CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

Perlindungan Hukum bagi Korban Kejahatan Digital dalam Perspektif UU ITE dan KUHP

Andika Rafa Hendrawan[1], Bagas Dava Aji Ramadhan[2],Bayu Arif Hi Ahdar[3], Triana[4]

Email: 240413003@mhs.udb.ac.id, 240413007@mhs.udb.ac.id, 240413086@mhs.udb.ac.id, triana@udb.ac.id

Universitas Duta Bangsa Surakarta

Abstrack

Digital cybercrime is increasingly complex and massive in line with the rapid development of information technology. Victims suffer not only material losses, but also psychological and social trauma. This research discusses common forms of digital crime in Indonesia, such as phishing, defamation, online fraud, and dissemination of immoral content, and evaluates the effectiveness of legal protection for victims under the ITE Law and the Criminal Code. The results of the discussion show that although both legal instruments regulate sanctions for perpetrators, the aspect of victim recovery is still very limited. Legal protection is often hampered by multiple interpretations of articles, the limitations of the Criminal Code in dealing with technology-based crimes, and the low capacity of the authorities in handling digital evidence. Solutions offered include strengthening victim-oriented regulations, increasing the competence of law enforcement in the field of digital forensics, optimizing the role of LPSK, and public education on legal literacy and digital security. This study emphasizes the importance of a responsive and pro-victim legal approach so that the Indonesian criminal justice system is able to face the challenges of digital crime fairly and effectively.

Keywords: digital crime, legal protection, victims, ITE Law, Criminal Code.

Article History
Received: Juli 2025
Reviewed: juli 2025
Published: Juli 2025

[1] 240413003, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta
[2] 240413007, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta
[3] 240413086, Fakultas Hukum dan Bisnis Universitas Duta Bangsa Surakarta

CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

Abstrak

Kejahatan digital cybercrime semakin kompleks dan masif seiring pesatnya perkembangan teknologi informasi. Korban tidak hanya menderita kerugian material, tetapi juga trauma psikologis dan sosial. Penelitian ini membahas bentuk-bentuk umum kejahatan digital di Indonesia, seperti phishing, pencemaran nama baik, penipuan daring, dan penyebaran konten asusila, serta mengevaluasi efektivitas perlindungan hukum bagi korban berdasarkan UU ITE dan KUHP. Hasil pembahasan menunjukkan bahwa meskipun kedua instrumen hukum tersebut mengatur sanksi bagi pelaku, aspek pemulihan korban masih sangat terbatas. Perlindungan hukum sering kali terhambat oleh multitafsir pasal, keterbatasan KUHP dalam menangani kejahatan berbasis teknologi, serta rendahnya kapasitas aparat dalam menangani bukti digital. Solusi yang ditawarkan meliputi penguatan regulasi yang berorientasi pada korban, peningkatan kompetensi penegak hukum di bidang digital forensik, optimalisasi peran LPSK, serta edukasi publik mengenai literasi hukum dan keamanan digital. Kajian ini menegaskan pentingnya pendekatan hukum yang responsif dan berpihak pada korban agar sistem peradilan pidana Indonesia mampu menghadapi tantangan kejahatan digital secara adil dan efektif.

Kata kunci: kejahatan digital, perlindungan hukum, korban, UU ITE, KUHP.

CAUSA

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

PENDAHULUAN

Perubahan struktur sosial akibat digitalisasi telah menciptakan ruang baru bagi terjadinya kejahatan yang tidak mengenal batas waktu maupun wilayah, yakni kejahatan digital *cybercrime*. Sifatnya yang cepat, tersembunyi, dan sulit dilacak menjadikan kejahatan digital sebagai tantangan serius dalam penegakan hukum di era informasi. Dalam kondisi tersebut, korban kejahatan digital tidak hanya dirugikan secara materi, namun juga rentan mengalami kerugian psikologis dan sosial, seperti intimidasi, pencemaran nama baik, atau penyebaran data pribadi tanpa izin. Meskipun Indonesia telah memiliki UU ITE sebagai dasar hukum untuk menanggulangi kejahatan di dunia maya dan KUHP sebagai acuan pidana umum, fokus implementasi regulasi sering kali lebih berat pada aspek penindakan terhadap pelaku, bukan pada perlindungan korban**.** Tidak jarang korban justru mengalami reviktimisasi—baik melalui proses hukum yang berbelit maupun melalui stigma sosial akibat rendahnya literasi digital dan hukum masyarakat. Kesenjangan antara perkembangan bentuk kejahatan digital dan adaptasi perangkat hukum yang melindungi korban menandakan adanya kebutuhan mendesak untuk mengevaluasi efektivitas perlindungan hukum yang tersedia saat ini. Tanpa adanya perbaikan paradigma dan regulasi yang berpihak pada korban, maka perlindungan hukum hanya akan menjadi formalitas belaka.

Perkembangan teknologi informasi dan komunikasi yang pesat dalam dua dekade terakhir telah membawa perubahan signifikan dalam kehidupan masyarakat, termasuk dalam pola interaksi sosial, ekonomi, hingga aktivitas hukum. Namun, kemajuan ini juga membuka ruang bagi munculnya bentuk-bentuk kejahatan baru yang bersifat digital atau *cybercrime*, yang tidak hanya merugikan secara materiil, tetapi juga berdampak psikologis dan sosial bagi para korbannya. Kejahatan digital memiliki karakteristik yang berbeda dengan kejahatan konvensional. Ia dapat dilakukan secara anonim, lintas yurisdiksi, dan dalam waktu yang sangat singkat, serta memanfaatkan celah sistem teknologi yang kerap kali sulit dideteksi secara langsung. Bentuknya pun beragam, mulai dari penipuan daring *online fraud* penyebaran data pribadi, penghinaan dan pencemaran nama baik di media sosial, hingga tindak pidana pornografi dan pelecehan berbasis digital. Dalam banyak kasus, korban tidak hanya mengalami kerugian finansial, tetapi juga kerugian immateril seperti rasa takut, malu, atau trauma berkepanjangan.

Secara faktual, praktik perlindungan hukum terhadap korban kejahatan digital di Indonesia masih menghadapi berbagai persoalan mendasar. Di tengah meningkatnya kasus cybercrime seperti penipuan online, pencemaran nama baik digital, dan penyebaran konten tanpa izin korban kerap kali mengalami kesulitan dalam mengakses keadilan. Banyak dari mereka tidak mengetahui prosedur hukum yang harus ditempuh, kesulitan mendapatkan bukti digital yang valid secara hukum, hingga menghadapi aparat penegak hukum yang belum sepenuhnya kompeten dalam menangani kasus berbasis teknologi. UU ITE sebagai instrumen hukum utama dalam menangani kejahatan digital sering kali lebih menitikberatkan pada aspek pemidanaan terhadap pelaku, tanpa memberikan mekanisme perlindungan dan pemulihan yang memadai bagi korban. Dalam banyak kasus, korban justru dikriminalisasi balik oleh pelaku melalui pasal-pasal multitafsir, seperti Pasal 27 ayat (3) tentang pencemaran nama baik. Sementara itu, KUHP yang digunakan secara subsidiari juga belum secara eksplisit mengatur mengenai tindak pidana yang dilakukan melalui sistem elektronik, sehingga korban terjebak dalam kekosongan hukum *legal vacuum* yang merugikan. Aparat penegak hukum sering tidak memiliki panduan teknis maupun pelatihan khusus untuk menangani laporan kejahatan digital secara profesional. Akibatnya, proses hukum menjadi lambat, tidak responsif, dan cenderung mengabaikan kebutuhan dasar korban untuk mendapatkan rasa keadilan dan jaminan perlindungan hukum yang memadai.

Secara normatif, perlindungan hukum terhadap korban kejahatan digital seharusnya menjadi bagian integral dari sistem hukum pidana nasional. Hukum tidak hanya bertugas menghukum pelaku, tetapi juga wajib menjamin hak-hak korban untuk mendapatkan perlindungan, pemulihan, dan keadilan. UU ITE dan KUHP,

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

sebagai instrumen hukum yang relevan, idealnya harus mampu secara seimbang mengatur pemberian sanksi pidana terhadap pelaku dan pemulihan martabat serta hak-hak korban**.** Prinsip perlindungan terhadap korban telah diakui dalam berbagai instrumen hukum internasional, seperti *Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power* PBB, 1985, yang mengamanatkan bahwa negara harus memastikan korban memperoleh informasi, restitusi, kompensasi, dan dukungan psikologis. Hal ini seharusnya diadopsi dalam sistem hukum nasional, termasuk dalam revisi dan pelaksanaan UU ITE serta pembaruan KUHP.

Indonesia melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik UU ITE yang kemudian diperbarui melalui UU Nomor 19 Tahun 2016, telah menyediakan landasan hukum untuk mengatur perilaku digital, termasuk upaya penindakan terhadap pelaku kejahatan siber. Di sisi lain, Kitab Undang-Undang Hukum Pidana KUHP masih digunakan sebagai dasar hukum pidana umum untuk memberikan perlindungan terhadap korban, termasuk dalam konteks kejahatan yang dilakukan melalui media elektronik. Namun, dalam praktiknya, implementasi kedua instrumen hukum tersebut masih menimbulkan berbagai persoalan. Banyak pasal dalam UU ITE yang justru lebih sering digunakan untuk menjerat pengguna internet secara represif, seperti dalam kasus pencemaran nama baik atau penyebaran informasi, sehingga korban seringkali justru menjadi pihak yang terpinggirkan atau bahkan dikriminalisasi. Sementara itu, KUHP sebagai hukum pidana umum belum secara spesifik mengakomodasi kebutuhan perlindungan korban kejahatan digital yang kompleks dan berkembang cepat.

Kondisi ini menimbulkan pertanyaan penting mengenai sejauh mana perlindungan hukum terhadap korban kejahatan digital telah diakomodasi secara adil, efektif, dan berpihak pada korban dalam sistem hukum pidana nasional Indonesia. Penelitian ini bertujuan untuk mengkaji secara kritis perlindungan hukum yang tersedia bagi korban dalam perspektif UU ITE dan KUHP, serta menilai efektivitasnya dalam konteks kejahatan digital yang terus berkembang. Melalui kajian ini, diharapkan muncul rekomendasi untuk penguatan regulasi dan kebijakan yang lebih adil serta berorientasi pada perlindungan hak-hak korban di ruang digital. Di tengah kemajuan teknologi informasi yang semakin masif, kejahatan digital telah menjadi fenomena yang tidak terelakkan dalam kehidupan modern. Akses masyarakat terhadap internet dan media sosial yang luas membuka ruang interaksi baru, tetapi sekaligus menciptakan celah bagi berbagai bentuk kejahatan yang memanfaatkan kerentanan sistem dan rendahnya literasi digital. Mulai dari penipuan daring *online fraud*, peretasan data pribadi, pencemaran nama baik di media sosial, hingga kekerasan berbasis gender online, seluruh bentuk ini menunjukkan kompleksitas dan dinamika baru dalam ranah hukum pidana.

Ironisnya, di tengah meningkatnya intensitas kejahatan digital, perlindungan terhadap korban sering kali tidak berjalan secara optimal. Banyak korban mengalami kesulitan dalam mengakses keadilan, baik karena kendala teknis seperti pembuktian digital yang rumit, maupun karena kurangnya pemahaman aparat penegak hukum terhadap sifat kejahatan berbasis teknologi. Tidak jarang pula korban justru mengalami reviktimisasi menjadi sasaran balik oleh pelaku atau bahkan oleh sistem hukum itu sendiri. Dalam beberapa kasus, seperti pencemaran nama baik di media sosial, korban kejahatan digital malah dilaporkan balik dengan pasal-pasal dalam Undang-Undang Informasi dan Transaksi Elektronik UU ITE, terutama Pasal 27 ayat 3, yang selama ini dikenal problematik karena tafsirnya yang lentur. Hal ini mengindikasikan adanya ketimpangan dalam penerapan hukum yang justru memperlemah posisi korban, bukan memberdayakannya.

Di sisi lain, meskipun KUHP menyediakan norma pidana umum yang dapat digunakan untuk menjerat pelaku, sebagian besar pasalnya belum sepenuhnya relevan dengan modus kejahatan berbasis teknologi digital. KUHP belum didesain untuk mengantisipasi bentuk kejahatan yang dilakukan tanpa kontak fisik, bersifat lintas batas, dan menggunakan perangkat lunak atau algoritma. Situasi ini menandakan bahwa perlindungan hukum bagi korban kejahatan digital di Indonesia masih berada dalam posisi yang lemah dan rentan, terutama dalam aspek kecepatan penanganan, akses terhadap bantuan hukum, dan pemulihan hak-

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

hak korban. Tanpa adanya pendekatan hukum yang progresif, korban kejahatan digital akan terus berada dalam posisi subordinat dalam sistem peradilan pidana.

Seiring dengan meningkatnya intensitas penggunaan teknologi informasi di berbagai aspek kehidupan, kejahatan berbasis digital atau *cybercrime* telah berkembang secara kompleks dan masif. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi, tetapi juga menyerang hak-hak personal warga negara, seperti privasi, rasa aman, dan kehormatan. Dalam konteks ini, hukum dituntut untuk tidak hanya berfungsi sebagai alat pemidanaan terhadap pelaku, tetapi juga sebagai sarana perlindungan dan pemulihan hak-hak korban secara menyeluruh. Indonesia telah memiliki perangkat hukum yang menjadi fondasi dalam menangani kejahatan digital, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik UU ITE yang kemudian direvisi melalui UU Nomor 19 Tahun 2016, serta Kitab Undang-Undang Hukum Pidana KUHP sebagai rujukan hukum pidana umum. Meskipun kedua instrumen ini memiliki peran penting dalam sistem penegakan hukum di Indonesia, terdapat sejumlah permasalahan krusial terkait efektivitas dan keberpihakan mereka terhadap korban kejahatan digital. UU ITE sering kali dikritik karena pasal-pasalnya yang multitafsir dan cenderung digunakan untuk membatasi kebebasan berekspresi, sementara perlindungan terhadap korban tidak diatur secara tegas dan menyeluruh. Di sisi lain, KUHP yang bersifat konvensional belum secara eksplisit mengatur tentang kejahatan berbasis sistem elektronik, sehingga penerapannya dalam kasus digital menjadi terbatas. Akibatnya, korban kerap kali terjebak dalam kebuntuan hukum ketika mencari keadilan, baik dalam aspek perlindungan, pemulihan, maupun pengakuan status hukumnya sebagai pihak yang dirugikan.

Maka dari itu, pengkajian yang mendalam terhadap instrumen UU ITE dan KUHP menjadi sangat penting dan relevan untuk menjawab tantangan hukum di era digital. Kajian ini bertujuan untuk mengidentifikasi sejauh mana kedua instrumen tersebut mampu menjamin perlindungan hukum yang adil, efektif, dan berpihak pada korban kejahatan digital. Lebih dari itu, pengkajian ini juga diperlukan untuk mendorong reformulasi kebijakan hukum pidana nasional yang adaptif terhadap perkembangan teknologi serta selaras dengan prinsip-prinsip keadilan modern dan hak asasi manusia.

METODE PENELITIAN

Kajian ini menggunakan pendekatan kualitatif berbasis yuridis normatif, dengan fokus pada analisis terhadap norma-norma hukum yang tertuang dalam Undang-Undang Informasi dan Transaksi Elektronik UU ITE serta Kitab Undang-Undang Hukum Pidana KUHP. Pendekatan ini bertujuan untuk menggambarkan dan menafsirkan ketentuan hukum yang mengatur perlindungan bagi korban kejahatan digital, sekaligus menilai efektivitas implementasinya di tengah dinamika perkembangan teknologi informasi. Sumber yang digunakan meliputi peraturan perundang-undangan, putusan pengadilan, doktrin hukum, serta berbagai literatur ilmiah yang relevan. Seluruh data dianalisis secara deskriptif-kualitatif melalui studi kepustakaan, dengan menekankan pada pemahaman mendalam mengenai struktur hukum yang berlaku, potensi kesenjangan norma, dan urgensi pembaruan kebijakan yang lebih responsif terhadap perlindungan hak-hak korban dalam ruang digital.

PEMBAHASAN

Perlindungan hukum dalam konteks hukum pidana merupakan upaya negara dalam menjamin hak-hak warga negara dari segala bentuk ancaman, gangguan, dan pelanggaran hukum, baik oleh individu maupun oleh negara sendiri. Menurut Satjipto Rahardjo, perlindungan hukum adalah segala upaya negara untuk menjamin kepastian hukum guna melindungi hak-hak warga negara Rahardjo, 2000. Dalam ranah hukum pidana, perlindungan hukum tidak hanya ditujukan bagi tersangka atau terdakwa, tetapi juga bagi korban, yang kerap kali mengalami kerugian fisik, psikis, dan sosial akibat kejahatan. Bentuk perlindungan hukum

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

pidana terhadap korban dapat dibedakan menjadi perlindungan normatif, prosedural, dan substantif. Perlindungan normatif diwujudkan dalam peraturan perundang-undangan seperti KUHP dan UU ITE, sedangkan perlindungan prosedural mencakup akses terhadap proses hukum yang adil dan tidak diskriminatif. Perlindungan substantif mencakup hak atas pemulihan, ganti rugi, dan rehabilitasi. Hal ini juga sejalan dengan pandangan Muladi, yang menekankan bahwa perlindungan hukum terhadap korban harus mencakup pemenuhan hak atas rasa aman, keadilan, serta bantuan psikologis dan sosial Muladi, 1995.

Dalam sistem hukum nasional Indonesia, hak-hak korban mulai memperoleh perhatian melalui instrumen hukum seperti Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang kemudian diperbarui melalui UU Nomor 31 Tahun 2014. Dalam undang-undang tersebut, korban berhak memperoleh perlindungan atas keamanan pribadi, identitas, serta tempat tinggal; mendapatkan informasi mengenai perkembangan perkara; dan memperoleh restitusi atau kompensasi LPSK, 2014. Sementara itu, KUHAP masih menunjukkan keterbatasan dalam mengakomodasi posisi dan hak-hak korban secara eksplisit, sehingga terjadi ketimpangan dalam sistem peradilan pidana yang lebih menitikberatkan pada pelaku. Di tingkat internasional, acuan utama dalam perlindungan korban adalah United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power tahun 1985. Deklarasi ini menyatakan bahwa korban memiliki hak untuk diperlakukan dengan hormat dan bermartabat, hak untuk memperoleh akses terhadap proses peradilan, informasi mengenai perkara, restitusi, kompensasi, dan bantuan dari negara United Nations, 1985. Selain itu, Statuta Roma Mahkamah Pidana Internasional Rome Statute of the International Criminal Court, 1998 juga secara eksplisit memberikan hak partisipasi kepada korban, termasuk penyampaian pandangan dan perhatian mereka dalam proses peradilan ICC, 1998, Pasal 68.

Kejahatan digital atau *cybercrime* merupakan tindak pidana yang dilakukan melalui atau terhadap sistem teknologi informasi. Kejahatan ini berkembang seiring dengan kemajuan teknologi digital dan memiliki berbagai bentuk. Menurut Nugroho dan Rachmadi 2020, bentuk kejahatan digital dapat diklasifikasikan antara lain ke dalam: phishing, yaitu upaya penipuan untuk memperoleh data pribadi seperti password atau informasi rekening melalui situs palsu; hacking, yakni aktivitas ilegal dalam mengakses sistem atau jaringan komputer tanpa izin; penyebaran konten ilegal, termasuk pornografi anak, ujaran kebencian, dan terorisme digital; serta pencemaran nama baik atau penghinaan melalui media elektronik, yang sering menjadi subjek dalam penerapan Pasal 27 ayat 3 UU ITE.

Sementara itu, menurut Soesilo 2018, jenis kejahatan digital juga mencakup penipuan daring, penyebaran malware, manipulasi data, dan pencurian identitas. Kejahatan ini biasanya memiliki korban yang tersebar secara geografis, serta dilakukan dengan modus yang sulit dilacak secara langsung, mengingat pelaku dapat menyembunyikan identitas melalui perangkat dan jaringan anonim. Kejahatan digital menjadi semakin kompleks karena tidak hanya menyerang individu, tetapi juga institusi, sektor keuangan, dan bahkan sistem pemerintahan.

Undang-Undang Informasi dan Transaksi Elektronik UU ITE merupakan instrumen hukum yang dirancang untuk menjawab tantangan hukum dalam perkembangan teknologi informasi. UU No. 11 Tahun 2008 menjadi tonggak awal pengaturan interaksi elektronik secara komprehensif di Indonesia, dan kemudian diperbarui melalui UU No. 19 Tahun 2016 untuk menyesuaikan dengan dinamika hukum dan kritik publik. UU ini mengatur berbagai aspek hukum seperti informasi elektronik, transaksi elektronik, tanda tangan digital, serta larangan terhadap perbuatan-perbuatan tertentu dalam ruang digital. Pasal-pasal dalam UU ITE yang relevan terhadap perlindungan korban kejahatan digital antara lain Pasal 27 hingga Pasal 29 yang mengatur mengenai larangan distribusi konten asusila, penghinaan atau pencemaran nama baik, pemerasan, serta ancaman melalui media elektronik. Selain itu, Pasal 30 hingga Pasal 33 memuat ketentuan mengenai akses ilegal terhadap sistem elektronik, perusakan data, dan gangguan sistem. Secara normatif, UU ITE juga memberikan pengakuan terhadap alat bukti elektronik dalam proses peradilan sebagaimana tertuang dalam Pasal 5 dan 44. Menurut Sembiring 2019, pengakuan terhadap bukti digital menjadi aspek penting

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

dalam membangun legitimasi hukum di era siber. Revisi tahun 2016 mencoba memperkuat perlindungan hak-hak pengguna internet dan menyeimbangkan antara kepentingan keamanan, kebebasan berekspresi, dan hak atas reputasi. Namun, sejumlah pasal terutama mengenai pencemaran nama baik Pasal 27 ayat 3 masih menimbulkan perdebatan karena dinilai multitafsir dan berpotensi digunakan secara represif terhadap kritik di ruang publik Gunawan, 2020.

Meskipun KUHP merupakan produk hukum yang lebih dahulu lahir dan belum secara spesifik mengatur kejahatan berbasis teknologi informasi, namun beberapa pasalnya tetap relevan sebagai dasar pemidanaan pelaku kejahatan digital. Misalnya, Pasal 310 dan 311 KUHP mengenai penghinaan dan fitnah dapat dikaitkan dengan pencemaran nama baik di dunia maya. Pasal 362 tentang pencurian juga sering digunakan dalam konteks pencurian data atau akses ilegal terhadap sistem elektronik, meskipun belum secara eksplisit menyebut teknologi digital. Selain itu, Pasal 378 KUHP mengenai penipuan dapat diterapkan pada kasus penipuan online yang kini semakin marak terjadi. KUHP juga mengatur pidana tambahan dan pertanggungjawaban pidana secara umum, yang dalam praktiknya sering dijadikan dasar oleh aparat penegak hukum dalam menangani kejahatan digital yang belum diatur secara spesifik oleh UU ITE. Keterbatasan KUHP dalam menjangkau kejahatan digital menunjukkan pentingnya sinkronisasi antara hukum pidana konvensional dan regulasi khusus seperti UU ITE. Menurut Marzuki 2017, integrasi antara KUHP dan UU ITE harus diarahkan pada perlindungan yang seimbang antara kepentingan korban, pelaku, dan sistem hukum itu sendiri.

Perkembangan teknologi informasi telah melahirkan berbagai bentuk interaksi sosial dan transaksi ekonomi yang berbasis digital. Namun, di balik kemajuan tersebut, muncul pula ancaman kejahatan digital cybercrime yang terus meningkat secara kuantitas dan kualitas. Fenomena ini menimbulkan persoalan hukum yang kompleks, terutama dalam aspek perlindungan terhadap korban. Kejahatan digital tidak hanya menimbulkan kerugian material, tetapi juga mengakibatkan penderitaan immaterial dan psikologis yang sering kali tidak tertangani secara memadai oleh sistem hukum yang berlaku. Oleh karena itu, penting untuk menelaah secara kritis bagaimana kerangka hukum yang ada khususnya UU ITE dan KUHP memberikan perlindungan nyata bagi korban.

1. Bentuk Kejahatan Digital yang Umum Terjadi di Indonesia

Kejahatan digital atau *cybercrime* merupakan bentuk kriminalitas yang memanfaatkan teknologi informasi dan komunikasi sebagai sarana maupun objek kejahatan. Di Indonesia, beberapa bentuk kejahatan digital yang paling sering terjadi antara lain: phishing, hacking, penipuan online, pencemaran nama baik melalui media sosial, penyebaran konten asusila, serta akses ilegal terhadap data pribadi. Data dari Kementerian Komunikasi dan Informatika serta laporan Direktorat Tindak Pidana Siber Bareskrim Polri menunjukkan peningkatan signifikan kasus cybercrime setiap tahun, terutama sejak meningkatnya penggunaan internet dan transaksi elektronik pasca pandemi. Salah satu kejahatan digital yang menonjol adalah penipuan berbasis e-commerce, yang memanfaatkan kelemahan konsumen dalam bertransaksi online. Selain itu, kejahatan doxxing dan penyebaran konten pornografi non-konsensual juga menjadi sorotan, terutama karena berdampak serius terhadap psikologis dan reputasi korban. Berbeda dengan kejahatan konvensional, kejahatan digital sering dilakukan secara anonim, bersifat lintas batas yurisdiksi, serta sulit dilacak secara teknis maupun hukum.

2. Perlindungan Hukum bagi Korban Kejahatan Digital Menurut UU ITE dan KUHP

UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik UU ITE merupakan dasar utama dalam pengaturan kejahatan digital di Indonesia. UU ini memuat ketentuan larangan dan sanksi terhadap perbuatan seperti pencemaran nama baik Pasal 27 ayat 3, penyebaran konten asusila Pasal 27 ayat 1, penghinaan, ancaman, penipuan, hingga akses ilegal terhadap sistem elektronik Pasal 30–32. Bagi korban, UU ITE juga memberikan pengakuan atas alat bukti elektronik dan membuka

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

jalan untuk pelaporan serta proses hukum yang lebih modern. Namun demikian, pendekatan dalam UU ITE cenderung bersifat penindakan terhadap pelaku, bukan pemulihan bagi korban.

KUHP sebagai hukum pidana umum tetap memiliki relevansi, meskipun belum secara spesifik mengatur kejahatan digital. Beberapa ketentuan seperti Pasal 310–311 tentang pencemaran nama baik, Pasal 378 tentang penipuan, dan Pasal 362 tentang pencurian kerap dijadikan rujukan tambahan dalam penanganan kasus-kasus siber. Namun, karakteristik kejahatan digital yang khas sering kali menyulitkan penerapan KUHP secara langsung tanpa bantuan perangkat hukum tambahan. Dari perspektif korban, baik UU ITE maupun KUHP masih belum secara komprehensif menyediakan mekanisme restitusi, rehabilitasi psikologis, atau jaminan perlindungan identitas. Oleh karena itu, keberadaan lembaga seperti Lembaga Perlindungan Saksi dan Korban LPSK menjadi sangat penting, meskipun aksesnya masih terbatas pada kasus-kasus tertentu.

3. Kendala dan Solusi dalam Implementasi Perlindungan Hukum terhadap Korban

Implementasi perlindungan hukum terhadap korban kejahatan digital di Indonesia menghadapi beberapa kendala yang signifikan. Pertama, terdapat celah regulasi, khususnya dalam hal pengaturan yang berfokus pada hak-hak korban. UU ITE belum secara tegas mengatur skema pemulihan korban secara menyeluruh, dan KUHP belum sepenuhnya mampu menjawab dinamika kejahatan digital. Kedua, minimnya literasi digital masyarakat menyebabkan banyak korban tidak memahami prosedur pelaporan, pembuktian digital, atau hak-hak hukumnya.Kendala lain adalah pada aspek teknis dan forensik digital, di mana tidak semua aparat penegak hukum memiliki kompetensi dalam mengidentifikasi, mengamankan, dan menganalisis bukti elektronik. Selain itu, hambatan yuridiksi lintas negara dalam kasus peretasan atau penipuan internasional juga menyulitkan proses penegakan hukum. Sebagai solusi, dibutuhkan pendekatan multi-sektoral: pembaruan regulasi untuk memperkuat posisi korban, peningkatan kapasitas aparat penegak hukum dalam digital forensics, serta penguatan peran lembaga non-yudisial seperti Kominfo dan LPSK. Selain itu, kampanye nasional mengenai literasi keamanan digital juga harus digalakkan agar masyarakat lebih waspada dan tahu cara bertindak saat menjadi korban kejahatan siber.

Dalam menghadapi kompleksitas kejahatan digital dan perlindungan bagi korbannya, diperlukan strategi yang bersifat menyeluruh dan berorientasi pada korban. Upaya pertama yang mendesak adalah penguatan regulasi, terutama dengan meninjau kembali Undang-Undang Informasi dan Transaksi Elektronik UU ITE agar tidak hanya fokus pada pemberian sanksi kepada pelaku, tetapi juga memberikan porsi yang cukup pada hak-hak korban, termasuk hak atas pemulihan, perlindungan data pribadi, serta akses terhadap keadilan. Selain itu, perlu adanya harmonisasi antara UU ITE dan KUHP agar perangkat hukum pidana mampu menjawab tantangan kejahatan digital yang terus berkembang. Di samping aspek normatif, peningkatan kapasitas aparat penegak hukum juga menjadi elemen penting. Aparat kepolisian dan kejaksaan harus dibekali pemahaman serta keterampilan dalam digital forensik agar mampu menangani bukti elektronik secara sah dan profesional. Tidak kalah penting adalah optimalisasi peran lembaga seperti LPSK, pos bantuan hukum, serta lembaga perlindungan lainnya dalam memberikan pendampingan hukum dan psikososial kepada korban. Strategi ini harus didukung oleh literasi digital dan edukasi hukum yang luas di masyarakat, agar pengguna internet memahami risiko digital serta prosedur hukum jika menjadi korban. Mengingat banyaknya kejahatan digital yang melibatkan pelaku lintas negara, kerja sama internasional juga perlu diperkuat, baik dalam bentuk perjanjian bantuan hukum timbal balik, pertukaran informasi, maupun partisipasi aktif dalam forum regional dan global. Seluruh strategi tersebut perlu dijalankan secara terpadu agar perlindungan hukum terhadap korban kejahatan digital tidak hanya bersifat formalistik, tetapi benar-benar menjadi instrumen keadilan substantif di era transformasi digital saat ini.

UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan UU No. 19 Tahun 2016, merupakan regulasi khusus yang mengatur aktivitas di ranah digital. Instrumen ini memuat ketentuan mengenai pelarangan konten ilegal Pasal 27–29, akses tanpa izin Pasal 30–32, serta

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

gangguan terhadap sistem elektronik. Dari perspektif korban, pengaturan ini memiliki potensi untuk melindungi hak-hak individu dari serangan digital seperti pencemaran nama baik, penyebaran data pribadi, peretasan akun, hingga penipuan daring. Namun, penerapannya sering kali lebih berorientasi pada penindakan terhadap pelaku dibanding pada pemulihan hak korban, terutama dalam hal restitusi, rehabilitasi psikologis, dan jaminan keadilan prosedural.

Di sisi lain, KUHP sebagai kodifikasi hukum pidana Indonesia masih belum mengatur secara eksplisit tentang kejahatan digital. Meskipun demikian, beberapa pasal di dalamnya tetap dapat dijadikan dasar pidana terhadap pelaku. Pasal 310 dan 311 KUHP tentang penghinaan dan fitnah, serta Pasal 378 tentang penipuan, sering kali dijadikan rujukan untuk menangani kasus yang berbasis media elektronik. Namun, kerangka hukum dalam KUHP ini lebih didesain untuk kejahatan konvensional dan belum sepenuhnya mampu mengakomodasi karakteristik kejahatan digital yang bersifat anonim, lintas batas, dan berbasis teknologi tinggi.

Salah satu tantangan utama dalam memberikan perlindungan hukum terhadap korban kejahatan digital adalah keterbatasan mekanisme pemulihan yang bersifat korban-sentris. Baik UU ITE maupun KUHP belum menyediakan pendekatan holistik yang mencakup aspek perlindungan data pribadi, trauma psikologis korban, serta akses yang mudah terhadap bantuan hukum. Dalam praktiknya, banyak korban yang enggan melapor karena tidak yakin akan efektivitas penanganan aparat atau khawatir mengalami reviktimisasi, terutama dalam kasus pencemaran nama baik atau penyebaran konten pribadi.

Dari sudut pandang hukum pidana progresif, perlindungan terhadap korban seharusnya tidak hanya dilihat dari keberhasilan menghukum pelaku, tetapi juga dari sejauh mana negara menjamin pemulihan menyeluruh terhadap korban. Dalam konteks ini, perlindungan hukum harus bersifat proaktif, responsif, dan adaptif terhadap perkembangan modus operandi kejahatan digital. Hal ini menuntut penguatan kebijakan hukum nasional, baik melalui revisi norma substantif, penyesuaian prosedur hukum acara, maupun penguatan lembaga pendukung seperti LPSK dan unit cyber crime di kepolisian.

Dengan demikian, meskipun UU ITE dan KUHP menyediakan dasar hukum bagi perlindungan korban, efektivitasnya sangat tergantung pada keberanian dan kecermatan para penegak hukum dalam menerapkan hukum dengan perspektif keadilan restoratif dan hak asasi manusia. Reformulasi hukum siber yang lebih komprehensif serta integrasi pendekatan victim-oriented dalam sistem peradilan pidana Indonesia menjadi kebutuhan mendesak di era digital saat ini.

KESIMPULAN DAN SARAN

Perkembangan teknologi informasi yang pesat telah melahirkan bentuk-bentuk kejahatan digital yang semakin kompleks dan sulit dilacak. Dalam konteks ini, korban kejahatan digital tidak hanya mengalami kerugian materiil, tetapi juga penderitaan psikologis dan sosial yang signifikan. Kajian ini menunjukkan bahwa meskipun Indonesia telah memiliki dua instrumen hukum utama—yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik UU ITE dan Kitab Undang-Undang Hukum Pidana KUHP perlindungan hukum terhadap korban masih bersifat terbatas dan belum komprehensif.

UU ITE lebih berfokus pada aspek penindakan terhadap pelaku, sementara hak-hak korban, seperti pemulihan, perlindungan identitas, bantuan psikososial, dan akses terhadap keadilan, belum diatur secara tegas. Bahkan dalam beberapa kasus, korban justru mengalami kriminalisasi ulang akibat multitafsir pasal-pasal tertentu, terutama terkait pencemaran nama baik. Di sisi lain, KUHP yang bersifat konvensional belum mampu mengakomodasi karakteristik khas kejahatan digital yang lintas batas, anonim, dan menggunakan teknologi tinggi.

Permasalahan ini diperparah oleh rendahnya literasi hukum dan digital di masyarakat, keterbatasan kapasitas teknis aparat penegak hukum dalam menangani bukti digital, serta minimnya sinergi antarlembaga dalam menangani kasus cybercrime. Kondisi tersebut menunjukkan adanya urgensi reformasi hukum pidana nasional agar lebih responsif terhadap dinamika kejahatan digital dan lebih berpihak pada korban.

Dengan demikian, diperlukan strategi menyeluruh berupa: reformulasi regulasi yang mengakomodasi hak-hak korban secara eksplisit, penguatan kapasitas aparat penegak hukum dalam bidang digital forensik, optimalisasi peran lembaga seperti LPSK, serta edukasi publik tentang hak-hak hukum dan keamanan digital. Perlindungan hukum yang berperspektif korban dan berbasis prinsip keadilan restoratif menjadi langkah krusial dalam memastikan bahwa sistem hukum Indonesia tidak hanya menghukum pelaku, tetapi juga menjamin keadilan dan pemulihan bagi korban kejahatan digital.

UCAPAN TERIMA KASIH

Dengan segala kerendahan hati, penulis menyampaikan apresiasi yang setinggi-tingginya kepada Dosen Pembimbing yang telah dengan penuh kesabaran dan ketekunan memberikan arahan, nasihat, serta kritik konstruktif selama proses penyusunan jurnal ini. Setiap bimbingan yang diberikan telah menjadi fondasi penting dalam membentuk landasan ilmiah dan sistematis dari karya ini.

Ucapan terima kasih juga penulis haturkan kepada para sahabat dan rekan seperjuangan atas dukungan moral, semangat, serta berbagai diskusi yang penuh makna selama proses penelitian ini berlangsung. Kebersamaan dan kerja sama yang terjalin telah menjadi sumber kekuatan dalam menyelesaikan berbagai tantangan yang dihadapi. Akhir kata, penulis berharap karya ini dapat memberikan sumbangsih nyata bagi pengembangan ilmu pengetahuan, khususnya dalam ranah hukum dan etika digital di era modern ini.

DAFTAR PUSTAKA

Campolo, A., Sanfilippo, M., Whittaker, M., & Crawford, K. (2017). *AI Now 2017 Report*. AI Now Institute. https://ainowinstitute.org/AI_Now_2017_Report.pdf

Chesney, R., & Citron, D. K. (2020). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 99(1), 147–155.

Custers, B., & Keymolen, E. (2022). Artificial intelligence and the right to explanation: Three legal bases under the GDPR. *Computer Law & Security Review*, 44, Article 105634. https://doi.org/10.1016/j.clsr.2022.105634

Dechesne, F. (2020). Ethics of AI and robotics. In *The Stanford Encyclopedia of Philosophy* (Fall 2020 Edition). https://plato.stanford.edu/entries/ethics-ai/

Effendy, M. (2022). Tantangan penegakan hukum terhadap kejahatan siber. *Jurnal Hukum & Teknologi*, 7(1), 45–60.

Electronic Frontier Foundation. (2020). Deepfakes and synthetic media. https://www.eff.org

European Union. (2022). *Digital Services Act (DSA)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yale University Press.

Gunawan, A. (2020). Problematika pasal pencemaran nama baik dalam revisi UU ITE. *Jurnal Media Hukum Digital*, 2(1), 25–34.

ICC. (1998). *Rome Statute of the International Criminal Court*.

Jong, M., & O'Neill, B. (2023). Deepfake regulation in Europe: Assessing the gaps in the Digital Services Act. *Journal of Cyber Policy*, 8(1), 67–82. https://doi.org/10.1080/23738871.2023.2184123

Kementerian Komunikasi dan Informatika. (2022). *Panduan Perlindungan Data Pribadi*. https://kominfo.go.id

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

Lembaga Perlindungan Saksi dan Korban (LPSK). (2014). *UU No. 31 Tahun 2014 tentang Perubahan atas UU No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban*.

Maulana, R. (2023). Kesenjangan hukum terhadap deepfake di Indonesia. *Jurnal Informasi Digital*, 4(2), 89–102.

Marzuki, P. M. (2017). *Pengantar Ilmu Hukum*. Prenadamedia Group.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. https://doi.org/10.1177/2053951716679679

Muladi. (1995). *Hak Asasi Manusia, Politik, dan Sistem Peradilan Pidana*. Badan Penerbit UNDIP.

Nugroho, H., & Rachmadi, E. (2020). Kejahatan dunia maya dan regulasinya. *Jurnal Kriminologi Modern*, 4(1), 10–22.

Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. *Data & Society*. https://datasociety.net/library/deepfakes-and-cheap-fakes/

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press.

Rahardjo, S. (2000). *Ilmu Hukum*. Citra Aditya Bakti.

Schick, W., & Slotwinski, M. (2024). Algorithmic accountability and fairness in digital platforms: A legal perspective. *AI and Ethics*, 4(1), 23–38. https://doi.org/10.1007/s43681-023-00256-1

Soesilo, R. (2018). *Kitab Undang-Undang Hukum Pidana serta Komentar-Komentarnya*. Politeia.

United Nations. (1985). *Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*.

Jurnal Hukum dan Kewarganegaraan
Vol. 14, No. 12 (2025)
Prefix doi.org/10.3783/causa.v2i9.2461

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking*. Council of Europe. https://www.coe.int/en/web/freedom-expression/information-disorder

West, D. M. (2020). The rise of deepfakes: How disinformation threatens democracy and what can be done about it. *Brookings Institution*. https://www.brookings.edu

Westerlund, M. (2021). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 11(2), 39–52. https://doi.org/10.22215/timreview/1412