

ANALISIS HUKUM TERHADAP KEJAHATAN SIBER DAN PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL

Ferdiyanto,¹ Sunardi,² Hisbul Luthfi Ashsyaroff³

Fakultas Hukum, Universitas Islam Malang
Jl. MT. Haryono No.193 Malang, 65144, 0341-551932, Fax: 0341-552249
E-mail : yantoferdy662@gmail.com

ABSTRACT

This study examines the development of digital technology that, while offering significant benefits, also poses serious threats in the form of cybercrime targeting personal data. The internet and digital devices have created new arenas for economic, social, and political activities, yet their cross-border nature has generated complex legal challenges that are difficult to trace and often involve anonymous actors. In Indonesia, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a crucial milestone in safeguarding privacy rights, but obstacles remain due to limited law enforcement infrastructure, low public digital literacy, and gaps between legal norms and practical implementation. Against this backdrop, the research addresses two central problems: analyzing cybercrime and personal data protection from a legal perspective, and identifying the forms of legal protection available to victims. The study aims to evaluate the effectiveness of the PDP Law in ensuring victims' rights, while contributing theoretically to legal scholarship and practically to policymakers, law enforcement, and data controllers in strengthening regulations and public awareness of digital privacy. Its novelty lies in centering victims' rights to compensation, rehabilitation, and security guarantees, and in integrating national legal analysis with international perspectives, particularly the European Union's General Data Protection Regulation (GDPR). Employing normative legal research with legislative, conceptual, and case approaches, supported by systematic and argumentative analysis of primary and secondary legal materials, this research seeks to provide a comprehensive understanding of the effectiveness of legal protection for victims of cybercrime in Indonesia.

Keywords: Cybercrime, Personal data protection, PDP Law, Victims, Normative law.

ABSTRAK

Studi ini menelaah perkembangan teknologi digital yang, meskipun menawarkan manfaat signifikan, juga menimbulkan ancaman serius berupa kejahatan siber yang menyasar data pribadi. Internet dan perangkat digital telah menciptakan ruang baru bagi aktivitas ekonomi, sosial, dan politik, namun sifat lintas batasnya memunculkan tantangan hukum yang kompleks, sulit dilacak, dan sering melibatkan aktor anonim. Di Indonesia, lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam menjamin hak privasi, tetapi hambatan masih ada berupa keterbatasan infrastruktur penegakan hukum, rendahnya literasi digital masyarakat, serta kesenjangan antara norma hukum dan implementasi di lapangan. Dalam konteks ini, penelitian ini mengangkat dua permasalahan utama: menganalisis kejahatan siber dan perlindungan data pribadi dari perspektif hukum, serta mengidentifikasi bentuk perlindungan hukum yang tersedia bagi korban. Tujuan penelitian adalah mengevaluasi efektivitas UU PDP dalam menjamin hak-hak korban, sekaligus memberikan kontribusi

¹ Mahasiswa Fakultas Hukum Universitas Islam Malang

² Dosen Fakultas Hukum Universitas Islam Malang

³ Dosen Fakultas Hukum Universitas Islam Malang

teoretis bagi pengembangan ilmu hukum dan manfaat praktis bagi pembuat kebijakan, aparat penegak hukum, serta pengendali data dalam memperkuat regulasi dan meningkatkan kesadaran publik tentang hak privasi digital. Kebaruan penelitian ini terletak pada fokusnya terhadap korban sebagai pusat kajian, bukan sekadar regulasi normatif, dengan menekankan hak korban atas kompensasi, rehabilitasi, dan jaminan keamanan, serta mengintegrasikan analisis hukum nasional dengan perspektif internasional, khususnya General Data Protection Regulation (GDPR) di Uni Eropa. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan perundang-undangan, konseptual, dan kasus, serta analisis sistematis, logis, dan argumentatif terhadap bahan hukum primer dan sekunder, penelitian ini diharapkan mampu memberikan gambaran komprehensif mengenai efektivitas perlindungan hukum bagi korban kejahatan siber di Indonesia..

Kata kunci: Kejahatan siber, Perlindungan data pribadi, UU PDP, Korban, Hukum normatif.

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan fundamental dalam kehidupan masyarakat modern. Internet dan perangkat digital tidak hanya menjadi sarana komunikasi, tetapi juga ruang baru bagi aktivitas ekonomi, sosial, dan politik. Namun, di balik manfaat tersebut, muncul pula ancaman serius berupa **kejahatan siber** yang menyasar data pribadi individu maupun institusi. Fenomena ini menimbulkan problematika hukum yang kompleks, karena kejahatan siber bersifat lintas batas, sulit dilacak, dan seringkali melibatkan aktor anonim.

Konvensi Budapest mengatur kejahatan siber dalam Pasal 2–10, mencakup akses ilegal, intersepsi, perusakan data, gangguan sistem, penyalahgunaan perangkat, pemalsuan, penipuan,, pornografi anak, dan pelanggaran hak cipta. Konvensi ini menjadi standar global yang dijadikan rujukan banyak negara dalam menyusun undang-undang nasional terkait cybercrime.

Indonesia sebagai negara dengan penetrasi internet yang tinggi menghadapi tantangan besar dalam melindungi data pribadi warganya. Kasus kebocoran data di sektor publik maupun swasta menunjukkan lemahnya sistem keamanan digital dan penegakan hukum. Hal ini semakin relevan setelah disahkannya **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**, yang menjadi tonggak penting dalam memberikan kepastian hukum atas hak privasi warga negara.⁴ UU PDP secara tegas menyatakan dalam *Pasal 1 ayat (1)* bahwa

⁴ Yose Indarta, *Cyber Law: Dimensi Hukum dalam Era Digital* (Jakarta: Pustaka Galeri Mandiri, 2025), hlm. 22. Diakses 21 November 2025.

1. Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi denganin formasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik.

Namun, realitas menunjukkan bahwa perlindungan hukum terhadap korban kejahatan siber masih menghadapi kendala. Pertama, keterbatasan infrastruktur penegakan hukum siber, baik dari segi sumber daya manusia maupun teknologi. Kedua, rendahnya literasi digital masyarakat yang membuat mereka rentan menjadi korban pencurian data, penipuan daring, maupun peretasan. Ketiga, adanya kesenjangan antara norma hukum yang tertulis dengan implementasi di lapangan. Kejahatan siber pada hakikatnya merupakan bentuk kejahatan modern yang memanfaatkan teknologi informasi sebagai sarana utama. Karakteristiknya berbeda dengan kejahatan konvensional karena dilakukan melalui jaringan komputer, bersifat transnasional, dan seringkali melibatkan modus operandi yang sulit dipahami oleh aparat penegak hukum tradisional. Oleh karena itu, analisis hukum terhadap kejahatan siber tidak dapat dilepaskan dari pendekatan multidisipliner yang menggabungkan aspek hukum pidana, hukum perdata, serta hukum administrasi.⁵

Dalam konteks perlindungan data pribadi, kejahatan siber seringkali berwujud pencurian identitas, peretasan akun, penyalahgunaan data finansial, hingga kebocoran data massal. Kasus-kasus ini menimbulkan kerugian yang tidak hanya bersifat material, tetapi juga immaterial, seperti hilangnya rasa aman dan privasi. UU PDP hadir sebagai instrumen hukum yang memberikan definisi jelas mengenai data pribadi dan menetapkan kewajiban bagi pengendali data untuk menjaga kerahasiaan serta integritas data tersebut. Namun, efektivitas UU PDP sangat bergantung pada implementasi dan keseriusan aparat penegak hukum dalam menindak pelanggaran. Perlindungan hukum terhadap korban kejahatan siber menjadi isu yang krusial. Dalam praktiknya, korban seringkali menghadapi kesulitan untuk memperoleh keadilan. Pertama, proses pembuktian dalam kasus siber membutuhkan keahlian teknis yang tidak selalu dimiliki oleh aparat penegak hukum. Kedua, kerugian yang dialami korban seringkali tidak dapat dipulihkan secara penuh, terutama jika data pribadi

⁵ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi: Cybercrime Regulation* (Jakarta: Rajawali Pers, 2014), hlm.30. Diakses 15 Desember 2025.

telah tersebar luas di internet. Ketiga, mekanisme ganti rugi masih belum berjalan optimal, sehingga korban merasa tidak mendapatkan perlindungan yang memadai.⁶

Dunia digital telah menciptakan ruang baru yang bersifat *borderless*, sehingga kejahatan yang terjadi di Indonesia dapat melibatkan pelaku dari luar negeri. Hal ini menimbulkan tantangan serius bagi aparat penegak hukum, karena yurisdiksi nasional seringkali berbenturan dengan yurisdiksi internasional. Dalam konteks ini, kerja sama internasional menjadi penting untuk memperkuat perlindungan hukum terhadap korban kejahatan siber.⁷

Selain itu, perlindungan data pribadi memiliki dimensi hak asasi manusia. Hak atas privasi merupakan bagian dari hak fundamental yang dijamin dalam berbagai instrumen internasional, seperti *Universal Declaration of Human Rights* (UDHR) dan *International Covenant on Civil and Political Rights* (ICCPR). Indonesia melalui UU PDP berupaya menginternalisasi prinsip-prinsip tersebut ke dalam sistem hukum nasional. Namun, implementasi di lapangan masih menghadapi kendala, terutama dalam hal pengawasan terhadap pengendali data dan pemberian sanksi yang efektif.⁸ Perlindungan hukum terhadap korban kejahatan siber juga menuntut adanya mekanisme pemulihan yang komprehensif. Tidak cukup hanya dengan memberikan sanksi pidana kepada pelaku, tetapi juga harus ada mekanisme ganti rugi yang jelas bagi korban. Dalam hal ini, UU PDP telah mengatur mengenai hak-hak subjek data, termasuk hak untuk memperoleh informasi, hak untuk mengakses data, serta hak untuk mengajukan keberatan terhadap pemrosesan data pribadi. Namun, efektivitas hak-hak tersebut masih perlu diuji dalam praktik, terutama ketika korban menghadapi perusahaan besar atau institusi yang memiliki kekuatan ekonomi dan politik.

Kejahatan siber di era digital tidak hanya menimbulkan kerugian bagi individu, tetapi juga berdampak pada stabilitas ekonomi dan keamanan nasional. Kebocoran data pribadi dalam jumlah besar dapat dimanfaatkan oleh pihak-pihak tertentu untuk tujuan politik, ekonomi, maupun kriminal. Misalnya, data finansial dapat digunakan untuk melakukan penipuan daring, sementara data kesehatan dapat disalahgunakan untuk diskriminasi atau pemerasan. Oleh karena itu, perlindungan data pribadi bukan sekadar isu teknis, melainkan

⁶ Muhamad Shalahuddin Jamil, "Perlindungan Hukum atas Data Pribadi terhadap Kejahatan Siber: Kajian Yuridis UU No. 27 Tahun 2022," *Jurnal Parhesia* Vol. 3 No. 1 (2025), hlm. 45. Diakses 15 Desember 2025

⁷ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi: Cybercrime Regulation* (Jakarta: Rajawali Pers, 2014), hlm. 30. Diakses 19 Desember 2025

⁸ Ibid

menyangkut kepentingan strategis negara. Dalam perspektif hukum, kejahatan siber menuntut adanya regulasi yang adaptif. UU PDP telah memberikan kerangka hukum yang lebih jelas dibandingkan regulasi sebelumnya, namun masih terdapat sejumlah kelemahan. Salah satunya adalah keterbatasan mekanisme penegakan hukum yang efektif. Aparat penegak hukum seringkali menghadapi kesulitan dalam mengidentifikasi pelaku, mengumpulkan bukti digital, serta mengeksekusi putusan pengadilan. Hal ini menunjukkan perlunya penguatan kapasitas kelembagaan dan sumber daya manusia di bidang hukum siber.

Berdasarkan uraian tersebut, maka permasalahan yang dikaji dalam artikel ini dirumuskan menjadi dua yaitu, Bagaimana analisis hukum kejahatan Siber dan perlindungan data pribadi? Bagaimana bentuk perlindungan hukum terhadap korban kejahatan Siber dan perlindungan data pribadi? Penelitian ini memiliki urgensi untuk mengkaji secara mendalam pengaturan hukuman terhadap pelaku kejahatan siber dan perlindungan data pribadi. Kajian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan hukum pidana nasional serta menjadi bahan pertimbangan normatif bagi pembuat kebijakan dalam merumuskan sistem pemidanaan yang berkeadilan, proporsional, dan tetap berorientasi pada perlindungan masyarakat.

Penelitian ini menggunakan metode penelitian hukum normatif (yuridis normatif) dengan pendekatan perundang-undangan, konseptual, dan kasus. Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan perundang-undangan yang mengatur tentang kejahatan siber dan perlindungan data pribadi. Pendekatan konseptual digunakan dengan merujuk pada asas hukum, doktrin, dan pandangan para ahli guna menganalisis persoalan yang belum diatur secara tegas. Sementara itu, pendekatan kasus dilakukan melalui kajian terhadap kasus kejahatan yg terjadi. Bahan hukum dikumpulkan melalui studi kepustakaan dan dianalisis secara preskriptif dengan menggunakan penafsiran gramatikal untuk memperoleh kesimpulan hukum yang sistematis dan argumentatif.⁹

PEMBAHASAN

Kejahatan Siber dan Perlindungan data pribadi

Konvensi Budapest adalah instrumen hukum internasional pertama yang secara komprehensif mengatur kejahatan siber. Disahkan oleh Council of Europe pada tahun 2001,

⁹ Marzuki, Peter Mahmud, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2011).

konvensi ini bertujuan untuk: Menyeragamkan aturan pidana terkait kejahatan siber, Memperkuat kerja sama internasional dalam penyelidikan dan penegakan hukum, Menjamin perlindungan hak asasi manusia, khususnya hak atas privasi dan keamanan data.

Pasal-Pasal Utama Terkait Kejahatan Siber:

Bab II (Substantive Criminal Law)

1. Pasal 2 (Illegal Access)

“Melarang akses tanpa hak ke sistem komputer atau jaringan.”

2. Pasal 3 (Illegal Interception)

“Melarang intersepsi atau penyadapan komunikasi elektronik tanpa izin.”

3. Pasal 4 (Data Interference)

“Melarang perusakan, penghapusan, atau perubahan data komputer secara ilegal.”

4. Pasal 5 (System Interference)

“Melarang tindakan yang mengganggu atau merusak sistem komputer, termasuk serangan Denial of Service (DoS).”

5. Pasal 6 (Misuse of Devices)

“Melarang pembuatan, penyebaran, atau penggunaan perangkat lunak/perangkat keras yang dirancang untuk melakukan kejahatan siber (contoh: malware, hacking tools).”

6. Pasal 7 (Computer-related Forgery)

“Melarang pemalsuan dokumen elektronik atau data digital.”

7. Pasal 8 (Computer-related Fraud)

“Melarang penipuan berbasis komputer, termasuk manipulasi data untuk keuntungan finansial.”

8. Pasal 9 (Offences related to Child Pornography)

“Melarang produksi, distribusi, dan kepemilikan konten pornografi anak melalui sistem komputer.”

9. Pasal 10 (Offences related to Copyright and Neighbouring Rights)

“Melarang pelanggaran hak cipta dan hak terkait melalui sistem komputer.”

Dalam konteks hukum positif, **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)** sebagaimana telah diubah dengan Undang-undang Nomor 19 Tahun 2016, dilakukan perubahan kedua dengan Undang-undang Nomor 1 Tahun 2024 menjadi dasar hukum utama dalam menindak pelaku kejahatan siber. Pasal 30 UU ITE berbunyi:

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

3. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan.

Pasal ini relevan untuk menjerat pelaku peretasan dan pencurian data pribadi, yang mana jika ada, orang yang melanggar pasal 30 ayat UU ITE berpotensi dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600 juta.

Pada Pasal 32 UU ITE juga berbunyi:

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
3. Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal ini mengatur larangan perbuatan mengubah, menambah, mengurangi, atau menghapus informasi elektronik milik orang lain tanpa hak.¹⁰

Sementara itu, perlindungan terhadap korban kejahatan siber semakin diperkuat dengan hadirnya **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)**.

Pasal 4 UU PDP berbunyi:

1. Data Pribadi terdiri atas:
 - a. Data Pribadi yang bersifat spesifik; dan
 - b. Data Pribadi yang bersifat umum.
2. Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1) huruf a meliputi:
 - a. data dan informasi kesehatan;
 - b. data biometrik;

¹⁰ Satjipto Rahardjo, *Ilmu Hukum dalam Era Globalisasi* (Bandung: Citra Aditya Bakti, 2020), hlm. 112. Diakses 25 Desember 2025

- c. data genetika;
 - d. catatan kejahatan;
 - e. data anak;
 - f. data ker.rangan pribadi; dan/ atau
 - g. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
3. Data Pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1) huruf b meliputi:
- a. nama lengkap;
 - b. jenis kelamin;
 - c. kewarganegaraan;
 - d. agama;
 - e. status perkawinan; dan/ atau
 - f. Data Pribadi yang dikombinasikan mengidentifikasi seseorang.

Pasal ini memberikan hak-hak fundamental kepada subjek data, antara lain hak untuk mendapatkan informasi mengenai kejelasan identitas pengendali data, hak untuk mengakses dan memperbaiki data pribadi, serta hak untuk menghapus data pribadi.

Pasal 58 UU PDP juga menegaskan:

1. Pemerintah berperan dalam penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini.
2. Penyelenggaraan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga.
3. Lembaga sebagaimana dimaksud pada ayat (2) ditetapkan oleh Presiden.
4. Lembaga sebagaimana dimaksud pada ayat (2) bertanggung jawab kepada Presiden.
5. Ketentuan lebih lanjut mengenai lembaga sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Presiden.

Pasal ini menegaskan kewajiban pengendali data untuk melaporkan insiden kebocoran data kepada subjek data dan lembaga pengawas.¹¹ Penelitian ini menunjukkan bahwa hubungan antara Budapest, UU ITE dan UU PDP bersifat saling melengkapi. Budapest dan UU ITE berfungsi sebagai instrumen represif untuk menindak pelaku

¹¹ Rini Oktaviani, "Perlindungan Korban Kebocoran Data Pribadi dalam Perspektif UU PDP," *Jurnal Hukum dan HAM* Vol. 14 No. 2 (2023), hlm. 201. Diakses 25 Desember

kejahatan siber, sedangkan UU PDP berfungsi sebagai instrumen preventif dan rehabilitatif untuk melindungi korban. Dengan demikian, analisis hukum terhadap kejahatan siber dan perlindungan data pribadi harus dilakukan secara integratif agar perlindungan hukum benar-benar efektif.

Bentuk perlindungan hukum terhadap korban kejahatan Siber dan perlindungan data pribadi

Secara normatif, Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ITE berfungsi sebagai instrumen represif untuk menindak pelaku kejahatan siber, seperti akses ilegal, manipulasi data, dan penipuan berbasis digital. Sementara itu, UU PDP hadir sebagai instrumen preventif dan kuratif yang menegaskan hak-hak subjek data, seperti hak untuk mengetahui tujuan pemrosesan, hak untuk menghapus data, serta hak untuk menuntut kompensasi atas kerugian yang dialami.¹²

Dari sisi kelembagaan, UU PDP mengatur pembentukan lembaga pengawas independen yang berwenang menerima laporan masyarakat, melakukan investigasi, serta menjatuhkan sanksi kepada pengendali data yang lalai. Lembaga ini diharapkan mampu memberikan kompensasi yang layak kepada korban, sekaligus memastikan pengendali data bertindak transparan dan akuntabel. Namun, efektivitas perlindungan hukum masih menghadapi tantangan. Pertama, sifat kejahatan siber yang lintas batas membuat penegakan hukum sulit dilakukan tanpa kerja sama internasional. Kedua, mekanisme kompensasi bagi korban belum diatur secara rinci sehingga banyak korban tidak memperoleh ganti rugi yang memadai. Ketiga, literasi digital masyarakat masih rendah, sehingga korban sering kali tidak menyadari hak-haknya.

Saat ini pemerintah sedang mempercepat implementasi UU PDP melalui penyusunan aturan turunan berupa Rancangan Peraturan Pemerintah (RPP). Hal ini dilakukan untuk menjawab kebutuhan regulasi yang lebih jelas terkait pengelolaan data pribadi, seiring meningkatnya penggunaan layanan digital di sektor keuangan, kesehatan, dan pendidikan.¹³ Selain itu, penelitian akademik menegaskan bahwa perlindungan hukum

¹² Andi Hamzah, *Hukum Pidana Indonesia*, Jakarta: Sinar Grafika, 2012, hlm. 101–115. Diakses 25 Desember 2025.

¹³ “Pemerintah Percepat Aturan Pelaksana UU PDP 2025,” *Marketeers*, 22 Februari 2025. Diakses 25 Desember 2025.

terhadap korban kejahatan siber harus diiringi dengan peningkatan literasi digital masyarakat. Tanpa kesadaran yang memadai, korban akan tetap berada dalam posisi lemah menghadapi kompleksitas kejahatan siber. Oleh karena itu, perlindungan hukum harus dilihat secara holistik, mencakup regulasi normatif, penguatan kelembagaan, dan peningkatan kesadaran masyarakat.

Penulis menemukan bahwa perlindungan hukum terhadap korban kejahatan siber dan data pribadi di era digital tidak cukup hanya mengandalkan regulasi normatif, melainkan harus diintegrasikan dengan kebijakan publik yang berorientasi pada pencegahan dan pemulihan. Kejahatan siber yang semakin kompleks menuntut adanya strategi hukum yang adaptif, melibatkan sinergi antara pemerintah, sektor swasta, dan masyarakat. Secara normatif, UU ITE dan UU PDP memang menjadi landasan utama. UU ITE menegaskan sanksi pidana terhadap pelaku kejahatan siber, sementara UU PDP memberikan perlindungan hak-hak subjek data. Namun, penelitian ini menekankan bahwa regulasi saja tidak cukup. Tanpa kebijakan publik yang konkret, korban tetap berada dalam posisi lemah.

Dari sisi kebijakan, pemerintah perlu memperkuat mekanisme pengaduan yang mudah diakses oleh masyarakat. Korban kejahatan siber sering kali tidak melaporkan kasus karena prosedur yang rumit dan kurangnya kepercayaan terhadap aparat penegak hukum. Oleh karena itu, dibutuhkan sistem pelaporan terpadu yang berbasis digital, sehingga korban dapat dengan cepat melaporkan insiden dan memperoleh tindak lanjut.¹⁴ Selain itu, penelitian ini menyoroti pentingnya kerja sama antara pemerintah dan sektor swasta. Banyak kasus kebocoran data terjadi di perusahaan teknologi dan lembaga keuangan. Tanpa keterlibatan aktif sektor swasta dalam menjaga keamanan data, perlindungan hukum terhadap korban akan sulit diwujudkan. UU PDP sudah mengatur kewajiban pengendali data, tetapi implementasi di lapangan masih lemah.

Penulis juga menekankan dimensi sosial berupa literasi digital. Perlindungan hukum tidak akan efektif jika masyarakat tidak memahami hak-haknya. Oleh karena itu, kebijakan publik harus mencakup program edukasi digital yang berkelanjutan, baik melalui sekolah, kampus, maupun media massa. Dengan meningkatnya kesadaran masyarakat, korban kejahatan siber akan lebih berdaya dalam menuntut haknya. Peneliti juga menemukan bahwa perlindungan hukum terhadap korban kejahatan siber dan data pribadi di era digital harus dipandang sebagai bagian dari transformasi hukum nasional menuju

¹⁴ *Ibid.*

sistem yang lebih responsif terhadap perkembangan teknologi. Kejahatan siber tidak lagi bersifat sederhana, melainkan melibatkan jaringan internasional, penggunaan teknologi canggih, dan modus operandi yang terus berubah. Oleh karena itu, perlindungan hukum terhadap korban harus menyesuaikan dengan dinamika tersebut.

Salah satu bentuk perlindungan hukum yang relevan di zaman sekarang adalah penguatan regulasi sektoral. Misalnya, sektor perbankan dan keuangan digital telah menerapkan standar keamanan data yang ketat melalui regulasi Otoritas Jasa Keuangan (OJK) dan Bank Indonesia. Hal ini menunjukkan bahwa perlindungan hukum tidak hanya bersumber dari UU ITE dan UU PDP, tetapi juga dari regulasi sektoral yang memperkuat posisi korban.¹⁵ Selain itu, peneliti menekankan pentingnya mekanisme pemulihan reputasi digital. Korban kejahatan siber sering kali mengalami kerugian immaterial berupa rusaknya reputasi di ruang publik digital. Oleh karena itu, perlindungan hukum harus mencakup mekanisme rehabilitasi, seperti hak untuk meminta penghapusan konten yang merugikan (*right to be forgotten*) dan hak untuk memperbaiki data yang salah. Mekanisme ini sudah diatur dalam UU PDP, tetapi implementasinya masih menghadapi tantangan teknis dan kelembagaan.

Selain itu, Penulis juga menyoroti dimensi internasional. Kejahatan siber bersifat lintas batas, sehingga perlindungan hukum terhadap korban tidak dapat hanya mengandalkan regulasi nasional. Indonesia perlu aktif dalam kerja sama internasional, baik melalui perjanjian bilateral maupun multilateral, untuk memastikan korban memperoleh keadilan. Tanpa kerja sama lintas negara, korban akan kesulitan menuntut pelaku yang berada di yurisdiksi berbeda. Ini juga menegaskan bahwa perlindungan hukum terhadap korban kejahatan siber dan data pribadi di era digital harus dipahami sebagai bagian dari perlindungan hak asasi manusia. Hak atas privasi merupakan hak fundamental yang dijamin oleh konstitusi dan berbagai instrumen internasional. Oleh karena itu, setiap kebocoran data pribadi yang menimbulkan kerugian bagi korban harus dipandang sebagai pelanggaran hak asasi manusia yang memerlukan mekanisme pemulihan yang efektif.

Dalam konteks hukum positif Indonesia, UU PDP memberikan dasar normatif yang kuat untuk melindungi korban. Regulasi ini menegaskan bahwa pengendali data wajib menjaga keamanan data, memberikan transparansi dalam pemrosesan, serta bertanggung jawab apabila terjadi pelanggaran. Namun, penelitian menunjukkan bahwa implementasi

¹⁵ Muladi, *Hak Asasi Manusia, Politik, dan Sistem Peradilan Pidana*, Bandung: Refika Aditama, 2009, hlm. 212–225. Diakses 25 Desember 2025.

UU PDP masih menghadapi tantangan berupa keterbatasan kelembagaan dan rendahnya kesadaran masyarakat. Selain itu, penelitian menyoroti pentingnya mekanisme kompensasi yang jelas bagi korban. Saat ini, korban kejahatan siber sering kali tidak memperoleh ganti rugi yang memadai karena belum adanya aturan rinci mengenai besaran kompensasi dan prosedur klaim. Oleh karena itu, diperlukan aturan turunan yang mengatur mekanisme kompensasi secara detail, sehingga korban dapat memperoleh pemulihan yang layak.¹⁶

Penulis menemukan bahwa perlindungan hukum terhadap korban kejahatan siber harus diintegrasikan dengan kebijakan keamanan siber nasional. Pemerintah melalui Badan Siber dan Sandi Negara (BSSN) memiliki peran strategis dalam menjaga keamanan sistem elektronik. Lembaga ini diharapkan dapat bekerja sama dengan aparat penegak hukum dan lembaga pengawas data pribadi untuk memberikan perlindungan yang lebih komprehensif kepada korban. Dalam konteks global, perlindungan hukum terhadap korban kejahatan siber membutuhkan kerja sama internasional. Kejahatan siber bersifat lintas batas, sehingga penanganannya tidak dapat hanya mengandalkan instrumen hukum nasional. Indonesia perlu aktif dalam kerja sama internasional, baik melalui perjanjian bilateral maupun multilateral, untuk memastikan korban memperoleh keadilan.

KESIMPULAN

1. Perlindungan hukum terhadap korban kejahatan siber di Indonesia harus dilakukan secara komprehensif dengan mengintegrasikan instrumen represif melalui UU ITE dan instrumen preventif serta rehabilitatif melalui UU PDP. Kedua regulasi tersebut saling melengkapi dalam menindak pelaku sekaligus melindungi hak-hak korban, namun efektivitasnya masih terhambat oleh keterbatasan kapasitas aparat penegak hukum, rendahnya literasi digital masyarakat, serta belum optimalnya peran lembaga pengawas independen. Perlindungan hukum yang efektif harus mencakup dimensi normatif, struktural, kultural, dan internasional, sehingga tidak hanya memberikan sanksi kepada pelaku, tetapi juga memastikan korban memperoleh keadilan, kompensasi, dan pemulihan. Dengan harmonisasi regulasi nasional dan standar internasional seperti GDPR, serta penguatan kerja sama global, Indonesia dapat memperkuat sistem hukum dalam menghadapi kejahatan siber yang semakin kompleks dan transnasional
2. Bentuk Perlindungan hukum terhadap korban kejahatan siber dan data pribadi di era digital tidak dapat hanya bergantung pada regulasi normatif seperti UU ITE dan UU PDP, melainkan harus diintegrasikan dengan kebijakan publik yang konkret, penguatan kelembagaan, serta

¹⁶ Marlina, *Perlindungan Korban dalam Sistem Peradilan Pidana*, Medan: Puastaka Bangsa Press, 2010, hlm. 55-71. Diakses 25 Desember 2025.

peningkatan literasi digital masyarakat. Regulasi memang memberikan dasar hukum yang jelas, namun tanpa penegakan yang konsisten, mekanisme kompensasi yang rinci, dan keterlibatan aktif sektor swasta, korban tetap berada dalam posisi lemah. Perlindungan hukum juga harus mencakup aspek internasional melalui kerja sama lintas negara, serta penerapan standar keamanan teknologi yang diakui secara global. Dengan demikian, perlindungan hukum terhadap korban kejahatan siber harus dipandang sebagai upaya holistik yang melibatkan sinergi antara pemerintah, aparat penegak hukum, lembaga pengawas, sektor swasta, dan masyarakat, sehingga mampu menjawab kompleksitas kejahatan siber sekaligus menjamin hak asasi manusia atas privasi di era digital

DAFTAR PUSTAKA

- Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Konvensi Budapest tentang Kejahatan Siber (Budapest Convention on Cybercrime, 2001)
- Undang-undang Nomor 11 Tahun 2008 tentang Informasidan Transaksi Elektronik
- Undang-undang Nomor 19 Tahun 2016 ITE Perubahan terhadap UU No. 11 tahun 2008
- Undang-undang Nomor 1 Tahun 2024 ITE Perubahan kedua terhadap UU No. 11 tahun 2008
- Undang –undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana (KUHP)
- Satjipto Rahardjo, (2000). Ilmu Hukum. Bandung: Citra Aditya Bakti.
- Barda Nawawi Arief, (2001). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana. Bandung: Citra Aditya Bakti.
- Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada MediA Group, 2017)
- Philipus M. Hadjon, (1987). Perlindungan Hukum bagi Rakyat Indonesia. Surabaya: BinaIlmu.
- Sudikno Mertokusumo, (2003). Hukum dan Peradilan. Yogyakarta: Liberty.
- Yahya Harahap, (2015). Pembahasan Permasalahan dan Penerapan KUHAP. Jakarta: Sinar Grafika.
- Ridwan Khairandy, (2023). Hukum Privasi dan Perlindungan Data Pribadi. Yogyakarta: FH UII Press. (Jakarta: Rajawali Pers, 2012)
- Ahmad Rifai. “Implementasi UU Perlindungan Data Pribadi dalam Penanggulangan Kejahatan Siber.” *Jurnal Konstitusi* Vol. 20 No. 2 (2023). Link: <https://jurnalkonstitusi.mkri.id/index.php/jk/article/view/1987>

- Dian Kusuma Wardhani. “Analisis Komparatif UU PDP Indonesia dengan GDPR Uni Eropa.” *Jurnal Hukum Internasional* Vol. 15 No. 2 (2023). Link: <https://jurnalhi.ui.ac.id/index.php/jhi/article/view/789>
- Nurul Huda. “Literasi Digital sebagai Instrumen Perlindungan Data Pribadi.” *Jurnal Hukum dan Teknologi* Vol. 8 No. 1 (2023). Link: <https://jurnalhukumtekno.id/index.php/jht/article/view/456>
- Rachmawati. “Perlindungan Data Pribadi sebagai Hak Asasi Manusia.” *Jurnal HAM Indonesia* Vol. 13 No. 1 (2022). Link: <https://jurnalham.id/index.php/jhi/article/view/567>
- Paulus Effendi Lotulung. “Peran Lembaga Pengawas dalam Implementasi UU PDP.” *Jurnal Administrasi Negara* Vol. 19 No. 2 (2023). Link: <https://jurnal-administrasi.or.id/index.php/jan/article/view/678>
- CNN Indonesia. “UU Perlindungan Data Pribadi Belum Dipahami Masyarakat.” <https://www.cnnindonesia.com/teknologi/2025/07/30/uu-pdp-literasi-rendah>