Perlindungan Hukum Data Pribadi Terhadap Korban Kejahatan Akses Ilegal dan Upaya Pencegahannya

Tania Tresna Kurnia *, Dr. Ade Mahmud, S.H.,M.H

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

taniatresna2002@gmail.com, ademahmud100@yahoo.com

Abstract. The digital era brings cyber challenges such as hacking and personal data leaks. The PDNS and BKN cases show the urgency of data protection. Law No. 27 of 2022 is present as an important legal basis to protect public privacy and prevent data misuse. This study uses a normative legal method with descriptive analysis of secondary data. The data is analyzed qualitatively and uses a deductive approach to draw conclusions regarding the legal protection of personal data and the prevention of illegal access crimes. Personal data protection needs to be optimized preventively (system strengthening, regulation, education) and repressively (law enforcement, restoration of victims' rights). Recent cases indicate that legal protection is not yet optimal, so the state needs to be more assertive in implementing the PDP Law. Personal data protection is a constitutional right that requires an integrated approach through regulation, law enforcement, public education, and individual control. The implementation of the Law still needs to be optimized with derivative regulations and implementing institutions, as well as effectiveness studies, technical standards, reporting systems, and digital literacy to minimize the risk of crime, protect victims, and enforce privacy rights.

Keywords: *Personal Data Protection, Illegal Access, Prevention.*

Abstrak. Era digital membawa tantangan siber seperti peretasan dan kebocoran data pribadi. Kasus PDNS dan BKN menunjukkan urgensi perlindungan data. UU No. 27 Tahun 2022 hadir sebagai landasan hukum penting untuk melindungi privasi masyarakat dan mencegah penyalahgunaan data. Penelitian ini menggunakan metode yuridis normatif dengan analisis deskriptif dari data sekunder. Data dianalisis kualitatif dan menggunakan pendekatan deduktif untuk menarik kesimpulan mengenai perlindungan hukum data pribadi dan pencegahan kejahatan akses ilegal. Perlindungan data pribadi perlu dioptimalkan secara preventif (penguatan sistem, regulasi, edukasi) dan represif (penegakan hukum, pemulihan hak korban). Kasus-kasus terbaru mengindikasikan perlindungan hukum belum maksimal, sehingga negara perlu lebih tegas mengimplementasikan UU PDP. Perlindungan data pribadi adalah hak konstitusional yang memerlukan pendekatan terintegrasi melalui regulasi, penegakan hukum, edukasi publik, dan kontrol individu. Implementasi UU masih perlu dioptimalkan dengan aturan turunan dan lembaga pelaksana, serta kajian efektivitas, standar teknis, sistem pelaporan, dan literasi digital untuk meminimalkan risiko kejahatan, melindungi korban, dan menegakkan hak privasi.

Kata Kunci: *Perlindungan Data Pribadi, Akses Ilegal, Pencegahan.*

*taniatresna2002@gmail.com

A. Pendahuluan

Kemajuan teknologi komunikasi dan informasi yang didukung globalisasi telah menciptakan era digital, ditandai dengan kemudahan akses informasi, konektivitas luas, dan pertukaran data yang cepat. Era ini mengubah cara masyarakat berkomunikasi dan beradaptasi dengan perkembangan zaman. Inovasi teknologi menciptakan pola hidup baru dan berdampak pada berbagai aspek kehidupan, baik positif maupun negatif. Selain memberi manfaat besar, era digital juga menghadirkan tantangan seperti kejahatan siber, pelanggaran privasi, dan penyalahgunaan data pribadi.

Data pribadi merupakan alat penting bagi bisnis dan organisasi untuk mengidentifikasi individu, mencakup informasi seperti nama, tanggal lahir, dan alamat, data ini termasuk hak privasi yang harus dilindungi. Keamanan komunikasi data elektronik merupakan bagian terpenting yang jauh dari perhatian publik, sehingga berpeluang terhadap terjadinya peretasan dan kejahatan siber atau cybercrime. Cybercrime yaitu suatu upaya ilegal pada sistem komputer atau transmisi data, yang dapat berupa malware, ransomware, hacking, dan pencurian identitas yang dipergunakan untuk melakukan akses ilegal. Kejahatan akses ilegal adalah peretasan sistem atau jaringan untuk mencuri data atau keuntungan lain, mencakup pencurian data pelanggan, informasi bisnis, sabotase sistem, hingga peretasan akun pribadi.

Menurut data Kementerian Komunikasi dan Digital, dari 2019 hingga 14 Mei 2024 terdapat 124 kasus dugaan pelanggaran perlindungan data pribadi. Mayoritas berupa kebocoran data (111 kasus), disusul pengumuman data tanpa izin (4 kasus), pengungkapan ke pihak tidak sah (2 kasus), pengumpulan data tidak relevan (3 kasus), dan pelanggaran lainnya (4 kasus) dengan kenaikan jumlah setiap tahunnya (Mediana, 2024).

Beberapa kasus pencurian data pribadi di Indonesia antara lain insiden serangan ransomware "*Brain Chipper*" terhadap PDNS pada Juni 2024 dengan tuntutan tebusan sebesar 8 juta dolar AS, dan kasus akses ilegal terhadap data BKN oleh seorang guru honorer yang dijual di situs gelap. Pada Januari 2025, juga terungkap kasus penggunaan AI untuk membuka rekening bank secara ilegal menggunakan identitas orang lain.

Penyalahgunaan data pribadi dapat menimbulkan kerugian besar bagi korban, sehingga perlindungan hak milik atas data pribadi menjadi penting untuk mencegah masyarakat terus menjadi sasaran kejahatan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan bagian dari hak asasi manusia dan upaya pemerintah untuk memberikan kepastian hukum dengan mengatur cara penanganan dan perlindungan data pribadi, termasuk catatan, persetujuan, akses, keamanan, penyalahgunaan, serta lembaga pengawasannya (Sutarli & Kurniawan, 2023). Data pribadi adalah hak privasi yang memiliki sensitivitas terhadap identitas seseorang dengan kemungkinan individu dapat mengontrol kepemilikan dan penggunaannya, sebagaimana dijamin dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM)

Hukum berperan penting dalam mencegah dan mengatasi kejahatan, namun penerapan aturan yang sesuai dengan perkembangan teknologi informasi menjadi tantangan tersendiri. Pencegahan dianggap lebih efektif daripada penanggulangan represif, meski kebijakan penal tetap diperlukan sebagai bentuk perlindungan sosial dan pencegahan tindak pidana siber. Kesulitan menangani kejahatan siber muncul karena faktor pelaku, korban, reaksi sosial, dan hukum yang saling terkait, serta peran negara yang masih pasif melindungi pemilik data pribadi. Indonesia sebagai negara hukum menjamin perlindungan hak asasi manusia, terutama dalam menghadapi potensi peningkatan pelanggaran data pribadi akibat pesatnya penggunaan teknologi informasi (Yudistira & Ramadani, 2023).

Perlindungan hukum adalah upaya melindungi harkat, martabat, dan hak asasi manusia dari penyalahgunaan kewenangan sesuai ketentuan hukum. Menurut Satjipto Rahardjo perlindungan hukum merupakan pengayoman terhadap HAM yang dirugikan, agar masyarakat dapat menikmati hak-hak hukum. Perlindungan data berkaitan erat dengan privasi, yang menurut Alan Westin (Djafar et al.,2016), adalah hak individu atau lembaga untuk mengatur akses terhadap informasi pribadinya. Di Indonesia, perlindungan hak atas privasi diatur dalam konstitusi sebagai bagian dari penghormatan terhadap HAM dan menjadi dasar hukum perlindungan data pribadi.

Perlindungan hukum terhadap korban dalam lingkup viktimologi tidak terbatas pada individu, tetapi juga kelompok, korporasi, swasta maupun pemerintah. Sedangkan yang dimaksud dengan akibat penimbulan korban adalah sikap atau tindakan terhadap korban dan/atau pihak pelaku serta mereka yang secara langsung atau tidak terlibat dalam terjadinya suatu kejahatan. Dalam teori

viktimologi modern, teori aktivitas rutin menyatakan bahwa target atau korban yang cocok merupakan salah satu faktor kejahatan terjadi. Suatu kejahatan akan menimbulkan respon terhadap upaya pencegahan yang dapat dilakukan melalui tiga pendekatan utama, yaitu *situational crime prevention*, *social crime prevention*, dan *community crime prevention*.

Berdasarkan uraian diatas fokus rumusan masalah pada penelitian ini yaitu, bagaimana perlindungan hukum data pribadi bagi korban kejahatan akses ilegal dalam hukum positif di Indonesia dan bagaimana bentuk upaya pencegahan terhadap kejahatan akses illegal. Tujuan dari penelitian ini adalah untuk menjelaskan bagaimana perlindungan hukum data pribadi bagi korban kejahatan akses ilegal dalam hukum positif di Indonesia dan menganalisis bagaimana bentuk upaya pencegahan terhadap kejahatan akses ilegal. Manfaat teoritis dalam penelitian ini dapat menambah wawasan dan pengetahuan keilmuan bagi perkembangan kajian studi Ilmu Hukum tentang perlindungan hukum data pribadi bagi korban dan upaya pencegahan terhadap kejahatan akses illegal. Manfaat praktis bagi masyarakat, kepolisian, pemerintah, dan mahasiswa dengan memberikan wawasan, masukan kebijakan, serta referensi dalam bidang Hukum Pidana terkait perlindungan data pribadi dan pencegahan kejahatan akses ilegal.

B. Metode

Penelitian ini menggunakan pendekatan yuridis normatif dengan spesifikasi deskriptif analisis, berupa penelitian yang menggambarkan keterkaitan peraturan perundang-undangan dengan teori-teori hukum positif terhadap suatu permasalahan. Data penelitian ini diperoleh dengan menggunakan data sekunder yaitu studi pustaka pada buku-buku hukum, jurnal-jurnal hukum, artikel, dan pendapat para ahli hukum. Penelitian ini bersifat kualitatif yang menghasilkan data deskriptif berupa data-data tertulis maupun lisan, dan perilaku-prilaku yang dapat diamati, dan dianalisis dengan metode berpikir deduktif yang mengurai permasalahan umum hingga dapat ditarik kesimpulan yang bersifat khusus sesuai dengan fokus permasalahan yang dikaji.

C. Hasil Penelitian dan Pembahasan

Badan Siber dan Sandi Negara (BSSN) mencatat ada 403 juta anomali trafik atau serangan siber ke Indonesia sepanjang 2023. Tim Pusat Kontak Siber BSSN telah mengirimkan sebanyak 1.367 notifikasi indikasi insiden siber tahun 2024. Dari 1.367 Notifikasi terkirim, Indikasi Insiden yang dinotifikasi oleh BSSN yaitu Data Breach sebanyak 535 yang mengalami kenaikan dari tahun 2023 sebanyak 268. Pada periode 2023 BBSN mengungkap deteksi terhadap 103 insiden kebocoran data dan mengalami kenaikan pada periode 2024 dimana ditemukan deteksi terhadap 241 insiden kebocoran data (BSSN, 2025).

Menurut data Kementerian Komunikasi dan Digital, dari 2019 hingga 14 Mei 2024 terdapat 124 Menteri Komunikasi dan Digital, Meutya Hafid mengatakan bahwa berdasarkan data *Surfshark Breach Data* per Januari 2025, Indonesia menempati peringkat ke-14 di dunia berkenaan dengan jumlah akun yang paling banyak mengalami kebocoran data.

Diprediksi terdapat 160 juta akun yang mengalami kebocoran data sepanjang 2004-2024. Sementara itu, di ASEAN Indonesia menempati peringkat ke-2 dengan jumlah kebocoran data terbanyak yaitu 1,77 juta. Data ini mencerminkan peningkatan yang signifikan dalam jumlah kasus kebocoran data yang melibatkan informasi pribadi, finansial, dan institusional di berbagai sektor.

Tabel 1. Kasus Kebocoran Data Terbesar di Indonesia 3 Tahun Terakhir

Kasus Kebocoran Data	Tahun	Jumlah Data Yang Bocor
Indihome	2022	26 juta
PLN	2022	17 juta
Komisi Pemilihan Umum	2022	105 juta
SIM Card	2022	1,3 miliar
Pedulilindungi	2022	3,2 miliar
Data Paspor	2023	34 juta

Kasus Kebocoran Data	Tahun	Jumlah Data Yang Bocor
Bank BSI	2023	15 juta
Dukcapil	2023	337 juta
BPJS Ketenagakerjaan	2023	19.56 juta
MyIndiHome	2023	35 juta
Komisi Pemilihan Umum	2023	204 juta

Sumber: Data Penelitian yang Sudah Diolah, 2025.

Kasus peretasan Pusat Data Nasional Sementara (PDNS) dimulai pada 17 Juni 2024 saat pelaku menonaktifkan sistem keamanan, yang kemudian memuncak pada 20 Juni dengan serangan *ransomware Brain Cipher* (varian LockBit 3.0) yang melumpuhkan layanan 282 instansi pemerintah, termasuk imigrasi. Pemerintah mengonfirmasi jenis serangan pada 24 Juni, namun hanya 2% data berhasil dicadangkan. Kelompok peretas merilis kunci dekripsi secara gratis pada awal Juli, menyatakan serangan ini sebagai peringatan. Pemulihan sistem berlangsung hingga September 2024, yang mendorong seruan reformasi tata kelola, penguatan backup, pembentukan CSIRT, dan evaluasi menyeluruh sistem keamanan nasional.

Selain itu pada 9 Agustus 2024, tersangka BAG, seorang guru honorer berusia 25 tahun asal Banyuwangi, mendapatkan akses ilegal ke sistem BKN melalui domain satudataasn.bkn.go.id dengan menggunakan kredensial admin yang diperolehnya. Ia kemudian mengunduh sekitar 6,3 GB data ASN dari sistem tersebut antara 22.00 WIB 9 Agustus hingga 10.16 WIB 10 Agustus 2024, dan menyebarkan sampel data tersebut melalui Pastebin serta menawarkan penjualan melalui akun Telegram pribadinya di forum Topiax di Breachforums st. Dari aksi ini, BAG memperoleh keuntungan sekitar USD 8.000 atau sekitar Rp 124 juta.

Tak hanya itu kasus yang juga menyoroti urgensi perlindungan data pribadi, dilakukan oleh tersangka berinisial PM dan MR. MR mengumpulkan data pribadi orang lain secara ilegal dari pihak ketiga misterius, lalu menyerahkannya kepada PM. PM kemudian menggunakan teknologi AI untuk memalsukan video verifikasi wajah agar bisa membuka rekening atas nama orang lain. Rekening tersebut digunakan oleh pihak ketiga untuk transaksi online. PM mendapat bayaran per video palsu, sementara MR mendapat keuntungan dari setiap akun yang berhasil dibuka. Keduanya ditangkap pada akhir 2024 dan awal 2025.

Perlindungan Hukum Data Pribadi Terhadap Korban Kejahatan Akses Ilegal Dalam Hukum Positif di Indonesia

Implementasi Indonesia sebagai negara hukum meletakan perlindungan hak asasi manusia dalam konstitusi, melalui penambahan Bab XA Hak Asasi Manusia pada perubahan ke-dua UUD 1945. Ketentuan dalam Pasal 28G ayat (1) UUD 1945. Rumusan dalam Pasal 28 G ayat (1) UUD NKRI 1945 memiliki landasan perlindungan yang sama dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia, hal ini dimasukkan dalam Pasal 17 ICCPR, yang secara jelas melindungi hak privasi. Perlindungan hukum terhadap data pribadi dalam penyalahgunaan data pribadi mengacu kepada sejauh mana peraturan yang ada secara komprehensif melindungi hak privasi korban. Korban dalam konteks kejahatan terhadap data pribadi tidak hanya terbatas pada Subjek Data secara langsung, tetapi juga mencakup pihak-pihak lain yang mengalami kerugian akibat dampak lanjutan dari kejahatan tersebut (Mahameru, 2025).

Dalam Teori Aktivitas Rutin menjelaskan bhawa kejahatan dapat terjadi karena tiga hal, yaitu pelaku yang termotivasi, target yang cocok, tidak ada pemgawas yang dapat mencegah kejahatan. Dalam hal kasus diatas pelaku termotivasi atas keuntungan finansial. Menurut data APJII, 79,5% masyarakat Indonesia menggunakan internet, namun 22,78% tidak menjaga keamanan data pribadi. Rendahnya kesadaran ini membuat masyarakat menjadi target yang cocok. Tidak adanya sistem deteksi dini dan mitigasi yang cepat mencerminkan ketiadaan "penjaga" yang efektif.

Menurut Philipus M. Hadjon bahwa perlindungan hukum di inisiasikan menjadi dua hal, yaitu Perlindungan Hukum Preventif dan Perlindungan Hukum Represif. Perlindungan hukum preventif dirancang untuk untuk mencegah terjadinya pelanggaran hak, sedangkan perlindungan represif memasuki ranah lembaga peradilan sehingga bertujuan untuk menyelesaikan sengketa yang telah terjadi (Hadjon, 1987).

Sebelum diundangkannya Undang-Undang Nomor 27 Tahun 2022. Dalam hukum positif Indonesia telah memberikan upaya perlindungan secara preventif, meskipun belum sepenuhnya komprehensif. Diantaranya, Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, UU No. 23 Tahun 2006 tentang Administrasi Kependudukan. Dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), tidak mendefinisikan secara jelas mengenai "data pribadi" (Karo dan Prasetyo, 2022). Tujuan dari perlindungan preventif ini adalah memastikan bahwa setiap proses pengelolaan data pribadi memenuhi prinsip-prinsip perlindungan privasi dan tidak merugikan subjek data.

Bentuk perlindungan hukum preventif dimuat dalam ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dalam Pasal 14 sampai Pasal 25 mengatur kewajiban pengendali data pribadi dalam pemrosesan data pribadi yang didasarkan atas persetujuan eksplisit dari subjek data, pemenuhan kewajiban hukum, perlindungan kepentingan vital, dan dapat diproses dalam tugas pelayanan publik atau kepentingan lain yang sah. Pengendali data wajib memberikan informasi jelas terkait pemrosesan, menunjukkan bukti persetujuan, serta melakukan pemrosesan terbatas pada tujuan yang sah. Jika pemrosesan data beresiko tinggi maka pengendali data wajib melakukan perlindungan dan menjaga kerahasiaan serta pengawasan yang ketat.

Hak-hak yang dimiliki oleh individu terkait data pribadi dijelaskan secara lengkap dalam Pasal 5 sampai Pasal 13. Setiap orang sebagai pemilik data pribadi berhak untuk memahami dengan jelas dasar hukum dan tujuan di balik pemrosesan data mereka. Mereka juga berhak untuk mengakses informasi yang ada, memperbaiki data yang tidak akurat, membatasi atau menghentikan pemrosesan, serta menghapus atau memindahkan data tersebut. Di samping itu, individu juga memiliki hak untuk menolak penggunaan data pribadi mereka dalam situasi tertentu dan hak untuk mengajukan keberatan atau menggugat jika ada tanda-tanda penyalahgunaan data oleh pengendali atau prosesor data. Meskipun hak gugat dan ganti rugi diatur, prosedur pelaksanaannya belum jelas sehingga mengurangi efektivitas perlindungan.

Pasal 39 UU PDP mengatur pencegahan akses tidak sah terhadap data pribadi dengan mewajibkan pengendali data untuk menggunakan sistem keamanan yang andal, aman, dan bertanggung jawab. Tindakan ini untuk meminimalkan risiko kebocoran data dan melindungi Subjek Data sebelum kejahatan terjadi. Pengamanan mencakup perlindungan sistem informasi agar tidak mudah diakses oleh pihak yang tidak berwenang serta penerapan langkah-langkah mitigasi risiko. Jika terjadi kebocoran data, pengendali wajib segera memberi pemberitahuan secara transparan kepada pemilik data dan otoritas terkait, agar dampak buruk dapat diminimalisir melalui tindakan pencegahan.

Perlindungan hukum secara represif memiliki tujuan untuk tujuan yakni penyelesaian atas sengketa. Penanganan perlindungan hukum oleh Pengadilan Umum serta Pengadilan Administrasi di Indonesia. Perlindungan hukum represif memberikan ketentuan mengenai transparansi atas kasus yang terjadi. Pengendali Data Pribadi wajib segera memberitahukan kepada subjek data dan masyarakat jika terjadi kebocoran data, sesuai dengan ketentuan UU PDP Pasal 46 Ayat (1) yang berbunyi "Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: subjek data pribadi dan lembaga." (Rusyda, 2025).

Bab IX UU PDP menegaskan perlunya pembentukan Lembaga Pengawas independen yang bertugas mengawasi dan menegakkan hukum perlindungan data pribadi serta menangani pemulihan hak korban melalui proses administratif. Lembaga ini dibentuk oleh Presiden dan memiliki kewenangan kebijakan, pengawasan, dan penegakan hukum. Namun, hingga kini lembaga tersebut belum terbentuk, sehingga pengawasan aktivitas siber, termasuk data publik dan pribadi, masih dilakukan oleh Kementerian Komunikasi Digital dan Badan Siber Sandi Negara.

Pasal 57 ayat (2) UU PDP mengatur sanksi administratif berupa peringatan tertulis, penghentian sementara pemrosesan data, hingga perintah penghapusan data yang diproses tidak sah, serta denda administratif maksimal 2% dari total pendapatan tahunan pelanggar. Sanksi dapat ditingkatkan jika pelanggaran berulang atau tidak diperbaiki, memberi fleksibilitas bagi regulator. Dalam kasus peretasan PDNS, kelalaian pengelola data seperti Kementerian Kominfo bisa dikenai sanksi administratif. Demikian pula Badan Kepegawaian Negara (BKN) dalam kasus penjualan data

ASN, dan bank atau penyedia layanan yang gagal melindungi proses verifikasi identitas digital pada kasus pembukaan rekening dengan data AI juga berpotensi mendapat sanksi serupa.

Selain sanksi administratif, diatur juga mengenai sanksi pidana. Sanksi pidana diberikan bertujuan memberikan efek jera kepada pelaku pelanggaran serta menjamin hak-hak subjek data. Serangan *ransomware* LockBit 3.0 terhadap PDNS tergolong perbuatan melawan hukum sesuai Pasal 30 ayat (3) UU ITE karena pelaku mengakses sistem pemerintah tanpa hak, dengan ancaman pidana hingga 13 tahun 4 bulan penjara setelah penambahan dua pertiga dari pidana pokok.

Tersangka BAG dalam kasus penjualan data ASN dijerat dengan UU PDP dan UU ITE karena secara ilegal mengakses, memperoleh, dan menyebarkan data pribadi, dengan ancaman pidana hingga 10 tahun dan/atau denda Rp5 miliar. Sementara itu, dalam kasus pembukaan rekening menggunakan data pribadi melalui AI, tersangka PM dikenai Pasal 35 dan 32 UU ITE dengan ancaman pidana hingga 12 tahun dan/atau denda Rp12 miliar, sedangkan MR dijerat dengan Pasal 67 jo. Pasal 65 UU PDP karena mengumpulkan dan memberikan data pribadi tanpa izin, dengan ancaman pidana hingga 5 tahun dan/atau denda maksimal Rp5 miliar.

Selain dua jenis sanksi di atas, UU PDP juga memberikan ruang bagi korban pelanggaran data pribadi untuk menempuh jalur perdata guna menuntut ganti rugi. Sanksi perdata ini sesuai dengan prinsip hukum yang tertuang dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata), yang menyatakan bahwa setiap tindakan yang melanggar hukum dan menyebabkan kerugian kepada pihak lain wajib untuk diganti kerugiannya. Namun, mekanisme gugatan perdata ini masih menghadapi hambatan karena UU PDP belum mengatur prosedur teknis secara rinci. Ketidakjelasan ini menyulitkan korban, terutama masyarakat umum, dalam menegakkan haknya dan mengurangi efektivitas perlindungan hukum secara represif (Uttari dan Dewi, 2025).

UU No. 19 Tahun 2016 dan UU PDP mengatur hak untuk dilupakan, di mana pemilik data dapat meminta penghapusan data pribadi yang tidak relevan. Pasal 43 dan 44 UU PDP mewajibkan penghapusan dan pemusnahan data yang diperoleh secara melawan hukum. Korban juga berhak menuntut ganti rugi materiil sesuai Pasal 12 ayat (1). Pemerintah juga diwajibkan untuk menyediakan layanan pemulihan identitas bagi mereka yang terdampak, di samping menerapkan langkah-langkah teknis. Pemerintah tidak hanya bertanggung jawab atas pemulihan identitas korban pelanggaran data tetapi juga kompensasi dan dukungan finansial mereka (Agustina dan Wiraguna, 2025).

Upaya Pencegahan Yang Dilakukan Terhadap Kejahatan Akses Ilegal

Pendekatan non-penal beroperasi di luar ranah hukum pidana dan bersifat lebih preventif, dengan fokus mengatasi akar masalah sebelum kejahatan terjadi. Dalam konteks kejahatan siber, upaya ini menyasar faktor-faktor pemicu seperti kondisi sosial dan perkembangan teknologi, sehingga dianggap memiliki posisi yang sangat strategis karena menanggulangi kejahatan langsung dari sumbernya (Agung et al.,2022). Upaya pencegahan non penal dalam khususnya dalam konteks kejahatan akses ilegal terhadap data pribadi, dapat dilakukan melalui pendekatan *Social Crime Prevention, Situational Crime Prevention,* dan *Community Crime Prevention.*

Situational Crime Prevention merupakan pendekatan pencegahan kejahatan digital yang berfokus pada penguatan kondisi sosial dan pengurangan faktor pemicu kejahatan melalui langkah-langkah pre-emtif. Salah satu upaya utamanya adalah edukasi dan sosialisasi masyarakat dengan meningkatkan literasi digital, etika penggunaan internet, serta kesadaran akan pentingnya perlindungan data pribadi. Masyarakat diajarkan cara menjaga keamanan data seperti menggunakan kata sandi kuat, mengaktifkan verifikasi dua faktor (2FA), mengganti password secara berkala, dan menggunakan VPN. Sosialisasi ini melibatkan instansi seperti BSSN, Kominfo, dan Direktorat Siber Polri melalui media massa dan kampanye publik yang aktif.

Selanjutnya, penguatan sumber daya manusia juga penting dilakukan melalui pelatihan berkala bagi pihak-pihak yang terlibat dalam pengelolaan data pribadi. Pelatihan ini mencakup simulasi serangan siber, peningkatan kompetensi teknis, dan dorongan untuk memperoleh sertifikasi keamanan seperti CISSP atau CISM. Di sisi lain, upaya pencegahan juga bisa dilakukan secara mandiri dengan cara sederhana seperti tidak membagikan data pribadi secara sembarangan, waspada terhadap tautan atau situs mencurigakan, serta rutin memperbarui sistem keamanan perangkat yang digunakan. Pendekatan ini bertujuan menciptakan ketahanan digital secara menyeluruh dari individu hingga institusi (Diskominfo, 2024)

Pendekatan *Situational Crime Prevention* bertujuan mengurangi peluang terjadinya kejahatan

dengan memodifikasi kondisi lingkungan yang memungkinkan kejahatan, termasuk pembatasan akses ilegal dan penguatan sistem penyimpanan data. Di Indonesia, meskipun pemanfaatan teknologi digital tinggi, kesiapan sistem keamanannya masih rendah. Oleh karena itu, penting menerapkan sistem keamanan canggih seperti enkripsi *end-to-end*, autentikasi dua faktor (2FA), *firewall*, dan sistem deteksi intrusi (IDS). Upaya ini diperkuat dengan segmentasi jaringan dan pemilihan penyedia cloud bersertifikasi seperti ISO 27001 untuk meminimalkan risiko serangan siber dan melindungi data sensitif.

Selain itu, audit keamanan berkala sangat penting untuk mendeteksi celah keamanan, dimulai dengan pemantauan sistem, pengujian teknis oleh ethical hacker, dan evaluasi terhadap kebijakan keamanan yang ada. Pemeriksaan ini menghasilkan laporan temuan, risiko, dan rekomendasi perbaikan yang harus ditindaklanjuti. Di samping itu, kebijakan akses data ketat perlu diterapkan melalui prinsip *least privilege* dan kontrol akses berbasis peran (RBAC), di mana akses hanya diberikan kepada pihak yang benar-benar membutuhkan. Setiap aktivitas akses juga harus dicatat untuk mengantisipasi potensi penyalahgunaan dan memastikan pertanggungjawaban (Fa'izi, 2024).

Pencegahan kejahatan berbasis masyarakat atau *Community Crime Prevention* merupakan pendekatan yang menekankan keterlibatan aktif masyarakat dalam mencegah kejahatan, termasuk kejahatan digital. Pendekatan ini menuntut partisipasi warga dalam mengidentifikasi, melaporkan, serta menyelesaikan masalah keamanan di lingkungannya melalui kerja sama dengan pemerintah dan aparat penegak hukum.

Salah satu bentuk konkret pencegahan adalah penyusunan aturan turunan dari UU Perlindungan Data Pribadi (UU PDP) dalam bentuk Peraturan Pemerintah. Regulasi ini harus memberikan panduan teknis dan hukum, mencakup standar keamanan data, mekanisme pelaporan insiden, serta penyelesaian sengketa. Pemerintah juga perlu mempercepat pembentukan UU Keamanan dan Ketahanan Siber untuk memperkuat kerangka hukum dalam menghadapi ancaman siber yang kompleks dan terorganisir.

Selain itu, pembentukan Badan Perlindungan Data Pribadi (BPDP) yang bersifat independen sangat mendesak. Lembaga ini bertugas untuk mengawasi kepatuhan terhadap UU PDP, menangani pelanggaran data, memberikan sanksi, serta meningkatkan perlindungan masyarakat di tengah pesatnya perkembangan teknologi digital dan kecerdasan buatan (AI). Dengan tingginya indeks keterampilan digital masyarakat Indonesia, keberadaan BPDP menjadi penting untuk menjamin pengelolaan data yang aman dan bertanggung jawab. BPDP diharapkan menjadi institusi utama dalam pengawasan, pemberdayaan masyarakat, dan perlindungan hukum atas data pribadi (Nugroho, 2024).

Forum tanggap keamanan juga diperlukan untuk mengatasi lemahnya koordinasi antar lembaga akibat ego sektoral dan ketidakjelasan peran. Koordinasi aktif antara BSSN, Polri, Komdigi, dan sektor swasta dapat memperkuat sistem pertahanan data nasional. Indonesia dapat meniru model Malaysia dengan membentuk pusat komando siber nasional terintegrasi.

Di sisi lain, kepatuhan terhadap UU PDP menjadi kunci dalam menjaga hak-hak individu dan membangun kepercayaan publik. Penerapan standar keamanan yang jelas, transparansi, serta akuntabilitas oleh pengendali data sangat penting dalam mencegah pelanggaran data pribadi dan meningkatkan kesadaran serta perlindungan masyarakat terhadap risiko kejahatan siber.

Di luar aspek regulasi dan kelembagaan, peningkatan literasi digital masyarakat merupakan langkah penting untuk meminimalisasi kejahatan siber. Literasi digital tidak sekadar berkaitan dengan kemampuan menggunakan teknologi, tetapi juga mencakup kesadaran kritis dalam menjaga data pribadi, memahami ancaman digital, serta menerapkan langkah pencegahan yang tepat. Upaya ini bisa dilakukan melalui kampanye edukasi publik, integrasi materi literasi digital dalam kurikulum pendidikan, serta pelatihan bagi komunitas lokal. Dengan demikian, masyarakat berperan aktif sebagai garda terdepan perlindungan data, sehingga tanggung jawab pengawasan tidak hanya bertumpu pada negara.

Selain itu, kerja sama internasional menjadi faktor penting mengingat karakter kejahatan siber yang lintas negara. Indonesia perlu memperkuat partisipasi dalam forum global, menjalin perjanjian ekstradisi, serta mengembangkan mekanisme bantuan hukum timbal balik (mutual legal assistance). Hal ini krusial karena banyak serangan siber, termasuk pencurian data pribadi dan penipuan daring, dilakukan oleh jaringan internasional yang sulit dijangkau hanya dengan hukum nasional. Oleh karena itu, penguatan strategi nasional yang terintegrasi dengan kolaborasi global akan memastikan perlindungan data pribadi yang lebih adaptif, komprehensif, dan berkelanjutan.

D. Kesimpulan

Perlindungan data pribadi sebagai bagian dari hak asasi manusia telah mendapatkan pengakuan konstitusional dan penguatan hukum positif melalui berbagai regulasi, termasuk UU PDP dan UU ITE. Implementasi perlindungan ini mencakup mekanisme preventif melalui pengaturan kewajiban pengendali data dan hak subjek data, serta mekanisme represif berupa sanksi administratif, pidana, dan perdata terhadap pelanggaran. Namun, efektivitas perlindungan ini masih dihambat oleh belum terbentuknya Lembaga Pengawas Independen, kurangnya regulasi teknis pelaksanaan, serta lemahnya kesadaran masyarakat dan koordinasi antar lembaga.

Oleh karena itu, perlindungan hukum atas data pribadi di Indonesia masih memerlukan penguatan kelembagaan, edukasi publik, dan harmonisasi kebijakan agar mampu menanggapi tantangan kejahatan digital yang semakin kompleks dan masif.

Pendekatan non penal dalam mencegah kejahatan siber, khususnya terhadap akses ilegal data pribadi, menekankan strategi preventif melalui tiga pendekatan utama: *Sosial Crime* Prevention, *Situational Crime Prevention*, dan *Community Crime Prevention*. Melalui edukasi digital, pelatihan SDM, penerapan teknologi keamanan, audit sistem, hingga regulasi dan koordinasi antar lembaga, pendekatan ini bertujuan menciptakan lingkungan yang tangguh terhadap kejahatan siber. Keterlibatan masyarakat dan negara menjadi kunci dalam membangun kesadaran kolektif, meningkatkan sistem pertahanan data nasional, serta memastikan perlindungan hukum berjalan efektif dan adaptif terhadap perkembangan teknologi. Pendekatan ini bukan hanya menjadi pelengkap dari penegakan hukum pidana, tetapi fondasi utama dalam membangun ketahanan digital Indonesia secara menyeluruh dan berkelanjutan.

Selain itu, kolaborasi internasional juga penting mengingat kejahatan siber bersifat lintas batas. Kerja sama dengan negara lain dalam pertukaran informasi, standar keamanan, dan penegakan hukum akan memperkuat efektivitas perlindungan data pribadi di Indonesia.

Ucapan Terimakasih

Alhamdulillahi rabbil'alamin, puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penelitian yang berjudul "*Perlindungan Hukum Data Pribadi Terhadap Korban Kejahatan Akses Ilegal Dan Upaya Pencegahannya*". Penghargaan terbesar penulis ucapkan kepada orang tua, ayahanda Wahyu Candra Kurnia dan ibunda Windi Widianingsih, atas do'a dan kasih sayang serta dukungan kepada penulis hingga dapat menyelesaikan penelitian ini. Selain itu, Terima kasih yang sebesar-besarnya penulis sampaikan kepada Yth. Dr. Ade Mahmud, S.H,. M.H. selaku dosen pembimbing yang telah memberikan banyak ilmu, bimbingan dan arahan dalam proses penelitian, semoga kebaikan beliau mendapat pahala yang berlipat ganda dari Allah SWT.

Daftar Pustaka

Arifah Hidayat, Diana Wiyanti, & Makmur. (2023). Perlindungan Hukum Terhadap Anggota Koperasi BMT Rindu Alam yang Dananya Disalahgunakan Pengurus. *Jurnal Riset Ilmu Hukum*, 21–24. https://doi.org/10.29313/jrih.v3i1.2113

Fadilla, M. F., & Nurcahyono, A. (2023). *Kajian Kriminologi terhadap Penyebaran Data Pribadi yang Dilakukan oleh Peretas (Hacker) Dihubungkan dengan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. https://journal.sbpublisher.com/index.php/lol

Ririn Puspita Dewi, & Diana Wiyanti. (2024). Perlindungan Hukum Nasabah atas Peretasan Data Pribadi ditinjau dari Undang Undang. *Jurnal Riset Ilmu Hukum*, 95–100. https://doi.org/10.29313/jrih.v4i2.5193

Agung, A., Hafrida., & Erwin. (2022). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal*, 3(2), 212-222. https://online-journal.unja.ac.id/Pampas/article/view/23367/15107

Agustina, M., & Wiraguna, S. (2025). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Media Hukum Indonesia (MIH)*, 2(6), 117-127. https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1397/1547

Badan Siber Sandi Negara. (2024). Lanskap Keamanan Siber Indonesia. https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf

Dinas Komunikasi & Informatika Batam. (2024). https://kominfo.batam.go.id/8-tips-untuk-mencegah-kebocoran-data-pribadi/

Djafar, W., Sumigar, B.R.F., Setianti, B.L. (2016). *Perlindungan Data Pribadi di Indonesia, Lembaga Studi dan Advokasi Masyarakat (ELSAM).*

Fa'izi, M.B.N. (2024). 7 Strategi Efektif untuk Mencegah Kebocoan Data di Perusahaan. https://csirt.or.id/pengetahuan-dasar/mencegah-kebocoran-data

Hadjon, P.M. (1987). Perlindungan Hukum Bagi Rakyat di Indonesia, PT Bina Ilmu.

Karo, R.P.P., & Prasetyo, T. (2022). Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermartabat, Nusa Media.

Mahameru, D.E. (2025). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia, *Jurnal Esensi Hukum*, 5(2), https://journal.upnvj.ac.id/index.php/esensihukum/article/download/240/114

Mediana. (2024, 3 Juni). Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024. *Kompas*.

Nugroho, N.P. (2024, Juni 24). BSSN Dorong Penyusunan RUU Keamanan dan Ketahanan Siber. *Tempo*.

Rusyda, N.K. (2025). Perlindungan Hukum Terhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022, *Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, 2(3), 247-262. https://doi.org/10.62383/desentralisasi.v2i3.940

Sutarli, A.F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Sosial Science Research*, 3(2), 4208-4221. https://j-innovative.org/index.php/Innovative/article/view/760

Uttari, I.G.A.A.M., & Dewi, G.A.A.P. (2025). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Untuk Melakukan Suatu Tindak Pidana Penipuan Pada Media Sosial. *Jurnal Kertha Wicara*, 14(8), https://doi.org/10.24843/KW.2024.v14.i8.p3

Yudistira, M., & Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No.27 Tahun 2022 Oleh Kominfo. *Unes Law Review*, 5(4), https://doi.org/10.31933/unesrev.v5i4.698