Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora
Volume. 5, Nomor. 4 Desember 2025
e-ISSN: 2962-4037; p-ISSN: 2962-4452, Hal. 205-230
DOI: https://doi.org/10.55606/khatulistiwa.v5i4.7487
Available Online at: https://researchhub.id/index.php/Khatulistiwa

Perlindungan Hukum terhadap Korban Tindak Pidana Pencurian Data Pribadi

Rosel Denis Pakasi[1*], Yoan B. Runtunuwu[2], Wenly R. J. Lolong[3]
[1-3] Program Studi Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Manado, Indonesia

Korepsondensi penulis: pakasirossel@gmail.com

Abstract: *This study aims to determine the legal protection provided to victims of personal data theft in Indonesia. This study uses a normative juridical research method by examining laws and regulations related to legal protection for victims of personal data theft. The results indicate that legal protection for victims of personal data theft in Indonesia is regulated by Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and Law No. 27 of 2022 concerning Personal Data Protection (PDP). However, more effective law enforcement efforts are still needed to protect victims' rights and prosecute perpetrators of personal data theft.*

Keywords: *ITE, Legal Protection, Personal Data Theft*

Abstrak: Penelitian ini bertujuan untuk mengetahui perlindungan hukum terhadap korban tindak pidana pencurian data pribadi di Indonesia. Penelitian ini menggunakan metode penelitian yuridis normatif dengan mengkaji peraturan perundangundangan yang terkait dengan perlindungan hukum terhadap korban tindak pidana pencurian data pribadi. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap korban tindak pidana pencurian data pribadi di Indonesia telah diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Namun, masih diperlukan upaya penegakan hukum yang lebih efektif untuk melindungi hak-hak korban dan menindak pelaku tindak pidana pencurian data pribadi.

Kata Kunci: ITE, Perlindungan Hukum, Pencurian Data Pribadi

1. PENDAHULUAN

Perlindungan hukum terhadap korban tindak pidana pencurian data pribadi di Indonesia menghadapi kompleksitas isu hukum yang melibatkan kekaburan norma dan konflik regulasi. Pertama, terjadi ketidakselarasan antara UU ITE No. 19/2016 dan UU PDP No. 27/2022. UU ITE fokus pada sanksi pidana penjara tanpa mengatur kompensasi bagi korban, sementara UU PDP meski menjamin restitusi, belum memiliki mekanisme eksekusi yang jelas. Hal ini menimbulkan dualisme penanganan kasus, di mana korban harus memilih antara jalur pidana dengan sanksi berat atau jalur perdata yang belum terjamin efektivitasnya.

Kekaburan norma muncul dalam definisi "kerugian" yang tidak mencakup kerugian immateriil seperti trauma psikologis, serta ketiadaan standar pembuktian khusus untuk kasus kebocoran data yang melibatkan pihak ketiga. Fragmentasi regulasi teknis memperparah situasi, seperti Permenkominfo No. 20/2016 yang hanya mengikat penyelenggara sistem elektronik, sementara pelaku individu lepas dari pengawasan. Di sisi penegakan hukum, sanksi yang tidak proporsional terhadap korporasi-yang sering hanya dikenai denda administratif-

Received: Juni 15, 2025; Revised: Juni 29, 2025; Accepted: Juli 13, 2025; Online Available: Juli 15, 2025

berbeda dengan ancaman pidana penjara bagi pelaku individu, menciptakan ketimpangan dalam pertanggungjawaban hukum.

Konflik kewenangan antarlembaga menjadi tantangan tambahan. Kominfo berfokus pada aspek administratif, sementara kepolisian cenderung menggunakan instrumen KUHP atau UU ITE yang tidak spesifik mengatur pemulihan korban. Otoritas Perlindungan Data Pribadi yang belum beroperasi optimal turut memperlambat penyelesaian kasus, karena lembaga ini belum memiliki kewenangan memaksa pelaku membayar kompensasi. Di tingkat praktis, korban dari kalangan rentan seperti penyandang disabilitas menghadapi hambatan akses keadilan akibat tidak adanya mekanisme pendampingan khusus, sementara biaya perkara perdata yang tinggi menjadi penghalang bagi korban dengan kerugian materi kecil.

Isu-isu ini mengindikasikan perlunya harmonisasi regulasi, penyempurnaan definisi kerugian immateriil, dan pembentukan lembaga khusus yang berwenang menangani restitusi secara terintegrasi. Tanpa penyelesaian menyeluruh terhadap kekaburan norma dan konflik regulasi, perlindungan hukum bagi korban pencurian data pribadi akan tetap bersifat parsial dan tidak efektif.

Indonesia merupakan salah satu negara yang masyarakatnya turut serta mengikuti kemajuan ilmu pengetahuan dan teknologi (IPTEK) yang semakin berkembang dan meningkat. Perkembangan teknologi terjadi karena seseorang menggunakan akalnya untuk menyelesaikan setiap masalah yang dihadapinya. Kemajuan teknologi merupakan sesuatu yang tidak dapat dihindari dalam kehidupan masyarakat sekarang ini, karena kemajuan teknologi akan selalu berjalan sesuai dengan kemajuan ilmu pengetahuan. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia.

Salah satu bentuk kemajuan teknologi yang masyarakat Indonesia gunakan untuk menunjang kemajuan ilmu pengetahuan adalah internet. Internet merupakan jaringan luas dari komputer yang lazim disebut dengan Worldwide network, internet juga merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi seperti kabel telpon, serat optik satelit ataupun gelombang frekuensi. Hukum pidana merupakan aturan hukum yang mengatur mengenai perbuatan-perbuatan hukum yang dilarang oleh undang-undang yang mana disertai dengan sanksi pidana bagi pelaku tindak pidana.

Kemajuan teknologi dan informasi juga dapat mengubah pola hidup dan pemicu adanya transmutasi masyarakat, budaya, ekonomi, keamanan, dan penegakkan hukum di dalam masyarakat Indonesia. Dengan perkembangan media elektronik dan komunikasi, waktu dan jarak bukan kembali menjadi permasalahan utama kepada semua individu,

termasuk pemerintah. Setiap individu dapat berkomunikasi satu sama lain tanpa bertemu di ruang fisik.

Pertanggungjawaban pidana adalah untuk menentukan apakah seseorang tersangka/terdakwa dapat dipertanggungjawaban terhadap suatu tindak pidana (crime) yang terjadi atau tidak. Dengan kata lain apakah terdakwa akan dipidana atau dibebaskan, ia dapat dipidana, bila tindakan yang telah dilakukan itu bersifat melawan hukum dan ia mampu bertanggungjawab. Kemampuan tersebut memperlihatkan kesalahan dari pelaku yang berbentuk kesengajaan atau kealpaan, sebab asas pertanggungjawaban dalam hukum pidana ialah tidak dipidana jika tidak ada kesalahan. Artinya tindakan tersebut tercela dan tertuduh menyadari tindakan yang dilakukan tersebut.

Orang tidak dapat dimintai pertanggungjawaban pidana apabila syaratsyarat pertanggungjawaban yang ditentukan tidak dipenuhi. Seperti yang dikatakan Moelyatno, bahwa: "orang tidak mungkin dibebani tanggungjawab atau dijatuhi hukuman jika ia tidak melakukan perbuatan pidana tetapi meskipun ia melakukan perbuatan pidana tidak selalu dapat dipidana. Orang yang melakukan perbuatan pidana akan dipidana apabila memenuhi syarat-syarat pertanggungjawaban pidana". Sanksi harus dipandang sebagai salah satu unsur yang esensial, bila kita melihat hukum sebagai kaedah. Hampir semua jenis yang berpandangan dogmatik, memandang hukum sebagai kaedah bersanksi yang didukung oleh otoritas tertinggi di dalam masyarakat.

Pengertian dari tindak pidana adalah "perbuatan yang oleh hukum pidana dilarang dan diancam dengan ancaman pidana". Hukum pidana merupakan aturan hukum yang mengatur mengenai perbuatan-perbuatan hukum yang dilarang oleh undang-undang yang mana disertai dengan sanksi pidana bagi pelaku tindak pidana.

Kehadiran internet dengan segala manfaat baik yang dapat diperoleh penggunanya, tidak dapat dipungkiri memiliki sisi negatif. Bentuk kontribusi yang diperoleh dari penggunaan internet seperti peningkatan kesejahteraan, kemajuan dan peradaban manusia. Namun, di sisi lain internet juga merupakan wadah bagi kejahatan baru yang ada pada dunia hukum saat ini yang dikenal dengan istilah kejahatan siber atau Cyber Crime. internet atau interconnected network mempunyai salah satu fungsinya yaitu menghubungkan jaringan dari jaringan-jaringan komputer yang ada di dunia yang jaringannya terbentuk bukanlah bersifat terpusat atau bahasa sederhananya jaringan mempunyai jangkauan luas yang tidak akan saling mengganggu antara satu jaringan dengan jaringan lainya.

Pengaturan tindak pidana siber dalam peraturan perundang-undangan Indonesia belum cukup mendukung baik terhadap hukum pidana materil maupun hukum pidana formil.

Berbagai upaya untuk mengatur pengaturan pada peraturan perundang-undangan yang dapat mencegah adanya dampak negatif akibat dari perbuatan hukum.

Pengaturan tindak pidana siber dalam peraturan perundang-undangan Indonesia belum cukup mendukung baik terhadap hukum pidana materil maupun hukum pidana formil. Berbagai upaya untuk mengatur pengaturan pada peraturan perundang-undangan yang dapat mencegah adanya dampak negatif akibat dari perbuatan hukum.

Pada satu sisi, perkembangan dunia IPTEK yang demikian mengagumkan itu memang telah membawa manfaat yang luar biasa bagi kemajuan peradaban umat manusia. Jenis-jenis pekerjaan yang sebelumnya menuntut kemampuan fisik yang cukup besar, kini relatif sudah bisa digantikan oleh perangkat mesin-mesin otomatis, Demikian juga ditemukannya formulasi-formulasi baru kapasitas komputer, seolah sudah mampu menggeser posisi kemampuan otak manusia dalam berbagai bidang ilmu dan aktivitas manusia. Kemajuan teknologi informasi yang serba digital membawa orang ke dunia bisnis yang revolusioner (digital revolution era) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi. Di sisi lain, berkembangnya teknologi informasi menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan kejahatan mayantara atau "cyber crime". Masalah kejahatan mayantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu extra ordinary crime (kejahatan luar biasa) bahkan dirasakan pula sebagai serious crime (kejahatan serius) dan transnational crime (kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat, bangsa dan negara.

Indonesia perlu memiliki persiapan yang memadai dalam menghadapi kejahatan siber (cyber crime). Salah satu persiapan yang penting adalah sumber daya manusia yang kompeten dan memiliki pengetahuan serta keterampilan dalam bidang keamanan siber. Sumber daya manusia yang berkualitas dapat menciptakan cara berpikir yang positif terhadap perubahan lingkungan global, meningkatkan kesadaran terhadap perkembangan teknologi dan informasi, serta memahami berbagai dampak yang timbul dalam kehidupan masyarakat terkait dengan ancaman siber. Selain itu, Indonesia juga perlu memiliki fasilitas produksi pengamanan negara yang memadai. Fasilitas ini mencakup infrastruktur dan teknologi yang diperlukan untuk mendeteksi, mencegah, dan menanggulangi serangan siber. Investasi dalam pengembangan fasilitas produksi pengamanan negara yang mutakhir dan efektif menjadi penting guna menghadapi ancaman kejahatan siber yang semakin kompleks dan terus berkembang.Dengan

memperkuat sumber daya manusia dan fasilitas produksi pengamanan negara, Indonesia dapat meningkatkan kemampuannya dalam menghadapi kejahatan siber. Ini melibatkan pendidikan dan pelatihan yang memadai untuk tenaga ahli keamanan siber, serta pengembangan dan peningkatan infrastruktur teknologi yang dapat mengidentifikasi, melindungi, dan merespons serangan siber dengan cepat dan efektif.

Tantangan lain dalam penyempurnaan kebijakan keamanan siber adalah sifat ancaman siber yang transnational. Hal ini mengakibatkan penanggulangannya tidak hanya menjadi tanggung jawab TNI atau Polri, tetapi melibatkan berbagai kementerian seperti Kementerian Pertahanan dan Kementerian Komunikasi dan Informatika. Menurut Sjafrie Sjamsoeddin, ancaman siber termasuk dalam kategori ancaman asimetris yang membutuhkan pendekatan yang komprehensif. Karena sifat multidimensinya, keamanan siber melibatkan tidak hanya satu departemen, tetapi juga berbagai departemen lainnya. Oleh karena itu, diperlukan kebijakan keamanan siber atau pertahanan siber, yang dalam pelaksanaannya memerlukan kerangka koordinasi yang baik.

Dampak dari kejahatan siber merupakan masalah yang sangat penting bagi pemerintah karena dapat mempengaruhi kerugian di masyarakat secara keseluruhan. Perlu disadari bahwa kejahatan siber dapat menyebabkan kerugian kolektif bagi masyarakat Indonesia. Setidaknya terdapat dua faktor Yang menyebabkan terjadinya kejahatan siber, yaitu faktor teknis dan faktor sosial ekonomi. Pencurian data melalui teknologi informasi di era modern disebut sebagai phising yaitu sebuah aktivitas secara melawan hukum untuk menguasai dan mendapatkan informasi pribadi seseorang atau sekelompok tertentu. Tindakan pencurian data pribadi memiliki tujuan, yaitu dengan memperoleh data pribadi maka selanjutnya dengan kejahatan terhadap harta, dengan meretas akun rekening keuangan atau hal berharga yang bisa di akses melalui data pribadi atau mengumpulkan semua data pribadi lalu dijual dalam situs gelap.

Indonesia masih berada dalam tahap awal pengembangan infrastruktur keamanan siber yang memadai. Sistem keamanan siber yang tidak optimal memberikan celah bagi para pelaku kejahatan untuk melakukan serangan, termasuk pencurian data pribadi. Hal ini diperparah dengan meningkatnya penggunaan teknologi berbasis internet tanpa diimbangi oleh literasi digital yang memadai di kalangan masyarakat. Kombinasi antara kelemahan teknis dan rendahnya kesadaran ini membuka peluang besar bagi tindak pidana tersebut. Dalam perspektif hukum, pencurian data pribadi juga memunculkan tantangan terkait pembuktian dan jurisdiksi. Tindak pidana siber sering kali melibatkan pelaku lintas negara, sehingga menimbulkan kompleksitas dalam penanganan kasus di tingkat internasional. Kerjasama antarnegara dalam

keamanan siber, termasuk melalui perjanjian ekstradisi dan harmonisasi regulasi, menjadi elemen penting yang perlu diperkuat. Namun, implementasi kerjasama ini di Indonesia masih jauh dari kata optimal.

Ada 2 hal yang bisa memicu munculnya cybercrime yakni teknis serta sosio ekonomi (kemasyarakatan). Pertama, pada hal teknis, Tak bisa dipungkiri jika dampak majunya teknologi (teknologi informasi) bisa memicu dampak buruk untuk kemajuan di masyarakat. Suksesnya teknologi itu pula bisa menghilangkan batas wilayah negara yang membuat dunia sangat sempit. Korelasi antar jaringan bisa mempermudah pelaku kriminal melancarkan kegiatannya. Lalu, tak meratanya distribusi teknologi membuat yang satu lebih kuat dari lainnya

Kajian hukum terhadap tindak pidana pencurian data pribadi juga relevan dalam rangka mengidentifikasi kesenjangan dalam peraturan yang ada. Meskipun telah ada berbagai instrumen hukum, kecepatan perkembangan teknologi seringkali melampaui adaptasi regulasi. Hal ini menciptakan vacuum of law yang menjadi celah bagi pelaku kejahatan untuk beroperasi tanpa takut akan sanksi yang efektif. Dengan demikian, evaluasi dan pembaharuan peraturan menjadi agenda penting dalam menjaga keamanan siber. Lebih lanjut, tindak pidana pencurian data pribadi memiliki implikasi luas terhadap kepercayaan masyarakat terhadap teknologi digital. Jika tidak ditangani dengan serius, kasus-kasus pencurian data dapat menurunkan tingkat kepercayaan publik terhadap penggunaan layanan berbasis digital, seperti e-commerce, perbankan online, dan aplikasi berbasis data lainnya. Hal ini tidak hanya merugikan individu, tetapi juga berpotensi menghambat pertumbuhan ekonomi digital di Indonesia.

Sebagai permasalahan hukum yang menjadi tolak ukur untuk perlindungan korban terhadap tindak pidana hacking yang berkaitan dengan pencurian data diungkapkan juga dalam Laporan National Cyber Security Index (NCSI) mencatat, skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022. Angka ini menempatkan Indonesia berada di peringkat ke-3 terendah di antara negara-negara G20.

Permasalahan ini membuktikan bahwa Negara Indonesia mempunyai sistem Keamanan siber yang buruk dan perlunya peningkatan baik peningkatan dalam keamanan siber dan juga penigkatan sumber daya manusia nya agar dapat mempelajari dan mencegah terjadinya peretahan atau hacking terjadi di Negara Indonesia.

2. METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian hukum normatif dengan studi kasus normatif berupa produk perilaku hukum, yang memfokuskan kajian pada hukum sebagai norma atau kaidah yang berlaku di masyarakat. Penelitian ini bertujuan untuk menganalisis norma-norma hukum terkait perlindungan data pribadi dan implementasinya di Indonesia, dengan mengkaji inventarisasi hukum positif seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), asas-asas hukum (legalitas, keadilan, perlindungan hak privasi), doktrin hukum, penemuan hukum dalam perkara in concreto melalui analisis kasus, sistematika hukum, taraf sinkronisasi, perbandingan hukum, dan sejarah hukum. Konteks penelitian "Perlindungan Hukum terhadap Korban Tindak Pidana Pencurian Data Pribadi" secara mendalam akan memahami bagaimana hukum berfungsi melindungi data individu.

Pendekatan masalah dalam penelitian ini meliputi tiga aspek. Pertama, pendekatan perundang-undangan (statute approach) digunakan untuk mengkaji berbagai ketentuan hukum positif seperti UU PDP, KUHP, dan UU ITE, guna memahami kerangka hukum perlindungan korban. Kedua, pendekatan konseptual (conceptual approach) bertujuan menggali gagasan, doktrin, dan teori hukum yang relevan, seperti hak atas privasi dan keadilan restoratif, sebagai dasar perumusan kebijakan perlindungan hukum. Ketiga, pendekatan kasus (case approach) melibatkan analisis putusan pengadilan terkait pencurian data pribadi untuk memahami penerapan hukum dalam praktik peradilan dan menilai efektivitas perlindungan hukum bagi korban.

Teknik pengumpulan bahan hukum dalam penelitian ini adalah studi kepustakaan (library research). Peneliti akan mengumpulkan dan menganalisis bahan hukum primer, sekunder, dan tersier yang relevan dengan permasalahan penelitian. Sumber bahan hukum primer mencakup UUD 1945 (khususnya Pasal 28G ayat (1)), UU PDP, UU ITE, KUHP, peraturan pelaksana terkait, serta putusan-putusan pengadilan. Bahan hukum sekunder terdiri dari buku literatur, jurnal, artikel, hasil penelitian, pendapat ahli, dan sumber internet, sementara bahan hukum tersier meliputi kamus hukum dan ensiklopedia hukum.

Analisis bahan hukum akan dilakukan dengan menggunakan metode analisis kualitatif. Metode ini dipilih untuk menganalisis data secara mendalam dan komprehensif dengan cara mendeskripsikan serta menginterpretasikan data yang telah berhasil dikumpulkan. Pendekatan kualitatif memungkinkan peneliti untuk memahami nuansa dan kompleksitas dalam penerapan norma hukum serta efektivitasnya dalam memberikan perlindungan terhadap korban tindak pidana pencurian data pribadi.

3. PEMBAHASAN

Pengaturan Hukum Positif Di Indonesia Terkait Perlindungan Terhadap Korban Tindak Pidana Pencurian Data Pribadi

Perlindungan hukum terhadap korban tindak pidana pencurian data pribadi di Indonesia diatur melalui berbagai peraturan perundang-undangan yang membentuk kerangka hukum positif. Kerangka ini bertujuan untuk memberikan jaminan perlindungan terhadap hak-hak individu atas data pribadinya serta menetapkan mekanisme penegakan hukum terhadap pelanggaran yang terjadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam perkembangan hukum perlindungan data di Indonesia. UU PDP lahir sebagai respons terhadap semakin kompleksnya tantangan era digital, di mana data pribadi telah menjadi aset penting dalam berbagai aspek kehidupan, mulai dari aktivitas ekonomi, pemerintahan, hingga interaksi sosial sehari-hari. Sebelum hadirnya UU PDP, pengaturan mengenai data pribadi tersebar di berbagai regulasi sektoral seperti UU ITE, UU Administrasi Kependudukan, dan sejumlah peraturan teknis lainnya, yang sayangnya seringkali tidak memberikan perlindungan yang utuh dan menyeluruh terhadap data pribadi sebagai hak fundamental setiap warga negara. Oleh karena itu, UU PDP hadir sebagai regulasi yang secara khusus dan komprehensif mengatur bagaimana data pribadi harus dikelola, dilindungi, dan diatur pemrosesannya dalam lingkup hukum nasional.

UU PDP secara jelas mendefinisikan data pribadi sebagai data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik maupun non-elektronik. Definisi ini penting karena menegaskan bahwa data pribadi bukan hanya sekedar informasi statis, tetapi juga mencakup data dinamis yang, apabila dikombinasikan dengan elemen lain, dapat mengungkap identitas seseorang secara spesifik. Pemahaman ini sejalan dengan konsep data pribadi yang digunakan dalam kerangka hukum internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang menekankan pentingnya identifikasi langsung maupun tidak langsung dalam konteks data pribadi.

Lebih jauh, UU PDP menetapkan prinsip-prinsip fundamental dalam perlindungan data pribadi yang menjadi pedoman utama bagi semua pihak yang terlibat dalam pengelolaan data, terutama pengendali data pribadi. Prinsip-prinsip tersebut antara lain meliputi prinsip keabsahan pemrosesan data (lawfulness of processing), yang mengharuskan setiap pemrosesan data dilakukan berdasarkan dasar hukum yang sah dan jelas, prinsip transparansi

(transparency), yang mewajibkan penyampaian informasi yang jelas, jujur, dan mudah diakses kepada subjek data pribadi, serta prinsip pembatasan tujuan (purpose limitation), yang mengatur agar data hanya digunakan untuk tujuan tertentu yang telah disampaikan sebelumnya kepada pemilik data. Selain itu, prinsip akuntabilitas (accountability) juga ditekankan, di mana setiap pengendali data pribadi bertanggung jawab atas seluruh kegiatan pemrosesan data yang dilakukan.

UU PDP juga mengatur hak-hak subjek data pribadi secara rinci, yang menjadi pilar penting dalam perlindungan hukum terhadap korban pencurian data pribadi. Hak-hak tersebut antara lain mencakup hak untuk mengetahui (right to know), hak untuk mengakses data pribadi (right to access), hak untuk memperbaiki kesalahan data (right to rectification), hak untuk menghapus data (right to erasure), serta hak untuk menarik persetujuan atas pemrosesan data pribadinya (right to withdraw consent). Hak-hak ini bukan hanya sekadar formalitas, tetapi merupakan instrumen konkret yang memungkinkan individu untuk mengontrol dan melindungi data pribadinya dari penyalahgunaan atau akses yang tidak sah. Dengan demikian, UU PDP memberikan dasar hukum yang kuat bagi korban pencurian data pribadi untuk menuntut haknya dan meminta pertanggungjawaban kepada pihak yang melakukan pelanggaran.

Selain itu, UU PDP juga menetapkan kewajiban penting bagi pengendali data pribadi, yang mencakup tanggung jawab untuk menjaga keamanan data pribadi agar tidak disalahgunakan oleh pihak yang tidak berwenang. Pengendali data pribadi diwajibkan menerapkan langkah-langkah teknis dan organisasi yang memadai, seperti penggunaan teknologi enkripsi, pengamanan jaringan, audit keamanan, dan penunjukan petugas perlindungan data pribadi (data protection officer) untuk memastikan bahwa data pribadi dikelola sesuai dengan standar keamanan yang berlaku. Kewajiban ini juga mencakup keharusan untuk memberitahukan kepada subjek data pribadi apabila terjadi insiden kebocoran data, sehingga korban dapat segera mengambil langkah-langkah perlindungan yang diperlukan.Tidak kalah penting, UU PDP juga menetapkan adanya sanksi administratif dan pidana terhadap pihak yang melanggar ketentuan dalam undang-undang ini. Sanksi administratif dapat berupa peringatan tertulis, penghentian sementara aktivitas pemrosesan data, hingga denda administratif yang signifikan, sementara sanksi pidana diatur untuk pelanggaran yang lebih berat, seperti pengungkapan data pribadi tanpa izin, penjualan data pribadi secara ilegal, atau penyalahgunaan data pribadi yang mengakibatkan kerugian bagi subjek data. Dengan adanya sanksi ini, UU PDP tidak hanya berfungsi sebagai norma etik,

tetapi juga sebagai instrumen hukum yang memaksa kepatuhan melalui mekanisme penegakan hukum yang jelas dan tegas.

Dengan demikian, UU PDP menjadi fondasi utama dalam kerangka perlindungan hukum terhadap korban pencurian data pribadi di Indonesia. Kehadiran undang-undang ini diharapkan tidak hanya menjadi regulasi semata, tetapi juga mampu menciptakan budaya perlindungan data pribadi yang lebih baik di masyarakat Indonesia. Meski demikian, tantangan implementasi UU PDP di lapangan, termasuk kesiapan infrastruktur, literasi digital masyarakat, dan kapasitas aparat penegak hukum, masih menjadi pekerjaan rumah yang harus diatasi agar perlindungan hukum terhadap korban tindak pidana pencurian data pribadi dapat berjalan optimal dan efektif.

Bentuk Perlindungan Hukum Yang Dapat Diperoleh Korban Tindak Pidana Pencurian Data Pribadi Menurut Ketentuan Perundang-undangan Yang Berlaku

a. Perlindungan Preventif

Perlindungan preventif merupakan salah satu bentuk perlindungan hukum yang sangat krusial dalam konteks pencegahan tindak pidana pencurian data pribadi di era digital. Perlindungan preventif bertujuan utama untuk mencegah terjadinya pelanggaran atau penyalahgunaan data pribadi sebelum insiden tersebut terjadi. Dalam kerangka teori hukum perlindungan konsumen, pendekatan preventif ini sejalan dengan prinsip *ex-ante protection*, yaitu langkah-langkah pencegahan yang dilakukan sebelum terjadinya kerugian pada individu sebagai subjek data. Menurut Sudikno Mertokusumo (2013), perlindungan preventif memiliki peran penting dalam memberikan rasa aman kepada individu dengan menekankan kewajiban penyedia layanan atau pengendali data untuk bertanggung jawab secara proaktif terhadap potensi risiko yang dapat merugikan pihak lain. Oleh karena itu, perlindungan preventif menjadi instrumen awal yang vital dalam melindungi hak asasi manusia, khususnya hak atas privasi dan perlindungan data pribadi.

Langkah pertama dalam perlindungan preventif adalah edukasi dan sosialisasi kepada masyarakat. Edukasi ini penting karena sebagian besar masyarakat Indonesia masih memiliki tingkat literasi digital yang rendah, sehingga belum sepenuhnya memahami potensi ancaman yang timbul dari penyalahgunaan data pribadi. Literasi digital yang minim ini membuka celah besar bagi tindak pidana pencurian data pribadi melalui berbagai modus seperti phising, malware, atau teknik social engineering lainnya. Oleh karena itu, pemerintah, melalui kementerian terkait seperti Kementerian Komunikasi dan Informatika (KOMINFO), bersama lembaga non-pemerintah dan sektor swasta, memiliki peran strategis dalam melakukan

kampanye edukasi publik secara masif dan berkesinambungan. Kampanye ini mencakup penyuluhan tentang pentingnya menjaga kerahasiaan data pribadi, mengenali potensi ancaman, memahami hak-hak individu sebagai subjek data, serta cara-cara praktis untuk mengamankan data pribadi di berbagai platform digital. Penelitian yang dilakukan oleh Prayoga dan Suharnoko (2022) juga menunjukkan bahwa peningkatan literasi digital masyarakat secara signifikan dapat mengurangi risiko terjadinya kejahatan siber, termasuk pencurian data pribadi.

Langkah berikutnya adalah penetapan regulasi dan standar keamanan**.** Perlindungan preventif dalam konteks ini diwujudkan melalui kewajiban hukum bagi penyelenggara sistem elektronik (PSE) dan pengendali data pribadi untuk menerapkan standar keamanan tertentu dalam pengelolaan data. UU PDP (2022) secara eksplisit mengatur bahwa setiap pengendali data wajib mengambil langkah-langkah teknis dan organisasi yang diperlukan untuk melindungi data pribadi dari ancaman penyalahgunaan, akses ilegal, dan kebocoran data. Standar keamanan ini mencakup penerapan enkripsi data, penggunaan sistem autentikasi ganda, pembatasan akses berdasarkan prinsip *least privilege*, hingga penerapan firewall dan sistem deteksi intrusi (IDS/IPS). Tidak hanya itu, regulasi turunannya seperti Peraturan Pemerintah dan Peraturan Menteri Kominfo juga diharapkan mempertegas kewajiban teknis tersebut agar implementasinya jelas dan terukur. Menurut Nurul Qamar (2023), penguatan standar keamanan teknis melalui regulasi yang ketat dapat menjadi *compliance driver* bagi para pengendali data untuk meningkatkan tata kelola keamanan data mereka secara lebih serius. Selanjutnya, audit dan pengawasan merupakan langkah preventif yang juga tidak kalah penting.

Audit bertujuan untuk memastikan bahwa penyelenggara sistem elektronik telah menerapkan standar keamanan sesuai dengan ketentuan yang berlaku. Pelaksanaan audit ini harus dilakukan secara berkala dan independen agar hasilnya objektif serta dapat digunakan sebagai dasar untuk perbaikan kebijakan keamanan data. Selain audit, pengawasan aktif dari otoritas perlindungan data, yaitu Lembaga Pengawas Perlindungan Data Pribadi (yang diamanatkan oleh UU PDP), menjadi instrumen penting untuk mencegah pelanggaran data sejak dini. Pengawasan ini dapat dilakukan melalui pemeriksaan rutin, pemantauan aktivitas pemrosesan data, serta mekanisme pelaporan insiden kebocoran data secara transparan. Sebagaimana dinyatakan oleh Warren dan Brandeis dalam teori *The Right to Privacy*, perlindungan privasi memerlukan intervensi negara melalui regulasi dan pengawasan yang efektif untuk mencegah dominasi penyalahgunaan kekuasaan oleh pengendali data terhadap individu sebagai subjek data.

Dalam konteks dimensi dan indikator penelitian, perlindungan preventif dapat diukur melalui beberapa indikator utama, yakni: (1) keberadaan program edukasi dan literasi digital yang diakses masyarakat, (2) penerapan standar teknis keamanan oleh penyelenggara sistem elektronik, (3) frekuensi audit keamanan data oleh pihak independen, (4) keberadaan mekanisme pengawasan dan pelaporan insiden kebocoran data, serta (5) tingkat kepatuhan penyelenggara sistem elektronik terhadap regulasi perlindungan data pribadi. Setiap indikator ini mencerminkan langkah konkret yang dilakukan oleh pemerintah, lembaga pengawas, maupun penyelenggara sistem elektronik untuk menciptakan ekosistem perlindungan data pribadi yang proaktif dan preventif.

Secara keseluruhan, perlindungan preventif merupakan fondasi utama dalam upaya melindungi korban pencurian data pribadi dari potensi kerugian yang timbul. Dengan meningkatkan literasi digital masyarakat, memperketat regulasi dan standar keamanan, serta melaksanakan audit dan pengawasan yang berkesinambungan, diharapkan risiko terjadinya pencurian data pribadi dapat diminimalisir secara signifikan. Namun, efektivitas perlindungan preventif ini sangat bergantung pada komitmen semua pihak, baik regulator, penyelenggara layanan, maupun masyarakat itu sendiri, untuk secara aktif menjalankan perannya dalam menjaga keamanan data pribadi di era digital.

b. Perlindungan Represif

Perlindungan represif merupakan salah satu bentuk perlindungan hukum yang diberikan kepada korban tindak pidana pencurian data pribadi setelah terjadinya pelanggaran. Perlindungan ini bersifat reaktif, yaitu bertujuan untuk memberikan keadilan kepada korban, memulihkan hak-hak yang telah dilanggar, serta memberikan sanksi kepada pelaku sebagai bentuk pertanggungjawaban hukum. Dalam kerangka pemikiran teori keadilan retributif yang dikemukakan oleh John Rawls (1971), perlindungan represif berfungsi sebagai upaya menegakkan keseimbangan moral dan hukum di masyarakat dengan memastikan bahwa setiap pelaku kejahatan mendapatkan ganjaran yang setimpal atas perbuatannya, sementara korban memperoleh pemulihan atas kerugiannya. Perlindungan represif ini menjadi penting karena tidak semua upaya preventif mampu mencegah terjadinya kejahatan pencurian data pribadi, sehingga diperlukan mekanisme hukum yang efektif untuk memberikan rasa keadilan dan kepastian hukum.

Salah satu bentuk utama perlindungan represif adalah melalui **proses hukum pidana.** Dalam konteks ini, pelaku pencurian data pribadi dapat dijerat dengan sanksi pidana sebagaimana diatur dalam berbagai peraturan perundang-undangan yang relevan, seperti UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan UU Nomor 11 Tahun

2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya. UU PDP secara tegas mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak memperoleh atau mengakses data pribadi milik orang lain dengan cara yang melanggar hukum dapat dikenakan pidana penjara dan/atau denda. Ketentuan ini diperkuat dengan UU ITE yang mengatur mengenai akses ilegal ke sistem elektronik dan pencurian informasi digital sebagai tindak pidana yang dapat dikenai sanksi pidana yang cukup berat. Penerapan hukum pidana ini bertujuan untuk menimbulkan efek jera (deterrent effect) bagi para pelaku serta memberikan perlindungan hukum yang konkret bagi korban. Menurut Moeljatno (2002), hukum pidana memiliki fungsi ganda, yaitu sebagai *ultimum remedium* (upaya terakhir) dan sebagai sarana untuk menegakkan ketertiban hukum di masyarakat. Dalam konteks pencurian data pribadi, sanksi pidana menjadi instrumen yang penting untuk menegaskan larangan dan memberikan konsekuensi hukum yang tegas kepada pelaku.

Selain jalur pidana, korban tindak pidana pencurian data pribadi juga memiliki hak untuk menuntut ganti rugi melalui gugatan perdata. Perlindungan ini diberikan berdasarkan asas tanggung jawab perdata yang diatur dalam Pasal 1365 KUHPerdata mengenai perbuatan melawan hukum (*onrechtmatige daad*). Dalam hal ini, korban dapat mengajukan gugatan perdata terhadap pelaku dengan tuntutan agar pelaku membayar ganti rugi atas kerugian materiil dan/atau immateriil yang timbul akibat pencurian data pribadi. Gugatan ini menjadi penting karena pencurian data pribadi tidak hanya menyebabkan kerugian secara finansial, tetapi juga dapat berdampak pada kerugian reputasi, kerugian psikologis, dan bahkan kehilangan kesempatan kerja atau bisnis di masa depan. Teori ganti rugi yang dikemukakan oleh Salim HS (2011) mendukung perlindungan represif ini dengan menekankan bahwa korban yang mengalami kerugian akibat perbuatan melawan hukum berhak mendapatkan pemulihan penuh agar berada dalam posisi yang sama seperti sebelum peristiwa tersebut terjadi. Oleh karena itu, mekanisme gugatan perdata menjadi salah satu instrumen penting dalam memberikan keadilan bagi korban tindak pidana pencurian data pribadi.

Selanjutnya, bentuk perlindungan represif yang juga perlu mendapat perhatian adalah pemulihan nama baik korban. Pencurian data pribadi sering kali disertai dengan penyalahgunaan data untuk kepentingan yang merugikan, seperti pemalsuan identitas, penyebaran informasi palsu, atau penggunaan data untuk kejahatan lain yang mencemarkan nama baik korban. Dalam hal ini, korban berhak untuk memulihkan reputasinya melalui mekanisme hukum yang tersedia, seperti mengajukan permohonan pemulihan nama baik ke pengadilan atau melalui lembaga penyelesaian sengketa non-litigasi. Pemulihan nama baik bukan hanya sekadar tindakan administratif, tetapi juga bagian dari pemenuhan hak asasi

manusia yang diatur dalam Pasal 28G ayat (1) UUD 1945, yaitu hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaan seseorang. Selain itu, pemulihan nama baik juga menjadi aspek penting dalam rehabilitasi sosial korban agar dapat kembali menjalankan aktivitasnya tanpa stigma negatif akibat penyalahgunaan data pribadinya. Penelitian oleh Rahmawati (2022) menunjukkan bahwa pemulihan nama baik merupakan langkah penting dalam mendukung pemulihan psikologis korban kejahatan siber, termasuk korban pencurian data pribadi.

Dimensi perlindungan represif dalam penelitian ini mencakup tiga aspek utama, yaitu: (1) keberadaan mekanisme hukum pidana yang tegas dan implementatif terhadap pelaku, (2) ketersediaan akses bagi korban untuk mengajukan gugatan perdata sebagai upaya pemulihan kerugian, dan (3) efektivitas prosedur pemulihan nama baik korban yang dapat diakses secara adil dan transparan. Indikator-indikator yang digunakan untuk mengukur efektivitas perlindungan represif antara lain: jumlah kasus pencurian data pribadi yang diproses secara pidana, jumlah gugatan perdata yang diajukan korban beserta tingkat keberhasilannya, dan adanya putusan pengadilan atau lembaga penyelesaian sengketa terkait pemulihan nama baik korban.

Secara keseluruhan, perlindungan represif memegang peranan penting dalam memberikan keadilan dan pemulihan kepada korban tindak pidana pencurian data pribadi. Namun, efektivitas perlindungan ini sangat bergantung pada seberapa responsif aparat penegak hukum, kesiapan infrastruktur peradilan, serta kesadaran masyarakat untuk menggunakan hak-haknya dalam rangka menegakkan keadilan. Oleh karena itu, diperlukan upaya harmonisasi regulasi, peningkatan kapasitas lembaga penegak hukum, dan penguatan edukasi hukum agar perlindungan represif tidak hanya bersifat normatif, tetapi juga implementatif dan mampu memberikan efek jera yang optimal bagi pelaku kejahatan siber di Indonesia.

c. Penerapan Hukum Terhadap Kebocoran Data Pribadi dalam Transaksi Elektronik

Dalam hal perlindungan data pribadi, di dalam Undang-undang Nomor 27 Tahun 2022 Pasal 58 disebutkan bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga. Lembaga sebagaimana dimaksud dalam UU tersebut ditetapkan oleh Presiden dan bertanggung jawab kepada Presiden. Pada Pasal 59 UU Nomor 27 Tahun 2022, perumusan dan penerapan strategi perlindungan data pribadi dilakukan oleh lembaga penyelenggara data pribadi tersebut. Pengawasan, penegakan hukum dilakukan oleh lembaga tersebut. Lembaga penyelenggara perlindungan data pribadi ini pun dapat menjatuhkan sanksi administrasi atas pelanggaran perlindungan data pribadi yang dilakukan pengendali data pribadi atau prosesor data pribadi. Lembaga ini juga dapat membantu aparat penegak hukum dalam kasus pidana data

pribadi sebagaimana dimaksud dalam UU Nomor 27 Tahun 2022. Fungsi berikutnya dari lembaga ini adalah menerima aduan atau laporan atas pelanggaran perlindungan data pribadi dan dapat memeriksa sekaligus menelusuri atas dugaan pelanggaran tersebut dan dapat meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa perlindungan data pribadi.

Salah satu yang belum lengkap dalam penegakan hukum pada perlindungan data pribadi ini juga karena belum adanya atau terbitnya aturan turunan seperti Peraturan Pemerintah terkait perlindungan data pribadi di Indonesia. Aturan turunan ini sangatlah penting karena maraknya kasus peretasan dan kebocoran data pribadi di dunia digital saat ini dengan masifnya penggunaan teknologi digitalisasi memungkinkan makin banyaknya kasus-kasus serupa apabila tidak diikuti dengan cepat melalui dasar hukum berupa aturan turunan untuk perlindungan data pribadi ini. Tetapi, di pasal 76 bagian penutup UU PDP ini menyebutkan bahwa UU ini berlaku sejak UU ini diundangkan yaitu pada 17 Oktober 2022. Seharusnya ini menjadi perhatian bagi para penegak hukum untuk segera menyelesaikan kasus-kasus kebocoran yang sudah terjadi sejak UU ini berlaku dan untuk pengendali data pribadi agar lebih memberikan keamanan terhadap perlindungan data pribadi di Indonesia.

Namun yang menjadi hambatan penegakan hukum terhadap kebocoran data pribadi sesudah disahkannya UU Nomor 27 Tahun 2022 adalah lembaga perlindungan data pribadi belum disahkan pada di dalam UU sudah diamanatkan pembentukan kelembagaannya. Karena Lembaga Penyelenggara Perlindungan Data Pribadi ini memiliki peran seperti perlindungan data, pengawasan penyelenggaraan perlindungan data pribadi, penegakan hukum administratif sampai penyelesaian sengketa di luar pengadilan atau arbitrase. Lembaga ini menjadi hal yang paling ditunggu kinerjanya karena maraknya kasus kebocoran data yang memerlukan pengawasan, perlindungan, penegakan hukum yang lebih tegas lagi. Terlebih, lembaga ini perlu pembentukan dan persiapan para anggotanya nanti untuk mencegah adanya kasus kebocoran data pribadi serupa.

d. Hak-Hak Korban

Dalam konteks perlindungan hukum terhadap korban tindak pidana pencurian data pribadi, pengakuan atas hak-hak korban menjadi aspek yang fundamental dalam upaya pemulihan keadilan dan pemenuhan hak asasi manusia. Pengaturan mengenai hak-hak korban tercermin dalam berbagai instrumen hukum nasional, terutama dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang secara khusus memberikan ruang bagi korban untuk mendapatkan perlindungan yang memadai. Perlindungan ini selaras dengan prinsip-prinsip perlindungan data pribadi yang berlaku secara internasional, seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang menekankan pentingnya

pemenuhan hak-hak subjek data sebagai bentuk perlindungan atas privasi dan kedaulatan individu. Dalam perspektif teori keadilan restoratif yang dikemukakan oleh Tony Marshall (1999), pemenuhan hak-hak korban tidak hanya bersifat simbolik, tetapi juga berorientasi pada pemulihan kerugian nyata yang dialami korban akibat kejahatan, termasuk pencurian data pribadi. Salah satu hak penting yang dimiliki korban adalah hak atas informasi**.**

Hak ini memberikan kesempatan bagi korban untuk memperoleh kejelasan mengenai bagaimana data pribadinya diproses, disimpan, dan digunakan oleh pengendali data. UU PDP, khususnya dalam Pasal 7 dan Pasal 8, menegaskan bahwa pengendali data wajib memberikan informasi yang jelas, benar, dan lengkap kepada subjek data mengenai kegiatan pemrosesan data pribadi, termasuk jika terjadi insiden pelanggaran data (data breach). Informasi ini mencakup identitas pengendali data, dasar hukum pemrosesan, tujuan pengumpulan data, periode penyimpanan, serta potensi risiko yang dapat timbul. Hak atas informasi menjadi penting karena tanpa adanya transparansi, korban akan kesulitan untuk memahami dampak dari pencurian data pribadi yang dialaminya dan menentukan langkah hukum yang perlu diambil. Menurut Smith (2017), transparansi adalah prinsip utama dalam perlindungan data pribadi karena menciptakan kepercayaan antara pengendali data dan subjek data. Selain itu, korban juga memiliki hak atas akses terhadap data pribadinya yang disimpan atau dikelola oleh pengendali data.

Hak ini diatur dalam Pasal 6 UU PDP, yang memberikan kewenangan kepada korban untuk meminta informasi mengenai keberadaan data pribadinya, tujuan penggunaannya, serta pihak-pihak yang telah menerima atau mengakses data tersebut. Hak atas akses memungkinkan korban untuk melakukan kontrol terhadap data pribadinya dan menjadi dasar penting dalam rangka menuntut pertanggungjawaban apabila terjadi pelanggaran. Dalam konteks ini, teori *informational self-determination* yang diperkenalkan oleh Westin (1967) relevan untuk dijadikan pijakan, yaitu bahwa setiap individu memiliki hak untuk menentukan bagaimana informasi pribadinya digunakan, disimpan, dan disebarluaskan. Tanpa adanya hak akses, korban kehilangan kontrol atas data pribadinya, yang justru menjadi salah satu penyebab utama kerentanan dalam era digital saat ini.

Hak penting lainnya adalah hak atas perbaikan dan penghapusan data pribadi (right to rectification and right to erasure). UU PDP secara tegas mengatur bahwa korban berhak untuk meminta perbaikan terhadap data pribadinya yang tidak akurat atau tidak lengkap (Pasal 6 ayat 4), serta meminta penghapusan data pribadinya yang telah disalahgunakan atau diproses tanpa persetujuan yang sah (Pasal 15). Hak ini menjadi instrumen penting dalam memulihkan kerugian korban, karena seringkali data pribadi yang dicuri digunakan untuk tujuan yang

merugikan, seperti penipuan, pencemaran nama baik, atau tindak kejahatan lain. Studi oleh Aldhouse (2021) menunjukkan bahwa hak untuk memperbaiki dan menghapus data pribadi merupakan langkah konkret dalam memastikan bahwa individu tetap memiliki kendali atas identitas digitalnya, sekaligus mencegah kerugian yang lebih besar akibat penyalahgunaan data. Hak ini juga mendukung prinsip *data minimization*, yaitu bahwa data pribadi hanya boleh disimpan selama diperlukan dan harus dihapus ketika sudah tidak relevan.

Tidak kalah penting, korban juga memiliki hak atas ganti rugi atas kerugian yang dialami akibat pencurian data pribadi. Hak ini diatur dalam Pasal 58 UU PDP, yang menyatakan bahwa setiap orang yang mengalami kerugian akibat pelanggaran data pribadi berhak untuk memperoleh ganti rugi melalui mekanisme hukum yang berlaku. Ganti rugi ini mencakup kerugian materiil, seperti kerugian finansial akibat penyalahgunaan data, maupun kerugian immateriil, seperti trauma psikologis, rasa takut, atau kehilangan rasa aman. Dalam konteks ini, teori *corrective justice* yang dikemukakan oleh Aristoteles menjadi relevan, yaitu bahwa keadilan menuntut agar pihak yang dirugikan menerima pemulihan setara dengan kerugian yang dideritanya, sementara pelaku bertanggung jawab untuk mengembalikan keadaan seperti semula sejauh mungkin. Gugatan ganti rugi dapat diajukan melalui mekanisme perdata di pengadilan atau melalui penyelesaian sengketa alternatif yang diatur oleh peraturan perundang-undangan. Hal ini menunjukkan adanya pengakuan negara terhadap hak korban untuk memperoleh pemulihan secara penuh, tidak hanya secara moral, tetapi juga secara material.

Secara keseluruhan, dimensi hak-hak korban dalam penelitian ini mencakup empat aspek utama, yaitu: (1) hak atas informasi sebagai dasar transparansi dan kontrol terhadap data pribadi; (2) hak atas akses untuk mengetahui keberadaan dan penggunaan data pribadi; (3) hak atas perbaikan dan penghapusan data sebagai upaya pemulihan; dan (4) hak atas ganti rugi sebagai bentuk kompensasi atas kerugian yang dialami. Indikator yang digunakan dalam penelitian ini untuk mengukur efektivitas pemenuhan hak-hak korban meliputi: tingkat kesadaran korban terhadap hak-haknya, kemudahan akses terhadap mekanisme pemulihan, serta realisasi pemberian ganti rugi dan pemulihan nama baik korban dalam praktik.

Dengan demikian, perlindungan hukum terhadap korban tindak pidana pencurian data pribadi tidak hanya terwujud dalam bentuk sanksi terhadap pelaku, tetapi juga melalui pemenuhan hak-hak korban yang menjadi landasan bagi terciptanya keadilan substantif. Oleh karena itu, penting bagi pemerintah, lembaga penegak hukum, serta masyarakat untuk memastikan bahwa hak-hak korban benar-benar dilaksanakan secara efektif dan bukan sekadar menjadi norma formal tanpa implementasi nyata.

4. PENUTUP

Kesimpulan

Perlindungan data pribadi sudah menjadi suatu kebutuhan penting di zaman digital kini, informasi pribadi mampu dengan mudah dikumpulkan, disimpan, dan ditransfer oleh organisasi, perusahaan, atau pihak ketiga. Kebutuhan akan perlindungan data pribadi juga semakin meningkat karena semakin banyak kasus pelanggaran keamanan data yang dilaporkan, seperti *kebocoran data, pencurian identitas, dan penipuan online.* Perlindungan data pribadi ialah upaya untuk mengamankan data pribadi seseorang dari penyelewengan, pengumpulan, dan pengolahan tanpa sepengetahuan dan persetujuannya. Konsep ini erat kaitannya dengan hak privasi individu, di mana setiap orang berhak atas kebebasan untuk menentukan penggunaan data pribadinya.

Undang-undang Nomor 27 Tahun 2022 Pasal 58 disebutkan bahwa *penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga*. Lembaga sebagaimana dimaksud dalam UU tersebut ditetapkan oleh Presiden dan bertanggung jawab kepada Presiden. Pada Pasal *59 UU Nomor 27 Tahun 2022,* perumusan dan penerapan strategi perlindungan data pribadi dilakukan oleh lembaga penyelenggara data pribadi tersebut. Pengawasan, penegakan hukum dilakukan oleh lembaga tersebut. Lembaga penyelenggara perlindungan data pribadi ini pun dapat menjatuhkan sanksi administrasi atas pelanggaran perlindungan data pribadi yang dilakukan pengendali data pribadi atau prosesor data pribadi, pelaku pencurian data pribadi dapat juga di jatuhkan pidana penjara maksimal *6 (enam) tahun.*

Saran

Penetapan undang- undang tentang perlindungan data pribadi diharapkan dapat melindungi data pribadi masyarakat sehingga data tersebut *terjamin dan dilindungi oleh Negara,* dan oknum yang selalu memanfaatkan data pribadi orang lain untuk keuntungan dirinya sendiri harus mendapatkan efek jera karena dengan sengaja melawan hukum. Bagi korban yang dirugikan atas pencurian data pribadi harus diberikan perlindungan yang maksimal oleh Negara dengan mengedepankan perlidungan hukum yang adil.

Penegakan hukum terhadap tindak pidana pencurian data pribadi dapat dilakukan dengan *peningkatan kapasitas sumber daya manusia*, peningkatan pengembangan infrastruktur forensik digital, penyempurnaan kelembagaan, peningkatan upaya keamanan pengelolaan data, penguatan kerjasama internasional, peningkatan kesadaran masyarakat, penerapan hukum yang konsisten terhadap pelaku pencurian data serta *penerapan sanksi administratif* dan *pidana* yang maksimal bagi pelaku pencurian data.

DAFTAR PUSTAKA

Abdul Kadir. (2004). *Hukum dan penelitian hukum*. Bandung: PT. Citra Aditya Bakti.

Adolf, H. (1991). *Aspek-aspek negara dalam hukum internasional*. Jakarta: Rajawali Press.

Adolf, H. (1991). *Aspek-aspek negara dalam hukum internasional*. Jakarta: Rajawali Press.

Afnesia, U., & Ayunda, R. (2022). Perlindungan data diri peminjam dalam transaksi pinjaman online: Kajian perspektif perlindungan konsumen di Indonesia. *Jurnal Komunitas Yustisia*, *4*(3), 1035–1044.

Akbar, G. H., & Simangunsong, F. (2023). Perlindungan hukum korban pencurian data pribadi (phishing cybercrime) dalam perspektif kriminologi. *Jurnal Kriminologi*, *3*(1).

Alan, F. W. (1967). *Privacy and freedom*. New York: Antheneum Press.

Alhakim, A. (2022). Urgensi perlindungan hukum terhadap jurnalis dari risiko kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Pembangunan Hukum Indonesia*, *4*(1), 89–106.

Ali, A. (2008). *Menguak tabir hukum*. Bogor: Ghalia Indonesia.

Ali, L., & Saraswati, R. (2019). *Metodologi penelitian hukum normatif: Teori dan praktek*. Mandar Maju.

Ali, Z. (2010). *Metode penelitian hukum*. Jakarta: Sinar Grafika.

Amiruddin, & Asikin, Z. (2017). *Pengantar metode penelitian hukum*. Jakarta: RajaGrafindo Persada.

Anggara, S., et al. (2015). *Menyeimbangkan hak: Tantangan perlindungan privasi dan menjamin akses keterbukaan informasi dan data di Indonesia*. Jakarta: ICJR.

Anggraeni, S. F. (2018). Polemik pengaturan kepemilikan data pribadi: Urgensi untuk harmonisasi dan reformasi hukum di Indonesia. *Jurnal Hukum & Pembangunan*, *48*(4), 814–825.

APPD. (n.d.). *From act to action: Strategi implementasi UU perlindungan data pribadi*.

Asril Sitompul. (2004). *Hukum internet: Pengenalan mengenai masalah hukum di cyberspace*. Bandung: Citra Aditya Bakti.

Asshiddiqie, J. (2006). *Teori Hans Kelsen tentang hukum*. Jakarta: Konstitusi Press.

Asshiddiqie, J. (2006). *Teori Hans Kelsen tentang hukum*. Jakarta: Konstitusi Press.

Badan Pengembangan dan Pembinaan Bahasa. (2008). *Kamus Besar Bahasa Indonesia* (Edisi ke-4). Jakarta: PT Gramedia Pustaka Utama.

Baehaki, K., & Hadis, T. R. (2021). Perlindungan hukum terhadap saksi dan korban dalam sistem peradilan pidana Indonesia. *Jurnal Media Hukum*.

Bambang Sunggono. (2001). *Metodologi penelitian hukum*. Jakarta: RajaGrafindo Persada.

Bambang Waluyo. (2014). *Pidana dan pemidanaan* (Cet. Ke-4). Jakarta: Sinar Grafika.

Barda Nawawi. (2006). *Tindak pidana mayantara*. Jakarta: RajaGrafindo Persada.

Bassar, S. (1999). *Tindak-tindak pidana tertentu*. Bandung: Ghalian.

Budi Suhariyanto. (2013). *Tindak pidana teknologi informasi (cybercrime)*. Jakarta: RajaGrafindo Persada.

Budiman, A. A., et al. (2021). *Mengatur ulang kebijakan tindak pidana di ruang siber*. Jakarta: Institute for Criminal Justice Reform.

Celina Tri Siwi Kristiyanti. (2011). *Hukum perlindungan konsumen*. Jakarta: Sinar Grafika.

Chairul Areasjid. (2000). *Dasar-dasar ilmu hukum*. Jakarta: Sinar Grafika.

Chee, B. J. S., & Franklin, C., Jr. (2010). *Cloud computing: Technologies and strategies of the ubiquitous data center*. Gainesville: CRC Press.

Cholid Narbuko, & Achmadi, A. (2010). *Metodologi penelitian*. Jakarta: Bumi Aksara.

Cindy Mutia Annur. (2022). Indeks keamanan siber Indonesia peringkat ke-3 terendah di antara negara G20.

Danny Kobrata. (2021). RUU perlindungan data pribadi: Sebuah penantian.

Danrivanto Budhijanto. (2010). *Hukum telekomunikasi, penyiaran & teknologi informasi: Regulasi & konvergensi*. Bandung: PT. Refika Aditama.

Dewi, S. (2009). *Perlindungan privasi atas informasi pribadi dalam e-commerce menurut hukum internasional*. Bandung.

Dewi, S. (2017). Prinsip–prinsip perlindungan data pribadi nasabah kartu kredit menurut ketentuan nasional dan implementasinya. *Sosiohumaniora*, *19*(3), 206–212.

Digital, M. (2023, July 17). Program edukasi, masyarakat harus menjaga data pribadi. *Harianjogja.com*.

Diyu Sulaeman, & Kemala, A. P. (2025). Analisis hukum terhadap tindak pidana pencurian identitas di Indonesia. *Jurnal Hukum Siber*, *3*(2), 134.

Djafar, W. (2019). Hukum perlindungan data pribadi di Indonesia: Lanskap, urgensi, dan kebutuhan pembaruan. *Seminar Hukum dalam Era Analisis Big Data*, Pascasarjana FH UGM, *26*.

Djafar, W., & Santoso, M. J. (2019). *Perlindungan data pribadi: Mengenali hak-hak subjek data, serta kewajiban pengendali dan prosesor data*. Jakarta: ELSAM.

Emmilia Rusdiana. (2023). Alternatif pidana bagi pelaku tindak pidana peretasan di Indonesia dalam Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Suara Hukum*, 250.

Farhan, F., Hamdani, F., et al. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Indonesia Berdaya*, *3*(3).

Febyola Indah, Sidabutar, A., & Annisa, N. (2022). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1).

Fitri Sucia. (2022). Pertanggungjawaban pidana terhadap pelaku hacker dengan tujuan pemesanan fiktif. *Jurnal Dialektika Hukum*, *4*(2), 157.

Freeman, M., & Van Ert, G. (2004). *International human rights law*. Toronto.

Friedman, L. M. (1975). *The legal system: A social science perspective*. New York: Russell Sage Foundation.

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Heidelberg: Springer.

GEMA AKTUALITA. (2025). *GEMA AKTUALITA*, 3(2), 14–25.

Greeneaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. New York: Oxford University Press.

Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspectives*. Oxford University Press.

Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information and Science*, 23(1), 1–48.

Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information and Science*, 23(1), 1.

Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(1), 154–167.

Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(1), 154–167.

Hamzah, A. (2009). *Delik-delik khusus*. Jakarta: Sinar Grafika.

Hamzah, A. (2009). *Delik-delik khusus*. Jakarta: Sinar Grafika.

Hart, H. L. A. (2010). *Konsep hukum* (M. Khozim, Trans.). Bandung: Nusamedia.

Hart, H. L. A. (2010). *Konsep hukum* (M. Khozim, Trans.). Nusamedia. (Karya asli diterbitkan 1961)

Hasoeprapto, H. (1998). *Pengantar tata hukum Indonesia*. Yogyakarta: Liberty.

Hasoeprapto, H. (1998). *Pengantar tata hukum Indonesia*. Yogyakarta: Liberty.

Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam: North-Holland Publishing Co.

Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam: North-Holland Publishing Co.

Ibnu Mas'ud. (1991). *Kamus pintar populer*. Yogyakarta: Ananda.

Ibrahim, J. (2006). *Teori & metodologi penelitian hukum normatif*. Bayumedia Publishing.

Ibrahim, J. (2006). *Teori & metodologi penelitian hukum normatif*. Malang: Bayumedia Publishing.

Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, Pasal 28G(1).

Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, Pasal 28G ayat (1).

Indonesia. (2016). *Undang-Undang Informasi dan Transaksi Elektronik*, No. 19 Tahun 2016, Pasal 26(1).

Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*, Pasal 26 ayat (1).

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).*

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Pasal 57.

Indonesia. (2022). *Undang-Undang Perlindungan Data Pribadi*, No. 27 Tahun 2022, Pasal 57.

Ineu Rahmawati. (2017). The analysis of cyber crime threat risk management to increase cyber defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66.

JDIH Kemkominfo. (2024). *Kepastian hukum pelindungan data pribadi pasca pengesahan UU PDP*.

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A., Asriyani, A., Hazmi, R. M., & Samara, M. R. (2023). *Metode penelitian hukum*. CV Gita Lentera.

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A., Asriyani, A., Hazmi, R. M., & Samara, M. R. (2023). *Metode penelitian hukum*. CV. Gita Lentera.

Karo Karo, R. P. P. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat*. Bandung: Nusa Media.

Karo, R. P. P. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat*. Nusa Media.

Karo, R. P. P. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat*. Bandung: Nusa Media.

KBBI. (2021). Definisi data pribadi. *Kamus Besar Bahasa Indonesia*. Retrieved February 11, 2021, 16:55 WIB.

Kelsen, H. (1961). *General theory of law and state*. Russell & Russell.

Kelsen, H. (1967). *Pure theory of law*. University of California Press.

Kelsen, H. (1967). *The pure theory of law*. University of California Press.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Era baru pelindungan data pribadi*. Indonesia.go.id.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Era baru pelindungan data pribadi*. Indonesia.go.id.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Kepastian hukum pelindungan data pribadi pasca pengesahan UU PDP*. JDIH Kemkomdigi.

Kencana Prenada Media. (2013). *Kejahatan siber (Cyber Crime)*. Jakarta: Kencana.

Khikam, D. (2023). *Kajian hukum perlindungan data pribadi dalam peraturan perundang-undangan di Indonesia* (Skripsi, Universitas Islam Sultan Agung).

Khikam, D. (2023). *Kajian hukum perlindungan data pribadi dalam peraturan perundang-undangan di Indonesia* (Skripsi, Universitas Islam Sultan Agung).

Klosek, J. (2000). *Data privacy in the information age*. Greenwood Publishing.

Klosek, J. (2000). *Data privacy in the information age*. Greenwood Publishing.

KOMINFO. (2023). *Memastikan data pribadi aman*. Website Resmi Kementerian Komunikasi dan Informatika RI. Retrieved November 13, 2023.

KOMINFO. (n.d.). Memastikan data pribadi aman. Retrieved November 13, 2023, from https://kominfo.go.id

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al Wasath: Jurnal Ilmu Hukum*, 2(1), 20–29.

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al-Wasath: Jurnal Ilmu Hukum*, 2(1), 20.

Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Ilmu Hukum*, 11(3), 189–203.

Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal*.

Lesmana, C. T., Elis, E., & Hamimah, S. (2021). Urgensi UU Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak privasi masyarakat Indonesia. *Jurnal Rechten: Penelitian Hukum dan Hak Asasi Manusia*, 3(2), 1–6.

Lesmana, C. T., Elis, E., & Hamimah, S. (2021). Urgensi UU Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak privasi masyarakat Indonesia. *Jurnal Rechten*, 3(2), 1–6.

Lukman Ali, & Saraswati, R. (2019). *Metodologi penelitian hukum normatif: Teori dan praktek*. Bandung: Mandar Maju.

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan hukum pidana terhadap pengaturan pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi. *Jurnal Hukum Pidana dan Kriminologi*, 2(2), 134–148.

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan hukum pidana terhadap pengaturan pencurian data pribadi. *Jurnal Hukum Pidana dan Kriminologi*, 2(2).

Mahiar, D. F., & Lisa, E. Y. N. A. (2020). Consumer Protection System (CPS): Sistem perlindungan data pribadi konsumen melalui collaboration concept. *Legislatif*, 3(2), 287–302.

Mahiar, D. F., & Lisa, E. Y. N. A. (2020). Consumer protection system (CPS): Sistem konsumen melalui collaboration concept. *Legislatif*, 3(2), 287–302.

Mas'ud, I. (1991). *Kamus pintar populer*. Yogyakarta: Ananda.

Moleong, L. J. (2017). *Metodologi penelitian kualitatif* (Rev. ed.). Bandung: Remaja Rosdakarya.

Moleong, L. J. (2017). *Metodologi penelitian kualitatif*. Bandung: Remaja Rosdakarya.

Prasetyo, T. (2018). *Pengantar ilmu hukum*. Depok: RajaGrafindo Persada.

Pratama, R., & Wulan, E. R. (n.d.). Urgensitas pembentukan lembaga penyelenggaraan perlindungan data pribadi.

Rahmawati, I. (2017). The analysis of cyber crime threat risk management to increase cyber defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.837

Rosadi, S. D. (2015). *Cyber law: Aspek data privasi menurut hukum internasional, regional dan nasional* (hal. 23). Jakarta: Refika Aditama.

Rosadi, S. D. (2018). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. *VeJ*, 4(1), 108–109. Bandung: Fakultas Hukum Universitas Padjadjaran.

Salahuddin. (1991). *Sistem sanksi dalam hukum pidana* (hlm. 3). Jakarta: Pradnya Paramitha.

Satria, M. K., & Yusuf, H. (2024). Analisis yuridis tindakan kriminal doxing ditinjau berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Jurnal Intelek Dan Cendikiawan Nusantara*, 1(2).

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi perbandingan hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 374.

Shaw, M. N. (2008). *International law* (6th ed.). New York: Cambridge University Press.

Shaw, M. N. (2008). *International law* (6th ed.). New York: Cambridge University Press.

Sianturi, S. R. (2002). *Asas-asas hukum pidana di Indonesia dan penerapannya* (Cet. 3). Jakarta: Storia Grafika.

Sieber, U. (2001). The emergence of information law: Object and characteristics of a new legal area. In E. Lederman & R. Shapira (Eds.), *Law, Information and Information Technology*. Kluwer Law International.

Soekanto, S., & Mamudji, S. (2001). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: RajaGrafindo Persada.

Soemitro, R. H. (1990). *Metodologi penelitian hukum dan jurimetri*. Jakarta: Ghalia Indonesia.

Sonjaya, A., & Setiawan, D. A. (2022, Januari). Perlindungan hukum bagi korban kebocoran data pribadi pengguna aplikasi Tokopedia berdasarkan UU No. 19 Tahun 2016 tentang perubahan atas UU No. 11 Tahun 2008 tentang informasi dan transaksi. *Bandung Conference Series: Law Studies*, 2(1), 420–427.

St. John's University School of Law. (2025). *Kelsen's pure theory of law*. "Austin, Kelsen, and the model of sovereignty." ResearchGate, 2024.

Sugeng. (2020). *Hukum telematika Indonesia*. Jakarta: Prenada Media.

Supiyati, S. (2020). Penerapan Pasal 27 Ayat 3 Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik terhadap tindak pidana pencemaran nama baik melalui internet sebagai cybercrime dihubungkan dengan kebebasan berekspresi. *Pamulang Law Review*, 2(1).

Sutedi, A. (2023). *Perlindungan hukum data pribadi di Indonesia*. Jakarta: Sinar Grafika.

Suteki, & Taufani, G. (2018). *Metodologi penelitian hukum: Filsafat, teori dan praktik*. Jakarta: Rajawali Pers.

Talinusa, S. C. (2015). Tindak pidana pemerasan dan/atau pengancaman melalui sarana internet menurut Undang-Undang Nomor 11 Tahun 2008. *Lex Crimen*, 4(6), 162.

Tektona, R. I. (2021). Arbitrase sebagai alternatif solusi penyelesaian sengketa bisnis di luar pengadilan. *Pandecta Research Law Journal*, 6(1).

Triadi, M. (2021). Perlindungan terhadap korban pencurian data pribadi melalui media digital. *REUSAM: Jurnal Ilmu Hukum*.

Wahyudi Djafar, & Komarudin, A. (2014). *Perlindungan hak atas privasi di internet: Beberapa penjelasan kunci*. Jakarta: ELSAM.

Wahyudi, H. S., & Sukmasari, M. P. (2018). Teknologi dan kehidupan masyarakat. *Jurnal Analisa Sosiologi*, 3(1), 16.

Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193.

Watkat, F. X., Ingratubun, M. T., & Apriyanti, A. (2021). Perlindungan data pribadi melalui...

Wibowo, I. Y. (2009). Perlindungan hukum terhadap korban tindak pidana menurut hukum...

Widya Padjajaran. (2015). *Cyber law: Aspek data privasi menurut hukum internasional, regional, dan nasional*. Bandung: Refika Aditama.

Wulan Sari, F. (n.d.). Perlindungan hukum atas data pribadi nasabah dalam penyelenggaraan layanan internet banking dihubungkan dengan Undang-Undang Nomor 10 Tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang perbankan.

Wulandari, I. W., & Hwihanus, H. (2023). Peran sistem informasi akuntansi dalam pengaplikasian enkripsi terhadap peningkatan keamanan perusahaan. *Jurnal Kajian dan Penalaran Ilmu Manajemen*, 1(1).

Yudha, M. A. (2023). Tanggung jawab penyedia atas keamanan data penggunaan layanan.

Yuhelizar. (2008). *10 jam menguasai internet: Teknologi dan aplikasinya*. Jakarta: PT Elex Media Komputindo.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Jurnal Becoss*, 1(1), 147–154.

Yurizal. (2018). *Penegakan hukum tindak pidana cyber crime*. Malang: Tim MNC Publishing.