

## HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA

Oleh:

Dewi Asri Puanandini<sup>1</sup>

Avika Sari Rahmallah Sapaat<sup>2</sup>

Muhammad Rafly Pasca Ramadhan<sup>3</sup>

Diva Philo Punggawa<sup>4</sup>

Derif Irfan purnama<sup>5</sup>

Universitas Islam Nusantara

Alamat: Jl. Soekarno-Hatta No.530, Sekejati, Kec. Buahbatu, Kota Bandung, Jawa Barat (40286).

Korespondensi Penulis: [dewipuannandini@gmail.com](mailto:dewipuannandini@gmail.com)<sup>1</sup>, [vikasari2405@gmail.com](mailto:vikasari2405@gmail.com)<sup>2</sup>,  
[rafly5975@gmail.com](mailto:rafly5975@gmail.com)<sup>3</sup>, [derifirfanpurnama@gmail.com](mailto:derifirfanpurnama@gmail.com)<sup>4</sup>, [difaphilo7@gmail.com](mailto:difaphilo7@gmail.com)<sup>5</sup>

**Abstract.** Individual protection is emphasized as a crucial issue given the rapid development of information technology. In Indonesia, the increasing incidence of data breaches and the widespread availability of personal information reflect weaknesses in regulation and oversight, as well as public understanding of the importance of online privacy. This article aims to examine the key challenges in protecting personal data and propose strategies applicable to Indonesia. The approach used is a normative-legal approach, analyzing existing laws and regulations, including Law No.27 of 2022 concerning personal data protection. The analysis shows the main challenges include the limited capacity of supervisory institutions, low digital literacy among the public, and weak law enforcement. Therefore, suggested solutions include strengthening independent supervisory institutions, developing comprehensive derivative regulations, improving digital literacy, and implementing strict sanctions for the many violations that occur. In conclusion, personal data protection in Indonesia requires a holistic and collaborative approach to create a system that is safe, fair, and in line with international standards.

# HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA

**Keywords:** *Personal Data, Legal Protection, Digital Privacy, PDP Law, Cyber Security.*

**Abstrak.** Perlindungan individu ditegaskan sebagai masalah penting mengingat perkembangan teknologi informasi yang sangat cepat. Di Indonesia, dengan meningkatnya insiden pelanggaran data dan luasnya informasi pribadi mencerminkan kelemahan dalam regulasi dan pengawasan, serta pemahaman masyarakat akan pentingnya privasi online. Artikel ini bertujuan untuk mengkaji tantangan utama dalam melindungi data pribadi dan mengusulkan strategi yang dapat diterapkan untuk Indonesia. Pendekatan yang di gunakan adalah pendekatan normatif- hukum dengan analisis terhadap peraturan perundang-undangan termasuk undang-undang No.27 tahun 2022 perlindungan data pribadi. Hasil analisis menunjukkan bahwa tantangan utama meliputi terbatasnya kapasitas lembaga pengawas, minimnya literasi digital di kalangan masyarakat, dan lemahnya penegakan hukum. Untuk itu, solusi yang disarankan antara lain penguatan lembaga pengawas yang independen, penyusunan regulasi turunan yang komprehensif, peningkatan literasi digital, dan penerapan sanksi yang tegas atas banyak nya pelanggaran yang terjadi. Kesimpulannya, perlindungan data pribadi di Indonesia memerlukan pendekatan holistik dan kolaboratif untuk menciptakan sistem yang aman, adil, dan sejalan dengan standar internasional.

**Kata Kunci:** Data Pribadi, Perlindungan Hukum, Privasi Digital, Undang-Undang PDP, Keamanan Siber.

## LATAR BELAKANG

Kemudahan akses terhadap data dan penggunaannya menimbulkan sejumlah risiko, seperti penyalahgunaan, pencurian identitas, dan pelanggaran privasi. Perlindungan data pribadi telah menjadi isu yang semakin penting, mengingat peningkatan signifikan dalam pertukaran informasi di dunia maya. Banyak individu yang tidak menyadari betapa pentingnya menjaga kerahasiaan data pribadi mereka, sementara banyak pelaku dapat dengan mudah mengeksploitasi informasi ini untuk tujuan komersial atau kriminal. Pemerintah Indonesia telah mengakui, Penting untuk melindungi data pribadi dengan menerapkan konsekuensi bagi pelanggaran yang terjadi.

Digitalisasi telah membawa sejumlah kemudahan, tetapi juga dapat menimbulkan risiko baru terkait dengan keamanan dan privasi, terutama mengenai perlindungan data

pribadi. Penggunaan aplikasi digital, media sosial, dan transaksi elektronik, serta sistem yang berbasis kecerdasan buatan, menghasilkan jejak digital yang besar dan beragam. Data pribadi, mulai dari identitas dan lokasi hingga preferensi perilaku, dapat dengan mudah dikumpulkan, dianalisis, dan bahkan dieksploitasi.

Dari perspektif teknologi, tantangan terbesar dalam melindungi data pribadi terletak pada kurangnya sistem keamanan siber yang kuat, kontrol akses yang lemah terhadap data, dan keterampilan digital pengguna yang terbatas. Banyak platform digital masih kekurangan penerapan prinsip keamanan data dari fase desain awal (Privasi dengan Desain), yang membuatnya sangat rentan terhadap serangan siber dan pelanggaran data. Selain itu, algoritma dan sistem otomatis sering memproses data tanpa transparansi dan keandalan yang memadai. Sementara itu, dari perspektif sosial, kurangnya kesadaran masyarakat tentang pentingnya perlindungan privasi data menjadi masalah serius. Sebagian besar pengguna internet di Indonesia masih tidak menyadari konsekuensi jangka panjang dari pelanggaran data atau penyalahgunaan data pribadi.

Dalam konteks ini, keamanan data sosial memerlukan perubahan dalam budaya digital dan peningkatan kemampuan pembelajar dalam masyarakat. Ini memerlukan sinergi antara pengembangan teknologi yang aman, regulasi adaptif, dan pendidikan umum yang berkelanjutan untuk menciptakan lingkungan digital yang sehat dan adil yang menghormati privasi masing-masing individu. Data pribadi adalah informasi sensitif bagi setiap individu dan mencakup hak atas privasi, yang harus dilindungi dari berbagai bidang kehidupan. Digitalisasi yang semakin meningkat dan penggunaan data individu juga meningkatkan kemungkinan penyalahgunaan. Kenaikan kejahatan siber di Indonesia juga dipengaruhi oleh kemajuan teknologi informasi. Istilah "hacking" atau "hacker" dalam Bahasa Indonesia merujuk pada tindakan ilegal mengakses data dari individu atau organisasi menggunakan komputer atau perangkat teknologi lainnya. Hacking adalah metode yang digunakan oleh individu seperti hacker, penyusup, atau pengganggu untuk menyerang sistem, jaringan, atau aplikasi dengan memanfaatkan kerentanan untuk mendapatkan akses yang tidak sah.<sup>1</sup> Saat ini, data individu mewakili nilai rendah yang tidak hanya melayani kepentingan tertentu tetapi juga perusahaan dan pemerintah. Di

---

<sup>1</sup> Ahmad Fachri yamin, DKK, PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL :TANTANGAN DAN SOLUSI, (Yogyakarta :penerbit Meraja Journal, 2024) hal 18

# **HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA**

Indonesia, laju perkembangan teknologi informasi dan komunikasi semakin cepat, yang mencakup berbagai bidang kehidupan, kebutuhan untuk melindungi data pribadi menjadi semakin mendesak. Sistem individu dan angka memberikan peluang untuk inovasi dan perbaikan efisiensi di beberapa area.

Dengan meningkatnya penyebaran internet dan ketergantungan masyarakat pada layanan digital, risiko kebocoran data informasi pribadi semakin meningkat dan memengaruhi berbagai kelompok. Ada banyak aplikasi dan platform elektronik yang mengumpulkan data tanpa transparansi dan tanpa persetujuan eksplisit dari pengguna. Ini menimbulkan pertanyaan penting tentang tingkat kontrol yang dimiliki Individu tersebut dilatih berdasarkan data pribadi mereka hingga Oktober 2023. Sebaliknya, kemajuan teknologi (AI) meningkatkan kemungkinan pemanfaatan data pribadi. Data yang sebelumnya dikumpulkan secara manual sekarang dapat ditangkap dan diproses secara otomatis, bahkan tanpa interaksi langsung antara individu dan sistem pengumpulan data. Dalam konteks ini, perlindungan data pribadi tidak lagi bersifat opsional, tetapi merupakan kebutuhan mendasar untuk memastikan hak asasi manusia di era digital.

Penurunan budaya digital dalam masyarakat juga berkontribusi pada semakin parahnya situasi ini. Banyak orang yang tidak menyadari bahaya membagikan data pribadi secara sembarangan di media sosial atau aplikasi informal. Selain itu, sanksi hukum yang lemah, dan kemampuan lembaga penegak hukum untuk bertindak terhadap pelanggaran data yang terbatas, menyebabkan kejahatan digital tetap ada tanpa ada pencegahan. memeriksa data pribadi dari perspektif hukum dianjurkan untuk mengevaluasi efektivitas undang-undang yang ada dan untuk menemukan solusi bagi berbagai tantangan yang muncul dalam penerapannya.

Dalam beberapa jurnal sebagai perbandingan penulis dalam teks ini, artikel pertama "Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi" oleh Ahmad Fashri Yamin dkk., Volume 7, Edisi 2, Tahun 2024, dan "Perlindungan Hukum Terhadap Pencurian Data Pribadi pada Penyedia Jasa Keuangan dibandingkan dengan Ancaman Keamanan Siber di Indonesia" oleh Amelia Hendaini, Volume 6, (4), Tahun 2023. Kedua jurnal tersebut berfokus pada perlindungan data pribadi, tantangan dan solusi, serta isu-isu di Indonesia dan apakah karya-karya ini merupakan pelanggaran hak asasi manusia atau hak fundamental bagi semua bagian masyarakat.

Dari kedua jurnal tersebut fokus penulis dalam tulisan ini adalah mengenai Peran Pemerintah dalam Privasi Perlindungan Data Pribadi, serta Tantangan Perlindungan Data dalam Cyber Security.

## **METODE PENELITIAN**

Setiap sumber yang ditemukan dievaluasi berdasarkan relevansi, kredibilitas, dan kualitas informasi yang disediakan. Tinjauan literatur yang komprehensif dilakukan untuk mengidentifikasi tema utama, tantangan, dan solusi yang diusulkan terkait perlindungan data pribadi. Data yang dikumpulkan kemudian disusun untuk memberikan pemahaman yang komprehensif tentang topik penelitian dan untuk mendukung argumen yang disajikan dalam artikel ini. Selain pendekatan penelitian literatur yang merupakan metode utama, penelitian ini juga menggunakan analisis hukum dengan fokus pada perbandingan kebijakan. Pendekatan ini diimplementasikan dengan membandingkan tentang Perlindungan Data Pribadi di Indonesia dengan regulasi internasional seperti Regulasi Perlindungan Data Umum (GDPR) Uni Eropa. Data sekunder yang dianalisis tidak terbatas pada literatur akademik, tetapi juga mencakup dokumen politik, publikasi dari institusi pemerintah, dan laporan dari organisasi non-pemerintah yang aktif di bidang hak digital dan keamanan siber.

Analisis dilakukan secara tematik untuk mengidentifikasi kesamaan dan perbedaan serta peluang untuk mengkoordinasikan regulasi dan memperkuat perlindungan data di Indonesia.

## **HASIL DAN PEMBAHASAN**

### **A. Peran Pemerintah dalam Perlindungan Privasi Data Pribadi**

Dalam konteks ini kebocoran data pribadi tidak bisa diremehkan. Selain tekanan psikologis pada korban, kerugian sosial dan ekonomi yang dihasilkan sangat besar. Penyebaran informasi pribadi, yang dikaitkan dengan ancaman atau teror psikologis, membuat korban merasa tidak aman bahkan di ruang pribadi mereka. Banyak korban menderita depresi, pengangguran, dan bahkan keretakan hubungan sosial akibat penyebaran informasi yang mencemarkan nama baik.

# **HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA**

Undang-Undang Nomor 27 Tahun 2022<sup>2</sup> yang mengatur tentang perlindungan data pribadi dan lebih dikenal sebagai Undang-Undang Perlindungan Data, berlaku di Indonesia. Data pribadi mencakup berbagai jenis informasi, seperti data spesifik, data kesehatan, biometrik, genetik, riwayat kriminal, informasi mengenai anak, data keuangan, informasi pribadi, serta data lainnya yang diwajibkan menurut ketentuan hukum. Sementara itu, data pribadi yang bersifat terbuka untuk umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data agregat pribadi yang bisa digunakan untuk mengenali individu.

Menurut Pasal 1 No. 2 Undang-Undang Perlindungan Data, data pribadi merujuk pada semua upaya keamanan untuk melindungi data pribadi dalam lingkup pemrosesan data untuk memastikan hak konstitusi individu yang bersangkutan. Undang-Undang Perlindungan Data mencakup petugas perlindungan data dan pengolah data pribadi. Petugas perlindungan data adalah orang, otoritas publik, atau organisasi internasional yang menentukan tujuan dan melaksanakan pengelolaan data pribadi secara sendiri atau bersama-sama. Pengolah data pribadi adalah orang, otoritas publik, atau organisasi internasional yang memproses data pribadi secara independen atau bersama-sama atas nama petugas perlindungan data. Otoritas eksekutif, legislatif, dan yudikatif serta lembaga lain yang tugas dan fungsinya terkait dengan organisasi pemerintah, yang sebagian atau sepenuhnya dibiayai oleh anggaran negara dan/atau anggaran pemerintah daerah atau organisasi non-pemerintah, selama sebagian atau seluruh uang berasal dari anggaran negara dan/atau anggaran pemerintah daerah, sumbangan dari masyarakat, dan/atau dari luar negeri. Oleh karena itu, otoritas publik seperti pemerintah dapat berfungsi sebagai badan pengawas atau sebagai pengolah data pribadi. Pasal 20 hingga 50 Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur sejumlah kewajiban bagi mereka yang berurusan dengan data pribadi, termasuk kewajiban untuk memberikan bukti persetujuan yang diberikan oleh subjek data pribadi selama pengolahan data, tanggung jawab

---

<sup>2</sup> Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP)

untuk menjaga kerahasiaan data pribadi, dan penekanan pada pencegahan akses yang tidak sah terhadap data pribadi ini. Di sisi lain, Pasal 51 hingga 52 UU PDP mencakup kewajiban bagi pengelola data pribadi untuk mematuhi berbagai ketentuan, termasuk pengolahan data pribadi berdasarkan instruksi mitra bisnis terkait data pribadi, dan mereka harus memperoleh persetujuan tertulis dari mitra bisnis terkait data pribadi sebelum melibatkan pihak ketiga sebagai pengolah data. Pejabat perlindungan data dan pengolah data pribadi harus menunjuk seorang pegawai atau orang yang bertanggung jawab untuk melaksanakan perlindungan data dalam pengolahan data pribadi untuk layanan publik. Jika kegiatan utama pejabat perlindungan data dicirikan oleh fitur, cakupan, dan tujuan yang memerlukan pemantauan data pribadi yang rutin dan sistematis dalam skala besar; dan jika kegiatan utama pejabat perlindungan data mencakup pengumpulan data pribadi yang luas dengan karakteristik tertentu dan/atau sehubungan dengan tindak pidana.

Dalam Undang-undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi yang di maksud Subjek data pribadi adalah individu yang memiliki data pribadi tentang diri mereka sendiri, dan memang, kita semua adalah anggota masyarakat. Pasal 5 hingga 15 Undang-undang perlindungan data merinci hak-hak individu yang terkena dampak, ini termasuk hak untuk mendapatkan informasi tentang kejelasan identitas mereka, dasar hukum yang digunakan, serta tujuan pengumpulan dan penggunaan data pribadi., di samping tanggung jawab entitas yang meminta data tersebut.

Pelanggaran perlindungan data pribadi menjadi kewajiban petugas dimana perlindungan data harus mengirimkan pemberitahuan tertulis kepada orang yang terkena dampak dan otoritas pengawas dalam waktu maksimum 3 hari kerja. Pemberitahuan mencakup: menangani pelanggaran data dan memulihkan data. Selain itu, dalam kasus tertentu, seperti ketika kegagalan mempengaruhi layanan publik dan/atau berdampak serius pada keselamatan publik, petugas perlindungan data harus memberi tahu publik tentang pelanggaran perlindungan data pribadi. Namun, kita harus mencatat bahwa kewajiban untuk memberikan pemberitahuan tertulis mengenai data pribadi, dalam kasus pelanggaran perlindungan data pribadi, dapat mengancam kepentingan perlindungan dan keamanan negara;

## **HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA**

kepentingan penegakan hukum; kepentingan publik dalam konteks administrasi urusan publik; atau kepentingan pengawasan di sektor layanan keuangan, dalam transaksi uang dan pembayaran, serta stabilitas sistem keuangan. keputusan ini hanya diterapkan dalam kerangka penegakan hukum. Sanksi administrasi dapat dikenakan, yang terdiri dari pemberitahuan tertulis, penarikan sementara oleh individu, serta penghapusan atau penghancuran data pribadi, dan sanksi administrasi untuk pelanggaran ketentuan sesuai dengan Undang-Undang Perlindungan Data. Otoritas memberlakukan perubahan administratif dan denda sebesar 2 persen dari total pendapatan tahunan atau pendapatan tahunan yang disetujui dalam hal pelanggaran.

Selain aturan dalam Undang-undang Nomor 27 Tahun 2022, Ada beberapa perundang- undangan lain yang mengatur privasi dan perlindungan data pribadi di Indonesia ,yaitu :

- a) Sanksi administrasi dapat dikenakan, yang terdiri dari pemberitahuan tertulis, penarikan sementara oleh individu, serta penghapusan atau penghancuran data pribadi, dan sanksi administrasi untuk pelanggaran Pasal 46 ayat (1) dan (3) sesuai dengan Pasal 47 Undang-Undang Perlindungan Data. Otoritas memberlakukan perubahan administratif dan denda sebesar 2% total pendapatan yang disetujui dalam hal pelanggaran.
- b) Undang-undang nomor 23 tahun 2006 yang berkaitan dengan pengelolaan penduduk sesuai dengan undang-undang nomor 24 tahun 2013, fokus pada perlindungan rahasia data penduduk (seperti nomor identifikasi nasional, kartu keluarga, dan informasi biometrik). Pasal 79 : Kerahasiaan donasi penduduk yang menjadi anak didiknya dan tidak dapat dilayani oleh juridiques tertentu .
- c) Hak-hak konsumen dilindungi oleh Undang-Undang No. 8 Tahun 1999. Ini termasuk perlindungan data pribadi konsumen yang diberikan kepada perusahaan perdagangan. Peraturan pelaksanaan dan peraturan sektor tertentu.
- d) Hak-hak konsumen dilindungi oleh Undang-Undang No. 8 Tahun 1999. Ini termasuk perlindungan data pribadi konsumen yang diberikan kepada

perusahaan perdagangan. Peraturan pelaksanaan dan peraturan sektor tertentu.

Contoh Analisis Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Fintech Pinjaman Online :

Data pribadi sering disebarkan oleh layanan kredit online, terutama dalam kasus pinjaman ilegal, di mana data seperti identifikasi, foto, dan informasi kontak korban dibagikan kepada pihak ketiga atau dipublikasikan untuk memberikan tekanan dalam penagihan utang. Praktik ini melanggar prinsip-prinsip hak asasi manusia.

Dampak dari pelanggaran terhadap korban mengalami kerugian psikologis, sosial, dan ekonomi akibat penyebaran data pribadi, termasuk ancaman, terorisme, dan pencemaran nama baik. Hal ini juga menyebabkan kecemasan dan rasa tidak aman dalam masyarakat. Upaya hukum untuk memulihkan hak-hak korban dapat mengejar jalur pidana, perdata, dan administratif, di samping melapor kepada pihak berwenang yang relevan seperti OJK, komisi hak asasi manusia, dan polisi. Selain itu, advokasi non-hukum dan kampanye publik merupakan bagian dari upaya untuk memulihkan hak asasi manusia korban. Namun, masih ada banyak hambatan untuk pelaksanaan undang-undang perlindungan data, seperti kurangnya pengawasan dan penegakan hukum terhadap pinjaman online ilegal, tingkat pemahaman hukum dan kewarganegaraan digital yang rendah, serta kurangnya perbaikan yang memadai terhadap peraturan-peraturan yang diturunkan dari undang-undang perlindungan data. Oleh karena itu, perlu untuk menemukan solusi komprehensif yang mencakup promosi regulasi dan otoritas pengawas, penguatan pendidikan digital dan hukum, kerja sama antara lembaga, serta advokasi dan dukungan psikososial bagi para korban. Ini dapat mencapai perlindungan hukum untuk data pribadi dan secara efektif dan adil memulihkan hak asasi manusia dari korban yang terdampak penerbitan data melalui peminjaman di era digital. Penerbitan data pribadi melalui peminjaman, terutama dalam praktik penagihan utang yang melibatkan ancaman dan terorisme digital, adalah pelanggaran serius yang harus menjadi perhatian khusus dari

# **HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA**

perspektif regulasi, penegakan hukum, dan peningkatan kesadaran masyarakat.

Dampak pelanggaran keamanan data dalam konteks pinjaman online tidak boleh dianggap remeh. Selain tekanan psikologis pada para korban, kerugian sosial dan ekonomi juga signifikan. Penyebaran informasi pribadi, disertai dengan ancaman atau teror psikologis, membuat korban merasa tidak aman bahkan di ruang mereka sendiri. Banyak korban yang kemudian menderita depresi, kehilangan pekerjaan, dan bahkan mengalami keruntuhan hubungan sosial akibat penyebaran data yang merugikan reputasi mereka. Dalam konteks ini, pentingnya negara sebagai pelindung hak-hak warganya menjadi jelas. Peran pemerintah tidak terbatas pada pembuatan undang-undang tetapi juga harus diwujudkan dalam bentuk pelaksanaan konkret yang dirasakan oleh masyarakat. Pemerintah memikul tanggung jawab untuk memastikan bahwa setiap pelanggaran data pribadi ditanggapi secara tegas, termasuk penerapan sanksi administratif, sipil, dan kriminal sesuai kebutuhan. Memperkuat peran badan pengawas untuk perlindungan data pribadi sangat mendesak agar pengendalian dan pengolahan data oleh penyedia sistem elektronik tidak disalahgunakan. Dalam konteks ini, pengawasan harus independen dan terorganisir, serta harus memiliki kewenangan yang jelas. Selain itu, pemerintah harus mendorong pengembangan sistem teknologi yang mampu mendeteksi pelanggaran atau kebocoran data potensial sejak dini, dan memberikan akses cepat dan mudah bagi warga untuk melaporkan. Menangani pelanggaran data dari pinjaman online ilegal adalah contoh nyata yang seharusnya menjadi pelajaran bersama untuk terus meningkatkan dan menerapkan sistem regulasi.

Dari Beberapa peraturan yang penulis jabarkan sejauh ini peran pemerintah dalam perlindungan data pribadi masih kurang efektif karena masih banyak nya kasus-kasus seperti data pribadi atau identitas pribadi tersebar.

## **B. Tantangan Perlindungan Data dalam Cyber Security**

Peningkatan Ancaman siber, termasuk, penipuan, semakin kompleks. Penjahat dunia maya sering kali menjadi korban kejahatan siber dan tidak dapat memperoleh manfaat dari pemodal atau penyebab kehancuran . Tantangan terbesar adalah memastikan bahwa sistem keamanan selalu berada pada satu langkah di depan ancaman. Dari hasil penelitian penulis terdapat beberapa tantangan dalam perlindungan data dalam Cyber Security :

- a) Ancaman serangan siber yang terus berkembang : jenis serangan baru seperti ransomware, phishing, malware, dan advanced persistent threat (APT) semakin canggih.
- b) Kurangnya kesadaran pengguna : banyak pengguna tidak menyadari pentingnya menjaga kerahasiaan pribadi, praktik buruk seperti penggunaan kata sandi lemah atau berbagai informasi di media sosial membuat data mudah disalgunakan.
- c) Minimnya keamanan sistem dan aplikasi : perusahaan sering mengabaikan pembaruan sistem keamanan (security patch), aplikasi yang dikembangkan tanpa memperhatikan keamanan rentan terhadap eksploitasi.
- d) Kekurangan sumber daya dan tenaga ahli : kurangnya tenaga ahli cyber security yang kompeten, terutama di negara berkembang, biayanya tinggi untuk membangun dan memelihara sistem keamanan yang solid.
- e) Peraturan dan penegakan hukum yang lemah : tidak semua negara memiliki undang-undang perlindungan data yang kuat, sulit menindak pelaku kejahatan siber lintas negara karena perbedaan yuridiksi.
- f) Ketergantungan pada cloud dan IoT : data kini banyak disimpan di cloud atau perangkat internet of things (IoT) ,yang meningkatkan potensi titik serangan ,jika tidak dikonfigurasi dengan benar ,data dalam cloud bisa bocor.
- g) Sulitnya menjaga privasi di era big data dan AI : teknologi AI dan big data memproses data jumlah besar, termasuk, data sensitif ,dilema muncul antara manfaat teknologi dan perlindungan privasi.

## **HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA**

- h) Insider threat (ancaman dari dalam) : karyawan atau orang dalam perusahaan bisa dengan sengaja atau tidak sengaja membocorkan data, sering kali lebih sulit dideteksi dibanding serangan dari luar .
- i) Kurangnya standar keamanan yang konsisten : perusahaan dan organisasi belum semuanya menerapkan standar keamanan siber yang sama seperti ISO 27001, NIST, Ini menciptakan celah yang bisa dimanfaatkan oleh pelaku kejahatan.
- j) Pemulihan dan repons insiden yang lemah : banyak organisasi belum memiliki rencana pemulihan bencana ,terlambatnya respons terhadap insiden menyebabkan kerugian yang lebih besar.

Berbagai solusi yang dapat diterapkan untuk meningkatkan keamanan data pribadi maupun organisasi, yaitu:

- a) Peningkatan pendidikan dan kesadaran Awareness di masyarakat tentang pendidikan digital untuk semua, sehingga mereka dapat memahami risiko dan melindungi staff mereka. Keamanan informasi terhadap phishing, malware, dan manipulasi sosial (rekayasa sosial).
- b) penguatan regulasi dan penegakan hukum
  - 1) Implementasi dan pengawasan UU perlindungan data pribadi
  - 2) Memberikan sanksi tegas terhadap pelanggaran ,kebocoran,atau penyalahgunaan data.
  - 3) Pengawas independen yang berwenang
- c) Teknologi keamanan siber
  - 1) Penggunaan enkripsi untuk menyimpan dan mengirim data pribadi.
  - 2) Penerapan autentikasi dua faktor atau multi faktor authentication
- d) Tanggung jawab organisasi dan perusahaan
  - 1) Menyediakan kebijakan privasi yang mudah dipahami pengguna.
  - 2) Melakukan audit keamanan data secara berkala.
  - 3) Membatasi akses ke data pribadi hanya untuk pihak yang berwenang
- e) Infrastruktur dan kolaborasi nasional
  - 1) Pengembangan pusat keamanan siber nasional untuk koordinasi

penganggulan insiden

- 2) Kerja sama antar lembaga, sektor swasta, dan akademisi dalam pengembangan standar keamanan data
- 3) Partisipasi aktif Indonesia dalam kerja sama internasional tentang perlindungan data.

## **KESIMPULAN DAN SARAN**

### **Kesimpulan**

Perlindungan data pribadi di Indonesia masih menghadapi berbagai tantangan, terutama dalam hal efektivitas peran pemerintah dan meningkatnya ancaman keamanan siber. Meskipun telah terdapat regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya belum sepenuhnya optimal. Pemerintah masih dianggap kurang sigap dalam mengawasi dan menindak pelanggaran data, serta belum mampu membangun sistem pengamanan digital yang andal secara menyeluruh.

Di sisi lain, ancaman keamanan siber terus berkembang seiring dengan kemajuan teknologi. Kebocoran data, pencurian identitas, dan serangan siber lainnya menjadi risiko serius yang mengancam hak privasi masyarakat. Ketidaksiapan infrastruktur digital dan minimnya literasi keamanan data di kalangan publik semakin memperburuk situasi.

### **Saran**

Perlindungan data pribadi memerlukan penguatan dari berbagai sisi: regulasi yang tegas dan operasional, peningkatan kapasitas kelembagaan, pengawasan yang aktif, edukasi masyarakat, serta kolaborasi yang erat antara pemerintah, sektor swasta, dan masyarakat sipil untuk membangun ekosistem digital yang aman dan berpihak pada hak asasi manusia.

Solusi yang dapat ditindaklanjuti meliputi:

1. memperkuat suborganisasi dan otoritas regulasi profesional yang independen;
2. (2) meningkatkan kesadaran digital di masyarakat untuk menciptakan pemahaman yang lebih baik tentang hak atas privasi;
3. (3) menerapkan sistem keamanan siber yang kuat melalui penyedia layanan digital; dan

# HAM PERLINDUNGAN DATA PRIBADI TANTANGAN DAN SOLUSI DI INDONESIA

4. menerapkan undang-undang yang konsisten dan transparan terhadap pelanggaran data pribadi. Melalui kolaborasi berbagai pemangku kepentingan, diharapkan Indonesia akan membangun sistem untuk melindungi data pribadi.

## DAFTAR REFERENSI

- Ahmad Fachri yamin,DKK,PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL :TANTANGAN DAN SOLUSI,(Yogyakarta :penerbit Meraja Journal,2024) hal 18
- Ashady, S. (2024). Cybercrime sebagai Kejahatan Dunia Maya dalam Perspektif Hukum dan Masyarakat. *Juridische: Jurnal Penelitian Hukum*, Query date: 2024-06-05 11:40:45. <https://jurnal.bisakonsul.com/index.php/juridische/article/view/19>
- Daeng, Y., Levin, J., Karolina, K., Prayudha, M., & ... (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. *Innovative: Journal Of ...*, Query date: 2024-06-05 11:40:45. <http://j-innovative.org/index.php/Innovative/article/view/6376>
- Daeng, Y., Linra, N., Darham, A., Handrianto, D., & ... (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of ...*, Query date: 2024-06-05 11:40:45. <http://j-innovative.org/index.php/Innovative/article/view/6662>
- Dm, M., & Hasibuan, R. (2022). Tindak Pidana Cyber Crime Dan Sanksinya Dalam Undang Undang Informasi Dan Transaksi Elektronik. *Andrew Law Journal*, Query date: 2024-0605 11:40:45. <https://journal.andrewlawcenter.or.id/index.php/ALJ/article/download/11/9>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam sistem hukum di Indonesia.
- Parulian, Sahat et al, 'Ancaman dan Solusi Serangan Siber di Indonesia' (2021), 1 Jurnal UPI.
- Undang-undang No. 27 TAHUN 2022 tentang Perlindungan Data Pribadi (PDP)