Journal of Law and Nation (JOLN)
Vol. 4 No. 4 (2026) hal. 382-392
e-ISSN: 2962-9675

HARMONISASI PERTANGGUNGJAWABAN PIDANA DAN GANTI KERUGIAN PERDATA DALAM KASUS PENCILAN DATA (DATA BREACH): TINJAUAN YURIDIS TERHADAP PERLINDUNGAN KORBAN DI ERA DIGITAL

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta,
widjaja_gunawan@yahoo.com

Abstract
This article discusses the harmonisation of criminal liability and civil damages in cases of data breaches in Indonesia as an effort to strengthen victim protection in the digital age. Breaches of personal data cause losses that are not only material but also immaterial, thus requiring a legal approach that goes beyond merely punishing the perpetrators to also restoring the victims' rights. This study demonstrates that Law No. 27 of 2022 on Personal Data Protection has provided a normative basis for the enforcement of criminal penalties and civil compensation; however, its implementation still faces challenges regarding the burden of proof, compensation mechanisms, and the integration of criminal and civil proceedings. Therefore, harmonisation of regulations and law enforcement is required to ensure that victim protection becomes more effective, fair, and responsive to developments in digital crime.
Keywords*: criminal liability; civil damages; data leakage; personal data protection; victim protection.*

Abstrak
Artikel ini membahas harmonisasi pertanggungjawaban pidana dan ganti kerugian perdata dalam kasus pencilan data (*data breach*) di Indonesia sebagai upaya memperkuat perlindungan korban di era digital. Kebocoran data pribadi menimbulkan kerugian yang tidak hanya bersifat material, tetapi juga immaterial, sehingga memerlukan pendekatan hukum yang tidak berhenti pada penghukuman pelaku, melainkan juga pemulihan hak korban. Kajian ini menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar normatif bagi penegakan pidana dan ganti rugi, namun implementasinya masih menghadapi tantangan dalam aspek pembuktian, mekanisme kompensasi, dan integrasi antara proses pidana serta perdata. Oleh karena itu, diperlukan harmonisasi regulasi dan penegakan hukum agar perlindungan korban menjadi lebih efektif, adil, dan responsif terhadap perkembangan kejahatan digital.
Kata kunci: pertanggungjawaban pidana; ganti kerugian perdata; pencilan data; pelindungan data pribadi; perlindungan korban.

Pendahuluan

Perkembangan teknologi digital telah mengubah cara masyarakat berinteraksi, bertransaksi, dan menyimpan informasi pribadi. Hampir setiap aktivitas modern kini meninggalkan jejak data, mulai dari identitas, alamat, nomor telepon, riwayat transaksi, hingga data biometrik, yang semuanya memiliki nilai ekonomi dan hukum yang tinggi. Dalam konteks ini, kebocoran data atau *data breach* bukan lagi sekadar persoalan teknis keamanan sistem, melainkan telah menjadi persoalan hukum yang menyentuh hak privasi, keamanan digital, dan perlindungan korban. Indonesia sendiri telah memperkuat kerangka hukumnya melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menegaskan pentingnya pengelolaan data secara bertanggung jawab (Taylor, 2020).

Fenomena kebocoran data semakin sering terjadi seiring meningkatnya penggunaan platform digital di berbagai sektor, termasuk perdagangan elektronik, layanan keuangan, pendidikan, dan pemerintahan. Dalam banyak kasus, korban tidak hanya mengalami gangguan administratif, tetapi juga kerugian material seperti penipuan, pencurian identitas, dan penyalahgunaan akun, bahkan kerugian immaterial berupa rasa cemas, hilangnya rasa aman, dan turunnya reputasi. Situasi ini menunjukkan bahwa kebocoran data tidak dapat dipandang sebagai kejadian yang berdiri sendiri, melainkan harus dipahami sebagai peristiwa yang menimbulkan akibat hukum kompleks dan berlapis (Vila Seoane, 2021).

Secara yuridis, perlindungan terhadap korban kebocoran data membutuhkan instrumen hukum yang mampu menjangkau dua ranah sekaligus, yaitu ranah pidana dan perdata. Ranah pidana berfungsi memberi sanksi kepada pelaku yang sengaja atau lalai dalam melanggar norma hukum, sedangkan ranah perdata memberikan ruang pemulihan bagi korban melalui ganti kerugian dan pemulihan hak. Namun dalam praktik, kedua rezim ini sering berjalan sendiri-sendiri sehingga perlindungan korban menjadi tidak optimal. Ketiadaan harmonisasi antara pertanggungjawaban pidana dan ganti kerugian perdata menyebabkan korban kerap memperoleh kepastian hukum yang terbatas, meskipun kerugian yang diderita nyata dan signifikan (Sylviana et al., 2025).

Dalam perspektif hukum perlindungan data, subjek data memiliki hak untuk mengetahui penggunaan data pribadinya, meminta perbaikan, menolak pemrosesan tertentu, dan menuntut pertanggungjawaban jika terjadi pelanggaran. UU PDP juga mewajibkan pengendali data memberi pemberitahuan apabila terjadi kegagalan perlindungan data pribadi dalam jangka waktu tertentu. Kewajiban tersebut menunjukkan bahwa negara menempatkan korban bukan sekadar sebagai pihak yang dirugikan, tetapi sebagai pemegang hak yang harus dipulihkan secara hukum (Supeno et al., 2025).

Meskipun demikian, pengaturan normatif belum sepenuhnya menjawab persoalan praktis yang muncul dalam kasus data breach. Salah satu persoalan utama adalah pembuktian hubungan kausal antara kelalaian pengelola data dan kerugian yang dialami korban. Dalam perkara digital, sumber kebocoran sering sulit diidentifikasi karena pelaku dapat berada di berbagai yurisdiksi, menggunakan teknik penyamaran, atau memanfaatkan kelemahan sistem yang kompleks. Akibatnya, pembuktian pidana maupun perdata menjadi menantang, sementara korban tetap membutuhkan perlindungan yang cepat dan efektif (Versaci, 2018).

Di sisi lain, pertanggungjawaban pidana dalam kasus kebocoran data memiliki fungsi penting sebagai instrumen pencegahan dan penjeraan. Sanksi pidana tidak hanya diarahkan kepada pelaku langsung, tetapi juga dapat menjadi tekanan normatif bagi korporasi dan penyelenggara sistem elektronik agar membangun standar keamanan yang lebih baik. Dalam UU PDP, sanksi pidana dan administratif menunjukkan bahwa pembentuk undang-undang menyadari bahwa pelanggaran data bukan sekadar kesalahan operasional, melainkan dapat mencapai derajat pelanggaran serius terhadap hak asasi dan kepentingan publik (Yudha et al., 2025). Namun, efektivitas sanksi pidana tidak selalu otomatis berbanding lurus dengan pemulihan korban. Dalam banyak sistem hukum, pidana lebih menekankan penghukuman terhadap pelaku, sedangkan korban masih harus menempuh jalur lain untuk memperoleh kompensasi. Di sinilah problem utama dalam kasus data breach muncul: korban dapat mengetahui bahwa ada pelanggaran hukum, tetapi belum tentu memperoleh ganti rugi yang

memadai. Oleh karena itu, pembahasan mengenai harmonisasi antara pidana dan perdata menjadi penting agar perlindungan hukum tidak berhenti pada penghukuman semata, melainkan juga menyentuh aspek reparasi (Sylviana et al., 2025).

Ganti kerugian perdata dalam kasus kebocoran data umumnya bertumpu pada prinsip perbuatan melawan hukum dan tanggung jawab atas kelalaian. Korban dapat mengajukan tuntutan apabila dapat menunjukkan adanya perbuatan yang melanggar kewajiban hukum, timbulnya kerugian, dan hubungan sebab-akibat antara keduanya. Akan tetapi, dalam perkara data breach, kerugian sering bersifat tidak langsung dan tersebar, misalnya biaya pemulihan akun, kehilangan kesempatan bisnis, atau tekanan psikologis akibat penyalahgunaan data. Kondisi ini menuntut pendekatan hukum perdata yang lebih adaptif terhadap realitas digital modern (Yudha et al., 2025).

Masalah lain yang muncul adalah belum seragamnya mekanisme kompensasi bagi korban. Dalam praktik, korban dapat menempuh gugatan individual, gugatan kelompok, atau langkah administratif sesuai mekanisme yang tersedia. Namun jalur-jalur tersebut sering memerlukan biaya, waktu, dan kemampuan pembuktian yang tidak ringan. Karena itu, perlindungan korban dalam kasus data breach seharusnya tidak hanya bergantung pada kemampuan individu untuk menggugat, tetapi juga pada desain hukum yang memungkinkan pemulihan lebih efisien, sederhana, dan berorientasi pada korban (Versaci, 2018).

Dalam konteks kebijakan hukum, harmonisasi pertanggungjawaban pidana dan ganti kerugian perdata penting untuk membangun sistem perlindungan yang utuh. Pidana berperan menegakkan norma dan memberi efek jera, sedangkan perdata berfungsi memulihkan posisi korban seperti sebelum kerugian terjadi sejauh mungkin. Keduanya tidak seharusnya dipertentangkan, melainkan disusun secara saling melengkapi. Dengan begitu, penegakan hukum tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada keadilan substantif bagi korban yang terdampak (Yu & Zhao, 2019).

Kebutuhan akan harmonisasi juga semakin mendesak karena kebocoran data berpotensi merusak kepercayaan publik terhadap ekosistem digital. Dalam era ekonomi digital, kepercayaan merupakan aset penting yang menentukan keberlangsungan layanan online dan partisipasi masyarakat. Jika korban merasa tidak terlindungi, maka ketakutan untuk menggunakan layanan digital akan meningkat dan hal ini dapat menghambat transformasi digital nasional. Oleh sebab itu, perlindungan korban kebocoran data tidak hanya relevan dari sisi hukum privat dan pidana, tetapi juga strategis bagi pembangunan ekonomi digital (Ventura & Coeli, 2018).

Berdasarkan uraian tersebut, artikel ini penting untuk menelaah bagaimana pertanggungjawaban pidana dan ganti kerugian perdata dapat diharmonisasikan dalam kasus pencilan data (*data breach*) guna memperkuat perlindungan korban di era digital. Kajian ini menempatkan korban sebagai pusat analisis, sekaligus menyoroti kebutuhan pembaruan hukum agar sistem perlindungan data di Indonesia tidak berhenti pada norma formal, tetapi benar-benar memberi keadilan, kepastian, dan kemanfaatan hukum.

Metode Penelitian

Metode penelitian yang digunakan dalam artikel ini adalah kajian pustaka dengan pendekatan yuridis normatif, yaitu penelitian yang menitikberatkan pada penelaahan bahan-bahan hukum primer, sekunder, dan tersier yang relevan dengan isu pertanggungjawaban pidana

serta ganti kerugian perdata dalam kasus pencilan data (*data breach*). Kajian dilakukan melalui analisis terhadap peraturan perundang-undangan, literatur ilmiah, jurnal nasional dan internasional, buku, dan dokumen lainnya yang membahas perlindungan data pribadi, hukum pidana, hukum perdata, serta perlindungan korban di era digital (Walliman & Walliman, 2021). Dengan metode ini, penulisan bertujuan untuk menemukan konsep, prinsip, dan konstruksi hukum yang dapat digunakan sebagai dasar harmonisasi antara rezim pidana dan perdata dalam rangka memberikan perlindungan hukum yang lebih efektif bagi korban kebocoran data (Eliyah & Aslan, 2025).

Hasil dan Pembahasan

Pertanggungjawaban Pidana dalam Kasus Data Breach di Indonesia

Pertanggungjawaban pidana dalam kasus "data breach" di Indonesia berangkat dari kenyataan bahwa kebocoran data bukan lagi sekadar insiden teknis, melainkan perbuatan yang dapat menimbulkan kerugian hukum bagi subjek data pribadi. Dalam era digital, data pribadi memiliki nilai ekonomi, sosial, dan strategis, sehingga penyalahgunaan, pengambilan tanpa hak, atau pengungkapan tanpa persetujuan dapat menimbulkan akibat yang serius. Karena itu, hukum pidana hadir sebagai instrumen represif untuk menindak pelaku yang dengan sengaja atau melawan hukum melanggar hak atas data pribadi (Supeno et al., 2025).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan tonggak penting dalam sistem hukum Indonesia karena untuk pertama kalinya terdapat pengaturan komprehensif yang secara eksplisit memuat larangan, kewajiban, serta sanksi bagi pelanggaran data pribadi. UU ini menegaskan bahwa pemrosesan data harus dilakukan secara terbatas, spesifik, sah, dan transparan, sehingga setiap penyimpangan dari prinsip tersebut dapat berimplikasi pada tanggung jawab hukum. Dengan demikian, kebocoran data tidak hanya dinilai sebagai kegagalan sistem, tetapi juga dapat dikualifikasikan sebagai perbuatan yang mengandung unsur pidana apabila terpenuhi unsur kesalahan dan melawan hukum (Yu & Zhao, 2019).

Dalam konstruksi hukum pidana, unsur pertanggungjawaban pidana mensyaratkan adanya perbuatan yang dilarang, kemampuan bertanggung jawab, adanya kesalahan, serta tidak adanya alasan pemaaf. Pada kasus "data breach", pertanggungjawaban dapat timbul baik karena kesengajaan maupun kelalaian, tergantung pada bentuk pelanggaran yang terjadi. Apabila pelaku secara sadar memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain untuk keuntungan diri sendiri atau pihak lain, maka perbuatannya memenuhi dimensi kesengajaan. Namun jika kebocoran timbul karena pengabaian standar keamanan yang semestinya dijalankan, maka kelalaian dapat menjadi dasar pertanggungjawaban yang tetap relevan dalam sistem perlindungan data pribadi (Santo et al., 2024).

Pasal-pasal pidana dalam UU PDP memperlihatkan bahwa pembentuk undang-undang menempatkan perlindungan data pribadi sebagai kepentingan hukum yang serius. Pasal 67, misalnya, mengatur ancaman pidana bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya, mengungkapkan data pribadi tanpa hak, atau menggunakan data pribadi tanpa hak. Ancaman pidana yang disediakan mencapai penjara dan denda miliaran rupiah, yang menunjukkan orientasi normatif untuk memberi efek jera terhadap pelaku pelanggaran data (Putri & Putra, 2024). Selain itu, UU PDP juga mengatur tanggung jawab yang dapat dikenakan kepada korporasi. Hal ini penting karena

dalam praktik, kebocoran data sering kali berasal dari sistem yang dikelola oleh badan usaha, platform digital, atau penyelenggara sistem elektronik. Ketika korporasi lalai menerapkan tata kelola keamanan yang memadai, maka korporasi tidak dapat berlindung di balik alasan teknis semata. Pertanggungjawaban korporasi menjadi penting agar tidak terjadi impunitas terhadap entitas bisnis yang memperoleh keuntungan dari pengelolaan data tetapi mengabaikan keamanan subjek data (Truli, 2018).

Model pertanggungjawaban korporasi dalam UU PDP sejalan dengan perkembangan hukum pidana modern yang mengakui korporasi sebagai subjek tindak pidana. Dalam konteks kebocoran data, korporasi dapat dikenai pidana denda yang besar dan pidana tambahan seperti perampasan keuntungan, pembekuan kegiatan usaha, penutupan tempat usaha, pencabutan izin, bahkan pembubaran korporasi. Pengaturan ini menunjukkan bahwa negara tidak hanya mengejar pelaku individu, tetapi juga struktur organisasi yang menjadi penyebab atau memungkinkan terjadinya pelanggaran data (Taylor, 2020).

Di samping UU PDP, rezim hukum lain juga dapat menjadi dasar penegakan pidana terhadap kebocoran data pribadi, khususnya Undang-Undang Informasi dan Transaksi Elektronik. Pasal 26 UU ITE selama ini memberi dasar bagi seseorang untuk mengajukan gugatan apabila data pribadinya digunakan tanpa persetujuan, dan ketentuan ini sering dikaitkan dengan perlindungan atas privasi digital. Walaupun UU ITE bukan undang-undang khusus perlindungan data, keberadaannya menunjukkan bahwa sistem hukum Indonesia telah lebih dahulu mengakui pentingnya hak atas data pribadi sebelum hadirnya UU PDP (Rotimi, 2025).

Dalam praktik penegakan hukum, tantangan utama pertanggungjawaban pidana pada kasus "data breach" adalah pembuktian. Pelaku kebocoran data sering kali tidak mudah dilacak karena menggunakan jaringan digital yang kompleks, berada di luar yurisdiksi nasional, atau bersembunyi di balik kelemahan sistem keamanan yang sulit diidentifikasi secara langsung. Di sisi lain, penegak hukum harus membuktikan unsur kesengajaan atau kelalaian, hubungan sebab akibat, dan adanya akibat kerugian. Kompleksitas pembuktian ini membuat proses pidana menjadi lebih rumit dibandingkan tindak pidana konvensional (Ventura & Coeli, 2018).

Masalah pembuktian juga berkaitan dengan karakteristik kerugian yang timbul dalam kasus kebocoran data. Tidak semua kerugian dapat segera terlihat, karena sebagian dampak baru muncul setelah data disalahgunakan dalam bentuk penipuan, pencurian identitas, atau transaksi ilegal. Oleh sebab itu, aparat penegak hukum perlu memahami bahwa kebocoran data memiliki sifat latent harm, yakni kerugian yang tersembunyi namun nyata. Konstruksi ini menuntut penafsiran hukum yang lebih adaptif agar pelaku tidak lolos hanya karena kerugian korban belum langsung tampak pada saat kejadian (Xiaying, 2019).

Dalam perspektif teori pemidanaan, sanksi pidana pada kasus kebocoran data tidak semata-mata bertujuan membalas kesalahan pelaku, tetapi juga mencegah terulangnya peristiwa serupa. Fungsi preventif ini penting karena keamanan data adalah fondasi kepercayaan publik terhadap ekosistem digital. Jika pelanggaran data terus dibiarkan tanpa konsekuensi pidana yang tegas, maka penyelenggara sistem elektronik akan cenderung menganggap perlindungan data sebagai beban administratif belaka, bukan sebagai kewajiban hukum yang substansial (Truli, 2018). Selain pidana pokok, UU PDP juga membuka ruang bagi penjatuhan pidana tambahan terhadap korporasi. Pidana tambahan ini penting karena dalam banyak kasus, denda saja belum cukup untuk menciptakan efek jera apabila keuntungan ekonomis yang diperoleh dari

pemrosesan data jauh lebih besar daripada sanksi yang dijatuhkan. Dengan demikian, perampasan keuntungan, pembekuan usaha, atau pencabutan izin merupakan instrumen penting agar pertanggungjawaban pidana memiliki daya tekan yang lebih kuat terhadap pelaku korporasi (Putri & Putra, 2024).

Kehadiran sanksi pidana dalam UU PDP juga menunjukkan adanya pergeseran paradigma dari sekadar perlindungan administratif menuju perlindungan yang lebih substantif. Negara tidak lagi memandang data pribadi hanya sebagai objek kepatuhan teknis, tetapi sebagai bagian dari hak asasi yang harus dilindungi dengan instrumen hukum yang tegas. Oleh karena itu, pelanggaran data pribadi yang memenuhi unsur kesalahan dapat diproses pidana sebagai bentuk pengakuan bahwa pelanggaran tersebut merugikan martabat, keamanan, dan kebebasan subjek data (Xiaying, 2019).

Namun demikian, keberadaan norma pidana yang tegas belum tentu otomatis menghasilkan perlindungan yang efektif. Efektivitas pertanggungjawaban pidana sangat bergantung pada konsistensi penegakan hukum, kemampuan forensik digital, koordinasi antarinstansi, dan kesadaran para pengendali data. Jika unsur-unsur tersebut lemah, maka norma pidana hanya menjadi ancaman di atas kertas tanpa daya guna nyata bagi korban. Karena itu, penguatan kapasitas institusional merupakan syarat mutlak agar aturan pidana dalam UU PDP benar-benar dapat bekerja dalam praktik (Vila Seoane, 2021).

Dengan demikian, pertanggungjawaban pidana dalam kasus "data breach" di Indonesia telah memiliki dasar hukum yang semakin kuat melalui UU PDP, UU ITE, dan prinsip-prinsip hukum pidana umum. Akan tetapi, keberhasilan implementasinya tetap bergantung pada pembuktian, penafsiran unsur kesalahan, dan kemampuan penegak hukum dalam menghadapi kejahatan digital yang bersifat lintas batas. Maka dengan itu, hukum pidana harus ditempatkan bukan hanya sebagai alat penghukuman, tetapi juga sebagai instrumen perlindungan hak konstitusional atas data pribadi di era digital.

Harmonisasi Pidana dan Perdata dalam Perlindungan Korban

Harmonisasi pidana dan perdata dalam perlindungan korban *data breach* pada dasarnya bertujuan menyatukan dua orientasi penegakan hukum yang selama ini kerap berjalan terpisah, yakni penghukuman pelaku dan pemulihan korban. Dalam kasus kebocoran data, korban tidak cukup hanya melihat pelaku dipidana, sebab kerugian yang dialami sering kali tetap berlangsung dalam bentuk penyalahgunaan identitas, hilangnya kendali atas data pribadi, kerugian ekonomi, serta gangguan psikologis. Oleh karena itu, perlindungan korban yang efektif harus dibangun melalui sistem yang memungkinkan sanksi pidana berjalan seiring dengan mekanisme ganti rugi perdata atau kompensasi yang nyata (Piansah, 2024).

Secara konseptual, hukum pidana dan hukum perdata memiliki fungsi yang berbeda tetapi saling melengkapi. Hukum pidana menitikberatkan pada pelanggaran terhadap ketertiban umum dan kepentingan publik, sehingga fokus utamanya adalah pembalasan, pencegahan, dan penjeraan terhadap pelaku. Sebaliknya, hukum perdata berorientasi pada pemulihan hak-hak privat pihak yang dirugikan melalui kompensasi, rehabilitasi, atau bentuk pemulihan lain. Dalam konteks kebocoran data, pemisahan yang terlalu kaku antara kedua rezim tersebut justru dapat mengakibatkan korban berada dalam posisi yang lemah karena harus menempuh jalur yang berbeda untuk memperoleh keadilan penuh (Rotimi, 2025).

Kebutuhan harmonisasi menjadi semakin relevan karena kebocoran data merupakan pelanggaran yang dampaknya bersifat ganda. Di satu sisi, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana apabila dilakukan secara sengaja, melawan hukum, atau dengan kelalaian serius yang menimbulkan kerugian. Di sisi lain, korban juga mengalami kerugian individual yang menuntut pemulihan secara privat. Dengan demikian, satu peristiwa hukum dapat melahirkan konsekuensi pidana sekaligus perdata, sehingga sistem hukum perlu dirancang agar tidak memaksa korban memilih salah satu jalur secara eksklusif (Rahman et al., 2024).

UU PDP pada dasarnya telah membuka ruang harmonisasi tersebut meskipun belum sepenuhnya terlembagakan secara rinci. Beberapa ketentuan menunjukkan bahwa pelanggaran data pribadi dapat berujung pada sanksi administratif, pidana, dan gugatan ganti rugi. Selain itu, pengaturan pidana tambahan terhadap korporasi yang mencakup pembayaran ganti kerugian memperlihatkan bahwa pembentuk undang-undang mulai menghubungkan fungsi penghukuman dengan pemulihan korban. Namun, hubungan antarmekanisme tersebut belum sepenuhnya diatur dalam bentuk prosedur yang jelas dan mudah diakses korban (Rahman et al., 2024).

Dalam praktik, salah satu persoalan terbesar adalah bahwa proses pidana tidak otomatis menghasilkan kompensasi yang efektif bagi korban. Walaupun pelaku dapat dituntut dan dipidana, korban sering kali tetap harus mengajukan gugatan terpisah untuk memperoleh ganti rugi. Kondisi ini menimbulkan beban tambahan karena korban harus menghadapi biaya perkara, proses pembuktian ulang, dan waktu penyelesaian yang lebih panjang. Bagi korban kebocoran data yang jumlahnya banyak dan kerugiannya tersebar, model seperti ini jelas tidak efisien dan berpotensi menghambat akses terhadap keadilan (Rotimi, 2025)

Dari sudut perlindungan korban, harmonisasi pidana dan perdata perlu diarahkan pada integrasi fungsi penegakan hukum. Putusan pidana idealnya tidak berhenti pada pembuktian kesalahan pelaku, tetapi juga dapat menjadi dasar yang memperkuat atau mempermudah penetapan kompensasi bagi korban. Pendekatan ini penting karena dalam banyak kasus kebocoran data, fakta-fakta mengenai perbuatan melawan hukum, kelalaian, dan hubungan sebab-akibat telah terungkap dalam proses pidana. Jika fakta tersebut masih harus dibuktikan ulang sepenuhnya dalam forum perdata, maka efisiensi dan kepastian hukum menjadi berkurang (Nyimasmukti et al., 2022).

Harmonisasi juga penting dalam kaitannya dengan pertanggungjawaban korporasi. Dalam kasus *data breach*, pelanggaran lebih sering terkait dengan kegagalan tata kelola, lemahnya pengamanan sistem, atau abainya pengendali data dalam memenuhi kewajiban hukum. Karena itu, penghukuman pidana terhadap pelaku individual saja tidak cukup apabila korporasi sebagai penerima manfaat utama dari pemrosesan data tidak turut dimintai tanggung jawab. Mekanisme yang harmonis harus memastikan bahwa korporasi dapat dikenai sanksi pidana sekaligus kewajiban perdata untuk memulihkan kerugian korban, baik secara langsung maupun melalui skema kompensasi tertentu (Rinjani & Firmansyah, 2025).

Dalam hal ini, pidana tambahan berupa pembayaran ganti kerugian sebagaimana tercermin dalam pembahasan UU PDP merupakan jembatan penting antara rezim pidana dan perdata. Ketentuan semacam ini menunjukkan bahwa sistem hukum Indonesia sebenarnya telah bergerak menuju model yang lebih terpadu, di mana penghukuman dan reparasi dapat

dijalankan dalam satu kerangka. Meskipun demikian, tantangan sesungguhnya terletak pada implementasi, terutama terkait siapa yang menghitung besaran ganti rugi, bagaimana prosedur pembayarannya, dan bagaimana hak korban dijamin ketika jumlah korban sangat banyak (Rinjani & Firmansyah, 2025).

Lebih jauh, harmonisasi pidana dan perdata perlu memperhatikan karakteristik kerugian dalam kebocoran data yang tidak selalu bersifat langsung dan mudah dihitung. Kerugian dapat berupa kerugian materiil, seperti kehilangan dana atau biaya pemulihan akun, tetapi juga kerugian immateriil berupa stres, ketakutan, kehilangan privasi, dan rusaknya reputasi. Dalam forum pidana, kerugian semacam ini sering tidak menjadi fokus utama, sedangkan dalam forum perdata pembuktiannya tidak selalu mudah. Karena itu, harmonisasi dibutuhkan agar sistem hukum mengakui kerugian digital sebagai kerugian hukum yang sah dan layak dipulihkan secara penuh (Nyimasmukti et al., 2022).

Aspek lain yang penting adalah penyediaan mekanisme yang sederhana bagi korban massal. Kebocoran data sering berdampak pada ribuan bahkan jutaan subjek data sekaligus, sehingga gugatan individual tidak selalu realistis. Dalam situasi seperti ini, harmonisasi pidana dan perdata harus dibarengi dengan penguatan mekanisme gugatan kelompok, kompensasi kolektif, atau skema pemulihan administratif yang dapat dijalankan secara cepat dan proporsional. Tanpa instrumen seperti itu, hak korban atas pemulihan hanya akan menjadi norma formal yang sulit diwujudkan (Piansah, 2024).

Perbandingan dengan perkembangan internasional juga menunjukkan bahwa perlindungan data yang efektif cenderung menggunakan pendekatan *dual-track enforcement*, yakni penegakan administratif atau pidana berjalan berdampingan dengan hak perdata untuk memperoleh pemulihan. Kajian terhadap perkembangan hukum perlindungan data menekankan pentingnya lembaga pengawas yang kuat, hak korban untuk mendapatkan remedinya secara efektif, dan prosedur yang tidak memberatkan pihak yang dirugikan. Pengalaman tersebut memberi pelajaran bahwa Indonesia perlu memperjelas hubungan antara penindakan pidana, pengawasan administratif, dan kompensasi keperdataan agar perlindungan korban tidak terfragmentasi (Nugroho et al., 2024).

Dalam perspektif kebijakan hukum, harmonisasi pidana dan perdata juga berfungsi membangun kepercayaan publik terhadap tata kelola data digital. Masyarakat akan lebih percaya pada penyelenggara sistem elektronik apabila mengetahui bahwa pelanggaran tidak hanya akan dihukum, tetapi juga akan menimbulkan kewajiban nyata untuk memulihkan korban. Sebaliknya, jika hukum hanya fokus pada penghukuman pelaku tanpa memperhatikan reparasi, maka korban akan tetap merasa tidak terlindungi. Oleh sebab itu, harmonisasi merupakan bagian dari strategi hukum untuk menjaga legitimasi transformasi digital dan mendorong kepatuhan korporasi terhadap standar perlindungan data (Piansah, 2024).

Dari segi pembaruan hukum, langkah yang perlu didorong adalah penyusunan aturan pelaksana yang secara rinci mengatur relasi antara putusan pidana, pembuktian perdata, dan mekanisme kompensasi korban. Selain itu, perlu ada pedoman mengenai penilaian kerugian material dan immaterial dalam kasus *data breach*, termasuk kemungkinan pembuktian yang lebih sederhana bagi korban. Penguatan kelembagaan otoritas perlindungan data juga penting agar tersedia saluran administratif yang dapat menjembatani korban dengan proses penghukuman maupun pemulihan kerugian (Nugroho et al., 2024).

Pada akhirnya, harmonisasi pidana dan perdata dalam perlindungan korban kebocoran data harus dipahami sebagai kebutuhan normatif dan praktis sekaligus. Secara normatif, harmonisasi mencerminkan pandangan bahwa keadilan tidak selesai pada pemidanaan, tetapi harus mencakup pemulihan korban. Secara praktis, harmonisasi memberi jalan agar korban tidak dibebani prosedur yang terpisah-pisah dalam mencari haknya. Dengan demikian, sistem hukum yang ideal adalah sistem yang menempatkan penghukuman pelaku dan reparasi korban dalam satu arsitektur perlindungan hukum yang saling menguatkan.

Kesimpulan

Kebocoran data pribadi di era digital merupakan bentuk pelanggaran hukum yang tidak hanya menimbulkan ancaman terhadap privasi, tetapi juga menimbulkan kerugian nyata bagi korban, baik secara materiil maupun immateriil. Dalam konteks tersebut, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah memberikan dasar normatif yang penting karena memuat pengaturan mengenai hak subjek data, kewajiban pengendali data, penyelesaian sengketa, serta ketentuan pidana terhadap pelanggaran data pribadi. Namun demikian, keberadaan norma tersebut masih menunjukkan bahwa perlindungan korban belum sepenuhnya optimal apabila pertanggungjawaban pidana dan mekanisme ganti kerugian perdata masih berjalan secara terpisah dalam praktik penegakan hukum.

Harmonisasi antara pertanggungjawaban pidana dan ganti kerugian perdata menjadi kebutuhan mendesak karena keadilan bagi korban tidak cukup diwujudkan melalui penghukuman pelaku semata, melainkan juga harus disertai pemulihan hak dan kompensasi yang efektif. Dalam banyak kasus, proses pidana belum otomatis memberikan reparasi kepada korban, sementara gugatan perdata sering menghadapi kendala pembuktian, prosedur, dan ketidakjelasan perhitungan kerugian. Oleh sebab itu, sistem hukum yang ideal harus menghubungkan fungsi pidana sebagai sarana penjeraan dengan fungsi perdata sebagai sarana pemulihan, sehingga korban tidak dibebani oleh jalur penyelesaian yang terfragmentasi dan berlarut-larut.

Dengan demikian, tinjauan yuridis terhadap perlindungan korban dalam kasus *data breach* menunjukkan perlunya penguatan regulasi pelaksana, penyederhanaan mekanisme kompensasi, serta penegasan hubungan antara putusan pidana dan tuntutan ganti rugi perdata. Harmonisasi ini penting untuk membangun sistem perlindungan hukum yang tidak hanya represif terhadap pelaku, tetapi juga responsif terhadap kebutuhan korban. Pada akhirnya, perlindungan data pribadi yang efektif di Indonesia harus diarahkan pada terciptanya keseimbangan antara kepastian hukum, keadilan bagi korban, dan akuntabilitas penyelenggara sistem elektronik dalam menjaga keamanan data di tengah perkembangan teknologi digital yang semakin kompleks.

Daftar Rujukan

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Nugroho, F. N. P., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Nyimasmukti, B. R., Wijayanti, M. S., & Juniarti, D. B. (2022). HAK KEBENDAAN DAN KEABSAHAN PERJANJIAN KEBENDAAN VIRTUAL LAND DI DALAM METAVERSE DITINJAU BERDASARKAN KUHPERDATA: Virtual Land's Material Rights and The Legality of The Virtual Land Agreement in Metaverse Reviewed Under Indonesian Civil Code. *Majalah Hukum Nasional*, *52*(2), 271–295.

Piansah, A. (2024). The Role of Civil Law in Realizing Personal Data Security in the Era of Digital Transformation in Indonesia. *Zona Law And Public Administration Indonesia*, *2*(4), 13–22.

Putri, T. S., & Putra, M. R. S. (2024). Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi. *Jurnal Hukum Lex Generalis*, *5*(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/730

Rahman, S., Sirazy, M. R. M., Das, R., & Khan, R. S. (2024). An exploration of artificial intelligence techniques for optimizing tax compliance, fraud detection, and revenue collection in modern tax administrations. *International Journal of Business Intelligence and Big Data Analytics*, *7*(3), 56–80.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Rotimi, O. (2025). *Digital Sovereignty and the Politics of Data Localization* (SSRN Scholarly Paper No. 5921642). Social Science Research Network. https://doi.org/10.2139/ssrn.5921642

Santo, M. F. O. da, Sari, L., Kamilah, A., & Reumi, F. (2024). *Pengantar Hukum Perdata: Teori & Referensi Komprehensif Dasar-dasar Hukum Perdata di Indonesia*. PT. Sonpedia Publishing Indonesia.

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. *Journal of Law and Legal Reform*, *6*(3), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Sylviana, G., Maharani, D. P., & Wibowo, A. M. (2025). Keabsahan Praktik Dark Patterns Terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi di Indonesia. *RechtJiva*. https://www.researchgate.net/profile/Afrizal-Wibowo/publication/392514975_Keabsahan_Praktik_Dark_Patterns_Terhadap_Pemerolehan_Persetujuan_Pemrosesan_Data_Pribadi_di_Indonesia/links/6846645fd1054b0207fab3bd/Keabsahan-Praktik-Dark-Patterns-Terhadap-Pemerolehan-Persetujuan-Pemrosesan-Data-Pribadi-di-Indonesia.pdf

Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Truli, E. (2018). The General Data Protection Regulation and Civil Liability. In M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (pp. 303–329). Springer. https://doi.org/10.1007/978-3-662-57646-5_12

Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, *34*, e00106818. https://doi.org/https://doi.org/10.1590/0102-311X00106818

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ercl-2018-1022

Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750. https://doi.org/10.1080/01436597.2021.1915122

Walliman, N., & Walliman, N. (2021). *Research Methods: The Basics* (3rd ed.). Routledge. https://doi.org/10.4324/9781003141693

Xiaying, M. (2019). The Legal Attributes of Electronic Data and the Positioning of Data in Civil Law*. *Social Sciences in China*, *40*(1), 82–99. https://doi.org/10.1080/02529203.2018.1519208

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yudha, Sahril, I., & Atmadja3, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897