Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.3813

Kebijakan Perlindungan Saksi Dan Korban Di Era Digital Terhadap Tantangan Administratif Dan Hukum

Khaiyyil Faizunan Nurun Nafi[1], Siti Nurhayati[2]
UIN Syekh Wasil Kediri, Indonesia[1-2]
Email Korespondensi: khaiyyil2001@gmail.com, sitinurhayati@uinkediri.ac.id

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 28 Maret 2026

ABSTRACT
Digital transformation has given rise to new cybercrimes, such as doxing (the unauthorized dissemination of personal data). Despite its prevalence, doxing is not yet explicitly regulated as a distinct offense under the ITE Law or the Personal Data Protection (PDP) Law, resulting in inadequate protection for victims. This research, employing a normative legal method and a statutory approach, aims to analyze the forms of legal protection (based on the ITE Law, the Criminal Code, and the Witness and Victim Protection Law), the mechanism of the LPSK in handling digital threats, and the administrative and legal challenges faced by this independent institution. The findings reveal that while LPSK provides protection through four stages (Application, Administrative Review, Plenary Meeting, and Implementation of Assistance), the mechanism is hindered by legal challenges, specifically a regulatory vacuum regarding doxing and weak restitution implementation due to LPSK's lack of executorial authority. Additionally, administrative hurdles such as limited digital forensic human resources and cross-border jurisdictional barriers persist. This study concludes that protection must be strengthened through victim-oriented criminal law reform, the harmonization of the ITE and PDP Laws, the establishment of specific sanctions for doxing, and the enhancement of human resource capacity and international cooperation to address the complexities of cybercrime.
Keywords: *LPSK, Digital Era, ITE Law.*

ABSTRAK
Transformasi digital telah memunculkan kejahatan siber baru seperti doxing (penyebaran data pribadi tanpa izin) yang marak terjadi, namun belum diatur secara eksplisit sebagai delik tersendiri dalam UU ITE maupun UU Perlindungan Data Pribadi (PDP), sehingga perlindungan bagi korban belum memadai. Penelitian ini, yang menggunakan metode normatif yuridis dan pendekatan perundang-undangan, yang bertujuan menganalisis bentuk perlindungan hukum (berdasarkan UU ITE, KUHP, dan UU PSK), mekanisme LPSK dalam menangani ancaman digital, serta tantangan administratif dan hukum yang dihadapi lembaga independen ini. Ditemukan bahwa LPSK menjalankan perlindungan melalui empat tahap (Permohonan, Administratif, Rapat Paripurna, dan Pelaksanaan Bantuan), namun mekanisme tersebut terhambat oleh tantangan hukum berupa kekosongan regulasi spesifik untuk doxing dan kelemahan implementasi restitusi karena LPSK tidak memiliki kewenangan eksekutorial, ditambah tantangan administratif seperti keterbatasan SDM forensik dan hambatan yurisdiksi lintas batas. Sebagai solusi, disimpulkan bahwa perlindungan harus ditingkatkan melalui reformasi regulasi yang berorientasi pada korban (victim-oriented criminal law), harmonisasi UU ITE dan UU PDP, penetapan sanksi doxing yang spesifik,

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

serta peningkatan kapasitas SDM dan kerja sama internasional untuk mengatasi kompleksitas kejahatan siber.
Kata Kunci: *LPSK, Era Digital, UU ITE*

PENDAHULUAN

Transformasi digital telah mempercepat interaksi sosial melalui teknologi informasi, namun juga melahirkan kejahatan baru seperti doxing—pengungkapan dan penyebaran data pribadi tanpa izin, yang dapat menyebabkan dampak psikologis, sosial, dan fisik pada korban. Di Indonesia, praktik ini semakin marak, didorong oleh motif ekonomi, politik, atau pembalasan pribadi, seperti tercatat dalam laporan OJK dengan lebih dari 15.000 kasus pelanggaran data pribadi oleh penyedia pinjaman online antara Januari 2024 hingga Maret 2025. Meskipun UU Informasi dan Transaksi Elektronik (ITE) serta UU Perlindungan Data Pribadi (PDP) ada, keduanya belum secara eksplisit mengatur doxing sebagai delik tersendiri, sehingga perlindungan hukum bagi korban kurang memadai. (Rahmayanti, 2025)

Berdasarkan Undang-Undang Perlindungan Saksi dan Korban (UU PSK), LPSK berkedudukan di ibu kota negara dan tidak ditempatkan di bawah instansi pemerintah mana pun, termasuk kepolisian, kejaksaan, atau Komnas HAM. Pendanaannya sepenuhnya dari anggaran negara, mirip dengan lembaga independen lain seperti Komnas KPK,HAM, dan PPATK.(Sofyan Rauf, 2022)

Perlindungan saksi dan korban merupakan aspek krusial dalam penegakan hukum untuk memberikan jaminan dasar untuk mereka. Pencegahan serta penanganan isu ini menjadi tanggung jawab bersama pemerintah, pemerintah daerah, masyarakat, dan keluarga. Oleh sebab itu, diperlukan kerjasama antarpihak yang erat guna menciptakan solusi yang tepat dan cepat. (Siti Nurhayati, 2015)

Independensi LPSK tercermin dari beberapa aspek, seperti pemberhentian anggota hanya berdasarkan undang-undang (bukan keputusan sepihak presiden), kepemimpinan kolektif tanpa dominasi partai politik, dan masa jabatan yang bergantian (staggered terms). Pemilihan model ini didasari dua pertimbangan utama yakni: untuk menciptakan lembaga khusus yang fokus pada perlindungan saksi dan korban tanpa bergantung pada institusi existing dan agar tidak membebani lembaga lain yang sudah memiliki tanggung jawab besar.

Dengan ini permasalahan ini dapat dirumuskan permasalahan sebagai berikut: Bagaimana bentuk Perlindungan Hukum bagi saksi dan Korban Di Era Digital Menurut UU ITE, KUHP dan UU Perlindungan Saksi dan Korban, bagaimana mekanisme Perlindungan oleh LPSK dalam menangani ancaman digital, serta apa saja Tantangan administratif dan hukum yang dihadapi LPSK, serta bagaimana Solusi peningkatannya.

METODE

Penelitian ini bersifat normatif yuridis, yang berfokus pada analisis norma hukum terkait kebijakan perlindungan saksi dan korban di era digital. Pendekatan Perundang-undangan (Statute Approach) adalah metode penelitian hukum yang berfokus pada penelaahan dan pengkajian secara menyeluruh terhadap semua peraturan perundang-undangan dan regulasi yang berkaitan erat dengan isu atau

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

permasalahan hukum yang sedang ditelit (Muhaimin). Peneliti akan mengkaji undang-undang terkait UU 31/2014, UU ITE 19/2016, serta KUHP. Penelitian ini juga menggunakan pendekatan conceptual approach yakni metode yang menelaah perlindungan korban serta administrasi digital.

HASIL DAN PEMBAHASAN

Kebijakan Perlindungan Saksi Dan Korban Di Era Digital

Indonesia sebagai negara hukum memiliki Konstitusi UUD 1945 sebagai landasan utama yang mengatur sistem pemerintahan, bermasyarakat, berbangsa, dan bernegara, di mana hukum ditandai oleh norma-norma berisi perintah dan larangan.(Alinda Julietha Adnan, 2024) Perkembangan zaman yang pesat, didorong oleh globalisasi dan kemajuan teknologi informasi, telah menciptakan kehidupan modern yang menghilangkan batas wilayah dan waktu, sehingga memengaruhi perubahan gaya hidup, budaya, ekonomi, keamanan, dan sistem penegakan hukum di Indonesia.

Meskipun teknologi informasi memberikan kemudahan akses dan berbagi informasi, pemanfaatan yang tidak sesuai bisa menimbulkan dampak buruk, salah satunya adalah kejahatan cyberbullying. Cyberbullying diartikan sebagai perbuatan perundungan atau intimidasi yang dilakukan secara sengaja dan berulang-ulang melalui media elektronik seperti: handphone, komputer, dan media sosial seperti Twitter, Instagram, TikTok, dll. Tindakan intimidasi di dunia maya ini bisa berupa ejekan, ancaman, hinaan, atau hacking, yang dipengaruhi oleh pengabaian norma dan sering didasari dengan diskriminasi ras, agama, gender, dll.

Korban dan pelaku mayoritas cyberbullying adalah anak berusia di bawah 18 tahun. Bagi yang berusia di atas 18 tahun, pelanggaran ini dianggap cyberstalking atau cyberharassment. Kurangnya kesadaran anak-anak dan remaja sering menyebabkan mereka tidak mengetahui bahwa yang dianggap lelucon adalah tindakan penindasan.

Cyberbullying telah menjadi fenomena global yang memerlukan penanggulangan segera karena dampaknya bagi anak-anak. Korban cenderung tidak melaporkan, orang tua sering tidak tahu, dan identitas pelaku sulit dilacak karena tidak adanya pertemuan langsung. Penegakan hukum terhadap cyberbullying dipengaruhi oleh pemahaman terhadap peraturan. Meskipun dapat dijerat Pasal 310 KUHP tentang pencemaran nama baik, ketentuan yang lebih terperinci diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE Pasal 27 ayat 3 dan 4, mengenai muatan penghinaan, pencemaran namba baik, pemerasan, dan pengancaman.

Komparasi Perlindungan Data Pribadi: UU ITE 2024 dan UU PDP 2022(Ghufron Rosadi Hidayah, 2024)

Kategori	**UU ITE 2024 (UU Informasi & Transaksi Elektronik)**	**UU PDP 2022 (UU Perlindungan Data Pribadi)**

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

Sifat Regulasi	Umum dan luas, berfokus pada transaksi elektronik, cybercrime, dan media sosial.	Khusus (Lex Specialis), sistematis, dan komprehensif.
Substansi PDP	Terbatas (Pasal 26): Hanya mengatur penggunaan informasi pribadi harus dengan persetujuan. Tidak rinci tentang prinsip, hak subjek data, atau sanksi administratif.	Komprehensif, Mengadopsi prinsip internasional (seperti GDPR) seperti legitimasi, transparansi, pembatasan tujuan, dan akuntabilitas. Mengatur hak subjek data (akses, hapus, tolak pemrosesan) dan kewajiban Pengendali Data.
Cakupan Perlindungan	Perlindungan data pribadi hanya bagian kecil dari pengaturan umum. Rawan multi-interpretasi oleh penegak hukum.	Berlaku untuk seluruh pihak yang memproses data pribadi di wilayah Indonesia dan entitas internasional yang memproses data subjek Indonesia. Menjadi payung hukum utama.
Peran Kelembagaan	terbatas pada pengawasan umum melalui kominfo, tidak ada otoritas khusus full time untuk PDP, menyebabkan pengawasan tidak maksimal,	Memandatkan pembentukan Otoritas Pengawas Perlindungan Data Pribadi khusus (Data Protection Authority) dengan kewenangan sanksi administratif investigasi.

Tantangan administratif dan hukum

Untuk mengatasi tantangan administratif dan hukum, diperlukan reformulasi regulasi yang berorientasi pada korban (victim-oriented criminal law),

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

mengintegrasikan UU ITE dan UU PDP melalui peraturan teknis seperti Peraturan Pemerintah. Usulan utama meliputi:(Rahmayanti, 2025)

a. Definisi eksplisit doxing sebagai "tindakan mengungkap, menyebarluaskan, atau membocorkan data pribadi tanpa izin dengan tujuan merugikan, mengintimidasi, atau mempermalukan korban".
b. Pasal khusus seperti Pasal 27C UU ITE dengan unsur pidana jelas (penyebaran tanpa izin, niat merugikan, dampak pada korban).
c. Sanksi spesifik minimal 2 tahun dan maksimal 7 tahun penjara serta denda Rp500 juta-Rp2 miliar, berdasarkan proporsionalitas kerugian.
d. Mekanisme perlindungan korban, termasuk hak atas informasi, perlindungan identitas, pendampingan hukum, dan rehabilitasi psikis.
e. Harmonisasi dengan prinsip HAM untuk memastikan yurisdiksi lintas batas dan penegakan hukum yang efektif.

Reformasi ini bertujuan menjadikan hukum pidana siber lebih responsif, adaptif, dan berpihak pada keadilan substantif, tanpa mengorbankan kebebasan berekspresi.

Tantangan administratif meliputi ketersediaan teknologi pendeteksi yang memadai, sementara tantangan hukum mencakup keseimbangan antara pembatasan akses dengan hak anak atas informasi dan kebebasan berekspresi.(Hardianto Djanggih, 2018) Serta tantangan administratif juga mencakup metode serangan siber yang canggih, kekurangan tenaga terlatih, dan kesadaran masyarakat yang rendah, yang mempersulit saksi/korban melaporkan kejahatan atau melindungi diri. Tantangan hukum melibatkan regulasi yang tidak mengikuti perkembangan teknologi, serta kerjasama antarlembaga penegak hukum yang belum optimal.(Rahma Agri Firdaus, 2024)

Selain doxing, perluasan definisi ancaman di era digital juga harus mencakup Non-Consensual Dissemination of Intimate Images (NCII). NCII merupakan alat marginalisasi yang efektif untuk membungkam saksi melalui stigma sosial dan ancaman kriminalisasi balik akibat norma hukum yang masih multitafsir. Berdasarkan studi mengenai Kekerasan Berbasis Gender Online (KBGO), ancaman digital terhadap saksi atau korban sering kali mewujud dalam bentuk Non-Consensual Dissemination of Intimate Images (NCII). NCII bukan sekadar pelanggaran privasi, melainkan instrumen intimidasi sistematis yang digunakan pelaku untuk membungkam suara korban melalui mekanisme marginalisasi. Ada tiga faktor utama mengapa NCII menjadi ancaman digital yang sangat melumpuhkan bagi saksi/korban:(Daffa Naufal Ramadhan, 2025)

a. Dominasi Patriarki dan Objektifikasi: NCII lahir dari budaya yang menempatkan tubuh perempuan sebagai objek kontrol. Pelaku menggunakan konten intim sebagai senjata (weaponization) untuk menekan korban agar mengikuti keinginan pelaku atau menarik kesaksiannya dalam proses hukum.
b. Stigmatisasi dan Victim Blaming: Ancaman digital berupa NCII sering kali berujung pada penghakiman sosial. Masyarakat cenderung melakukan victim blaming (menyalahkan korban) dengan mempertanyakan moralitas

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

atau perilaku korban di masa lalu, yang pada akhirnya membuat saksi/korban merasa terisolasi dan enggan melanjutkan proses hukum.

c. Ancaman Kriminalisasi Balik: Terdapat celah dalam perangkat hukum (seperti UU ITE atau UU Pornografi) di mana korban NCII justru berisiko dikategorikan sebagai pihak yang "turut menyebarkan" atau memproduksi konten asusila. Kekaburan norma ini sering digunakan pelaku untuk mengancam balik korban secara hukum (revictimization).

Tantangan administratif dalam melindungi saksi di era digital semakin kompleks akibat fenomena viralitas yang menciptakan jejak digital permanen (digital eternity). Program perlindungan identitas tradisional, seperti pemberian identitas baru secara fisik, menjadi tidak efektif apabila data pribadi saksi telah tersebar luas di media sosial.(Karunia Fitri Rahmadani, 2023) Oleh karena itu, diperlukan rekonstruksi hukum yang mengoptimalkan hak untuk dilupakan (right to be forgotten) sebagaimana diatur dalam Pasal 26 UU ITE. Hal ini menekankan bahwa LPSK harus mampu memfasilitasi permohonan penetapan pengadilan untuk melakukan 'pembersihan digital' (digital scrubbing) dan penghapusan hasil mesin pencari (delisting). Langkah ini krusial agar saksi dapat terbebas dari intimidasi berkelanjutan yang berbasis pada data masa lalu yang sudah tidak relevan namun masih dapat diakses publik secara bebas.

Implementasi perlindungan saksi dan korban di ruang siber memerlukan pola sinergi yang terintegrasi antara mandat yuridis LPSK dengan infrastruktur keamanan digital nasional.(Muhammad Aabid Tyas Dzaky, 2025) Efektivitas UU ITE dalam menangani kejahatan siber sering kali terhambat oleh lemahnya koordinasi antarinstansi dan kebijakan preventif yang belum sepenuhnya terintegrasi. Dalam konteks perlindungan saksi, LPSK tidak dapat bekerja secara parsial, diperlukan kolaborasi teknis dengan Kominfo untuk percepatan pemutusan akses konten ancaman serta dukungan BSSN dalam mengamankan sistem data perlindungan saksi dari risiko peretasan atau kebocoran data. Sinergi ini harus diwujudkan melalui sistem koordinasi terpadu yang memanfaatkan teknologi Artificial Intelligence (AI) dan Big Data Analytics guna mendeteksi ancaman secara dini. Dengan demikian, respons terhadap intimidasi siber tidak lagi bersifat birokratis-reaktif, melainkan menjadi sistem perlindungan yang proaktif dan adaptif terhadap perkembangan modus kriminalitas siber yang semakin kompleks.

Perlindungan Korban

Dalam penganannya pemerintah menggunakan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar utama untuk menangani kasus ini.(Rido Roniasi Hutasoit, 2024) Karena teknologi sudah berkembang pesat, kasus cybercrime atau dikenal dengan istilah cyber bullying yakni, membully orang melalui media sosial dengan membagikan konten yang menyinggung, menghina, atau menyebabkan kerugian menjadi lebih sering terjadi.

UU ITE membahas berbagai aspek, tapi yang paling relevan untuk cyber bullying ada di Pasal 29. Di pasal itu, dijelaskan bahwa siapa saja yang sengaja menyebarkan konten penghinaan, pencemaran nama baik, hoax yang bisa

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

menimbulkan kerugian, ajakan kebencian (khususnya berdasarkan SARA), atau ancaman kekerasan melalui media elektronik, bisa dikenakan hukuman. Sanksi yang diberikan bisa berupa penjara hingga 6 tahun atau denda hingga Rp1 miliar, tergantung seberapa besar dampaknya.

Dari segi mekanisme, hukum ini melibatkan polisi, jaksa, dan pengadilan dalam proses penegakannya. Namun, penerapannya bisa berbeda-beda sesuai kasus, jadi sebaiknya konsultasi dulu dengan ahli hukum agar tidak salah langkah. UU ITE juga mengatur hal-hal lain seperti keamanan data atau transaksi online, tapi untuk cyber bullying, fokus utamanya adalah aturan untuk mencegah dan menghukum pelaku. Untuk hukum di Indonesia sudah mempunyai tools yang bagus untuk melindungi korban cyber bullying melalui UU ITE, asal diterapkan dengan benar agar lebih efektif.

Di era digital, kebijakan perlindungan saksi dan korban di Indonesia, sebagaimana diatur dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (sebagaimana diubah dengan UU No. 31/2014), menghadapi tantangan administratif dan hukum yang semakin kompleks akibat kemajuan teknologi. LPSK sebagai lembaga utama bertanggung jawab memberikan perlindungan fisik, psikis, hukum, dan ekonomi, termasuk kompensasi serta restitusi.(Zulkifli Ismail, 2023) Kemajuan teknologi digital terutama internet membawa peluang sekaligus tantangan bagi perlindungan saksi dan korban oleh Lembaga Perlindungan Saksi dan Korban (LPSK). Di satu sisi, aksesibilitas digital memudahkan masyarakat mengajukan permohonan melalui aplikasi, web, platform online, serta memungkinkan monitoring keselamatan secara real time, seperti penggunaan kamera pengawasan jarak jauh untuk mendeteksi ancaman.

UU ITE (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016) menjadi fondasi utama pengaturan kejahatan digital di Indonesia. Undang-undang ini melarang dan memberi sanksi bagi tindakan seperti pencemaran nama baik (Pasal 27 ayat 3), penyebaran konten asusila (Pasal 27 ayat 1), penghinaan, ancaman, penipuan, serta akses ilegal ke sistem elektronik (Pasal 30–32). Bagi korban, UU ITE mengakui bukti elektronik dan mempermudah pelaporan serta proses hukum modern. Namun, fokus utamanya adalah penindakan pelaku, bukan pemulihan korban seperti restitusi atau rehabilitasi.(Andika Rafa Hendrawan, 2025)

Lembaga Perlindungan Saksi dan Korban (LPSK) memiliki peran penting dalam menjamin hak korban kekerasan seksual atas restitusi (ganti kerugian), yaitu mengajukan permohonan dan membantu menghitung nilai kerugian yang wajib dibayar pelaku (sesuai UU PSK dan UU TPKS).

Namun, dalam praktiknya peran LPSK menghadapi hambatan serius yang menyebabkan restitusi tidak terealisasi:(Dea Prida Oktavia, 2025)

a) Ketiadaan Kewenangan Eksekutorial: LPSK tidak memiliki kewenangan untuk mengeksekusi putusan restitusi atau melakukan pelelangan aset pelaku. Kewenangan eksekusi tetap berada pada Jaksa.
b) Lemahnya Koordinasi: Terjadi koordinasi yang lemah antara LPSK, Jaksa Penuntut Umum (JPU), dan pengadilan. Dalam studi kasus, tidak ditemukan bukti LPSK mengajukan permohonan restitusi secara formal atau JPU

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

mencantumkannya dalam tuntutan, padahal UU TPKS mewajibkan kolaborasi.

c) Ketiadaan Mekanisme Jelas: Meskipun LPSK diatur dapat membayar restitusi terlebih dahulu jika pelaku tidak mampu (melalui PP No. 43/2017), negara belum hadir sebagai penjamin terakhir, dan amar putusan sering tidak mencantumkan klausul substitusi ini. Hal ini menyebabkan restitusi macet, apalagi jika pelaku divonis mati, yang secara hukum menghapuskan kewajiban perdatanya.

Oleh karena itu, LPSK terbatasi oleh kewenangan yang tidak mencakup eksekusi, dan implementasi restitusi menjadi mandek akibat kekosongan regulasi teknis serta kurangnya sinergi antarlembaga penegak hukum.

Proses bantuan dari Lembaga Perlindungan Saksi dan Korban (LPSK) bertujuan membangun kerjasama dan kepercayaan antara LPSK dengan saksi atau korban.(Djamaludin, 2024) Permohonan harus diajukan secara sukarela dan sadar, sebagai kebutuhan mendesak, bukan sekadar laporan. Proses ini terdiri dari empat tahapan utama, yakni:

a. Permohonan

Saksi atau korban mengajukan secara tertulis ke Ketua LPSK, baik secara proaktif maupun atas permintaan pejabat berwenang. Pengajuan bisa dilakukan langsung ke kantor LPSK, melalui email, pos, atau form online di situs web resmi. LPSK menangani dengan cermat untuk memastikan keseriusan pemohon.

b. Administratif

Dokumen diserahkan ke Unit Penerimaan Permohonan (UPP) LPSK untuk verifikasi kelengkapan berkas. UPP memeriksa secara teliti agar semua persyaratan terpenuhi, sesuai prosedur UU Perlindungan Saksi dan Korban (UU PSK), sebagai bentuk komitmen profesional.

c. Rapat Paripurna Anggota (RPP)

Berkas dirangkum dan diserahkan ke anggota LPSK (termasuk Ketua, Wakil Ketua, dan enam anggota lainnya) untuk kajian mendalam. Mereka menganalisis kasus, latar belakang, dan investigasi agar keputusan perlindungan tepat dan efektif.

d. Perlindungan dan Bantuan

Setelah RPP, LPSK langsung memberikan perlindungan sesuai hakhak di Pasal 5 hingga 10A UU PSK, seperti keamanan pribadi, identitas baru, dan bantuan medis. Bidang Perlindungan atau Divisi Pemenuhan Hak Saksi dan Korban bertanggung jawab penuh, menyesuaikan dengan kebutuhan saksi/korban sepanjang proses kasus hingga selesai. LPSK berkolaborasi dengan instansi terkait (seperti Polri atau Kejaksaan) untuk mengeksekusi keputusan secara integratif dan bertanggung jawab, memastikan tidak ada yang terabaikan.

Untuk melindungi korban cyberstalking, UU ITE memungkinkan ganti rugi berdasarkan Pasal 1365 KUH Perdata, di mana korban dapat mengajukan kompensasi atas kerugian materiil dan immateriil melalui putusan pengadilan. Namun, regulasi ini belum berorientasi pada pemulihan korban secara holistik, seperti pendampingan hukum atau rehabilitasi psikis.(Khadafi Yusuf, 2024) Tantangan administratif diperparah oleh ketiadaan mekanisme kerja sama

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

internasional untuk kejahatan lintas batas, serta kelemahan dalam digital forensics. Oleh karena itu, diperlukan reformulasi kebijakan, termasuk undang-undang pidana khusus cyberstalking dengan definisi jelas, sanksi proporsional berdasarkan dampak korban, dan penguatan perlindungan data pribadi untuk mencegah penyalahgunaan. Pendekatan victim-oriented criminal law harus diadopsi, mengintegrasikan UU ITE dan PDP melalui peraturan teknis, sambil meningkatkan literasi digital dan kolaborasi lintas pihak untuk menciptakan lingkungan siber yang aman.

Faktor Penghambat dan Solusi Penegakan Hukum Cybercrime

Terdapat enam faktor utama yang menghambat penegakan hukum terhadap kejahatan siber (cybercrime):(Andry Rachman Martin Stefani Maria Putri, 2025)

a) Kekosongan dan Keterlambatan Regulasi: Hukum formal (termasuk UU ITE) tertinggal dari perkembangan teknologi yang sangat cepat, gagal mengakomodasi varian baru cybercrime (seperti deepfake), menyebabkan kesulitan penjeratan pelaku.
b) Keterbatasan Kapasitas SDM: Banyak aparat penegak hukum (APH) kekurangan kemampuan teknis dan forensik digital, berakibat pada kegagalan atau ketidakakuratan dalam pengumpulan bukti digital yang rentan rusak.
c) Tantangan Yurisdiksi Lintas Batas: Indonesia belum menjadi pihak dalam konvensi internasional (misalnya Budapest Convention), menghambat kerja sama pertukaran informasi, ekstradisi, dan bantuan hukum lintas negara.
d) Teknologi Penyembunyi Jejak Pelaku: Pelaku memanfaatkan enkripsi, VPN, dan dark web untuk menyembunyikan identitas dan lokasi, menyulitkan APH menelusuri jejak digital.
e) Rendahnya Literasi Digital Masyarakat: Masyarakat mudah menjadi korban dan jarang melaporkan insiden karena ketidakpahaman prosedur hukum dan kurangnya kehati-hatian dalam berinternet, menyebabkan banyak kasus tidak terdeteksi.
f) Kesenjangan Infrastruktur Teknologi: Ketersediaan laboratorium forensik digital dan infrastruktur teknologi tinggi belum merata dan alokasi anggaran masih rendah, terutama di daerah.

Solusi Strategis:

Solusi yang diperlukan bersifat menyeluruh dan kolaboratif:

a. Reformasi dan Sinkronisasi Hukum: Melakukan pembaruan hukum yang adaptif, mencakup perlindungan data pribadi dan keamanan digital, serta menyinkronkan regulasi sektoral.
b. Peningkatan Kapasitas SDM: Melakukan pelatihan teknis dan sertifikasi rutin bagi penyidik, jaksa, dan hakim agar mampu menangani kasus dan menyusun bukti yang kuat.
c. Kerja Sama Internasional Aktif: Membangun kesepakatan bilateral dan multilateral untuk mempermudah ekstradisi, pertukaran data, dan bantuan hukum lintas batas.

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

d. Pemerataan Infrastruktur: Mengembangkan laboratorium digital forensik dan pusat tanggap insiden (CSIRT) hingga tingkat provinsi/kabupaten untuk mempercepat penanganan kejahatan lokal.
e. Peningkatan Literasi Digital: Pemerintah, akademisi, dan swasta bekerja sama meningkatkan kesadaran dan kecerdasan masyarakat dalam mengamankan data dan melaporkan insiden.

SIMPULAN

Perlindungan hukum bagi saksi dan korban di era digital di Indonesia dijamin melalui kombinasi regulasi, terutama Undang-Undang ITE, UU Perlindungan Saksi dan Korban (UU PSK), serta UU Perlindungan Data Pribadi (UU PDP). UU ITE berfungsi sebagai dasar penindakan kejahatan siber (seperti pencemaran nama baik) dengan fokus pada sanksi pidana bagi pelaku. Sementara itu, UU PSK memberikan mandat kepada Lembaga Perlindungan Saksi dan Korban (LPSK) untuk menyediakan perlindungan fisik, psikis, dan bantuan hukum. Adapun UU PDP berperan sebagai payung hukum khusus yang komprehensif terkait pengelolaan data pribadi. Meskipun dasar hukum tersedia, perlindungan ini belum secara eksplisit mengakomodasi delik kejahatan baru seperti doxing, dan UU ITE masih cenderung berfokus pada penindakan ketimbang pemulihan korban secara holistik (restitusi dan rehabilitasi). Dalam menangani ancaman digital, LPSK menjalankan mekanisme perlindungan melalui empat tahapan utama: Permohonan, Verifikasi Administratif, Rapat Paripurna Anggota (RPP), dan Pelaksanaan Perlindungan. Proses ini kini telah memanfaatkan platform digital untuk mempermudah pengajuan permohonan. Namun, dalam pelaksanaannya, LPSK menghadapi tantangan signifikan. Tantangan hukum meliputi kekosongan regulasi yang gagal mengejar laju teknologi khususnya dalam mendefinisikan doxing dan kelemahan implementasi restitusi karena LPSK tidak memiliki kewenangan eksekutorial dan kurangnya sinergi dengan Kejaksaan, sering menyebabkan restitusi mandek. Untuk meningkatkan efektivitas perlindungan, solusi strategis perlu dilakukan, yaitu melalui reformasi regulasi yang berorientasi pada korban (victim-oriented criminal law). Ini mencakup harmonisasi UU ITE dan UU PDP, penetapan definisi dan sanksi spesifik untuk doxing, serta penguatan mekanisme restitusi. Secara administratif, diperlukan peningkatan kapasitas SDM dan infrastruktur forensik digital pada aparat penegak hukum, pemerataan teknologi, serta kerjasama internasional yang lebih aktif untuk mengatasi tantangan yurisdiksi lintas batas.

DAFTAR RUJUKAN

Adnan, A. J., Putriyana, D., Wibowo, H. A., & Ramadan, S. (2024). Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Cyberbullying. *Indonesian Journal Of Criminal Law And Criminology (IJCLC)*, 5(1), 25.

Djanggih, H. (2018). Konsepsi Perlindungan Hukum Bagi Anak Sebagai Korban Kejahatan Siber Melalui Pendekatan Penal Dan Non Penal. *Mimbar Hukum*, 30(2), 327.

Djamaludin, D., & Arrasyid, Y. (2024). Pemenuhan Keadilan Dalam Sistem Hukum Pidana Indonesia Melalui Tugas LPSK. *Jurnal Ilmu Hukum Kyadiren*, 5(2), 35.

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi Pencegahan Kejahatan Siber di Indonesia: Sinergi antara UU ITE dan Kebijakan Keamanan Digital. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(2), 3618.

Firdaus, R. A. (2024). Perlindungan Hukum Dan Pencegahan Kejahatan Siber Di Era Digital dalam Sistem Hukum Di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, 4(1), 10–25.

Hendrawan, A. R., dkk. (2025). Perlindungan Hukum Bagi Korban Kejahatan Digital Dalam Perspektif UU ITE Dan KUHP. *Jurnal Hukum Dan Kewarganegaraan*, 14(12), 3.

Hidayahp, G. R., Ma'shum, H. D., & Awaluddin, M. (2025). Studi Komparatif Perlindungan Data Pribadi Dalam UU ITE 2024 Dan UU PDP 2022. *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 4(4), 66.

Hutasoit, R. R. (2024). Tinjauan Yuridis Perlindungan Korban Terhadap Kejahatan Cyber Bullying Dalam Sistem Hukum Pidana Indonesia. *Jurnal Yuridis Unaja*, 7(1), 44.

Nurhayati, S. (2015). Aspek Hukum Perlindungan Saksi Dan Korban Perdagangan Anak (Human Trafficking). *Yudisia: Jurnal Pemikiran Hukum Dan Hukum Islam*, 6(1), 92.

Oktavia, D. P., Apriyani, R., & Wati, A. (2025). Tanggung Jawab LPSK Dalam Pelaksanaan Restitusi Korban Kekerasan Seksual Oleh Pelaku Yang Tidak Mampu Atau Terpidana Mati. *Referendum: Jurnal Hukum Perdata Dan Pidana*, 2(3), 64.

Rachman, A., Putri, M. S. M., & Panjaitan, J. D. (2025). Korban Kejahatan Siber (Cybercrime): Perlindungan Dan Kendala Dalam Penegakan Hukum. *Jurnal Prisma Hukum*, 9(6), 57.

Rahmadani, K. F., & Mu'allifin, M. D. A. (2023). Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Legacy: Jurnal Hukum dan Perundang-undangan*, 3(1), 22.

Rahmayanti, Ula, R. F., Ridho, A., & Aini, N. (2025). Regulasi Tentang Kejahatan Siber Dalam Bentuk Doxing Yang Berbasis Perlindungan Hukum Terhadap Korban. *Indonesian Journal Of Law*, 2(8), 133.

Ramadhan, D. N., Widarini, D. A., & Gunawan. (2025). Representasi Kekerasan Berbasis Gender Online dalam Film "Like & Share". *Ikon*, 29(2), 50.

Rauf, S., Hasjad, & Guntur, S. (2022). Efektifitas Peran Lembaga Perlindungan Saksi Dan Korban (LPSK) Dalam Melindungi Saksi Tindak Pidana Gratifikasi. *Sibatik Journal*, 1(3), 212.

Yusuf, K., Frasetyo, M., Gumilar, R. R., & Hosnah, A. U. (2024). Perlindungan Hukum Terhadap Korban Kejahatan Identitas Online Di Indonesia. *Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, 2(1), 241.

Budiyanto, M. A. K., Waluyo, L., & Mokhtar, A. (2016). Implementasi Pendekatan Saintifik dalam Pembelajaran di Pendidikan Dasar di Malang. *Proceeding Biology Education Conference*, 13(1), 48.

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati

Laal, M. (2011). Knowledge Management in Higher Education. *Procedia Computer Science*, 3, 544–549.

Ismail, Z. (2023). *Buku Ajar Perlindungan Saksi Dan Korban*. Malang: PT Literasi Nusantara Abadi Grup.

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Lisensi: Creative Commons Attribution ShareAlike 4.0 International License (CC BY SA 4.0)

Copyright; Khaiyyil Faizunan Nurun Nafi, Siti Nurhayati