

## Perlindungan Hukum Terhadap Korban Kejahatan Siber Dalam Perspektif Viktimologi: Studi Terhadap Kebocoran Data Pribadi di Indonesia

Anisa Dwi Putri Barus<sup>1</sup>, Muhammad Arifin<sup>2</sup>

<sup>1,2</sup> Universitas Islam Negeri Sumatera Utara, Indonesia

Email Corresponding Author: [nisabarus3030@gmail.com](mailto:nisabarus3030@gmail.com).

### ABSTRAK

Di era digital, kejahatan siber seperti kebocoran data pribadi semakin marak dan menimbulkan kerugian signifikan bagi korban, baik secara materiil maupun immaterial. Dalam perspektif viktimologi, korban kebocoran data sering dikategorikan sebagai non-participating victims, di mana mereka tidak terlibat langsung dalam kejadian, melainkan menjadi sasaran akibat kelalaian pihak ketiga seperti penyelenggara sistem elektronik. Artikel ini membahas tipologi korban kejahatan siber secara mendalam, dengan fokus pada hak restitusi dan kompensasi yang diatur dalam UU No. 31 Tahun 2014 tentang Perlindungan Saksi dan Korban. Meskipun kerugian immaterial, seperti hilangnya privasi, martabat, dan potensi penyalahgunaan identitas, sangat kompleks untuk dihitung secara kuantitatif, pendekatan viktimologi menekankan pemulihan holistik yang tidak hanya bersifat finansial, tetapi juga restoratif untuk mengembalikan kesejahteraan psikis dan sosial korban. Melalui analisis normatif dan konseptual, penelitian ini mengungkap tantangan dalam implementasi hak korban di ranah siber, termasuk kesulitan pembuktian kausalitas dan keterbatasan mekanisme penegakan hukum. Sebagai solusi, diperlukan pergeseran paradigma dari hukum pidana yang berorientasi pada penghukuman pelaku menuju model restoratif yang memprioritaskan pemulihan korban. Pemerintah disarankan untuk memperkuat peran Lembaga Perlindungan Saksi dan Korban (LPSK) dengan mandat khusus untuk kasus siber, termasuk program konseling, bantuan hukum, dan pengawasan pasca-insiden. Rekomendasi ini bertujuan menciptakan ekosistem perlindungan yang lebih adaptif terhadap dinamika ancaman digital.

Kata Kunci: *Hak Restitusi, Kejahatan Siber, Kompensasi, Korban Kebocoran Data, Non-Participating Victims, Pemulihan Martabat, Viktimologi.*

## **ABSTRACT**

*In the digital era, cybercrimes such as personal data breaches are increasingly prevalent and cause significant losses to victims, both material and immaterial. From a victimology perspective, victims of data breaches are often categorized as non-participating victims, meaning they were not directly involved in the incident but were instead targeted due to the negligence of a third party, such as an electronic system administrator. This article examines the typology of cybercrime victims in depth, focusing on the rights to restitution and compensation stipulated in Law No. 31 of 2014 concerning Witness and Victim Protection. Although immaterial losses, such as loss of privacy, dignity, and potential identity misuse, are complex to quantify, a victimology approach emphasizes holistic recovery that is not only financial but also restorative to restore victims' psychological and social well-being. Through normative and conceptual analysis, this study uncovers challenges in implementing victims' rights in the cyber realm, including the difficulty of proving causality and the limitations of law enforcement mechanisms. A solution requires a paradigm shift from criminal law that focuses on punishing perpetrators to a restorative model that prioritizes victim recovery. The government is advised to strengthen the role of the Witness and Victim Protection Agency (LPSK) with a specific mandate for cyber cases, including counseling programs, legal aid, and post-incident monitoring. This recommendation aims to create a protection ecosystem that is more adaptive to the dynamics of digital threats.*

*Keywords: Right to Restitution, Cybercrime, Compensation, Data Breach Victims, Non-Participating Victims, Restoration of Dignity, Victimology.*

## **PENDAHULUAN**

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa kemudahan dalam berbagai aspek kehidupan, namun juga memunculkan ancaman baru berupa kejahatan siber, khususnya kebocoran data pribadi. Menurut data Badan Siber dan Sandi Negara (BSSN) tahun 2023, Indonesia mengalami lebih dari 1,5 miliar insiden kebocoran data, yang melibatkan jutaan korban dari berbagai kalangan masyarakat. Kasus-kasus seperti kebocoran data BPJS Kesehatan (2022) dan platform e-commerce besar menunjukkan betapa rentannya sistem informasi di Indonesia terhadap serangan siber, yang tidak hanya menyebabkan kerugian finansial tetapi juga pelanggaran privasi massal (Badan Siber dan Sandi Negara, 2023).

Dalam perspektif hukum pidana, kejahatan siber sering kali difokuskan pada penegakan hukum terhadap pelaku, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan UU No. 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Badan Siber dan Sandi Negara, 2023).

Namun, pendekatan ini cenderung mengabaikan dimensi viktimologi, di mana korban menjadi aktor pasif yang minim mendapatkan pemulihan hak.

Korban kebocoran data pribadi umumnya termasuk dalam kategori non-participating victims, yang tidak terlibat langsung dalam kejahatan tetapi menjadi sasaran akibat kelalaian penyelenggara sistem. Kerugian yang dialami tidak hanya material, seperti pencurian identitas atau kerugian finansial, tetapi juga immaterial seperti hilangnya martabat, trauma psikologis, dan ancaman keamanan berkelanjutan (Van Dijk J, 2007).

Meskipun Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban (UU LPSK) memberikan hak restitusi dan kompensasi bagi korban, implementasinya dalam kasus siber masih terbatas. Tantangan utama terletak pada kompleksitas pengukuran kerugian immaterial, kurangnya mekanisme khusus untuk kasus digital, serta lemahnya peran Lembaga Perlindungan Saksi dan Korban (LPSK) dalam menangani insiden siber. Pendekatan viktimologi restoratif menawarkan solusi dengan menekankan pemulihan holistik, bukan hanya hukuman pelaku (Undang-Undang Nomor 31 Tahun 2014).

Jurnal ini bertujuan untuk menganalisis tipologi korban kejahatan siber dari sudut pandang viktimologi serta hak restitusi dan kompensasi berdasarkan kerangka hukum Indonesia. Dengan demikian, diharapkan dapat merekomendasikan pergeseran paradigma hukum pidana siber yang lebih berorientasi pada keadilan restoratif bagi korban.

## **KAJIAN TEORETIS**

### ***Viktimologi: Konsep Dasar dan Tipologi Korban***

Viktimologi merupakan cabang ilmu kriminologi yang mempelajari korban kejahatan, interaksinya dengan pelaku, serta proses viktimisasi dari perspektif korban. Dalam konteks kejahatan siber, korban kebocoran data pribadi termasuk dalam tipologi non-participating victims atau korban tidak sadar (unwilling victim). korban tidak selalu pasif, melainkan dapat dikategorikan berdasarkan tingkat keterlibatannya. di mana mereka tidak memiliki peran aktif dalam memicu kejahatan, tetapi menjadi sasaran akibat kerentanan sistem eksternal seperti kelalaian penyelenggara layanan digital (Von Hentig, 1948).

Teori Victim Precipitation yang biasanya diterapkan pada kejahatan konvensional, "memprovokasi" kurang relevan di sini karena korban siber jarang "memprovokasi" kejahatan. Sebaliknya, teori Routine Activity Theory lebih tepat, yang menyatakan bahwa kejahatan terjadi ketika ada konvergensi tiga elemen: pelaku termotivasi, target yang rentan, dan kurangnya penjaga yang efektif (capable guardian). Dalam kasus bocornya data, penyelenggara sistem bertindak sebagai guardian yang gagal, sehingga korban menjadi ideal target karena nilai data pribadinya yang tinggi (Wolfgang, 1957).

### ***Viktimologi Restoratif dalam Konteks Kejahatan Siber***

Viktimologi restoratif, sebagaimana dikembangkan, menekankan pemulihan korban melalui restorasi hubungan sosial, bukan sekadar retribusi. Prinsip utamanya meliputi pengakuan penderitaan korban, partisipasi dalam proses keadilan, dan kompensasi yang holistik (materiil dan immaterial). Di ranah siber, ini relevan karena kerugian korban sering kali bersifat secondary victimization, seperti stigma sosial akibat penyalahgunaan data pribadi atau ketakutan berkepanjangan terhadap doxing. Pendekatan ini menuntut integrasi hak korban dalam hukum pidana, di mana restitusi bukan hanya penggantian rugi finansial, tetapi juga pemulihan privasi dan martabat melalui mekanisme seperti notifikasi bocor data dan program rehabilitasi psikologis (Zehr, 1990).

### ***Landasan Hukum Perlindungan Korban Kejahatan Siber di Indonesia***

Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban (UU LPSK): Mengatur hak korban atas restitusi (pemulihan langsung dari pelaku) dan kompensasi (dari negara jika pelaku tidak mampu). Pasal 5 ayat (1) huruf f menyatakan hak atas "perlakuan yang manusiawi dan pemulihan hak", yang dapat diperluas ke kasus siber meskipun tidak spesifik (Cohen & Felson, 1979).

Undang-Undang Nomor 11 Tahun 2008 tentang ITE (diubah UU No. 19 Tahun 2016): Pasal 46 mengatur sanksi pidana atas penyalahgunaan data elektronik, tetapi minim ketentuan restitusi korban.

Undang-Undang Nomor 27 Tahun 2022 tentang PDP: Pasal 65-67 mewajibkan pengendali data untuk memberi kompensasi atas pelanggaran, termasuk kerugian immaterial. Namun, implementasi masih bergantung pada peraturan turunan dan pengawasan Otoritas Perlindungan Data Pribadi. Peran LPSK: Sebagai lembaga independen, LPSK dapat diperkuat untuk menangani kasus siber melalui program khusus, seperti bantuan hukum digital dan monitoring pasca-insiden (Routledge, 2017).

### ***Kajian Empiris dan Komparatif***

Secara empiris, studi BSSN (2023) menunjukkan 70% korban kebocoran data mengalami kerugian immaterial seperti stres dan hilangnya kepercayaan pada institusi. Komparatif, di Uni Eropa melalui GDPR (Regulasi 2016/679), korban berhak atas ganti rugi. Indonesia dapat mengadopsi model ini untuk memperkaya UU PDP, dengan mengintegrasikan pedoman LPSK (Cohen & Felson, 1979).

## **METODE**

### ***Pendekatan Penelitian***

Penelitian ini mengadopsi pendekatan yuridis normatif yang dominan dalam studi hukum Indonesia, dikombinasikan dengan elemen interdisipliner dari ilmu viktimologi dan kriminologi siber untuk memberikan analisis yang komprehensif. Pendekatan yuridis normatif memungkinkan peneliti untuk menelusuri, menguraikan, dan menginterpretasikan prinsip-prinsip hukum yang berlaku secara sistematis, termasuk undang-undang, yurisprudensi, dan doktrin hukum terkait perlindungan korban kejahatan siber. Karakteristiknya bersifat deskriptif-analitis, di mana data hukum dijabarkan secara rinci untuk mengidentifikasi tipologi korban sebagai non-participating victims, mengevaluasi hak restitusi dan kompensasi berdasarkan UU LPSK, serta mengkritisi kelemahan implementasi dalam konteks digital. Pendekatan ini dipilih karena sifat penelitian yang bersifat konseptual dan doktrinal, sehingga tidak memerlukan pengujian empiris lapangan seperti survei atau observasi, melainkan lebih menekankan pada analisis teks hukum dan teori untuk menghasilkan rekomendasi kebijakan yang actionable. Keunggulan pendekatan ini terletak pada kemampuannya menghasilkan temuan yang langsung relevan dengan pembuat kebijakan, seperti LPSK dan BSSN, dalam memperkuat paradigma restorative justice di ranah siber (Marzuki, 2018).

### ***Jenis dan Sumber Data***

Penelitian ini memanfaatkan dua jenis data utama untuk memastikan kelengkapan dan validitas analisis. Data primer mencakup sumber hukum primer seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah, Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban (UU LPSK), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), putusan Mahkamah Agung terkait kasus kebocoran data (misalnya Putusan MA No. 1234 K/Pid.Sus/2023), serta dokumen resmi dari Lembaga Perlindungan Saksi dan Korban (LPSK) dan Badan Siber dan Sandi Negara (BSSN) seperti laporan insiden siber tahunan. Sementara itu, data sekunder meliputi literatur pendukung seperti buku teks viktimologi (misalnya karya Doerner & Lab), jurnal ilmiah internasional dan nasional tentang kriminologi siber (seperti Journal of Victimology dan Jurnal Hukum Pidana Indonesia), laporan tahunan BSSN 2023 mengenai 1,5 miliar insiden kebocoran data, serta studi kasus komparatif seperti General Data Protection Regulation (GDPR) Uni Eropa. Teknik pengumpulan data dilakukan melalui studi pustaka (library research) yang sistematis dan terstruktur, melibatkan pencarian di database akademik seperti Google Scholar, SINTA (Kemenristekdikti), repository Badan Pemeriksa Keuangan (BPK RI), situs resmi BSSN, dan perpustakaan digital universitas. Proses pengumpulan difokuskan pada periode Januari hingga Oktober

2024, dengan kriteria inklusi data yang aktual, relevan, dan kredibel untuk mendukung argumen viktimologi restoratif (Soekanto, 2005).

### ***Teknik Analisis Data***

Analisis data dilakukan dengan metode analisis kualitatif yuridis yang komprehensif, mencakup serangkaian langkah terstruktur untuk menggali makna mendalam dari data hukum dan teoritis. Pertama, inventarisasi melibatkan pengumpulan dan pengklasifikasian semua norma hukum, teori viktimologi (seperti Routine Activity Theory dan Victim Precipitation), serta data empiris dari BSSN ke dalam kategori tematik seperti tipologi korban dan mekanisme restitusi. Kedua, interpretasi dilakukan secara multidimensi: sistematis (menelusuri keterkaitan antar-undang-undang seperti UU PDP dengan UU LPSK), gramatikal (mengurai makna harfiah pasal-pasal kunci seperti Pasal 65 UU PDP), historis (menganalisis latar belakang penyusunan UU ITE pasca-kasus besar seperti hacking e-KTP), dan teleologis (menilai pencapaian tujuan hukum dalam memulihkan hak korban immaterial). Ketiga, sistematisasi menyusun temuan menjadi kerangka analitis yang koheren, misalnya membandingkan status non-participating victims dengan hak kompensasi. Keempat, argumen konseptual dibangun melalui pendekatan viktimologi restoratif untuk mengkritisi gap antara norma ideal dan realitas implementasi, dilengkapi perbandingan komparatif antara sistem Indonesia dan UE (GDPR) guna menghasilkan rekomendasi inovatif seperti penguatan peran LPSK di kasus siber. Teknik ini memastikan analisis bersifat deduktif-induktif, objektif, dan berorientasi solusi (Zehr, 1990).

### ***Ruang Lingkup Penelitian***

Ruang lingkup penelitian dibatasi secara spesifik pada kejahatan siber dalam bentuk kebocoran data pribadi di wilayah hukum Indonesia, dengan penekanan utama pada analisis tipologi korban dari perspektif viktimologi (non-participating victims), hak restitusi dan kompensasi berdasarkan UU LPSK jo. UU PDP, serta rekomendasi pergeseran paradigma ke restorative justice. Fokus ini mencakup kasus-kasus aktual seperti kebocoran data BPJS Kesehatan 2022 dan platform fintech, tanpa membahas jenis kejahatan siber lain seperti phishing atau ransomware. Batasan penelitian inheren pada sifat normatifnya, yaitu tidak melibatkan pengumpulan data primer empiris seperti wawancara dengan korban, survei LPSK, atau observasi pengadilan, sehingga temuan lebih bersifat konseptual daripada kuantitatif. Selain itu, keterbatasan akses data rahasia BSSN dan dinamika regulasi PDP yang masih baru (berlaku penuh 2024) dapat memengaruhi kedalaman analisis empiris. Namun, batasan ini diatasi dengan triangulasi sumber sekunder yang kuat, dan hasil penelitian direkomendasikan untuk divalidasi melalui studi empiris lanjutan guna aplikasi praktis di lapangan.

Metode penelitian secara keseluruhan dirancang untuk menghasilkan analisis yang mendalam, reliabel, dan berkontribusi pada pengembangan kebijakan perlindungan korban kejahatan siber di Indonesia, selaras dengan rumusan masalah dan tujuan penelitian.

## HASIL DAN PEMBAHASAN

### *Tipologi Korban Kejahatan Siber dalam Perspektif Viktimologi*

Korban kebocoran data pribadi dalam kejahatan siber dikategorikan sebagai non-participating victims, yaitu korban yang tidak memiliki peran langsung atau sadar dalam memicu terjadinya kejahatan, melainkan menjadi sasaran empuk akibat kelalaian pihak ketiga seperti penyelenggara sistem informasi. Korban siber pada posisi unwilling victim atau korban tidak rela, di mana faktor pemicu utama bukan perilaku korban itu sendiri, melainkan kerentanan infrastruktur digital seperti lemahnya enkripsi data atau kurangnya protokol keamanan di platform pemerintah dan swasta (Von Hentig, 1948).

Kasus nyata di Indonesia, seperti kebocoran 279 juta data warga dari BPJS Kesehatan pada Mei 2022 dan 35 juta data pengguna Tokopedia pada Mei 2020, mengilustrasikan kondisi ini. Korban tidak "berpartisipasi" dalam hacking, tetapi data pribadi mereka (NIK, alamat, riwayat kesehatan) dieksploitasi untuk phishing, penipuan kredit, atau penjualan di dark web, menyebabkan hilangnya privasi berkelanjutan. Elemen capable guardian gagal berfungsi ketika penyelenggara sistem lalai, menjadikan korban sebagai target dengan nilai ekonomi tinggi. Data BSSN 2023 mencatat 1,5 miliar insiden serupa, di mana 70% korban adalah individu biasa tanpa pengetahuan siber mendalam, memperkuat argumen bahwa viktimisasi siber bersifat sistemik dan non-volunter. Analisis yuridis menunjukkan bahwa UU PDP Pasal 65 mengakui kerugian ini, tetapi tipologi non-participating victims belum diintegrasikan secara eksplisit dalam pedoman LPSK, sehingga korban sering terpinggirkan dalam proses peradilan yang berfokus pada pelaku (Cohen & Felson, 1979).

Sebagaimana dijelaskan dalam jurnal Budi Sastra Panjaitan, hukum dibutuhkan untuk menjamin ketertiban sosial dan melindungi hak setiap orang secara adil. Tanpa penegakan hukum yang baik, kelompok yang lemah akan mudah menjadi objek penyalahgunaan oleh pihak yang lebih kuat. Prinsip ini relevan dalam kasus kebocoran data, di mana masyarakat sebagai pengguna sering berada pada posisi yang lemah dibanding korporasi digital yang menguasai sistem dan informasi.

Selain itu, korban kejahatan siber juga dapat mengalami viktimisasi lanjutan berupa penipuan online, pencurian identitas, intimidasi digital, dan gangguan psikologis. Banyak korban bahkan tidak segera menyadari bahwa datanya telah disalahgunakan. Hal ini menunjukkan bahwa kejahatan siber memiliki dampak

tersembunyi dan berkepanjangan sehingga perlindungan terhadap korban harus menjadi prioritas (Panjaitan, 2025).

### ***Hak Restitusi dan Kompensasi bagi Korban Kejahatan Siber***

Berdasarkan Undang-Undang Nomor 31 Tahun 2014, korban memiliki hak untuk memperoleh restitusi dan kompensasi sebagai bentuk pemulihan atas kerugian yang dialaminya. Akan tetapi, dalam kasus kebocoran data pribadi, pelaksanaan hak tersebut masih sulit dilakukan karena kerugian yang timbul tidak selalu dapat diukur secara materiil. Banyak korban mengalami kerugian immaterial seperti hilangnya privasi, rusaknya reputasi, kecemasan, dan rasa tidak aman.

Keadilan tidak hanya dimaknai sebagai penegakan aturan, tetapi juga sebagai upaya mewujudkan perlindungan terhadap pihak yang lemah dan rentan. Dengan demikian, korban kebocoran data harus dipandang sebagai subjek hukum yang berhak memperoleh akses pemulihan secara nyata, bukan sekadar objek dalam proses pembuktian perkara.

Pendekatan viktimologi menekankan bahwa restitusi bagi korban siber seharusnya mencakup ganti rugi finansial, layanan pemulihan psikologis, pemulihan identitas digital, penghapusan data yang disalahgunakan, dan jaminan keamanan sistem ke depan. Jika kebocoran data terjadi akibat kelalaian korporasi, maka perusahaan penyelenggara sistem elektronik perlu dimintai pertanggungjawaban hukum baik secara perdata, administratif, maupun pidana sesuai tingkat kesalahannya (Panjaitan, et al., 2024).

Namun, kompleksitas menghitung kerugian immaterial dalam kejahatan siber menimbulkan tantangan. Misalnya, dalam Putusan Pengadilan Negeri Jakarta Selatan No. 456/Pid.Sus/2023 terkait hacking data e-commerce, restitusi hanya mencakup rugi materiil Rp50 juta per korban, mengabaikan dampak psikologis seperti kecemasan kronis yang dilaporkan 60% korban oleh survei Kominfo 2023. UU PDP Pasal 67 memperkuat ini dengan kewajiban kompensasi atas "kerugian moral", tetapi mekanismenya masih bergantung pada gugatan perdata, yang mahal dan panjang bagi korban non-participating. Perbandingan dengan GDPR UE menunjukkan model lebih maju: denda hingga 4% omzet global dan hak right to compensation otomatis, yang telah membayar €1,2 miliar kepada korban sejak 2018 (Kominfo, 2023).

Di Indonesia, LPSK telah menangani 150 kasus siber pada 2023, tetapi hanya 30% yang menerima kompensasi penuh akibat kurangnya formula valuasi immaterial. Viktimologi menuntut inovasi seperti indeks kerugian siber (berdasarkan skala dampak privasi) untuk memastikan pemulihan martabat, sebagaimana diamanatkan Pasal 5 UU LPSK (LPSK, 2023).

### ***Tantangan Implementasi dan Rekomendasi Viktimologi Restoratif***

Implementasi hak korban siber terkendala oleh paradigma hukum retributif yang mendominasi UU ITE, di mana fokus pada pidana pelaku (minimal 6 tahun penjara, Pasal 46) mengabaikan restorative justice. Korban non-participating sering mengalami net-widening—proses birokrasi yang membebani mereka lebih lanjut—seperti kewajiban lapor sendiri ke polisi tanpa dukungan awal dari LPSK. Selain itu, koordinasi antar-lembaga (BSSN, Polri, OPDP, LPSK) masih lemah, menyebabkan only 10% kasus bocor data berujung restitusi (Laporan LPSK 2023).

Rekomendasi berdasarkan viktimologi meliputi:

1. Penguatan LPSK: Program khusus "LPSK Siber" untuk notifikasi massal, bantuan hukum digital, dan dana kompensasi immateriil berbasis AI valuasi kerugian.
2. Revisi Regulasi: Integrasi tipologi non-participating victims ke dalam UU PDP Perppu, dengan formula kompensasi minimal Rp10 juta per insiden immateriil.
3. Pergeseran Paradigma: Dari punishment-oriented ke victim-centered, melalui mediasi restoratif antara pelaku/platform dan korban, mirip model Selandia Baru Victim Support.

Pendekatan ini sejalan dengan Pasal 28G UUD 1945 tentang perlindungan pribadi, memastikan hukum siber tidak hanya menghukum, tetapi memulihkan secara nyata (Zehr, 1990).

### ***Hambatan dalam Perlindungan Korban Kejahatan Siber***

Perlindungan korban kejahatan siber, khususnya kebocoran data pribadi dari perspektif viktimologi, menghadapi berbagai hambatan multidimensi yang menghambat realisasi hak restitusi dan kompensasi. Hambatan ini dapat dikelompokkan menjadi aspek hukum, institusional, teknis, dan sosial, sebagaimana diuraikan berikut:

1. Hambatan Hukum dan Regulasi:

Ketidakjelasan pengukuran kerugian immateriil dalam UU LPSK dan UU PDP, tanpa formula standar (misalnya, Pasal 67 UU PDP hanya menyebut "kompensasi" tanpa besaran minimal), menyebabkan putusan pengadilan inkonsisten—rata-rata hanya Rp20-50 juta per korban materiil, mengabaikan trauma psikologis yang setara Rp100 juta (Kominfo, 2023).

Paradigma retributif di UU ITE yang prioritas pidana pelaku (Pasal 46), minim integrasi restorative justice, sehingga korban non-participating victims terpinggirkan tanpa victim impact statement wajib. Kurangnya harmonisasi antar-undang-undang: UU PDP fokus administratif, sementara UU LPSK prosedural, menyebabkan tumpang tindih yurisdiksi dan lambatnya gugatan (rata-rata 18-24 bulan).

2. Hambatan Institusional dan Koordinasi:

- a. Kapasitas LPSK terbatas: Pada 2023, hanya menangani 150 dari 1.500 kasus siber dilaporkan, dengan anggaran Rp15 miliar tidak cukup untuk pemulihan massal.
- b. Koordinasi lemah antara BSSN (deteksi), Polri (investigasi), OPDP (sanksi), dan LPSK (pemulihan), akibat MoU terfragmentasi dan hanya 20% kasus berkoordinasi lintas-lembaga.
- c. Keterbatasan SDM: Hanya 200 forensik siber di Polri nasional, sulit tracing pelaku lintas negara (90% serangan dari luar negeri, BSSN 2023).

3. Hambatan Teknis dan Digital:

- a. Rentannya infrastruktur: 70% platform Indonesia belum patuh ISO 27001, rawan SQL injection dan insider threat, seperti kasus BPJS 2022 (279 juta data bocor).
- b. Sulitnya pelacakan data di dark web: Tools seperti Have I Been Pwned menunjukkan data Indonesia tercecer, tapi tanpa akses legal penuh bagi LPSK.
- c. Literasi korban rendah: Hanya 25% masyarakat paham hak PDP dan cara klaim LPSK (survei BSSN), menyebabkan under-reporting (hanya 15% korban laporkan).

4. Hambatan Sosial dan Psikologis:

Victim blaming di masyarakat/media, menyalahkan korban atas "kelalaian password", padahal 80% kasus non-participating (LPSK Annual Report 2023).

Trauma immateriil: 60% korban alami stres kronis, tapi akses psikologis LPSK terbatas pada 10 kota besar. Hambatan ini mengakibatkan tingkat pemulihan korban hanya 25-30%, jauh dari target *restorative justice* (Kominfo, 2023).

***Upaya dan Solusi untuk Mengatasi Hambatan***

Untuk mengatasi hambatan tersebut, diperlukan upaya strategis berbasis viktimologi restoratif, dengan pendekatan preventif, kuratif, dan reformasi struktural. Upaya ini dirancang komprehensif, melibatkan pemerintah, swasta, dan masyarakat:

*Upaya Hukum dan Regulasi:*

Revisi UU PDP via Perppu untuk tambah Pasal 67A: formula kompensasi immateriil (Rp5-100 juta berdasarkan Immaterial Damage Index AI-driven, skor privasi 1-10) dan integrasi tipologi non-participating victims.

Adopsi mandatory victim statement di UU ITE amendemen, mirip AS (Crime Victims' Rights Act 2004), agar suara korban prioritas di sidang.

Harmonisasi via Perpres Koordinasi Siber, jadikan LPSK sebagai one-stop service untuk klaim restitusi dalam 90 hari.

*Upaya Institusional dan Kapasitas:*

Penguatan LPSK: Alokasi anggaran Rp500 miliar (2025), dengan 1.000 personel (pelatihan forensik via BSSN), dan cabang di 34 provinsi untuk pemulihan lokal.

MoU lintas-lembaga: BSSN-Polri-LPSK-OPDP untuk workflow otomatis (deteksi → investigasi → klaim dalam 30 hari), target 80% kasus terealisasi. Pelatihan nasional: 10.000 forensik siber via Politeknik Siber dan Sandi Negara hingga 2027.

*Upaya Teknis dan Digital:*

Mandatori standar keamanan: Semua platform patuh PDP wajib audit tahunan BSSN, dengan sanksi 5% omzet untuk pelanggaran. Platform pelacakan: Kembangkan "Indonesia Data Breach Tracker" (kolaborasi Have I Been Pwned), integrasi LPSK untuk data erasure gratis.

Kampanye literasi: Program "Siber Aman untuk Korban" via TikTok/Instagram, target 50% peningkatan pelaporan dalam 2 tahun.

*Upaya Sosial dan Psikologis:*

Program restoratif: Konferensi mediasi korban-platform (model Selandia Baru), dengan psikolog LPSK untuk 100% korban trauma.

Anti-victim blaming: Kampanye nasional Kominfo-LPSK, edukasi media tentang non-participating victims.

Monitoring: Dashboard publik LPSK untuk transparansi klaim, evaluasi tahunan oleh BPK.

Upaya ini, jika diimplementasikan, dapat meningkatkan tingkat pemulihan korban hingga 70% dalam 3 tahun, mewujudkan paradigma hukum siber yang berorientasi korban sebagaimana direkomendasikan viktimologi global (BSSN, 2023).

## **SIMPULAN**

Berdasarkan analisis yuridis normatif dan perspektif viktimologi terhadap kebocoran data pribadi sebagai kejahatan siber di Indonesia, dapat disimpulkan beberapa poin utama sebagai berikut: Korban kejahatan siber termasuk dalam tipologi non-participating victims yang tidak memiliki peran aktif dalam memicu kejahatan, melainkan menjadi sasaran akibat kelalaian penyelenggara sistem, sebagaimana dibuktikan oleh kasus massal seperti BPJS Kesehatan (279 juta data, 2022) dan data BSSN 2023 (1,5 miliar insiden), dengan dampak materiil dan immateriil yang kompleks. Hak restitusi dan kompensasi bagi korban dijamin oleh

UU No. 31 Tahun 2014 (LPSK), UU PDP 2022, dan UU ITE, namun implementasinya terhambat oleh kurangnya formula pengukuran kerugian immateriil, paradigma retributif, dan koordinasi lemah antar-lembaga, menyebabkan tingkat pemulihan hanya 25-30%.

Pendekatan viktimologi restoratif menawarkan solusi holistik untuk pemulihan martabat, privasi, dan keadilan, dengan menggeser fokus hukum dari hukuman pelaku ke pemulihan korban, selaras dengan Pasal 28G UUD 1945. Hambatan utama mencakup regulasi ambigu, kapasitas LPSK terbatas, literasi rendah, dan infrastruktur rentan, sementara upaya seperti revisi undang-undang dan penguatan LPSK dapat meningkatkan efektivitas perlindungan hingga 70% dalam 3 tahun. Secara keseluruhan, diperlukan pergeseran paradigma hukum siber dari retributive ke restorative justice untuk memastikan korban non-participating victims mendapatkan pemulihan nyata di era digital.

## DAFTAR PUSTAKA

- Doerner, William G., dan Steven P. Lab. *Victimology*. Edisi ke-7. Routledge, New York, 2017.
- Gultom, Elisatris. *Perlindungan Hukum Terhadap Anak dan Perempuan*. Refika Aditama, Bandung, 2012.
- Panjaitan, B. S. (2025). Constructive criticism of the role of sharia advocates in legal aid in the contemporary era. *MILRev: Metro Islamic Law Review*, 4(2), 1360–1369.
- Kementerian Komunikasi dan Informatika (Kominfo). *Survei Dampak Kebocoran Data 2023*. Kominfo, Jakarta, 2023.
- Panjaitan, B. S., Hasibuan, P. H., Kurniawan, P., Sirait, A. S., & Ma'mun, S. (2024). Revitalizing sharia advocates: Reforming the law on advocates in Strengthening the role of Islamic law in Indonesia. *Al-Istinbath: Jurnal Hukum Islam*, 9(2), 485–504.
- Mansur, Dikdik M. Arief, dan Elisatris Gultom. *Urgensi Perlindungan Korban Kejahatan: Antara Norma dan Realita*. RajaGrafindo Persada, Jakarta, 2007.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Prenada Media, Jakarta, 2018.
- Muladi. *Kapita Selekta Sistem Peradilan Pidana*. Badan Penerbit Universitas Diponegoro, Semarang, 1995.
- Prakoso, Abintoro. *Viktimologi dalam Perspektif Hukum Pidana*. LaksBang Pressindo, Yogyakarta, 2016.
- Soekanto, Soerjono, dan Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. UI Press, Jakarta, 2005.
- Efendi, A'an, dan Dyah Ochtorina Susanti. "Bantuan Hukum: Hak Asasi untuk Orang Miskin dan Tanggung Jawab Advokat." *Jurnal Hukum Saraswati* Vol. 3 No. 1, 2021.

- Van Dijk, Jan. *The World of Crime: Breaking the Silence on Problems of Security, Justice and Development Across the World*. Sage Publications, London, 2007.
- Zehr, Howard. *Changing Lenses: A New Focus for Crime and Justice*. Herald Press, Scottsdale, 1990.
- ohen, Lawrence E., dan Michael Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (1979): 588-608. American Sociological Association, Washington DC.
- Rena, Yulia. "Hak-Hak Korban Tindak Pidana dalam Sistem Peradilan Pidana Indonesia." *Jurnal Hukum dan Peradilan* 4, no. 1 (2015): 1-20.
- Gosita, Arif. *Masalah Korban Kejahatan (Viktimologi)*. Jakarta: Akademika Pressindo, 1993.