CAPITAN
Constitutional Law & Administrative Law Review

Volume 3 Nomor 1, Juni 2025: h. 54 - 65
E-ISSN: 3021-8349 / P-ISSN: 3021-8330
doi : 10.47268/capitan.v3i1.18137


# Tanggung Jawab Pemerintah Terhadap Keamanan Data Diri Warga Negara Indonesia

**Riska Putri Yesika Nainggolan[1*], Jantje Tjiptabudy[2], Merlien Irene Matitaputty[3]**

[1,2,3] Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.
: riskapynainggolan@gmail.com
Corresponding Author*

***Abstract***

*Personal data is a human right protected by the constitution. Protection of personal data of Indonesian citizens is still weak, causing an increase in many cases of data leaks that are exploited by irresponsible parties. Protection of personal data in Indonesia is still sectoral, based on the authority granted by regulations governing personal data. The absence of specific regulations governing the protection of personal data causes frequent data leaks. The Ministry of Communication and Information has the authority to maintain personal security in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which gives the Ministry of Communication and Information the authority to supervise the implementation of electronic systems and transactions. The government's responsibility has been regulated in Article 58 paragraph 1 of Law Number 27 of 2022 concerning Protection of Personal Data, which states that "The government plays a role in realizing the implementation of personal data protection in accordance with the provisions of the law." The forms of efforts made by the government regarding the protection of its citizens' personal data are in the form of increasing system security, conducting security supervision, providing security certification, security auditors, cooperation with the security industry and the government has the authority to require violators to inform the public or related parties of the violation. Additional types of administrative sanctions may include written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or financial fines.*

***Keywords: Liability; Protection; Data Leakage.***

**Abstrak**

Data pribadi merupakan hak asasi manusia yang dilindungi oleh konstitusi. Perlindungan data diri warga negara Indonesia masih lemah menyebabkan meningkatnya banyak kasus kebocorandata yang dimanfaatkan oleh pihak tidak bertanggung jawab. Perlindungan data pribadi di Indonesia masih bersifat sektoral, berdasarkan pada kewenangan yang diberikan oleh peraturan yang mengatur data pribadi. Ketidakadaann aturan khusus yang mengatur perlindungan data diri menyebabkan sering terjadinya kebocoran data. Kominfo memiliki kewenangan untuk menjaga keamanan pribad dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan kewenangan kepada Kominfo untuk melakukan pengawasan terhadap penyelenggaraan sistem dan transaksi elektronik. Tanggung jawab pemerintah telah diatur dalam Pasal 58 ayat 1 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi menyatakan "Pemerintah berperan dalam mewujudkan penyelenggaraan pelindungan data pribadi sesuai dengan ketentuaan undang-undang." Bentuk upaya yang dilakukan pemerintah terkait perlindungan data pribadi warga negaranya yakni berupa penngkatan kemanan sistem, melaukan pengawasan keamanan, memberikan sertifikasi keamanan, auditor keamanan, kerjasama dengan industri keamanan dan Pemerintah berwenang untuk mewajibkan pelanggar untuk menginformasikan pelanggaran tersebut kepada publik atau pihak terkait. Jenis sanksi administratif tambahan dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda finansial.

**Kata Kunci: TanggungJawab; Perlindungan; Kebocoran Data.**

## PENDAHULUAN

Data diri warga negara Indonesia merupakan bagian yang bersifat privasi yang perlu dilindungi dari bentuk penyalahgunaan. Penyalahgunaan terhadap data-data dapat mempengaruhi dan sehingga menimbulkan kerugian Hak Asasi Manusia (HAM) warga negara Indonesia berhubungan dengan penggunan data.[1] Dalam Pelindungan data pribadi diselenggarakan oleh lembaga yang dipilih oleh Presiden dan diatur dalam Peraturan Presiden.

Kemenkominfo memiliki peran dalam pengawasan serta penegakan undang-undang perlindungan data pribadi, termasuk melakukan penyelidikan terhadap kebocoran data dan pemberian sanksi administratif.[2] Adapun asas-asas dalam Pasal 3 Undang-Undang Nomor 27 Tahun 2022 Tentang perlindungan data berupa asas Perlindungan, asas kepastian hukum, asas kepentingan umum, asas kemanfaatan, asas kehatihatian, asas kesimbangan, asas pertanggungjawaban dan asas kerahasian. Salah satu masalah terbongkarnya rahasia tentang data diri warga negara Indonsia sehingga membawa kerugian secara materiil dan immaterial.[3] Penyebarluasaan data diri adalah pelanggaran terhadap privasi seseorang dikarenakan hal tersebut mencakup hak memberi atau tidak memberi data diri tersebut.[4] Pada 20 Juni 2024 warga Indonesia di hebohkan dengan adanya serangan hecker yang menyerang Pusat Data Nasional Sementara (PDNS) di Surabaya beserta terdapat 282 data lembaga pemerintah disekap hacker, serangan ini bermula setelah Windows Defender dinonaktifkan yang memberi kesempatan bagi peretas untuk memanfaatkan celah tersebut dan merusak sistem, akibatnya beberapa layanan pemerintah, seperti keimigrasian mengalami gangguan signifikan.

Serangan siber ini disebabkan oleh perangkat keras perusak atau *ransomware* yang dikenal sebagai *Brain Chipper*. Pada rapat kerja 27 Juni 2024 komisi 1 DPR RI bersama Menteri Komunikasi dan Informatika Republik Indonesia (Menkominfo RI) dan Kepala badan Siber Negara (BSSN) menyampaikan bahwa yang diserang Pusat Data Nasional milik PT. Telkom di Surabaya dan PT. Lintas Arta Serpong yang di serang oleh hacker. Hacker melakukan penyerangan dan meminta tebusan sebesar US$8 Juta atau sekitar Rp.131,6 M. Namun, pemerintah bersitegas untuk menolak untuk membayar uang tebusan tersebut. Peretas menyerang PDNS di Surabaya adalah kelompok hacker yang dinamakan Lockbit 3.0. Penyerangan siber atas Pusat Data Nasional menunjukkan bahwa pengamanan atas data nasional pada PDNS belum dapat diandalkan dan perlu dikaji.

## METODE PENELTIAN

Penelitian ini menggunakan penelitian yudiris normatif yang bermetodekan deskriptif kualitatif. [5]Pendekatan masalah yang digunakan dalam penelitian ini adalah pendekatan perundang-undang, pendekatan konseptual dan pendekatan kasus. Sumber bahan hukum primer, sekunder dan tersier serta pengolahan dan analisa bahan hukum menggunakan analisis berpikir deduktif.

---

[1] Anantia Ayu D., dkk, *Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital,* (Jakarta: Pusat Penelitian dan Pengkajian Perkara dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, 2019), p. 9.

[2] Nuruddin, M. I., & Iqbal, M. R, *Dinamika Sistem Hukum Tata Negara dalam Konteks Perubahan Konstitusi di Era Digital*, (2024).

[3] Romanosky, Sasha, and Alessandro Acquisti. " Privacy Costs and Personal Data Protection: Economic and Legal Perspectives", *Berkeley Technology Law Journal*, Volume 24, Nomor 3 (2009): 1061–1101. http://www.jstor.org/stable/24118273.

[4] Makarim, E., *Kompilasi hukum telematika*, (Jakarta: RajaGrafindo Persada, 2003), p. 14.

[5] Cholid Nabuko dan Abu Achmadi, *Metodologi Peneitian*, (Jakarta: Cet.VI, PT. Bumi Aksara, 2005), p. .44.



*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

## HASIL DAN PEMBAHASAN

### A. Tanggung Jawab Pemerintah Dalam Menegakkan Perlindungan Data Diri

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan peraturan khusus yang mengatur perlindungan data pribadi. Undang-undang ini mencakup subjek data pribadi, pengelolaan, transfer data pribadi, sanksi administratif, kelembagaan, penyelesaian sengketa dan prosedur hukum, larangan penggunaan data pribadi, ketentuan pidana. Namun beberapa ketentuan dalam undang-undang perlindungan data pribadi belum dapat diterapkan secara optimal karena ada pasal-pasal yang membutuhkan adanya aturan pelaksana untuk implementasikan lembaga yang bertugas untuk melaksanakan perlindungan data pribadi dan memiliki wewenang penting dalam pengawasan serta penerapan aturan dalam UU PDP belum terbentuk.[6]

UU PDP dapat diimplementasikan secara maksimal dan efektif pemerintah perlu membentuk dan mengesahkan peraturan pemerintah serta peraturan presiden sesuai dengan amanat yang terdapat dalam UU PDP. Pembentukan aturan pelaksana ini akan menciptakan kerangka kerja yang jelas dan komprehensif dalam hal perlindungan, pengelolaan, dan penegakan hukum terkait data pribadi di Indonesia.[7]

Ketiadaan aturan pelaksana dan belum terbentuknya lembaga khusus menyebabkan kewenangan perlindungandata pribadi sering mengalami kebocoran data. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memberikan kewenangan kepada Kominfo untuk melakukan pengawasan terhadap penyelenggaraan sistem dan transaksi elektronik.

Bentuk upaya yang dilakukan pemerintah terkait perlindungan data pribadi warga negaranya yakni berupa penngkatan kemanan sistem, melaukan pengawasan keamanan, memberikan sertifikasi keamanan, auditor keamanan, kerjasama dengan industri keamanan.

1. Tanggung Jawab Keamanan Data Digital Oleh Penyelenggara Sistem Elektronik

   Penyelenggara sistem elektronik harus memberikan akses atau kesempatan kepada pemilik data pribadi untuk melakukan perubahan atau pembaruan terhadap data pribadi tanpa mengganggu sistem pengelolaan data pribadi, kecuali jika diatur secara berbeda oleh ketentuan peraturan perundang-undangan.[8]

   Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik untuk menciptakan penyelenggara sistem dan transaksi elektronik yang dapat diandalkan, aman, tepercaya, dan bertanggung jawab, sehingga mampu memberikan pelayanan yang cepat akan mendorong peningkatan kualitas penyelenggara sistem transaksi elektronik. Lemahnya pelindungan data di Indonesia mengakibatkan maraknya kebocoran data adanya peretasan maupun pembajakan media sosial yang berakhir pada pembobolan data pribadi, penipuan dan pemerasan secara daring.

---

[6] M Iqsan Sirie, *From Act To Action*: *Strategi Implementasi UU Perlindungan Data Pribadi*, https://appdiorid-fromactto-action strategi implementasi-uu-perlindungan-data-pribadi diakses pada Selasa 04 Februari 2025 pukul 23.27 WIT.

[7] Erlyns Yolanda dan Ragun Romaida Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif", *Syntax Literate: Jurnal Ilmiah Indonesia*, Vol. 8, No. 6, Juni (2025), p. 417.

[8] J Lee Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy", *Boston College International and Comparative Law Review*, Volume 6, Issue 1, (1983), p.24.



*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

Data pribadi harus disimpan dalam sistem elektronik sesuai dengan ketentuan peraturan perundang-undangan yang mengatur kewajiban waktu penyimpanan data pribadi. Pengelola data pribadi memiliki kewajiban untuk mencegah kebocoran data pribadi dengan menjaga keamanan data pribadi agar tidak dapat diakses, disalahgunakan, atau dihilangkan. Jika terjadi kebocoran data pribadi maka pemerintah dalam hal ini Kominfo, harus memberitahukan kegagalan pelindungan data pribadi (kebocoran) tersebut kepada masyarakat.

2. Perlindungan Privasi dan Data Pribadi Dalam HAM

Perlindungan data pribadi yang sensitif diatur dalam Pasal 28G ayat 1 Undang-undang Dasar Tahun 1945. Pemerintah bertanggung jawab untuk melindungi data pribadi warga negara Indonesia bagian dari hak asasi manusia diatur oleh Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Undang-undang ini bertujuan untuk memastikan keadilan sosial dan melindungi warga dari potensi pelanggaran privasi, termasuk program terkait pemerintah.

Pemerintah memiliki tanggung jawab untuk melindungi data diri warga negara diatur dalam Pasal 281 ayat 4 Undang-undang Dasar Tahun 1945 menyatakan "Perlindungan, pemajuan, penegakan, dan pemenuhan hak asasi manusia adalah tanggung jawab negara, terutama pemerintah." Undang-Undang tentang kebebasan umum juga melindungi keyakinan pribadi setiap individu, terutama yang tercantum dalam Pasal 29 Ayat (1) menyatakan bahwa "Setiap orang berhak mendapatkan perlindungan atas diri pribadi, keluarga, kehormatan, martabat dan hak miliknya."

Beberapa prinsip-prinsip perlindungan data pribadi menurut OECD 2013 berupa: Prinsip pembatasan pengumpulan, prinsip kualitas data, prinsip pembatasan penggunaan, prinsip perlindungan keamanan, pengontrol data.

3. Perlindungan Pusat Data Nasional

Pusat Data Nasional (PDN) merupakan program dari Kementerian Komunikasi dan Informatika (Kominfo) untuk mengintegrasikan dan memusatkan pengelolaan data pemerintah. Upaya ini dilakukan untuk mencapai efisiensi, keamanan, dan interoperabilitas data yang lebih baik, serta untuk mendukung kebijakan berdasarkan data yang akurat bertujuan untuk meningkatkan kualitas pelayanan publik dan mengelola penyimpanan data masyarakat secara terpusat. PDN perlu dijaga dengan baik untuk mencegah peretasan yang dapat menyebabkan kebocoran data.[9]

PDN merupakan kumpulan pusat data yang dikelola oleh Menteri yang bertanggung jawab dalam urusan pemerintahan di bidang komunikasi dan informatika Kominfo dan/atau pusat data dari instansi pusat serta pemerintah daerah yang telah memenuhi kriteria tertentu, PDN menyimpan semua informasi masyarakat Indonesia mulai dari data KTP hingga data terkait layanan penerbangan. Di era digital saat ini, tantangan keamanan yang utama adalah *ransomware*.

*Ransomware* merupakan perangkat lunak berbahaya yang dirancang untuk menyerang komputer dan mengunci semua data di dalamnya dengan tujuan

[9] Siti Yuniarti, *Perlindungan Data Pribadi Di Indonesia*, p. 151.


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

meminta tebusan uang dari korban atau data tersebut akan hilang. Selain kemunculan teknologi seperti *Microsoft Kinect* telah membuka peluang baru untuk peretasan, memungkinkan individu untuk menciptakan proyek dan aplikasi inovatif melalui pemrograman dan interpretasi aliran data.

Peretasan Pusat Data Nasional merujuk pada akses ilegal atau pelanggaran keamanan yang terjadi di fasilitas pusat yang bertanggung jawab untuk menyimpan dan mengelola data dalam jumlah besar di tingkat nasional. Munculnya permasalahan dalam peretasan PDN di Indonesia saat ini menjadi sumber kekhawatiran bagi masyarakat.

Pemerintah memiliki kewajiban untuk memastikan keamanan data dalam *government cloud* atau Pusat Data Nasional Sementara (PDNS), yang merupakan tanggung jawab bersama antara penyelenggara dan pengguna layanan PDN. Pemerintah juga memiliki tanggung jawab hukum untuk segera melakukan tindakan keamanan yang diperlukan guna mencegah penyebaran data pribadi yang diduga telah bocor. Kasus kebocoran data dari PDNS perlindungan data pribadi terus menunjukkan banyak celah yang memerlukan perhatian.

Meskipun Undang-Undang Perlindungan Data Pribadi berfungsi sebagai landasan penting, efektivitasnya telah terhambat oleh kurangnya pemahaman di antara penegak hukum dan masyarakat umum. Selain itu, kerentanan PDNS terhadap serangan siber berasal dari kerangka kerja keamanan yang lama dan terbatasnya investasi dalam kemajuan teknologi.

Penegak hukum menghadapi tantangan dalam mengelola insiden kebocoran data karena kurangnya keahlian mengenai forensik digital dan keamanan siber. Kelemahan sistem keamanan siber di PDNS diuraikan sebagai berikut:

a. Pemerintah terkhusus Kemenkominfo RI belum adanya keseriusan dalam mempersiapkan sistem pengamanan siber untuk PDNS.
b. Data nasional belum didukung oleh infrastruktur pengamanan yang cukup memadai.
c. Ketidaksiapan SDM yang berkompeten dalam menghadapi serangan siber.
d. Kemenkominfo dan Kepala BSSN memilih untuk menggunakan Windows Defender sebagai perlindungan data, suatu program bawaan Windows yang keefektifitasan sering dipertanyakan.

4. Kebocoran Data Pribadi

Data yang tersimpan dalam riwayat penelusuran di perangkat elektronik rentan terhadap serangan siber. Setelah data pribadi diunggah ke internet jejak digital akan tetap ada dan tidak dapat dihapus karena data tersebut disimpan secara digital. Keamanan data pribadi rentan karena sistem keamanan yang belum optimal, pemahaman masyarakat yang terbatas tentang perlindungan data dan kesadaran yang rendah akan pentingnya menjaga informasi pribadi, Pengawasan yang buruk dapat menyebabkan kelalaian manusia.

Data pribadi yang bocor meliputi nama, alamat, informasi kontak, KTP, informasi rekening dan lain-lain. Beberapa data yang mengalami kebocoran data akibat serangan

siber pada tahun 2024 sebagai berikut:

a. BPJS Ketenagakerjaan

Pada akhir Juni 2024 adanya informasi di media sosial bahwa data BPJS Ketenagakerjaan diduga bocor. Data yang diduga bocor meliputi nama lengkap, tanggal lahir, alamat email, nomor telepon, alamat tempat tinggal, kode pos, kelompok usia, dan lainnya.[10]

b. Kartu Indonesia Pintar (KIP)

Data penerima KIP yang mencakup informasi tentang biodata diri, keluarga dan alamat akibat serangan pada platform administrasi KIP. Kerentanan pada server PDN mengakibatkan hilangnya data 800 ribu calon mahasiswa penerima KIP Kuliah.

c. Bank

Bank sering menghadapi serangan yang menyebabkan kebocoran data nasabah termasuk nomor rekening, informasi transaksi, dan data pribadi lainnya. Pada bulan Mei, Bank Syariah Indonesia (BSI) diduga mengalami kebocoran data. Peretas yang dikenal sebagai LockBit mengklaim telah mencuri 1,5 TB data layanan serta informasi pribadi nasabah dan data pinjaman.[11]

d. Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri (Dukcapil Kemendagri)

Dukcapil Kemendagri diduga mengalami kebocoran data pada tahun 2024. Diduga terjadi kebocoran data sebanyak 337 juta masyarakat yang tercatat di Dukcapil Kemendagri, dan data tersebut diperkirakan telah dijual di forum *online hacker breach forums*. Data yang dipastikan bocor antara lain mencakup nama, Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (KK), tanggal lahir, alamat, nama orang tua, NIK keluarga, nomor akta lahir, nomor akta nikah, serta informasi lainnya.

e. Paspor

Pada tahun 2024, diduga terjadi kebocoran data paspor warga negara Indonesia. Sekitar 34 juta data paspor diduga telah bocor, dengan informasi kebocoran data yang dipastikan bocor antara lain mencakup nama lengkap, nomor paspor, tanggal berlaku paspor, tanggal lahir, jenis kelamin, dan informasi lainnya.

f. Direktorat Jenderal Pajak (DPJ)

Pada September 2024, pada Direktoral Jenderal Pajak (DPJ) mengahadapi kebocoran pajak sekitar 6,6 juta data. Data yang bocor seperti NIK, NPWP, alamat, nomor handphone, e-mail.

g. Komisi Pemilihan Umum (KPU)

---

[10] A. A. Zaman, J. Anwar, and A. Fadlian, "Pertanggungjawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE," *Juncto Delictio*, Vol. 1, No. 2, February, (2024).

[11] Annur, C. M., *BSI, Bank Syariah yang Paling Banyak Digunakan Masyarakat Indonesia,* https://databoks.katadata.co.id/datapublish/2023/05/03/bsi-bank-syariahyang-paling-banyak-digunakan-masyarakat-indonesia, diakses 17 Februari 2025.


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

Data yang bocor termasuk NIK, NKK, nomor KTP, paspor, nama, tempat pemungutan suara, status disabilitas, jenis kelamin, tanggal dan tempat lahir, serta alamat tinggal. Lebih dari 252 juta data warga negara Indonesia yang terkait dengan data pemilih Pemilu 2024 dilaporkan bocor dan diperjualbelikan.[12]

**B. Perbandingan Privasi Atas Data Diri Warga Negara Indonesia dan Jerman**

1. Penerapan Perlindungan Hak Privasi di Indonesia

Penerapan perlindungan hak privasi di Indonesia merupakan proses yang terus berkembang dengan fokus pada penguatan peraturan peningkatan kesadaran masyarakat, dan penegakan hukum yang lebih baik. Indonesia menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menunjukkan komitmen pemerintah untuk menyediakan dasar hukum yang kuat dalam mengatur dan melindungi data pribadi masyarakat untuk mencegah risiko pelanggaran data.

Implementasi UU PDP memerlukan kolaborasi antara pemilik data organisasi yang memproses data dan pemerintah sebagai regulator dan penyelenggara. Pedoman dari Kementerian Komunikasi dan Informatika, data pribadi adalah informasi spesifik individu yang disimpan dengan aman, dipelihara keasliannya, dan dijamin kerahasiaannya dalam Pasal 17 ayat (3) Permen Kominfo Nomor 12 Tahun 2016 mewajibkan perusahaan telekomunikasi menjaga privasi informasi dan identitas pengguna. Instrumen hukum dalam perlindungan data pribadi Indonesia memiliki peraturan dan pedoman terkait perlindungan dan keamanan data diri antara lain:

a. Perlindungan Data Pribadi dalam Konstitusi

Perlindungan data pribadi telah diatur dalam Pasal 28G ayat 1 Undang-Undang Dasar Tahun 1945 yang menyatakan "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

b. Informasi Elektronik dalam Undang-Undang Perubahan ITE

Data pribadi merupakan data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannnya. Undang-Undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa Pengaturan privasi dan perlindungan data privasi di Indonesia tidak hanya merujuk pada satu peraturan perundang-undangan.

c. Data Pribadi dalam Undang-Undang Administrasi Kependudukan

Undang-Undang Administrasi Kependudukan awalnya dibuat dengan tujuan peraturan perundang-udangan sebelumnya tidak sesuai dengan tuntutan pelayanan administrasi kependudukan dan nondiskriminatif. Undang-undang ini mengatur ketentuan mengenai data pribadi tetapi definisi dalam norma undang-undang tersebut kurang jelas. Undang-Undang No. 23 Tahun 2006 Jo

[12] Ramli dan M. Ahmad, *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*, (Bandung: Refika Aditama, 2004).


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

Undang-Undang No. 24 Tahun 2013 tentang Administrasi Kependudukan mengatur tentang perlindungan data pribadi

d. Jaminan Perlindungan Data Pribadi dalam Undang-Undang Pelayanan Publik

Pembentukan UU tersebut untuk meningkatkan mutu dan menjamin terselenggaranya pelayanan publik yang sesuai dengan prinsip pemerintahan yang baik. Undang-undang ini juga melindungi warga negara dari penyalahgunaan wewenang dalam pelayanan publik. Namun, UU ini tidak memberikan kriteria yang lengkap tentang data pribadi, informasi, atau dokumen yang harus dirahasiakan.

Di Indonesia Undang-Undang Perlindungan Data Pribadi menjadi landasan hukum yang kuat untuk mengatur dan melindungi data pribadi masyarakat. Jenis-jenis data pribadi menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan antara lain:

1) Data Diri Bersifat Umum

Data diri bersifat umum dapat diidentifikasikan oleh banyak orang. Contoh dari jenis data ini meliputi:

a. Nama lengkap
b. Jenis kelamin
c. Kewarganegaraan
d. Agama
e. Status perkawinan

2) Data Pribadi Bersifat Spesifik

Data pribadi bersifat spesifik merupakan informasi apabila diproses dapat berdampak signifikan ada individu yang bersangkutan. Contoh jenis data ini antara lain:

a. Catatan Kejahatan
b. Riwayat keuangan
c. Data dan informasi kesehatan
d. Data biometrik (Data yang mencakup sidik jari dan wajah).

2. Perlindungan Data Diri di Jerman

Perlindungan data diri di Jerman diatur oleh Undang-Undang Perlindungan Data Federal (FDPA) dan *Bundesdatenschutzgesetz* (BDSG). Kedua undang-undang tersebut bertujuan untuk melindungi informasi pribadi dan menjamin privasi individu. Di negara Jerman Undang-Undang Perlindungan Data Federal *Bundesdatenschutzgesetz* (BDSG) telah diberlakukan sejak 1978 untuk mengatur pengelolaan data pribadi.[13]

Ketentuan bagian dari Uni Eropa dan Jerman berada dibawah yurisdiksi Peraturan Perlindungan Data Umum (GDPR). Hukum perlindungan data Jerman didefenisikan dalam Pasal 4 ayat GDPR menyatakan "Semua informasi yang berhubungan dengan orang perseorangan yang teridentifikasi atau dapat diidentifikasi." Undang-Undang Eropa *Datenschutz-Grundverordnung* (DSGVO) diterapkan untuk melindungi data pribadi

[13] *European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law*, (Belgium: 2019), p. 36.


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

warga Jerman dengan tingkat keamanan yang melebihi standar internasional. Hal ini memberikan dua lapisan perlindungan bagi warga negara Jerman terkait data pribadi.

Undang Undang Perlindungan Data Federal (FDPA) Jerman yang disahkan pada tahun 1977 untuk melindungi privasi data pribadi. Jerman menyelenggarakan Peraturan Uni Eropa 95/46/EC dan 2002/58/EC dengan pendekatan yang kompleks dan spesifik. Jika pemerintah Jerman lalai dalam melindungi data pribadi warganya, sanksi yang dapat dikenakan adalah denda yang signifikan berdasarkan ketentuan General Data Protection Regulation (GDPR).

Denda ini bisa mencapai 20 juta euro atau 4% dari pendapatan global perusahaan yang melanggar, peringatan atau teguran, pembatasan larangan pemprosesan data dan pencabutan izin. Selain itu, individu atau lembaga yang merasa dirugikan dapat mengajukan gugatan terhadap pemerintah atau pihak swasta yang dianggap telah melanggar aturan perlindungan data. Sanksi-sanksi ini diberikan oleh Otoritas Perlindungan Data Pribadi *Bundesbeauftragte fur den Datenschutz und die Informationsfreiheit* di Jerman yang memiliki kewenangan untuk menilai dan memberikan tindakan sesuai dengan peraturan yang berlaku di bawah GDPR.

## C. Analisis Terhadap Politik Hukum dalam Pembentukan RUU di Indonesia

1. Proses Pembentukan RUU PDP

Pembahasan RUU PDP dirampung sebelum periode DPR RI 2014-2019 yang mengindikasikan bahwa RUU tersebut tidak masuk dalam Prolegnas tahun 2018. Setelah itu, Presiden Joko Widodo menandatangani RUU PDP dan selanjutnya dibahas di DPR. Informasi perkembangan mengenai RUU PDP disampaikan melalui Siaran Pers No. 231/HM/KOMINFO/07/2021 yang menyatakan bahwa:

a. Tim Panja Pemerintah Khusus Kominfo dan Tim Panja Komisi I DPR RI mengadakan rapat di Jakarta pada 29-30 Juni 2021 untuk melakukan pembahasan RUU PDP.
b. Perlu peraturan hukum yang kuat untuk melindungi data diri untuk mempercepat proses legislasi RUU PDP menjadi UU PDP.
c. Dalam proses penyusunan RUU PDP, Tim Panja berupaya merumuskan substansi pasal-pasal penting secara tepat dan akurat, khususnya yang berkaitan dengan pembentukan lembaga yang akan mengawasi dan menegakkan perlindungan data pribadi.
d. Pengurusan penyelenggaraan perlindungan data diri menjadi hak Kominfo yang bertanggung jawab kepada Presiden berdasarkan sistem pemerintahan yang berlaku.[14]

2. Substansi Pengaturan RUU PDP

Rancangan Undang-Undang Perlindungan Data Pribadi memuat unsur-unsur berhubungan dengan perlindungan hukum terkait hak-hak yang dimiliki individu atas data pribadi, diantaranya hak untuk menerima beserta meminta informasi tentang identitas diri berdasarkan kepentingan hukum.

[14] Samuel A. Pangerapan, *Perkembangan Pembahasan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP*), dalam Kominfo.go.id diakses pada 20 Februari 2025.


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

RUU PDP tidak mengatur pembentukan badan independen yang bertindak sebagai pengawas dan regulator perlindungan data pribadi, seperti komisi administrasi keamanan informasi individu dan yang berwenang dibawah Koordinasi Kominfo. Kemendagri mengelola data penduduk, Kemenkumham data identitas dan keimigrasian beserta OJK bertanggungjawab atas data keuangan.

## D. Akibat Hukum Bagi Pemerintah Jika Data Diri Tidak Dilindungi

Undang-undang yang mengatur terkait perlidungan data pribadi di Indonesia masih terbatas hanya UU ITE yang memberikan pengaturan yang lebih spesifik dan UU lainnya hanya mengatur secara umum. Peraturan terkait perlindungan data pribadi diatur dalam berbagai undang-undang dan peraturan turunan lainnya, namun bersifat parsial dan sektoral. Pemerintah memiliki tanggung jawab untuk memastikan bahwa data yang dikumpulkan dan dikelolanya tidak disalahgunakan atau diakses tanpa persetujuan.[15]

Tanggung jawab hukum akan berkaitan dengan kewajiban hukum yaitu seseorang bertanggung jawab secara hukum atas perbuatannya dan dapat dikenakan sanksi jika tindakan yang dilakukan melanggar kewajiban tersebut. Undang-undang khusus terkait perlindungan data pribadi tidak ada sehingga sering terjadinya kebocoran data, pemerintah dapat dikenakan sanksi administratif jika lalai melindungi informasi pribadi warga negaranya hanya sebatas sanksi administratif, tanpa adanya sanksi pidana sehingga tidak memberikan efek jera.

Sanksi tersebut dapat mencakup pemberitahuan tertulis kepada badan pemerintah yang lalai melindungi data pribadi. Selain itu, pemerintah memiliki kewenangan untuk meminta pelanggar untuk memberi tahu publik atau pihak terkait tentang pelanggaran tersebut. Bentuk sanksi administratif lainnya dapat mencakup peringatan tertulis, penghentian sementara operasi pemrosesan data pribadi, penghapusan atau pemusnahan data diri, dan/atau denda finansial.

1. Konsep Tanggung Gugat Pemerintah

   Konsep tanggung gugat pemerintah dalam perlindungan data pribadi mengacu pada kewajiban hukum pemerintah untuk melindungi data pribadi warga negara. Pemerintah bertanggung jawab menjaga kerahasiaan dan keamanan data yang dikelola terutama dalam era digital yang semakin berkembang. Tanggung jawab ini mencakup pencegahan pelanggaran serta penanganan permasalahan kebocoran data sebagaimana diatur dalam UU PDP. Prinsip tanggung jawab pemerintah menegaskan bahwa pemerintah bertanggung jawab atas tindakan yang menyebabkan kerugian bagi warga negaranya.

   Tanggung gugat ketika adanya pelanggaran hak asasi manusia, kesalahan dalam kebijakan publik, atau kelalaian dalam penyediaan layanan publik. Pengadilan tata usaha negara atau administrasi negara yang bertanggung jawab untuk memerintahkan ganti rugi atau tindakan perbaikan lainnya terlibat dalam proses penyelesaian. Upaya untuk meningkatkan efektivitas mekanisme akuntabilitas pemerintah sedang berlangsung. Mekanisme ini memainkan peran penting dalam memastikan akuntabilitas dan menumbuhkan kepercayaan publik.

2. Kerugian Pihak Terhadap Penyalahgunaan Data Pribadi

[15] Titik Triwulan dan Shinta, *Perlindungan Hukum Pasien*, (Jakarta: Prestasi Pustaka, 2010), p. 48.


*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

Penyalahgunaan data pribadi telah menimbulkan kerugian baik bagi individu maupun kelompok. Penyalahgunaan data pribadi dapat diartikan sebagai pemanfaatan informasi pribadi seseorang tanpa adanya izin atau secara ilegal, termasuk tindakan mengumpulkan dan menggunakan data pribadi tanpa persetujuan dari pemiliknya. Adapun dampak/kerugian terhadap penyalahgunaan data pribadi berupa kerugian finansial, kerugian reputasi dan kerugian emosioal dan psikologis serta kerugian bagi masyarakat berupa peninaatan kejahatan siber dan hilangnya kepercayaan publik.

## KESIMPULAN

Bentuk tanggungjawab pemerintah terhadap keamanan data pribadi warga negara Indonesia yakni berupa peningkatan keamanan sistem, memberikan sertifikasi keamanan layanan yang mengelola data pribadi, melibatkan auditor keamanan untuk mengawasi pelaksanaan UU PDP, pelatihan karyawan dapat memberikan pemahaman tentang pentingnya perlindungan data pribadi dan adanya kerjasama kemitraan dengan perusahaan yang memiliki keahlian di bidang keamanan siber untuk mencegah terjadinya kebocoran data. Hal ini tidak hanya berkaitan dengan perlindungan hak privasi warga negara tetapi juga untuk menjaga keamanan negara serta menciptakan kepercayaan publik terhadap pengelolaan data. Pemerintah dapat dikenakan sanksi administratif apabila lalai dalam melindungi data pribadi warga negara. Sanksi ini hanya terbatas pada tindakan administratif, seperti peringatan tertulis, penghentian sementara proses pengelolaan data, penghapusan atau pemusnahan data pribadi, serta denda finansial. Pihak yang memberikan sanksi kepada pemerintah atau lembaga terkait adalah otoritas yang berwenang dalam bidang perlindungan data pribadi. Di beberapa negara melibatkan lembaga seperti Komisi Perlindungan Data Pribadi atau Ombudsman yang mengawasi pelaksanaan peraturan perlindungan data pribadi.

## REFERENSI


A. A. Zaman, J. Anwar, and A. Fadlian, "Pertanggungjawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE," *Juncto Delictio*, Vol. 1, No. 2, February, (2024).

Anantia Ayu D., dkk, *Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital,* Jakarta: Pusat Penelitian dan Pengkajian Perkara dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, 2019.

Annur, C. M., *BSI, Bank Syariah yang Paling Banyak Digunakan Masyarakat Indonesia*, https://databoks.katadata.co.id/datapublish/2023/05/03/bsi-bank-syariahyang-paling-banyak-digunakan-masyarakat-indonesia.

Cholid Nabuko dan Abu Achmadi, *Metodologi Peneitian*, Jakarta: Cet.VI, PT. Bumi Aksara, 2005.

Erlyns Yolanda dan Ragun Romaida Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif", *Syntax Literate: Jurnal Ilmiah Indonesia*, Vol. 8, No. 6, Juni (2025).

*European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law*, Belgium: 2019.





*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura

J Lee Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy", *Boston College International and Comparative Law Review*, Volume 6, Issue 1, (1983).

M Iqsan Sirie, *From Act To Action*: *Strategi Implementasi UU Perlindungan Data Pribadi*, https://appdiorid-fromactto-action strategi implementasi-uu-perlindungan-data-pribadi.

Makarim, E., *Kompilasi hukum telematika*, Jakarta: RajaGrafindo Persada, 2003.

Nuruddin, M. I., dan Iqbal, M. R., *Dinamika Sistem Hukum Tata Negara dalam Konteks Perubahan Konstitusi di Era Digital*, (2024).

Ramli & M. Ahmad, *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*. Bandung; Refika Aditama, 2004.

Romanosky, Sasha, and Alessandro Acquisti, "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives", *Berkeley Technology Law Journal*, Volume 24, Nomor 3 (2009): 1061–1101. http://www.jstor.org/stable/24118273.

www.kominfo.go.id.

Siti Yuniarti, *perlindungan data pribadi di Indonesia*.

Titik Triwulan dan Shinta, *Perlindungan Hukum Pasien*, Jakarta: Prestasi Pustaka, 2010.



*CAPITAN Constitutional Law & Administrative Law Review*, 3 (1) Juni 2025: 54 - 65
e-ISSN: 3021-8349 / p-ISSN: 3021-8330
Penerbit: Pusat Studi Hukum Dan Pemerintahan Fakultas Hukum Universitas Pattimura