Legal Note
Vol. 1 No. 1, July 2025, pages: 26-30
e-ISSN XXXX-XXXX | DOI: https://doi.org/10.70716/legalnote.v1i1.24

Tinjauan Yuridis Terhadap Kejahatan Siber dan Perlindungan Data Pribadi

David Tendean [*1], William Susanto [1]
[1] Program Studi Ilmu Hukum, Universitas Hasanuddin, Makassar, Indonesia
**Corresponding Author: skylark101@gmail.com*

Article History

Manuscript submitted:
June 11, 2025
Manuscript revised:
July 17, 2025
Accepted for publication:
July 25, 2025

Keywords

Cybercrime;
Personal Data;
Legal Protection;
ITE Law;
PDP Law;

Abstract

The rapid development of information and communication technology has had a significant impact on global society, including in Indonesia. Behind the benefits it offers, this digital transformation also presents serious risks in the form of cybercrime, one of which is the violation of personal data. Crimes such as identity theft, account hacking, and the unauthorized dissemination of personal information have become increasingly prevalent threats. This indicates that the protection of personal data is becoming more crucial, both from technical and legal perspectives. This study aims to normatively examine the forms of cybercrime related to personal data breaches and the effectiveness of existing regulations in providing legal protection. The research is conducted using a normative juridical approach by analyzing relevant legislation, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The analysis shows that although there is a legal basis in place, its implementation still faces several challenges, including weak law enforcement, inadequate digital infrastructure, and low public awareness regarding the importance of protecting data privacy. Considering the complexity of the issues and the highly dynamic technological developments, this study recommends the need for the refinement of national legal policies to be more adaptive and progressive. Synergy among institutions, strengthening the capacity of law enforcement in digital forensics, and increasing public digital literacy are strategic steps toward building a robust and equitable personal data protection system. Only through a comprehensive and responsive legal approach that keeps pace with the times can the security of personal data in the digital realm be effectively ensured.

Copyright © 2025, The Author(s)
This is an open access article under the CC BY-SA license

How to Cite: Tendean, D., & Susanto, W. (2025). Tinjauan Yuridis Terhadap Kejahatan Siber dan Perlindungan Data Pribadi. *Legal Note, 1*(1), 19-24. https://doi.org/10.70716/legalnote.v1i1.24

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) telah memberikan transformasi besar terhadap cara manusia berinteraksi, bekerja, dan mengakses informasi. Di era digital saat ini, hampir seluruh aktivitas masyarakat—baik sosial, ekonomi, maupun pemerintahan—berlangsung dalam ruang siber yang mengandalkan pertukaran data secara cepat dan masif (Suryanto, 2021). Kemajuan ini membawa manfaat luar biasa, seperti efisiensi layanan publik, kemudahan transaksi daring, hingga

kemunculan ekonomi digital yang inklusif. Namun, perkembangan teknologi juga membawa dampak negatif, salah satunya adalah meningkatnya kejahatan siber (cybercrime), termasuk kejahatan yang melibatkan pelanggaran terhadap data pribadi. Fenomena ini menunjukkan adanya ketidakseimbangan antara akselerasi teknologi dan kesiapan regulasi hukum dalam melindungi hak-hak warga negara.

Kejahatan siber telah berevolusi menjadi bentuk-bentuk baru yang kompleks dan sulit diidentifikasi dengan pendekatan hukum konvensional. Di antara jenis kejahatan siber yang paling mengkhawatirkan adalah pencurian identitas digital, peretasan akun pribadi, penyebaran data pribadi tanpa izin, dan eksploitasi data untuk kepentingan komersial atau kejahatan lainnya (Yulianto, 2019). Data pribadi yang seharusnya bersifat rahasia kini menjadi komoditas yang diperjualbelikan secara ilegal melalui jaringan gelap. Kasus kebocoran data di berbagai platform digital membuktikan bahwa perlindungan terhadap data pribadi masih sangat lemah, bahkan di era ketika data menjadi aset paling berharga dalam infrastruktur digital global.

Di Indonesia, kasus-kasus pelanggaran data pribadi terus meningkat setiap tahunnya. Sejumlah insiden kebocoran data berskala besar yang melibatkan instansi publik dan swasta telah menimbulkan kekhawatiran serius terkait lemahnya sistem keamanan siber dan ketidaksiapan hukum dalam merespons tantangan ini (Rahmawati, 2022). Hal ini diperburuk oleh rendahnya kesadaran masyarakat terhadap pentingnya menjaga kerahasiaan data pribadi mereka di ruang digital. Banyak individu tidak menyadari konsekuensi dari berbagi informasi pribadi secara sembarangan di media sosial atau aplikasi daring lainnya, sehingga memperbesar risiko eksploitasi data oleh pihak-pihak yang tidak bertanggung jawab.

Secara yuridis, Indonesia telah memiliki beberapa regulasi yang berfungsi sebagai payung hukum untuk menanggulangi kejahatan siber dan melindungi data pribadi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta perubahannya, menjadi salah satu dasar hukum pertama yang mengatur aktivitas digital, termasuk kejahatan siber. Namun demikian, pengaturan perlindungan data pribadi dalam UU ITE masih bersifat umum dan belum memberikan kepastian hukum yang kuat bagi individu sebagai subjek data (Simanjuntak, 2018). Oleh karena itu, kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP) Tahun 2022 menjadi tonggak penting dalam penguatan hak privasi warga negara dan perlindungan hukum atas data pribadi.

UU PDP memberikan definisi yang lebih jelas mengenai data pribadi, hak-hak subjek data, serta kewajiban bagi pengendali dan pemroses data untuk menjaga keamanan informasi yang dikumpulkan, disimpan, dan digunakan (Kementerian Kominfo, 2022). Undang-undang ini juga mengatur mekanisme penyelesaian sengketa dan sanksi bagi pelanggaran, baik dalam bentuk administratif maupun pidana. Namun, keberhasilan UU PDP dalam memberikan perlindungan nyata sangat bergantung pada efektivitas implementasinya di lapangan. Dalam praktiknya, penegakan hukum terhadap pelanggaran data pribadi masih menghadapi hambatan, seperti lemahnya kapasitas aparat penegak hukum dalam menangani kasus berbasis digital dan kurangnya koordinasi antar lembaga (Nurhadi, 2023).

Tantangan lainnya adalah soal kesiapan infrastruktur digital dan budaya hukum masyarakat. Dalam banyak kasus, korban kejahatan siber tidak melaporkan pelanggaran yang mereka alami karena ketidaktahuan atau ketidakpercayaan terhadap proses hukum yang ada (Panjaitan, 2020). Di sisi lain, aparat penegak hukum juga kerap mengalami kesulitan dalam menelusuri pelaku kejahatan digital yang umumnya bekerja lintas negara dan menggunakan teknik penyamaran yang canggih. Kondisi ini menunjukkan bahwa pendekatan hukum yang digunakan harus bersifat multidisipliner, tidak hanya mengandalkan instrumen legal, tetapi juga melibatkan teknologi, edukasi publik, dan kerja sama internasional.

Permasalahan ini mendorong perlunya tinjauan yuridis yang lebih mendalam terhadap regulasi yang ada serta evaluasi terhadap efektivitas pelaksanaannya. Tidak hanya sebatas menganalisis norma hukum yang tertulis, tetapi juga menilai sejauh mana hukum dapat menjawab kebutuhan perlindungan warga

negara di ruang digital yang terus berkembang. Evaluasi ini penting agar hukum nasional tidak tertinggal dari dinamika teknologi, dan mampu memberikan perlindungan yang adil, adaptif, dan berorientasi pada hak asasi manusia, khususnya hak atas privasi.

Oleh karena itu, penelitian ini bertujuan untuk mengkaji secara yuridis bentuk-bentuk kejahatan siber yang berkaitan dengan pelanggaran data pribadi serta menilai efektivitas dan tantangan implementasi UU ITE dan UU PDP sebagai payung hukum perlindungan data di Indonesia. Melalui pendekatan normatif, studi ini diharapkan dapat memberikan kontribusi ilmiah bagi pengembangan kebijakan hukum nasional yang lebih responsif terhadap realitas digital saat ini, sekaligus memberikan perlindungan yang maksimal bagi masyarakat sebagai subjek data di era informasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu metode penelitian hukum yang bertujuan untuk menelaah dan menganalisis norma-norma hukum tertulis yang mengatur tentang kejahatan siber dan perlindungan data pribadi dalam sistem hukum Indonesia. Pendekatan ini dipilih karena fokus utama penelitian adalah pada studi terhadap asas-asas hukum, aturan hukum positif yang berlaku, serta keterkaitannya dengan fenomena pelanggaran data pribadi dalam konteks kejahatan siber. Penelitian yuridis normatif juga memungkinkan peneliti untuk mengkaji secara mendalam bagaimana regulasi hukum di Indonesia telah merespons perkembangan teknologi informasi dan tantangan digital.

Sumber data dalam penelitian ini dibedakan menjadi dua, yaitu sumber hukum primer dan sumber hukum sekunder. Sumber hukum primer meliputi peraturan perundang-undangan yang relevan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahan dan peraturan pelaksananya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Di samping itu, sumber primer juga mencakup putusan-putusan pengadilan yang berkaitan dengan kasus kejahatan siber dan penyalahgunaan data pribadi. Adapun sumber hukum sekunder berupa literatur hukum, buku teks, artikel jurnal ilmiah, hasil penelitian terdahulu, serta analisis pakar hukum yang dapat memperkaya perspektif teoretis dan praktis terhadap permasalahan yang dikaji.

Pengumpulan data dilakukan melalui teknik studi kepustakaan (library research), dengan menelusuri dan mengkaji berbagai dokumen hukum, publikasi akademik, serta sumber-sumber kredibel lainnya secara sistematis dan kritis. Data yang diperoleh kemudian dianalisis menggunakan teknik analisis kualitatif, dengan cara menginterpretasikan ketentuan-ketentuan hukum yang ada, mengidentifikasi kelemahan dan celah regulasi, serta mengevaluasi efektivitas implementasinya di lapangan. Penelitian ini juga bersifat deskriptif-analitis, yang tidak hanya menggambarkan dan menjelaskan peraturan hukum yang berlaku, tetapi juga menganalisis bagaimana hukum tersebut bekerja secara praktis dalam memberikan perlindungan terhadap data pribadi masyarakat dari kejahatan siber.

Tujuan dari penggunaan metode ini adalah untuk memberikan rekomendasi kebijakan hukum yang bersifat normatif dan konstruktif, guna mendukung penguatan sistem perlindungan data pribadi yang sesuai dengan perkembangan teknologi serta menjawab tantangan yuridis yang timbul akibat transformasi digital di Indonesia.

HASIL DAN PEMBAHASAN

Perkembangan teknologi digital telah menjadi pendorong utama dalam transformasi sosial, ekonomi, dan budaya masyarakat. Kemajuan ini memungkinkan pertukaran informasi secara cepat dan efisien, tetapi juga membuka peluang baru bagi kejahatan siber, terutama pelanggaran terhadap data pribadi. Di Indonesia, kasus-kasus kebocoran data pribadi semakin meningkat, baik di sektor publik maupun swasta. Beberapa insiden besar seperti peretasan data pelanggan operator seluler dan bocornya

informasi pengguna dari platform layanan kesehatan menunjukkan kerentanan serius dalam sistem keamanan data nasional (Simanjuntak, 2022).

Kejahatan siber yang menyasar data pribadi dapat berupa pencurian identitas digital, manipulasi data akun, hingga penjualan data ke pihak ketiga untuk kepentingan komersial. Dampak dari kejahatan ini tidak hanya bersifat ekonomi, tetapi juga psikologis dan sosial, karena korban merasa privasinya dilanggar dan dapat mengalami tekanan mental atau diskriminasi. Menurut Prayoga dan Wulandari (2021), pencurian data pribadi menjadi bentuk kejahatan siber paling umum dan sulit ditelusuri karena pelaku sering menggunakan jaringan anonim atau berada di yurisdiksi luar negeri.

Dari sisi regulasi, Indonesia memiliki dua instrumen hukum utama yang berkaitan dengan perlindungan data pribadi, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ITE, meskipun tidak secara spesifik mengatur data pribadi, memberikan dasar hukum terhadap tindakan akses ilegal dan peretasan. Sementara itu, UU PDP hadir sebagai bentuk pengakuan negara terhadap pentingnya perlindungan data pribadi sebagai bagian dari hak privasi yang dilindungi oleh konstitusi (Suryadi, 2023).

UU PDP membawa sejumlah ketentuan penting, seperti prinsip transparansi, minimalisasi pengumpulan data, serta hak pemilik data untuk mengakses, memperbarui, dan menghapus data mereka. Namun, dalam praktiknya, pelaksanaan UU ini masih menghadapi tantangan besar, terutama dari aspek kesiapan kelembagaan. Belum adanya lembaga pengawas independen yang secara khusus menangani pelanggaran data pribadi menjadi kendala dalam penegakan hukum yang efektif (Putri & Ramadhan, 2023).

Selain itu, kesadaran masyarakat Indonesia terhadap pentingnya menjaga data pribadi masih tergolong rendah. Banyak individu yang dengan mudah membagikan informasi pribadi mereka di media sosial atau dalam transaksi daring tanpa memahami risiko yang ditimbulkan. Literasi digital yang belum merata, terutama di daerah-daerah nonperkotaan, semakin memperbesar risiko terjadinya pelanggaran data pribadi (Nugroho & Safitri, 2021). Kondisi ini diperparah dengan minimnya edukasi tentang hak-hak data pribadi di lingkungan pendidikan formal maupun informal.

Penegakan hukum atas kejahatan siber di Indonesia juga menghadapi persoalan klasik, yaitu keterbatasan sumber daya manusia dan teknologi. Aparat penegak hukum sering kali belum dibekali dengan kompetensi yang memadai di bidang digital forensik. Akibatnya, proses pembuktian hukum terhadap pelaku kejahatan siber berjalan lambat dan tidak efektif. Menurut riset oleh Lestari (2022), hanya sekitar 40% dari laporan kejahatan siber yang dapat ditindaklanjuti secara hukum hingga tahap pengadilan.

Di samping itu, pendekatan hukum di Indonesia masih cenderung reaktif dan belum mampu mengejar kecepatan perkembangan teknologi. Misalnya, definisi “data pribadi” dalam UU PDP masih bersifat umum dan membutuhkan peraturan turunan agar dapat diterapkan secara teknis. Tanpa peraturan pelaksana yang jelas, terdapat celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan siber untuk menghindari tanggung jawab hukum (Wahyuni, 2023).

Untuk menghadapi kompleksitas tantangan tersebut, diperlukan sinergi yang kuat antara pemerintah, sektor swasta, dan masyarakat sipil. Pemerintah perlu mempercepat pembentukan lembaga otoritatif pengawas data pribadi serta menyusun standar keamanan data nasional yang wajib diterapkan oleh penyelenggara sistem elektronik. Di sisi lain, perusahaan dan penyedia layanan digital juga harus bertanggung jawab dalam melindungi data pengguna, termasuk melalui audit sistem keamanan secara berkala.

Akhirnya, untuk menciptakan sistem perlindungan data pribadi yang efektif dan berkeadilan, pendekatan hukum yang digunakan harus bersifat responsif, partisipatif, dan berbasis hak asasi manusia. Reformasi hukum tidak hanya sebatas pada pembentukan undang-undang, tetapi juga menyangkut

penguatan kapasitas lembaga, peningkatan literasi digital, serta penegakan hukum yang adil dan transparan. Dengan langkah-langkah tersebut, Indonesia dapat membangun ekosistem digital yang aman dan menghormati hak privasi setiap warganya.

KESIMPULAN

Perkembangan teknologi informasi yang begitu cepat telah membawa perubahan besar dalam pola interaksi dan transaksi masyarakat modern. Namun, di sisi lain, kemajuan ini juga menciptakan celah yang memungkinkan munculnya berbagai bentuk kejahatan siber, khususnya yang menyasar data pribadi. Kejahatan semacam ini bukan hanya menyerang hak privasi individu, tetapi juga berpotensi menimbulkan kerugian sosial, ekonomi, dan psikologis yang tidak sedikit. Dalam konteks ini, kejahatan siber tidak bisa dianggap sebagai persoalan teknis semata, melainkan sebagai persoalan hukum yang harus dihadapi secara serius dan menyeluruh.

Indonesia telah memiliki sejumlah regulasi yang mengatur mengenai perlindungan data pribadi, antara lain UU ITE dan UU PDP yang menjadi landasan utama. Namun dalam praktiknya, masih terdapat berbagai kendala dalam implementasi, mulai dari ketidaksiapan infrastruktur digital, minimnya kapasitas aparat penegak hukum dalam menangani kejahatan digital, hingga rendahnya kesadaran masyarakat akan pentingnya melindungi data pribadi. Banyak kasus pelanggaran data yang tidak tertangani secara tuntas, atau bahkan tidak dilaporkan karena ketidaktahuan korban akan hak-hak hukumnya. Hal ini mencerminkan bahwa perlindungan hukum belum berjalan secara optimal.

Dari perspektif yuridis, perlindungan terhadap data pribadi membutuhkan pendekatan yang lebih holistik dan adaptif terhadap perkembangan zaman. Tidak cukup hanya mengandalkan aturan hukum yang telah ada, tetapi juga diperlukan pembaruan regulasi secara berkala yang mampu mengakomodasi dinamika dunia digital. Sinergi antara lembaga-lembaga terkait, baik dari sektor pemerintah, penegak hukum, maupun swasta, menjadi kunci dalam menciptakan sistem perlindungan data yang solid. Edukasi kepada masyarakat juga harus digencarkan agar individu lebih sadar akan risiko dan tahu cara menjaga keamanan data pribadinya.

Dengan demikian, untuk menjamin hak atas privasi di era digital, Indonesia perlu mengembangkan sistem perlindungan data pribadi yang kuat, responsif, dan berkeadilan. Sistem ini harus ditopang oleh perangkat hukum yang jelas, penegakan hukum yang tegas, serta keterlibatan masyarakat secara aktif. Melalui penguatan regulasi, literasi digital, dan kapasitas kelembagaan, diharapkan ruang digital nasional dapat menjadi lingkungan yang aman, terpercaya, dan mendukung pembangunan yang inklusif di era informasi.

DAFTAR PUSTAKA

Kementerian Kominfo. (2022). *UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Jakarta: Kominfo.

Lestari, N. (2022). Penegakan Hukum Terhadap Kejahatan Siber di Era Digital. *Jurnal Hukum & Teknologi, 14*(2), 123–135.

Nugroho, D., & Safitri, M. (2021). Literasi Digital dan Kesadaran Perlindungan Data Pribadi. *Jurnal Komunikasi Digital, 8*(1), 45–59.

Nurhadi, A. (2023). Tantangan Penegakan Hukum Kejahatan Siber di Indonesia. *Jurnal Hukum dan Teknologi, 7*(1), 33–45.

Panjaitan, R. (2020). Privasi Digital dan Perlindungan Data Pribadi dalam Era Revolusi Industri 4.0. *Jurnal Hukum & Masyarakat, 15*(2), 87–96.

Prayoga, A., & Wulandari, S. (2021). Dampak Kejahatan Siber terhadap Privasi Individu di Indonesia. *Jurnal Kriminologi Indonesia, 10*(3), 87–99.

Putri, A. F., & Ramadhan, Y. (2023). Implementasi UU Perlindungan Data Pribadi: Tantangan dan Solusi. *Jurnal Legislasi dan Teknologi, 5*(1), 33–48.

Rahmawati, S. (2022). Penyalahgunaan Data Pribadi di Internet dan Urgensi Perlindungan Hukum. *Jurnal Siber Indonesia, 9*(3), 112–124.

Simanjuntak, R. (2022). Kebocoran Data dan Perlindungan Konsumen di Era Digital. *Jurnal Hukum Siber, 3*(4), 201–215.

Simanjuntak, T. (2018). Analisis Kelemahan UU ITE dalam Menanggulangi Kejahatan Siber. *Jurnal Ilmu Hukum, 14*(1), 56–66.

Suryadi, E. (2023). Perkembangan Hukum Perlindungan Data Pribadi di Indonesia. *Jurnal Hukum dan HAM, 11*(1), 12–27.

Suryanto, A. (2021). Transformasi Digital dan Implikasinya Terhadap Hukum Nasional. *Jurnal Kebijakan Publik, 11*(2), 71–83.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Wahyuni, D. (2023). Evaluasi Terhadap UU PDP dan Peraturan Turunannya. *Jurnal Regulasi Digital, 9*(2), 54–68.

Yulianto, D. (2019). Hak Privasi dan Ancaman Kejahatan Siber: Tinjauan Filosofis dan Hukum. *Jurnal Hukum Kontemporer, 5*(4), 134–145.