as-Shahifah:
Journal of Constitutional Law and Governance, Vol. 5 No. 1 2025: (page 78-99) ISSN: 2829-4246, E-ISSN: 2829-6206
DOI: http://doi.org/10.19105/asshahifah.v5i1.22148

Perlindungan Data Pribadi Di Indonesia Pasca Pengesahan UU No. 27 Tahun 2022 di Era Digital

Yurike Maulina
Program Studi Hukum Tata Negara, Uin Sunan Ampel Surabaya
email: rikemaulina24@gmail.com

Abstract

The rapid development of information technology and the enormous potential of the digital economy have had positive impacts, but have also given rise to new challenges, particularly regarding the protection of the right to privacy and personal data. Privacy is a fundamental right that, while not absolute, still requires strong legal protection, especially in today's digital era, which is rife with online activity. The enactment of Law Number 27 of 2022 concerning Personal Data Protection is a crucial step in providing legal certainty for the public, particularly consumers conducting online transactions. This law unifies various sectoral regulations into a single, comprehensive and consistent legal framework, aligning with global data protection principles. This research uses a normative legal method that examines applicable laws and regulations. Law Number 27 of 2022 introduces a modern approach to personal data protection, which aligns with the European Union's General Data Protection Regulation (GDPR). It regulates data controllers, data processors, and the rights of data subjects. One of the advantages of this law is its broad scope, encompassing the personal data of both Indonesian citizens and foreign nationals, both within and outside Indonesian jurisdiction, as stated in Article 2 paragraph (1). This demonstrates Indonesia's commitment to protecting personal data in accordance with global standards. With the enactment of this law, the public now has a stronger legal basis for demanding their rights to personal data and encourages accountability among electronic system administrators.

Keywords :
Law No. 27 of 2022, Legal Protection, Personal Data Protection.

Author correspondence email: rikemaulina24@gmail.com
Available online at: http://ejournal.iainmadura.ac.id/index.php/asShahifah/

Abstrak

Perkembangan teknologi informasi yang pesat serta potensi besar dari ekonomi digital membawa dampak positif, namun juga memunculkan tantangan baru, khususnya terkait perlindungan hak atas privasi dan data pribadi. Privasi merupakan bagian dari hak fundamental yang meskipun tidak absolut, tetap membutuhkan perlindungan hukum yang kuat, terlebih di era digital saat ini yang penuh dengan aktivitas daring. Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi langkah penting dalam memberikan kepastian hukum bagi masyarakat, khususnya konsumen yang bertransaksi secara online. Undang-undang ini menyatukan berbagai regulasi sektoral ke dalam satu kerangka hukum yang komprehensif dan konsisten, serta sejalan dengan prinsip-prinsip perlindungan data global. Penelitian ini menggunakan metode hukum normatif yang menelaah norma dan peraturan perundang-undangan yang berlaku. UU No. 27 Tahun 2022 memperkenalkan pendekatan modern terhadap pelindungan data pribadi, yang telah sejalan dengan aturan pelindungan data pribadi yang telah berlaku di UniEropa, yaitu General Data Protection Regulation (GDPR) Uni Eropa. Di dalamnya terdapat pengaturan mengenai pengendali data, prosesor data, serta hak-hak subjek data. Salah satu keunggulan undang-undang ini adalah cakupannya yang luas, mencakup data pribadi WNI maupun WNA, baik yang berada di dalam maupun di luar wilayah hukum Indonesia, sebagaimana tercantum dalam Pasal 2 ayat (1). Hal ini menunjukkan komitmen Indonesia dalam melindungi data pribadi sesuai standar global. Dengan berlakunya UU ini, masyarakat kini memiliki landasan hukum yang lebih kuat dalam menuntut hak atas data pribadi dan mendorong tanggung jawab penyelenggara sistem elektronik.

Kata Kunci :

UU No. 27 Tahun 2022, Perlindungan Hukum, Pelindungan Data Pribadi.

Pendahuluan

Dalam era kemajuan teknologi komunikasi dan informasi, data pribadi seperti Kartu Tanda Penduduk (KTP), Nomor Induk Kependudukan (NIK), dan Kartu Keluarga (KK) memiliki nilai ekonomi yang signifikan dalam dunia bisnis digital. Informasi tersebut,

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 2

yang dikenal sebagai *digital dossier*, merupakan kumpulan data pribadi yang disimpan secara digital oleh individu dan umumnya dikelola melalui infrastruktur berbasis internet oleh entitas swasta. Meskipun memberikan peluang besar untuk inovasi dan efisiensi, pemanfaatan data pribadi tersebut juga menimbulkan potensi pelanggaran terhadap hak privasi individu. Data pribadi merupakan keterangan yang benar dan nyata yang melekat pada diri seseorang, sehingga dapat mengidentifikasikan orang tersebut. Pentingnya perlindungan data pribadi adalah untuk memastikan bahwa data pribadi seseorang yang terkumpul digunakan sesuai dengan tujuan pengumpulan, sehingga tidak terjadi penyalahgunaan data. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut *the right to private life*. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi.[1]

Teknologi informasi telah merevolusi pola hidup masyarakat, menciptakan perubahan yang signifikan dalam aspek sosial, budaya, ekonomi, hingga kerangka hukum. Salah satu dampak nyata dari perubahan ini adalah lahirnya ekonomi digital, yang tumbuh seiring dengan meningkatnya penggunaan teknologi informasi dan komunikasi secara global. Ekonomi digital telah mendorong transformasi dari sistem ekonomi tradisional berbasis industri manufaktur ke arah sistem yang mengandalkan data, platform digital, dan konektivitas.

Indonesia sebagai negara terpadat di Asia Tenggara dengan populasi 262 juta dengan 140 juta terhubung internet, sekitar 28 juta orang (13% growth YoY) aktif melakukan transaksi online. Kapasitas Indonesia dengan sekitar 49 juta UMKM (SME's) membuat pemerintah Indonesia bertekad menjadi negara dengan digital ekonomi terbesar di Asia Tenggara dimana pada tahun 2020 menyakini akan

[1] European Union Agency for Fundamental Rights and Council of Europe, Supra No. 5, hlm. 37.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 3

mampu akan menyerap 26 juta lebih tenaga kerja.[2] Indonesia memiliki potensi besar sebagai pasar ekonomi digital yang menjanjikan. Hal ini tercermin dari jumlah populasi yang mencapai 265,4 juta jiwa, di mana sekitar 50% atau 132,7 juta penduduk telah terhubung dengan internet. Dari jumlah tersebut, pengguna perangkat seluler tercatat sebanyak 177,9 juta orang, sementara pengguna aktif media sosial melalui perangkat seluler mencapai 120 juta orang. Berdasarkan hasil riset yang dilakukan oleh Google dan Temasek pada tahun 2018, nilai pasar ekonomi digital Indonesia diproyeksikan mencapai USD 100 miliar pada tahun 2025.[3]

Namun, pesatnya digitalisasi ini juga menghadirkan resiko yang kompleks terhadap perlindungan data pribadi. Sebelum hadirnya regulasi yang spesifik, perlindungan data pribadi di Indonesia tersebar dalam berbagai peraturan perundang-undangan, seperti UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, UU No. 39 Tahun 1999 tentang Hak Asasi Manusia, UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik, serta UU No. 23 Tahun 2006 jo. UU No. 24 Tahun 2013 tentang Administrasi Kependudukan.[4] Pengaturan yang tersebar ini menimbulkan celah hukum dan kelemahan dalam pengawasan, yang pada akhirnya memungkinkan terjadinya penyalahgunaan, pencurian,

---

[2] Olisias Gultom, Katrin Schneider, dan Lea Mareen Preis, Ekonomi Digital, Harapan, dan Ancaman Belajar dari Indonesia,diunduhmelaluihttp://igj.or.id/wp-content/uploads/2018/11/Industrial-Revolution4_IGJ_AEPF12_Ind 1.pdf, diakses tanggal 12 Juli 2024.

[3] Ekon.go.id, "Menko Airlangga: Pengembangan Ekonomi Digital di Indonesia, Tidak Hanya Target Pasar Tapi Harus Jadi Pemain Global", terdapat dalam Website: https://ekon.go.id/publikasi/detail/3433/menko airlangga-pengembangan-ekonomi-digital-di-indonesia-tidak-hanya-target-pasar-tapi-harus-jadi-pemain-global, diakses tanggal 12 Juli 2024 Pukul 06.47 WIB.

[4] Lina Miftahul Jannah, "UU Perlindungan Data Pribadi dan Tantangan Implementasinya", Artikel online 03 Oktober 2022 terdapat dalam situs: https://jdih.sukoharjokab.go.id/informasi/detail/89, diakses tanggal 12 Juli 2024.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 4

hingga penjualan data pribadi secara ilegal. Tindakan-tindakan tersebut tidak hanya melanggar hukum di bidang teknologi informasi, tetapi juga merupakan pelanggaran terhadap hak asasi manusia. Sebagai respon terhadap kondisi tersebut, pemerintah Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang diresmikan pada 17 Oktober 2022 oleh Presiden Joko Widodo. Pengesahan UU ini merupakan tonggak penting dalam sistem hukum Indonesia, karena untuk pertama kalinya pengaturan perlindungan data pribadi diatur secara komprehensif dalam satu instrumen hukum khusus.

Sehubungan dengan itu, artikel ini akan membahas secara mendalam mengenai konsep perlindungan data pribadi dalam perspektif hukum, pengaturan data pribadi sebagaimana diatur dalam UU No. 27 Tahun 2022, serta tantangan-tantangan utama yang dihadapi dalam upaya perlindungan data pribadi di era digital. Pembahasan ini diharapkan dapat memberikan kontribusi terhadap pengembangan kerangka hukum yang adaptif, responsif, dan menjamin perlindungan hak-hak individu dalam ekosistem digital yang terus berkembang.

Metode Penelitian

Jenis Penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif (doctrinal legal research), yakni penelitian tentang hukum sebagai norma dan kenyataan (perilaku) atau sebagai sesuatu yang dicita citakan dan sebagai realitas atau hukum yang hidup, bahkan disiplin hukum terkait jenis penelitian ini memiliki segi umum dan khusus.[5] Adapun metode pendeketan dalam penelitian ini menggunakan pendekatan perundang-undangan (statute approach) yakni pendekatan dengan menggunakan legislasi dan regulasi.[6]

[5] Sonata, D. L. Metode Penelitian Hukum Normatif dan Empiris: Karakteristik Khas dari Metode Meneliti Hukum.Fiat Justisia Jurnal Ilmu Hukum, 8(1), (2014). Hlm. 15-35.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 5

[6] Marzuki, P.M. Penelitian Hukum. (Jakarta: Kencana, 2005), hlm. 141.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 6

Hasil dan Pembahasan

Konsep Perlindungan Data Pribadi Dalam Hukum

Perlindungan data pribadi merupakan aspek penting dalam era digital saat ini, di mana data pribadi individu sering kali dikumpulkan, diproses, dan disimpan oleh berbagai entitas, baik pemerintah maupun swasta. Dalam konteks hukum, perlindungan data pribadi mengacu pada upaya legislasi dan regulasi untuk menjamin hak individu atas data pribadinya tetap terlindungi dari penggunaan yang tidak sah, penyalahgunaan, dan pelanggaran keamanan. Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara manusia berinteraksi, memperoleh informasi, dan melakukan transaksi ekonomi maupun sosial. Salah satu dampaknya adalah meningkatnya volume data pribadi yang dikumpulkan, diproses, dan disimpan oleh berbagai entitas. Oleh karena itu, perlindungan data pribadi menjadi isu penting yang harus diatur secara hukum agar hak-hak individu tetap terlindungi dan mengurangi risiko penyalahgunaan data.[7]

Data pribadi menurut UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP**)** didefinisikan sebagai setiap data mengenai orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik.[8] Van der Sloot menyatakan bahwa istilah data pribadi tidak hanya mencakup informasi yang bersifat sensitif atau pribadi, tetapijuga mencakup data yang bersifat publik dan non-sensitif Bukannya memberikan hak untuk mengendalikan (data), inti dari prinsip-prinsip perlindungan data terletak pada keadilan dan kesetaraan dalam pemrosesan data.[9]

---

[7] H. T. S. Putra, Perlindungan Data Pribadi dalam Perspektif Hukum Nasional dan Internasional, (Jakarta:Kencana,2021), hlm. 1.
[8] UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 Ayat (1)
[9] Van der Sloot, Bart., The Boundaries of Data, Amsterdam University Press, 2024

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 7

Konsep perlindungan data pribadi dalam hukum berakar pada prinsip hak atas privasi, yang secara internasional diakui sebagai bagian dari hak asasi manusia. Dalam konteks hukum modern, perlindungan data pribadi berarti bahwa setiap individu memiliki hak untuk mengontrol bagaimana data pribadinya dikumpulkan, digunakan, disimpan, dan disebarluaskan oleh pihak lain.

Perlindungan ini mencakup beberapa prinsip dasar, antara lain:

1. Legitimasi dan Keabsahan Pemrosesan
   Data pribadi hanya boleh diproses jika ada dasar hukum yang sah, seperti persetujuan subjek data, kewajiban hukum, atau kepentingan yang sah. Ini mencegah pemrosesan yang sewenang-wenang dan memastikan penggunaan data sesuai tujuan yang sah.

2. Transparansi dan Tujuan yang Jelas
   Setiap pemrosesan data harus dilakukan dengan transparan dan untuk tujuan yang jelas. Subjek data berhak mengetahui siapa yang mengumpulkan data, untuk apa digunakan, dan sejauh mana data tersebut dibagikan.

3. Minimisasi Data dan Pembatasan Retensi
   Hanya data yang relevan dan diperlukan yang boleh dikumpulkan. Selain itu, data tidak boleh disimpan lebih lama dari yang dibutuhkan. Hal ini bertujuan mengurangi risiko penyalahgunaan.

4. Keamanan dan Integritas Data
   Pengendali data memiliki tanggung jawab untuk melindungi data pribadi dari akses ilegal, kebocoran, atau kerusakan, dengan menerapkan langkah-langkah teknis dan organisasi yang memadai.

5. Akses dan Koreksi oleh Subjek Data

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 8

Individu memiliki hak untuk mengakses data pribadi

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 9

> mereka, meminta perbaikan jika data tidak akurat, dan dalam kondisi tertentu, meminta penghapusan data.

Konsep ini menjadi semakin penting karena data pribadi telah menjadi komoditas dalam ekonomi digital, dan pengguna sering kali tidak menyadari sejauh mana data mereka dikumpulkan dan digunakan. Dengan demikian, hukum perlindungan data bertujuan menyeimbangkan antara kebutuhan pengolahan data dan perlindungan hak-hak individu.

Pengaturan Perlindungan Data Pribadi Dalam Undang-Undang Nomor 27 Tahun 2022

Saat ini, Indonesia telah memiliki regulasi khusus yang secara eksplisit mengatur mengenai perlindungan data pribadi, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Undang-undang ini disahkan oleh pemerintah bersama Dewan Perwakilan Rakyat (DPR) pada 20 September 2022, dan mulai berlaku efektif pada 17 Oktober 2022. Tujuan utama dari UU ini adalah untuk memberikan kepastian hukum dalam menjamin hak setiap warga negara atas data pribadinya. Dalam Pasal 1 ayat (2), UU PDP menegaskan bahwa *"Pelindungan data pribadi adalah upaya menyeluruh untuk melindungi data pribadi dalam proses pengolahan data guna menjamin hak konstitusional subjek data pribadi."* Ketentuan ini menunjukkan bahwa data pribadi diakui sebagai bagian dari hak asasi manusia, dan oleh karena itu dilindungi secara hukum. Pasal 2 ayat (1) menyatakan bahwa "UU ini berlaku bagi seluruh pihak, baik individu, institusi publik, badan hukum, maupun organisasi internasional, tanpa memandang lokasi geografis mereka." Artinya, aturan ini tidak hanya berlaku di wilayah Indonesia, tetapi juga

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 10

menjangkau pihak di luar negeri sepanjang aktivitas pengolahan data tersebut menimbulkan dampak hukum di Indonesia.[10]

Ketentuan ini mencerminkan prinsip ekstra-teritorialitas, di mana yurisdiksi hukum Indonesia meluas ke luar batas negara dalam hal pelindungan data pribadi. Dengan demikian, UU PDP mengadopsi prinsip bahwa setiap entitas yang memproses data pribadi warga negara Indonesia, baik di dalam maupun di luar negeri, tetap terikat pada ketentuan hukum nasional selama tindakan mereka memiliki konsekuensi hukum di Indonesia. Untuk menjamin serta melindungi hak atas data pribadi, Undang-Undang ini menetapkan delapan prinsip utama, yaitu kepastian hukum, perlindungan, kemanfaatan, kehati- hatian, kepentingan publik, pertanggungjawaban,keseimbangan serta kerahasiaan sesuai dalam Pasal 3 Data pribadi yang dilindungi mencakup informasi yang mampu mengidentifikasi individu, baik secara langsung maupun tidak langsung, dalam berbagai bentuk, baik di sistem elektronik maupun non-elektronik.[11] Undang-Undang ini juga memberikan aturan pemrosesan data pribadi pada Pasal 16, yang menjadi prinsip dasar perlindungan data pribadi. Pemrosesan data pribadi meliputi berbagai kegiatan, mulai dari pengumpulan, pengolahan, analisis, penyimpanan, pembaruan, sampai penghapusan ataupun pemusnahan data. Semua kegiatan pemrosesan ini harus dilakukan dengan tetap mematuhi prinsip perlindungan data pribadi, yaitu bahwa data harus diproses secara sah, terbatas, dan transparan.[12]

Selain itu, tujuan dari pemrosesan data harus dijelaskan secara jelas, akurat, Serta lengkap supaya tidak menimbulkan kebingungan. Penting juga untuk memastikan bahwa hak subjek data dilindungi. Pemrosesan data pribadi mesti mendahulukan perlindungan terhadap

[10] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 ayat (2) dan Pasal 2 ayat (1).

[11] Nur Alfiana Alfitri. (2024). Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. 4(2): 92–111, p. 98

[12] M. Ciko Ar Rasyid. (2024). kajian yuridis undang-undang perlindungan data pribadi terhadap tanggung jawab perusahaan pada kasus kebocoran data konsumen (Studi Kasus Pada PT Telkom Indonesia). (Fakultas HukumUniversitas Muhammadiyah Magelang), p. 39.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 11

data dari akses atau pengungkapan yang tidak sah. Selain itu, data harus dimusnahkan atau dihapus setelah periode retensinya berakhir, kecuali jika terdapat aturan lain yang diatur dalam peraturan perundang-undangan.[13] Pasal 19 UU No. 27 Tahun 2022 mengatur mengenai pengendali data pribadi dan prosesor data pribadi, yang mencakup individu, lembaga publik, dan organisasi internasional. Pengendali data adalah pihak yang menentukan tujuan dan cara pemrosesan data pribadi, baik sendiri maupun bersama pihak lain. Sementara itu, prosesor data merupakan pihak yang memproses data atas nama pengendali. Selanjutnya, Pasal 20 ayat (1) dan (2) menetapkan bahwa setiap pemrosesan data pribadi harus didasarkan pada landasan hukum yang sah. Dasar hukum tersebut dapat berupa: persetujuan eksplisit dari subjek data untuk tujuan tertentu, pelaksanaan perjanjian, kewajiban hukum, perlindungan kepentingan vital subjek data, atau pelaksanaan tugas dalam kepentingan umum dan pelayanan publik.[14]

Menurut pasal-pasal yang ada, Pemrosesan data pribadi hanya boleh dilakukan dengan persetujuan yang sah dari individu yang bersangkutan.Pengendali data harus memberikan informasi yang cukup tentang tujuan pemrosesan data.[15]

Tantangan Perlindungan Data Pribadi di Era Digital

Urgensi perlindungan data pribadi semakin mengemuka seiring meningkatnya kasus kebocoran informasi di ruang digital. Fenomena ini menuntut hadirnya regulasi yang tidak hanya komprehensif, tetapi

[13] Jonathan Elkana Soritua Aruan.(2024). Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi. Jurnal Globalisasi Hukum, 1(1): 1–22 DOI 10.25105/jgh.v1i1.19499, p. 14.

[14] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 19 dan Pasal 20 ayat (1) dan (2).

[15] Merry Christian Putri Erlina Maria Christin Sinaga. (2020). Formulasi legislasi perlindungan data pribadi. Jurnal Rechts Vinding, 9(2): 237–56, p. 249.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 12

juga mampu mengikuti dinamika perkembangan teknologi. Regulasi yang kuat harus disertai dengan penegakan hukum yang efektif serta peran aktif dari berbagai pihak, baik pemerintah, sektor swasta, maupun masyarakat. Dengan demikian, perlindungan data pribadi tidak semata menjadi isu teknis, melainkan juga bagian integral dari perlindungan hak asasi manusia di era digital.

a. Kurangnya Kesadaran Pengguna

Banyak pengguna internet belum menyadari pentingnya melindungi data pribadi, terutama karena minimnya edukasi tentang privasi dan keamanan digital. Informasi yang dibagikan secara bebas, misalnya di media sosial, rentan disalahgunakan untuk penipuan atau pencurian identitas. Kurangnya pemahaman ini diperburuk oleh teknologi yang semakin kompleks, sehingga pengguna sering mengabaikan langkah-langkah dasar perlindungan seperti penggunaan kata sandi yang kuat atau autentikasi dua faktor. Mereka juga jarang membaca kebijakan privasi layanan digital yang digunakan, sehingga tidak memahami bagaimana data mereka dikelola. Akibatnya, pengguna menjadi target empuk serangan siber seperti phishing dan malware. Oleh karena itu, peningkatan kesadaran melalui edukasi publik sangat penting agar masyarakat dapat lebih proaktif dalam melindungi data pribadinya.[16]

b. Kelemahan Regulasi Perlindungan Data Pribadi

Hingga kini, regulasi perlindungan data pribadi masih menunjukkan ketimpangan antarnegara. Uni Eropa, misalnya, telah mengimplementasikan General Data Protection Regulation (GDPR) dengan standar tinggi, sementara banyak negara lain masih dalam tahap penyusunan atau belum memiliki payung hukum yang memadai. Ketidakharmonisan ini menyulitkan perusahaan multinasional untuk mematuhi regulasi yang berbeda di tiap yurisdiksi dan berdampak pada efektivitas perlindungan data secara global.Perusahaan yang beroperasi

[16] Tasya Zahwani, Syfa; Irwan Padli Nasution, Muhammad. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital". *JoSES*, Universitas Islam Negeri Sumatera Utara, 2024.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 13

di negara dengan regulasi lemah cenderung tidak menerapkan standar keamanan setinggi negara dengan regulasi ketat, sehingga meningkatkan risiko kebocoran dan penyalahgunaan data. Perbedaan hukum ini juga menjadi hambatan dalam kerja sama internasional penegakan hukum terhadap pelanggaran data pribadi.[17]

Selain itu, regulasi yang ada kerap tertinggal dari perkembangan teknologi, seperti kecerdasan buatan, big data, dan Internet of Things (IoT), yang menghadirkan tantangan baru dalam pengelolaan data pribadi. Regulasi perlu bersifat adaptif dan progresif agar mampu menjawab dinamika ancaman digital yang terus berkembang. Masalah lain adalah lemahnya implementasi hukum. Bahkan di negara dengan regulasi ketat, penegakan hukum sering terhambat oleh keterbatasan sumber daya, birokrasi, dan kurangnya koordinasi antarinstansi. Oleh karena itu, penguatan institusi penegak hukum dan peningkatan kerja sama lintas negara menjadi hal krusial dalam memastikan perlindungan data berjalan efektif.

Di Indonesia, tantangan ini juga muncul seiring meningkatnya penggunaan internet. Diperlukan regulasi yang responsif dan penegakan hukum yang jelas, terutama terhadap penyalahgunaan data di platform digital. Hal ini tercermin dalam Pasal 30 ayat (1) dan Pasal 46 ayat (1) UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), yang mengatur sanksi pidana bagi pelaku akses ilegal terhadap sistem elektronik. Namun, masih banyak masyarakat yang belum memahami dasar hukum penggunaan platform digital secara benar.[18]

---

[17] Gunawan Karnedi dan R. G. Guntur Alam, "Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa," El-Mujtama: Jurnal Pengabdian Masyarakat 5, no. 3 (2025): 610-622,

[18] Damayanti, A., & Prastyanti, R. (2024). Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital DiIndonesia Indonesian Center Journal Query date: 2024-06-05 11:40:45.https://ejurnal.jurnalcenter.com/index.php/micjo/article/view/117

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 14

c. Ancaman dari Cybercrime

Kejahatan siber seperti hacking, phishing, dan malware terus berkembang, menjadi ancaman serius terhadap keamanan data pribadi. Pelaku kejahatan siber semakin canggih dalam mengeksploitasi kelemahan sistem untuk memperoleh informasi sensitif, termasuk data pribadi, kartu ATM, dan kartu kredit. Menurut Organization Of European Comunnity Development Cybercrime (OECD), cybercrime mencakup segala bentuk akses ilegal terhadap data menggunakan perangkat digital. Infrastruktur teknologi yang lemah, sistem yang tidak diperbarui, atau kebijakan keamanan yang buruk sering menjadi celah yang dimanfaatkan penjahat siber.[19] Phishing digunakan untuk menipu individu agar memberikan data pribadi dengan menyamar sebagai pihak terpercaya. Sementara itu, serangan *malware* dan *hacking* bisa mencuri atau mengenkripsi data dengan motif pemerasan. Kemunculan teknologi seperti *AI, machine learning*, dan *deepfake* menambah kompleksitas serangan, membuatnya lebih sulit dideteksi. Bahkan serangan seperti *Distributed Denial of Service* (DDoS) kini dapat melumpuhkan layanan digital secara masif.[20]

Untuk mengatasi tantangan yang ada, diperlukan berbagai solusi agar perlindungan data pribadi dapat berjalan lebih baik dan efektif. Berikut Solusi untuk perlindungan data pribadi:

a. Peningkatan Edukasi dan Kesadaran

Salah satu cara utama melindungi data pribadi adalah dengan meningkatkan edukasi dan kesadaran masyarakat. Hal ini dapat dilakukan melalui kampanye publik di media massa dan digital, serta lewat seminar dan pelatihan. Kampanye tersebut dapat mengajarkan pentingnya penggunaan kata sandi yang kuat, autentikasi dua faktor,

[19] Hamid dan Djollong, *The Strategy of Spiritual Education in Anticipating the Impact of Globalization on Society*, *The Journal Al-Athfal* 1, no. 2 (2019): 55–65.
[20] 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

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 15

dan kehati-hatian saat membagikan informasi pribadi secara online. Seminar di sekolah, universitas, dan komunitas juga berperan penting dalam memberikan pemahaman sejak dini, sementara pelatihan untuk pegawai perusahaan membantu meningkatkan kewaspadaan terhadap ancaman siber. Edukasi tentang keamanan data juga sebaiknya diintegrasikan ke dalam kurikulum pendidikan formal. Selain itu, penggunaan teknologi seperti aplikasi edukatif, e-learning, webinar, dan podcast dapat memperluas akses masyarakat terhadap informasi keamanan data. Kolaborasi antara pemerintah, swasta, dan organisasi non-pemerintah juga penting dalam membangun kesadaran kolektif dan menciptakan ekosistem digital yang lebih aman. Cybercrime adalah kejahatan yang dilakukan menggunakan teknologi komputer, jaringan internet, atau media digital. Penelitian ini bertujuan untuk menjelaskan tindak pidana cybercrime dan sanksinya dalam Undang-Undang Informasi dan Transaksi Elektronik.[21]

b. Penguatan Kerangka Regulasi

Perlindungan data pribadi butuh regulasi kuat dan fleksibel seperti GDPR, yang mengatur hak individu, kewajiban perusahaan, dan sanksi pelanggaran. Regulasi harus mampu mengikuti perkembangan teknologi dan didukung oleh penegakan hukum yang efektif dengan otoritas yang berwenang. Kerja sama internasional penting untuk menyelaraskan standar dan menangani ancaman siber lintas negara. Selain itu, sektor swasta harus dilibatkan agar regulasi praktis dan keamanan data terjaga. Kolaborasi

[21] Dm, M., & Hasibuan, R. (2022). Tindak Pidana Cyber Crime Dan Sanksinya Dalam Undang-Undang Informasi Dan Transaksi Elektronik. Andrew Law Journal, Query date: 2024-06-05 11:40:45. https://journal.andrewlawcenter.or.id/index.php/ALJ/article/download/11/9

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 16

pemerintah, swasta, dan masyarakat menjadi kunci perlindungan data yang efektif.[22]

c. Penerapan Teknologi Keamanan

Penggunaan teknologi keamanan seperti enkripsi data, autentikasi multi-faktor (MFA), serta sistem deteksi dan pencegahan intrusi (IDS/IPS) sangat penting untuk melindungi data pribadi dari serangan siber.[23] Enkripsi mengubah data menjadi format yang tidak bisa dibaca tanpa kunci khusus, sehingga data tetap aman meski dicuri. MFA menambah lapisan keamanan dengan meminta lebih dari satu bukti identitas sebelum akses diberikan, mengurangi risiko pencurian akun. Sistem IDS dan IPS membantu mendeteksi dan menghentikan serangan secara cepat dengan analisis canggih, sehingga organisasi bisa merespons ancaman lebih efektif. Selain itu, pemantauan keamanan terus-menerus dan audit rutin penting untuk mengidentifikasi kerentanan baru dan memastikan kepatuhan pada kebijakan keamanan. Namun, teknologi saja tidak cukup. Edukasi dan kesadaran pengguna tentang praktik keamanan, seperti mengenali phishing dan mengelola kata sandi dengan baik, juga krusial. Kombinasi teknologi canggih dan kesadaran pengguna dapat menciptakan perlindungan data pribadi yang lebih kuat di era digital.[24]

[22] Rudi Natamiharja dan Ikhsan Setiawan, "Menjaga Privasi di Era Digital: Analisis Perbandingan Strategi Perlindungan Data di Indonesia dan Perancis," *Jambe Law Journal* 7, no. 1 (2024): 33–50.

[23] Cindy Vania, Markoni, Horadin Saragih, dan Joko Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," Jurnal Multidisiplin Indonesia v2, no. 3 (2023)

[24] Louis Saroha, Rendy Octavianto, dan Essy Malays Sari Sakti, "Pencegahan dan Konsep IDS (Intrusion Detection System) dalam Mendeteksi Serangan

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 17

Permasalahan perlindungan data pribadi tidak semata-mata bersifat teknis, melainkan juga struktural. Beban keamanan sering kali diletakkan pada individu melalui imbauan penggunaan kata sandi kuat atau aktivasi MFA, padahal akar masalahnya terletak pada model bisnis penyelenggara layanan digital yang cenderung mengumpulkan data berlebihan. Oleh karena itu, regulasi harus mampu mengubah insentif dengan mendorong prinsip *privacy by design* dan *privacy by default*, sehingga keamanan menjadi tanggung jawab penyelenggara sejak tahap perancangan layanan, bukan sekadar pilihan tambahan bagi pengguna.[25]

Selain itu, regulasi yang kuat tanpa penegakan yang memadai berisiko menjadi simbolik. Indonesia masih menghadapi keterbatasan sumber daya, keahlian teknis, dan koordinasi antarinstansi, sehingga implementasi perlindungan data berjalan kurang efektif.[26] Tanpa otoritas independen yang memiliki kapasitas teknis dan kewenangan jelas, sulit memastikan kepatuhan penyelenggara publik maupun swasta terhadap ketentuan UU PDP.[27] Perbedaan standar regulasi antarnegara juga mendorong *regulatory arbitrage*, yakni perusahaan memilih yurisdiksi yang lebih longgar, sehingga mengurangi efektivitas perlindungan data pribadi secara global.

Teknologi keamanan seperti enkripsi, MFA, IDS, atau audit sistem memang penting, tetapi efektivitasnya bergantung pada tata

---

Siber pada Sistem Keamanan di Universitas Persada Indonesia Y.A.I," Jurnal Ilmiah Teknik Informatika (TEKINFO) 25, no. 1 (2024).

[25] Dwi Fajar Saputra, "Literasi Digital untuk Perlindungan Data Pribadi," Jurnal Ilmu Kepolisian 17, no. 3 (2023).

[26] Agus Susanto, Miwha Deawati, Darwati Rossa Damayanti, Gilang Akbar Maulana, dan Nina Luisa, "Penguatan Literasi Privasi Digital melalui Penyuluhan Interaktif di SMP Negeri 10 Surakarta," Jurnal Bengawan : Jurnal Pengabdian Masyarakat 5, no. 1 (2025).

[27] ELSAM, "Usul Otoritas Perlindungan Data Pribadi Berdiri Independen," (2022).

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 18

kelola organisasi dan budaya keamanan yang konsisten. Oleh karena itu, solusi harus bertahap: jangka pendek menekankan kampanye literasi digital dan penerapan standar minimum, jangka menengah membangun kapasitas pengawasan dan mendorong pembentukan Data Protection Officer (DPO) independen di korporasi, serta jangka panjang memperkuat kerja sama internasional. Dengan indikator keberhasilan yang terukur seperti tingkat adopsi MFA, waktu rata-rata respon insiden, atau survei literasi privasi Masyarakat perlindungan data pribadi di Indonesia dapat berjalan lebih efektif sekaligus adaptif terhadap dinamika teknologi digital.

Kesimpulan

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan langkah besar dalam menjamin hak atas privasi di era digital. Undang-undang ini memberikan landasan hukum yang jelas dan komprehensif, serta sejalan dengan standar internasional seperti GDPR. Perlindungan data pribadi kini diatur secara lebih sistematis, mulai dari hak subjek data hingga kewajiban pengendali data. Namun, tantangan seperti rendahnya kesadaran masyarakat, lemahnya penegakan hukum, dan meningkatnya kejahatan siber masih menjadi hambatan utama. Oleh karena itu, perlindungan data pribadi perlu didukung dengan edukasi, penguatan regulasi, dan penggunaan teknologi keamanan. Kolaborasi semua pihak sangat penting untuk menciptakan ekosistem digital yang aman dan bertanggung jawab.

Daftar Pustaka

Agus Susanto, Miwha Deawati, Darwati Rossa Damayanti, Gilang Akbar Maulana, dan Nina Luisa, "Penguatan Literasi Privasi Digital melalui Penyuluhan Interaktif di SMP Negeri 10 Surakarta," Jurnal Bengawan : Jurnal Pengabdian Masyarakat 5, no. 1 (2025).

Ashady, S. (2024). Cybercrime sebagai Kejahatan Dunia Masyarakat dalam Perspektif Hukum dan Masyarakat. Juridische: Jurnal Penelitian Hukum, Query date: 2024-06-05 11:40:45.

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 19

https://jurnal.bisakonsul.com/index.php/juridische/article/view/19

Cindy Vania, Markoni, Horadin Saragih, dan Joko Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," Jurnal Multidisiplin Indonesia v2, no. 3 (2023)

Damayanti, A., & Prastyanti, R. (2024). Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital DiIndonesia Indonesian Center Journal Query date: 2024-06-05 11:40:45.https://ejurnal.jurnalcenter.com/index.php/micjo/article/view/117

Dm, M., & Hasibuan, R. (2022). Tindak Pidana Cyber Crime Dan Sanksinya Dalam Undang-Undang Informasi Dan Transaksi Elektronik. Andrew Law Journal, Query date: 2024-06-05 11:40:45.https://journal.andrewlawcenter.or.id/index.php/ALJ/article/download/11/9

Dwi Fajar Saputra, "Literasi Digital untuk Perlindungan Data Pribadi," Jurnal Ilmu Kepolisian 17, no. 3 (2023).

Ekon.go.id, "Menko Airlangga: Pengembangan Ekonomi Digital di Indonesia, Tidak Hanya Target Pasar Tapi Harus Jadi Pemain Global", terdapat dalam Website: https://ekon.go.id/publikasi/detail/3433/menkoairlangga pengembangan-ekonomi-digital-di-indonesia-tidak-hanya-target-pasar-tapi-harus-jadi-pemain-global, diakses tanggal 12 Juli 2024 Pukul 06.47 WIB.

ELSAM, "Usul Otoritas Perlindungan Data Pribadi Berdiri Independen," (2022).

European Union Agency for Fundamental Rights and Council of Europe, Supra No. 5, hlm. 37.

Gunawan Karnedi dan R. G. Guntur Alam, "Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 20

GDPR Uni Eropa," El-Mujtama: Jurnal Pengabdian Masyarakat 5, no. 3 (2025): 610-622,

H. T. S. Putra, Perlindungan Data Pribadi dalam Perspektif Hukum Nasional dan Internasional, (Jakarta: Kencana,2021), hlm. 1.

Hamid dan Djollong, *The Strategy of Spiritual Education in Anticipating the Impact of Globalization on Society*, *The Journal Al-Athfal* 1, no. 2 (2019): 55–65.

Jonathan Elkana Soritua Aruan. (2024). Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi. Jurnal Globalisasi Hukum, 1(1): 1–22 DOI 10.25105/jgh.v1i1.19499, p. 14.

Lina Miftahul Jannah, "UU Perlindungan Data Pribadi dan Tantangan Implementasinya", Artikel online 03 Oktober 2022 terdapat dalam situs: https://jdih.sukoharjokab.go.id/informasi/detail/89, diakses tanggal 12 Juli 2024.

Louis Saroha, Rendy Octavianto, dan Essy Malays Sari Sakti, "Pencegahan dan Konsep IDS (Intrusion Detection System) dalam Mendeteksi Serangan Siber pada Sistem Keamanan di Universitas Persada Indonesia Y.A.I," Jurnal Ilmiah Teknik Informatika (TEKINFO) 25, no. 1 (2024).

M. Ciko Ar Rasyid. (2024). kajian yuridis undang-undang perlindungan data pribadi terhadap tanggung jawab perusahaan pada kasus kebocoran data konsumen (Studi Kasus Pada PT Telkom Indonesia). (Fakultas HukumUniversitas Muhammadiyah Magelang), p. 39.

Marzuki, P.M. Penelitian Hukum. (Jakarta: Kencana, 2005), hlm. 141.

Merry Christian Putri Erlina Maria Christin Sinaga. (2020). Formulasi legislasi perlindungan data pribadi. Jurnal Rechts Vinding, 9(2): 237–56, p. 249.

Nur Alfiana Alfitri. (2024). Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. 4(2): 92–111, p. 98

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 21

Olisias Gultom, Katrin Schneider, dan Lea Mareen Preis, Ekonomi Digital, Harapan, dan Ancaman Belajar dari Indonesia,diunduhmelaluihttp://igj.or.id/wpcontent/uploads/2018/11/Industrial-Revolution4_IGJ_AEPF12_Ind 1.pdf, diakses tanggal 12 Juli 2024.

Rudi Natamiharja dan Ikhsan Setiawan, "Menjaga Privasi di Era Digital: Analisis Perbandingan Strategi Perlindungan Data di Indonesia dan Perancis," *Jambe Law Journal* 7, no. 1 (2024): 33–50.

Sonata, D. L. Metode Penelitian Hukum Normatif dan Empiris: Karakteristik Khas dari Metode Meneliti Hukum.Fiat Justisia Jurnal Ilmu Hukum, 8(1), (2014). Hlm. 15-35.

Tasya Zahwani, Syfa; Irwan Padli Nasution, Muhammad. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital". *JoSES*, Universitas Islam Negeri Sumatera Utara, 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 ayat (2) dan Pasal 2 ayat (1).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 19 dan Pasal 20 ayat (1) dan (2).

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 1 Ayat (1)

Van der Sloot, Bart., The Boundaries of Data, Amsterdam University Press, 2024

As-Shahifah: Journal of Constitutional Law and Governance, Vol. 5 (1), 2025: 78- 22