



Analisis Perlindungan Hukum terhadap Korban Pelanggaran Pencurian Data Pribadi untuk Pinjaman Online berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Muhammad Ilham Muladi Wilopo

Universitas Pembangunan Nasional "Veteran" Jawa Timur, Kota Surabaya, Indonesia

ilhammuladi86@gmail.com

Abstrak

Penyalahgunaan data pribadi pelamar kerja oleh pihak tidak bertanggung jawab untuk pencairan dana pinjaman daring merupakan kejahatan siber yang menimbulkan kerugian materiil dan imateriil bagi korban. Penelitian ini bertujuan untuk menganalisis mekanisme perlindungan hukum bagi korban pencurian data identitas berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual yang bersumber dari data sekunder. Hasil penelitian menunjukkan bahwa regulasi tersebut memberikan perlindungan preventif melalui kewajiban pengendali data untuk melakukan verifikasi keaslian data dan memperoleh persetujuan eksplisit dari subjek data sebelum pemrosesan. Sementara itu, perlindungan represif diwujudkan melalui penerapan sanksi pidana penjara, denda administratif yang berat bagi perseorangan maupun korporasi, serta hak korban untuk mengajukan gugatan ganti rugi. Penelitian ini menyimpulkan bahwa Undang-Undang Perlindungan Data Pribadi telah memperkuat posisi hukum korban dengan menetapkan prinsip pertanggungjawaban mutlak kepada penyelenggara sistem elektronik yang lalai dalam menjaga keamanan data, meskipun efektivitas penagakannya sangat bergantung pada pembentukan lembaga pengawas yang independen dan berwenang.

Kata kunci: Data Pribadi, Kejahatan Siber, Perlindungan Hukum, Pinjaman Daring, Undang-Undang Perlindungan Data Pribadi

Abstract

The misuse of job applicants' personal data by irresponsible parties for disbursing online loan funds is a cybercrime causing material and immaterial losses to victims. This study aims to analyze the legal protection mechanisms for identity theft victims based on Law Number 27 of 2022 concerning Personal Data Protection. The research method used is normative legal research with statutory and conceptual approaches derived from secondary data. The results show that the regulation provides preventive protection through the obligation of data controllers to verify data authenticity and obtain explicit consent from data subjects before processing. Meanwhile, repressive protection is realized through the imposition of imprisonment sanctions, heavy administrative fines for individuals and corporations, and the victim's right to file for compensation. This study concludes that the Personal Data Protection Law has strengthened the legal position of victims by establishing strict liability principles for electronic system operators who are negligent in maintaining data security, although the effectiveness of its enforcement relies heavily on the establishment of an independent and authorized supervisory institution.

Key words: Cyber Crime, Legal Protection, Online Loans, Personal Data, Personal Data Protection Law.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa transformasi fundamental dalam berbagai aspek kehidupan manusia, termasuk dalam ekosistem keuangan melalui layanan teknologi finansial (*financial technology/fintech*). Inovasi ini menawarkan efisiensi dan inklusi keuangan, namun secara simultan menghadirkan ancaman serius terhadap privasi dan keamanan data pribadi. Data pribadi kini telah bertransformasi menjadi aset bernilai ekonomi tinggi yang rentan dieksploitasi. Di Indonesia, fenomena penyalahgunaan data pribadi untuk pengajuan pinjaman online (*peer-to-peer lending*) tanpa persetujuan pemilik data menjadi salah satu modus kejahatan siber yang paling meresahkan. Kasus konkret yang mencerminkan urgensi permasalahan ini adalah insiden di Jakarta Timur pada pertengahan tahun 2024, di mana data pribadi milik 27 pelamar kerja disalahgunakan oleh oknum pemberi kerja berinisial R untuk mengajukan pinjaman di berbagai platform seperti ShopeePayLater, Adakami, dan Kredivo, yang mengakibatkan kerugian kolektif mencapai satu miliar rupiah (Noviansah, 2024).

Secara konstitusional, perlindungan terhadap data pribadi merupakan manifestasi dari hak asasi manusia sebagaimana diamanatkan dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945). Negara telah merespons kebutuhan mendesak akan payung hukum yang komprehensif melalui pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini diharapkan menjadi *lex specialis* yang menjamin kedaulatan individu atas data pribadinya. Namun, efektivitas implementasi regulasi ini masih menghadapi tantangan struktural, terutama terkait kekosongan lembaga pengawas independen yang dimandatkan oleh undang-undang tersebut (Hardafi, 2025).

Sejumlah penelitian terdahulu telah mengkaji isu perlindungan data pribadi dari berbagai perspektif. Firdaus (2022) menyoroti perlindungan hak privasi dari kejahatan peretasan dengan fokus pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sementara Soraja (2021) menganalisis perlindungan data pribadi dalam perspektif Hak Asasi Manusia. Lebih spesifik pada sektor *fintech*, Afiudin (2022) membahas peran Otoritas Jasa Keuangan (OJK) dalam melindungi nasabah dari penyalahgunaan data. Namun, mayoritas literatur domestik tersebut disusun sebelum berlakunya UU PDP secara penuh atau masih menggunakan UU ITE sebagai landasan analisis utama, sehingga belum menyentuh mekanisme perlindungan spesifik yang ditawarkan oleh rezim hukum perlindungan data pribadi yang baru.

Dalam konteks global, perlindungan data pribadi dalam layanan *fintech* telah menjadi diskursus intensif. Studi komparatif oleh Sofia & Putra (2025) serta Maleno & Kusumawati (2024) menunjukkan bahwa meskipun Indonesia telah memiliki UU PDP yang mengadopsi prinsip-prinsip *General Data Protection Regulation* (GDPR) Uni Eropa, mekanisme penegakan hukum dan kelembagaan di Indonesia masih tertinggal dibandingkan standar internasional. Literatur internasional seperti Acquisti et al. (2015) menekankan bahwa tanpa otoritas pengawas yang independen dan kuat seperti Information Commissioner's Office (ICO) di Inggris atau otoritas perlindungan data di bawah GDPR, regulasi perlindungan data cenderung tidak efektif dalam menanggulangi pencurian identitas di sektor keuangan digital (Sofia & Putra, 2025). Kesenjangan (*gap*) inilah yang menjadi fokus utama penelitian ini. Penelitian ini menawarkan kebaruan (*novelty*) dengan menganalisis secara spesifik perlindungan hukum bagi korban pencurian data pribadi dalam modus operandi pinjaman online ilegal maupun legal, menggunakan pisau analisis UU PDP yang belum banyak dieksplorasi secara mendalam dalam kaitannya dengan kasus *identity theft* berkedok rekrutmen kerja.

Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum preventif dan represif yang tersedia bagi korban penyalahgunaan data pribadi berdasarkan UU PDP, serta mengidentifikasi hambatan yuridis dan semiotik dalam implementasinya. Melalui pendekatan yuridis normatif, artikel ini akan menguraikan bagaimana UU PDP dapat menjadi instrumen perlindungan yang efektif sekaligus menyoroti urgensi pembentukan lembaga pengawas perlindungan data pribadi untuk menjamin kepastian hukum di era ekonomi digital.

METODE

Penelitian ini merupakan penelitian hukum normatif (yuridis normatif) yang difokuskan pada pengkajian kaidah-kaidah atau norma hukum yang berlaku dalam hukum positif di Indonesia (Pratama & Apriani, 2023). Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan dilakukan dengan menelaah regulasi terkait, khususnya UU PDP serta peraturan terkait lainnya seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan UU ITE, guna memahami konstruksi hukum perlindungan data pribadi. Sementara itu, pendekatan perbandingan digunakan untuk mengevaluasi efektivitas regulasi nasional dengan membandingkannya terhadap prinsip-prinsip hukum yang lebih luas atau mekanisme perlindungan di yurisdiksi lain yang relevan, guna memberikan rekomendasi penyempurnaan sistem perlindungan data di Indonesia.

Data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi kepustakaan (*library research*). Sumber data sekunder ini menurut Muhaimin (2020) dalam S et al. (2024) diklasifikasikan menjadi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi regulasi yang mengikat, antara lain UUD 1945, KUHP, UU ITE beserta perubahannya, serta fokus utama pada UU PDP. Bahan hukum sekunder mencakup literatur, buku-buku hukum, jurnal ilmiah, dan hasil penelitian terdahulu yang memberikan penjelasan mengenai bahan hukum primer (S et al., 2024), sedangkan bahan hukum tersier seperti kamus hukum dan ensiklopedia digunakan untuk memberikan petunjuk atau penjelasan terhadap istilah-istilah hukum yang dianalisis (Pratama et al., 2025).

Teknik pengumpulan data dilakukan melalui penelusuran literatur dan dokumentasi hukum secara sistematis. Bahan hukum yang telah terkumpul kemudian diinventarisasi, diklasifikasikan, dan diseleksi relevansinya dengan rumusan masalah mengenai pencurian data pribadi dalam praktik pinjaman online. Teknik analisis data yang diterapkan adalah analisis kualitatif dengan metode logika deduktif. Proses analisis dimulai dari premis mayor berupa aturan hukum positif (UU PDP dan regulasi terkait), yang kemudian dihubungkan dengan premis minor berupa fakta hukum terkait kasus pencurian data pribadi untuk pinjaman online. Dari proses tersebut, ditarik kesimpulan preskriptif untuk menjawab bagaimana bentuk perlindungan hukum serta upaya penyelesaian hambatan hukum yang dihadapi korban.

HASIL DAN PEMBAHASAN

Dinamika kejahatan siber di sektor finansial Indonesia telah mengalami evolusi yang signifikan seiring dengan masifnya adopsi teknologi digital dalam layanan keuangan. Fenomena penyalahgunaan data pribadi, khususnya Kartu Tanda Penduduk atau KTP, untuk kepentingan pencairan dana pada aplikasi pinjaman online ilegal atau yang sering disebut dengan pinjol, merupakan manifestasi nyata dari kerentanan ekosistem digital nasional. Sebelum disahkannya UU PDP, kerangka hukum di Indonesia tersebar secara parsial dalam berbagai regulasi sektoral seperti UU ITE serta peraturan Otoritas Jasa Keuangan, yang sering kali tidak harmonis dan menyisakan celah hukum yang dimanfaatkan oleh sindikat kejahatan siber. Kehadiran regulasi terbaru ini menandai pergeseran paradigma hukum dari pendekatan yang bersifat administratif murni menuju pendekatan yang berbasis pada hak asasi manusia, di mana perlindungan data pribadi ditempatkan sebagai hak konstitusional yang wajib dilindungi oleh negara dan dihormati oleh korporasi. Analisis yuridis terhadap fenomena pencurian data pelamar kerja yang digunakan untuk pinjol menunjukkan bahwa undang-undang ini menawarkan konstruksi perlindungan hukum yang bersifat ganda, yakni perlindungan preventif dan perlindungan represif, yang keduanya dirancang untuk bekerja secara simultan dalam menciptakan ekosistem digital yang aman.

Perlindungan hukum preventif dalam kerangka undang-undang ini dibangun di atas fondasi kewajiban pengendali data untuk mematuhi prinsip-prinsip pemrosesan data yang ketat dan transparan. Filosofi dasar dari perlindungan preventif ini adalah meminimalisir risiko pelanggaran sebelum kerugian terjadi pada subjek data. Salah satu pilar utama dalam aspek preventif ini adalah pengaturan mengenai persetujuan atau *consent* yang diatur secara eksplisit dalam Pasal

20 ayat (2) huruf a. Ketentuan ini menegaskan bahwa setiap pemrosesan data pribadi wajib didasarkan pada persetujuan yang sah dari subjek data. Dalam konteks kasus penyalahgunaan data pelamar kerja, para korban menyerahkan data KTP mereka dengan tujuan spesifik untuk melamar pekerjaan, bukan untuk pengajuan pinjaman. Ketika data tersebut dialihkan fungsi dan digunakan oleh pihak ketiga untuk mencairkan dana pinjaman tanpa sepengetahuan pemiliknya, maka telah terjadi pelanggaran fundamental terhadap prinsip limitasi tujuan dan persetujuan. Konstruksi hukum ini menutup celah bagi praktik *predatory lending* yang sering kali menyembunyikan persetujuan penggunaan data dalam klausul baku yang rumit dan tidak terbaca, dengan mewajibkan persetujuan tersebut dinyatakan secara terpisah, jelas, dan sadar.

Lebih jauh dalam kerangka preventif, undang-undang ini membebaskan tanggung jawab verifikasi dan validasi data kepada pengendali data, sebagaimana diamanatkan dalam Pasal 35. Kewajiban ini memiliki implikasi yang sangat krusial bagi penyelenggara layanan teknologi finansial. Dalam banyak kasus pencurian identitas, platform pinjol sering kali meloloskan pengajuan pinjaman yang menggunakan data curian karena lemahnya sistem *Electronic Know Your Customer* atau e-KYC yang mereka terapkan. Kegagalan mendeteksi bahwa wajah pengaju pinjaman berbeda dengan foto pada KTP, atau kegagalan memverifikasi keaslian dokumen digital yang diunggah, kini tidak lagi dapat dipandang sekadar sebagai masalah teknis operasional, melainkan sebagai bentuk pelanggaran hukum atas kewajiban undang-undang. Dengan adanya pasal ini, beban pencegahan *fraud* bergeser dari masyarakat ke penyedia platform. Penyelenggara sistem elektronik wajib memastikan bahwa data yang mereka proses adalah akurat dan mutakhir, sehingga jika terjadi pencairan dana ke pihak yang tidak berhak akibat kelalaian verifikasi, penyelenggara tersebut turut memikul beban pertanggungjawaban hukum karena gagal menjalankan mandat preventif yang digariskan undang-undang.

Selain kewajiban verifikasi, aspek keamanan data juga menjadi sorotan utama dalam upaya preventif. Pasal 39 mewajibkan pengendali data untuk menerapkan langkah-langkah teknis dan operasional guna melindungi data pribadi dari gangguan pemrosesan yang tidak sah. Ketentuan ini relevan untuk menyoroti modus operandi pengumpulan data melalui lowongan kerja fiktif. Para pelaku kejahatan sering kali menggunakan formulir daring yang tidak terenkripsi atau sistem penyimpanan data yang rentan untuk menampung ribuan data pelamar kerja. Ketentuan dalam undang-undang ini memaksa setiap entitas yang mengumpulkan data masyarakat untuk memiliki standar keamanan siber yang memadai. Ketidadaan sistem keamanan yang andal bukan hanya merupakan risiko bisnis, tetapi merupakan perbuatan melawan hukum. Hal ini menciptakan standar baru di mana kepatuhan terhadap protokol keamanan siber menjadi prasyarat mutlak bagi legalitas operasional sebuah entitas bisnis yang mengelola data publik.

Ketika upaya preventif tidak mampu membendung terjadinya kejahatan, hukum menyediakan mekanisme perlindungan represif yang bertujuan untuk memulihkan hak korban dan memberikan sanksi bagi pelaku. Analisis terhadap aspek represif dalam UU PDP menunjukkan adanya peningkatan signifikan dalam bobot sanksi pidana dibandingkan regulasi sebelumnya. Pasal 67 ayat (1) mengatur ancaman pidana penjara paling lama lima tahun dan denda paling banyak lima miliar rupiah bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain. Unsur "menguntungkan diri sendiri" dalam pasal ini sangat tepat untuk menjerat pelaku yang menjual data KTP atau menggunakannya untuk mencairkan dana pinjaman. Ketentuan ini dirancang untuk memberikan efek jera atau deterrence effect yang kuat, mengingat kejahatan identitas sering kali dianggap sebagai kejahatan kerah putih dengan risiko rendah namun keuntungan tinggi.

Undang-undang ini juga secara spesifik membedakan antara tindakan memperoleh data secara ilegal dengan tindakan menggunakan data tersebut. Pasal 67 ayat (3) memberikan ancaman pidana yang sama beratnya bagi mereka yang menggunakan data pribadi yang bukan miliknya. Pembedaan ini sangat penting dalam konteks pemberantasan sindikat kejahatan siber yang terorganisir, di mana sering kali terdapat pemisahan peran antara peretas yang mencuri data (*data harvester*) dan pihak yang menggunakan data tersebut untuk penipuan (*carder* atau

fraudster). Dengan adanya pasal ini, penegak hukum memiliki landasan yang kuat untuk menjerat seluruh rantai pelaku kejahatan, mulai dari hulu hingga hilir. Hal ini menjawab tantangan penegakan hukum sebelumnya yang sering kali kesulitan membuktikan keterlibatan pihak-pihak yang "hanya" menggunakan data hasil curian tanpa terlibat langsung dalam proses pencuriannya.

Terobosan signifikan lainnya dalam aspek represif adalah pengakuan terhadap pertanggungjawaban pidana korporasi yang diatur dalam Pasal 70. Ketentuan ini memungkinkan penjatuhannya pidana tidak hanya kepada individu pelaku lapangan, tetapi juga kepada entitas perusahaan jika tindak pidana tersebut dilakukan untuk dan atas nama korporasi. Dalam ekosistem pinjol ilegal, sering kali perusahaan didirikan semata-mata untuk menampung dana hasil kejahatan atau untuk melakukan penagihan secara masif. Pasal ini memungkinkan negara untuk membubarkan korporasi semacam itu dan merampas aset-asetnya, serta menjatuhkan denda yang dilipatgandakan. Ancaman pidana korporasi ini memaksa perusahaan teknologi finansial yang legal untuk lebih berhati-hati dalam mengelola bisnisnya dan memastikan tidak ada oknum internal yang menyalahgunakan data nasabah, karena risiko hukumnya dapat berujung pada matinya entitas bisnis tersebut.

Selain sanksi pidana, perlindungan represif juga mencakup pemulihan hak perdata korban. Pasal 12 ayat (1) memberikan hak kepada subjek data untuk menggugat dan menuntut ganti rugi atas pelanggaran pemrosesan data pribadinya. Dalam kasus korban pencurian data untuk pinjaman online, kerugian yang dialami sangatlah nyata, mulai dari kerugian materiil berupa tagihan utang yang tidak pernah mereka buat, hingga kerugian imateriil berupa rusaknya reputasi keuangan dalam Sistem Layanan Informasi Keuangan dan tekanan psikologis akibat teror penagihan. Mekanisme gugatan ganti rugi ini memberikan saluran hukum bagi korban untuk mendapatkan kompensasi yang layak. Hal ini merupakan kemajuan dibandingkan mekanisme Pasal 1365 Kitab Undang-Undang Hukum Perdata yang bersifat umum, karena undang-undang ini secara spesifik mengakui pelanggaran pemrosesan data sebagai dasar tuntutan, sehingga memudahkan pembuktian unsur perbuatan melawan hukum.

Di sisi administratif, keberadaan sanksi denda administratif yang diatur dalam Pasal 57 memberikan daya paksa yang luar biasa bagi kepatuhan korporasi. Sanksi denda yang dapat mencapai dua persen dari total pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran merupakan adopsi dari standar internasional yang bertujuan mendisiplinkan perusahaan raksasa. Bagi platform pinjol, ancaman denda administratif ini jauh lebih menakutkan secara bisnis dibandingkan sanksi kurungan bagi pegawai tingkat rendah. Sanksi ini dapat dijatuhkan oleh lembaga pengawas tanpa harus melalui proses peradilan pidana yang panjang, sehingga menawarkan solusi yang lebih cepat dan responsif terhadap pelanggaran. Jika sebuah platform terbukti lalai menjaga keamanan datanya sehingga terjadi kebocoran massal, negara dapat langsung menjatuhkan sanksi denda besar yang berdampak langsung pada neraca keuangan perusahaan tersebut.

Namun demikian, implementasi dari kerangka hukum yang ideal ini dihadapkan pada tantangan struktural dan kelembagaan yang tidak ringan. Hambatan utama yang teridentifikasi dalam analisis ini adalah belum beroperasinya secara penuh lembaga otoritas perlindungan data pribadi yang independen sebagaimana diamanatkan dalam Pasal 58. Ketiadaan lembaga khusus ini pada masa transisi menciptakan kekosongan otoritas dalam penegakan sanksi administratif dan penanganan sengketa. Saat ini, fungsi pengawasan masih dijalankan oleh kementerian terkait yang memiliki keterbatasan sumber daya dan potensi konflik kepentingan karena juga berperan sebagai regulator industri digital. Ketidakjelasan mengenai siapa yang berwenang melakukan investigasi dan menjatuhkan sanksi membuat banyak kasus pelanggaran data berakhir tanpa penyelesaian yang memuaskan bagi korban. Pembentukan lembaga pengawas yang independen dan memiliki kewenangan eksekutorial yang kuat merupakan prasyarat mutlak bagi efektivitas implementasi undang-undang ini di masa depan.

Hambatan lain yang sangat dirasakan oleh korban adalah kesulitan dalam aspek pembuktian. Sistem hukum acara di Indonesia yang masih menganut prinsip "siapa yang mendalilkan, dia yang membuktikan" menempatkan korban pencurian data pada posisi yang

sangat lemah. Korban sering kali diminta untuk membuktikan bahwa mereka tidak melakukan transaksi, padahal bukti jejak digital transaksi tersebut berada dalam penguasaan penuh penyelenggara sistem elektronik. Asimetri informasi dan kekuasaan ini sering kali membuat korban enggan menempuh jalur hukum dan memilih pasrah menanggung kerugian. Oleh karena itu, diperlukan interpretasi hukum yang progresif atau peraturan turunan yang mengatur mengenai pembalikan beban pembuktian secara terbatas dalam sengketa perlindungan data pribadi. Seharusnya, pengendali data atau platform pinjol-lah yang diwajibkan membuktikan bahwa mereka telah memiliki persetujuan yang sah dan telah melakukan verifikasi sesuai standar sebelum mencairkan dana. Jika mereka gagal membuktikannya, maka transaksi tersebut harus dianggap tidak sah dan segala kerugian menjadi tanggung jawab platform.

Selain masalah teknis hukum, rendahnya literasi digital masyarakat juga menjadi faktor kriminogen yang memperparah situasi. Banyak masyarakat yang belum memahami nilai ekonomis data pribadi mereka dan dengan mudah membagikan foto KTP atau data sensitif lainnya di media sosial atau platform yang tidak terpercaya. Modus penipuan berkedok lowongan kerja yang meminta data diri lengkap sebelum proses wawancara masih sangat efektif menjerat korban karena kurangnya kewaspadaan ini. Oleh karena itu, perlindungan hukum tidak dapat hanya bergantung pada instrumen regulasi, tetapi juga memerlukan upaya edukasi publik yang masif dan berkelanjutan. Pemerintah, akademisi, dan sektor swasta perlu bersinergi untuk membangun budaya sadar privasi di tengah masyarakat, sehingga individu dapat menjadi garda terdepan dalam melindungi data pribadinya sendiri.

Analisis komprehensif ini bermuara pada kesimpulan bahwa UU PDP telah menyediakan landasan hukum yang kokoh dan modern untuk melindungi korban pencurian data pribadi dalam ekosistem pinjaman online. Kombinasi antara kewajiban preventif yang ketat, sanksi pidana yang berat, pertanggungjawaban korporasi, dan mekanisme ganti rugi perdata merupakan instrumen yang ampuh jika dijalankan dengan benar. Namun, efektivitas undang-undang ini masih terhambat oleh masalah kelembagaan dan budaya hukum. Keberhasilan perlindungan data di masa depan akan sangat bergantung pada seberapa cepat lembaga pengawas dibentuk, seberapa progresif aparat penegak hukum dalam menerapkan pasal-pasal baru ini, dan seberapa sadar masyarakat akan hak-hak digital mereka. Tanpa sinergi antara substansi hukum, struktur hukum, dan budaya hukum, aturan yang baik ini hanya akan menjadi dokumen macan kertas yang tidak mampu memberikan keadilan substantif bagi para korban kejahatan siber di Indonesia.

SIMPULAN DAN SARAN

Penelaahan yuridis terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menghasilkan kesimpulan bahwa kerangka hukum positif Indonesia telah mengalami transformasi fundamental dalam melindungi korban penyalahgunaan data pribadi pada sektor pinjaman online. Temuan penelitian ini menjawab permasalahan utama mengenai mekanisme perlindungan hak subjek data, di mana undang-undang ini tidak lagi menempatkan beban keamanan sepenuhnya pada individu pemilik data, melainkan menggeser tanggung jawab utama kepada pengendali data melalui prinsip akuntabilitas yang ketat. Secara substansial, perlindungan hukum terwujud dalam dua dimensi yang saling menguatkan, yakni dimensi preventif yang mewajibkan adanya persetujuan eksplisit dan verifikasi validitas data oleh penyelenggara jasa keuangan sebelum transaksi terjadi, serta dimensi represif yang menghadirkan ancaman sanksi pidana kumulatif, pertanggungjawaban korporasi, dan hak ganti rugi perdata yang spesifik. Hal ini mengonfirmasi bahwa penyalahgunaan identitas untuk pencairan dana pinjaman bukan hanya sekadar kelalaian administratif, melainkan pelanggaran serius terhadap hak asasi manusia yang berimplikasi pada pertanggungjawaban hukum berlapis bagi pelaku kejahatan maupun platform yang lalai dalam sistem verifikasi.

Berdasarkan implikasi hukum yang ditemukan, saran konstruktif yang dapat diajukan untuk penyempurnaan implementasi regulasi ini berfokus pada aspek kelembagaan dan hukum acara. Bagi pemerintah, urgensi pembentukan lembaga pengawas perlindungan data pribadi yang independen merupakan prioritas mutlak yang harus segera direalisasikan untuk mengisi

kekosongan otoritas penegakan sanksi administratif. Sementara itu, bagi konsep penelitian selanjutnya, disarankan agar akademisi dan peneliti hukum memfokuskan kajian pada aspek hukum acara pembuktian dalam sengketa data pribadi. Penelitian masa depan perlu mengkaji secara mendalam mengenai penerapan asas pembalikan beban pembuktian (*shifting burden of proof*) dalam kasus kejahatan siber sektor finansial, serta melakukan studi komparatif dengan negara lain mengenai efektivitas mekanisme pemulihan kerugian korban secara kolektif (*class action*) dalam insiden kebocoran data massal, guna memperkaya khazanah hukum yang adaptif terhadap perkembangan teknologi.

DAFTAR PUSTAKA

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Afiudin, U. T. A. (2022). *Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi dalam Pinjaman Online* [Universitas Sriwijaya]. <https://repository.unsri.ac.id/68202/>
- Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, 4(2), 23–31. <https://doi.org/10.52005/rechten.v4i2.98>
- Hardafi, S. N. (2025). *Ketiadaan Lembaga PDP: Celah Hukum dalam Pelindungan Data Pribadi*. Hukum Online. <https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/>
- Maleno, M., & Kusumawati, A. (2024). Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights. *Indonesia Law College Association Law Journal*, 3(2), 91–98. <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>
- Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.
- Noviansah, W. (2024). *Terungkap Modus "Pencuri" Data Pelamar Kerja Buat Pinjol hingga Rp 1,1 M*. Detik News. <https://news.detik.com/berita/d-7429484/terungkap-modus-pencuri-data-pelamar-kerja-buat-pinjol-hingga-rp-1-1-m?page=2>
- Pratama, D. E., & Apriani, R. (2023). Analisis Perlindungan Hukum Konsumen bagi Penonton Bola dalam Tragedi di Stadion Kanjuruhan. *SUPREMASI HUKUM*, 19(1), 1–15. <https://doi.org/10.33592/jsh.v19i1.2921>
- Pratama, D. E., Syafaat, M. A., & Apriani, R. (2025). Legal Lacunae in Work Accident Insurance. *Jurnal Ilmiah Wahana Pendidikan*, 11(11. A), 64–74. <http://www.jurnal.peneliti.net/index.php/JIWP/article/view/11444>
- S, G. N., Faridah, H., Masrifah, & Pratama, D. E. (2024). Tanggung Jawab Pidana terhadap Masyarakat yang Mengajak Orang Lain untuk Golput dalam Pemilu. *Krtha Bhayangkara*, 18(2), 328–342. <https://doi.org/https://doi.org/10.31599/krtha.v18i2.755>
- Sofia, R., & Putra, M. R. S. (2025). Personal Data Subject Rights Protection: A Comparative Study Between Indonesian PDP Law And the UK Data Protection Act. *JURNAL USM LAW REVIEW*, 8(2), 825–835. <https://doi.org/10.26623/julr.v8i2.12076>
- Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi dan Data Pribadi dalam Perspektif HAM. *Seminar Nasional - Kota Ramah Hak Asasi Manusia*, 1, 20–32. <https://conference.untag-sby.ac.id/index.php/semnas/article/view/168>