutan dengan unsur tindak pidana yang diterapkan. Penegak hukum tidak boleh memperluas rumusan delik hanya karena tindakan tersebut dipandang tidak patut. Sebaliknya, apabila seseorang menyebarkan alamat dan nomor telepon korban tanpa mengajukan tuntutan apa pun, perbuatan itu dapat menimbulkan persoalan perlindungan data

pribadi, tetapi unsur pemerasan tidak dapat langsung dianggap terpenuhi. Berdasarkan berbagai persoalan tersebut, penguatan penegakan hukum perlu dilakukan melalui penyusunan pedoman pemeriksaan yang membantu membedakan perkara pemerasan, ancaman, pengungkapan data pribadi, dan akses tanpa hak. Peningkatan kapasitas aparat penegak hukum dalam bidang forensik digital juga perlu disertai pemahaman mengenai autentikasi bukti, rantai penguasaan barang bukti, prosedur permintaan data kepada penyedia layanan, dan perlindungan informasi sensitif. Koordinasi dengan platform perlu diarahkan pada pengamanan bukti dan pembatasan penyebaran ulang, sedangkan pendidikan publik perlu menekankan keamanan digital dan pilihan bantuan yang tersedia bagi korban. Edukasi tersebut harus dilakukan tanpa menyalahkan korban atas informasi yang pernah dibagikan atau hubungan yang pernah dipercayainya. Evaluasi penegakan hukum juga sebaiknya tidak hanya berorientasi pada jumlah laporan atau pemidanaan, tetapi turut memperhatikan kualitas pembuktian, waktu respons, keberhasilan membatasi penyebaran data, serta pengalaman korban selama proses hukum. Dengan demikian, penanganan praktik pemerasan melalui penyebaran data pribadi memerlukan pendekatan yang mengintegrasikan ketepatan penerapan hukum pidana, pembuktian elektronik yang dapat dipertanggungjawabkan, perlindungan terhadap korban, dan penguatan tata kelola keamanan data. Penerapan sanksi pidana harus didasarkan pada terpenuhinya unsur tindak pidana, sedangkan langkah pemulihan perlu diarahkan pada perlindungan hak dan pengurangan dampak yang dialami korban. Melalui pendekatan tersebut, penegakan hukum diharapkan tidak hanya memberikan kepastian hukum, tetapi juga menghadirkan keadilan yang menghormati martabat manusia dan mencegah penyalahgunaan data pribadi sebagai sarana ancaman maupun pemaksaan secara melawan hukum.

KESIMPULAN

Praktik pemerasan melalui penyebaran data pribadi memadukan ancaman, pemanfaatan informasi privat, dan tuntutan untuk memperoleh keuntungan atau memaksa tindakan. UU ITE sebagaimana diubah dengan UU Nomor 1 Tahun 2024 relevan ketika fakta memenuhi unsur Pasal 27B ayat (2), termasuk penggunaan informasi atau dokumen elektronik, ancaman pencemaran atau membuka rahasia, dan pemaksaan untuk memenuhi tuntutan yang ditentukan norma. UU PDP dapat menjangkau perolehan, pengungkapan, atau penggunaan data pribadi secara melawan hukum. Kedua rezim perlu dianalisis secara cermat berdasarkan unsur dan fakta yang terbukti. Penerapan hukum harus memperhatikan asas legalitas, kepastian hukum, waktu terjadinya perbuatan, dan hubungan antarketentuan. KUHP nasional yang berlaku sejak 2 Januari 2026 serta aturan penyesuaian pidana perlu diperiksa apabila relevan dengan waktu dan konstruksi perkara. Tidak setiap pengungkapan data merupakan pemerasan, dan tidak setiap konflik pembayaran otomatis menjadi tindak pidana. Penentuan pasal membutuhkan pemeriksaan unsur secara individual. Bukti elektronik perlu diamankan dengan memperhatikan autentisitas, konteks, dan rantai penguasaan. Perlindungan korban tidak boleh berhenti pada proses penindakan, tetapi perlu mencakup pembatasan penyebaran ulang, kerahasiaan identitas, pendampingan, dan pemulihan. Penegakan hukum yang baik menggabungkan ketepatan norma, kualitas pembuktian, respons yang aman bagi korban, dan koordinasi dengan pihak yang relevan.

DAFTAR PUSTAKA

- Moeljatno. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta, berbagai edisi. Edisi yang digunakan perlu dicantumkan oleh penulis.
- Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.
- Republik Indonesia. Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.