PERLINDUNGAN TERHADAP DATA PRIBADI DI ERA DIGITAL BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Skripsi

Diajukan Untuk Memenuhi Syarat Guna Memperoleh Gelar Sarjana Hukum (S.H) Pada Program Studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo

Oleh:

Nur Alfiana Alfitri

20 0302 0010

PROGRAM STUDI HUKUM TATA NEGARA
FAKULTAS SYARIAH
INSTITUT AGAMA ISLAM NEGERI PALOPO
2025

PERLINDUNGAN TERHADAP DATA PRIBADI DI ERA DIGITAL BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Skripsi

Diajukan Untuk Memenuhi Syarat Guna Memperoleh Gelar Sarjana Hukum (S.H)

Pada Program Studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo

Oleh:

Nur Alfiana Alfitri

20 0302 0010

Pembimbing

1. Dr. Rahmawati, M.Ag

2. Firmansyah, S.Pd., S.H., M.H.

PROGRAM STUDI HUKUM TATA NEGARA
FAKULTAS SYARIAH
INSTITUT AGAMA ISLAM NEGERI PALOPO
2025

HALAMAN PERNYATAAN KEASLIAN

Saya yang bertandatangan dibawah ini:

Nama	: Nur Alfiana Alfitri
NIM	: 20 0302 0010
Fakultas	: Syariah
Program Studi	: Hukum Tata Negara

menyatakan dengan sebenarnya bahwa:

1. Skripsi/tesis ini merupakan hasil karya saya sendiri, bukan plagiasi atau duplikasi dari tulisan/karya orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri,
2. Seluruh bagian dari skripsi/tesis ini adalah karya saya sendiri selain kutipan yang ditunjukkan sumbernya. Segala kekeliruan dan atau kesalahan yang ada di dalamnya adalah tanggungjawab saya.

Bilamana di kemudian hari pernyataan ini tidak benar, maka saya bersedia menerima sanksi administratif atas perbuatan tersebut dan gelar akademik yang saya peroleh karenanya dibatalkan.

Demikian pernyataan ini dibuat untuk dipergunakan sebagaimana mestinya.

Palopo, 27 Februari 2025

Yang membuat pernyataan,

Nur Alfiana Alfitri

20 0302 0010

HALAMAN PENGESAHAN

Skripsi Berjudul Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang ditulis oleh Nur Alfiana Alfitri Nomor Induk Mahasiswa (NIM) 2003020010, Mahasiswa Program Studi Hukum Tata Negara (Siyasah) Fakultas Syariah Institut Agama Islam Negeri Palopo, yang telah dimunaqasyahkan pada hari Selasa, tanggal 04 Februari 2025 M, bertepatan dengan 5 Syaban 1446 H, telah diperbaiki sesuai cacatan dan permintaan tim penguji, dan diterima sebagai syarat meraih gelar Sarjana Hukum (S.H).

Palopo, 04 Februari 2025

TIM PENGUJI

1.	Dr. Muhammad Tahmid Nur, M.Ag.	Ketua Sidang	( )
2.	Dr. H. Haris Kulle, Lc.,M. Ag.	Sekretaris Sidang	( )
3.	Dr. Muhammad Tahmid Nur, M.Ag.	Penguji I	( )
4.	Fitriani Jamaluddin, S.H., M.H.	Penguji II	( )
5.	Dr. Rahmawati, M.Ag.	Pembimbing I	( )
6.	Firmansyah, S. Pd., S.H., M.H.	Pembimbing II	( )

Mengetahui:

a.n Rektor IAIN Palopo
Dekan Fakultas Syariah

Dr. Muhammad Tahmid Nur, M.Ag.
NIP 19740630 200501 1 004

Ketua Program Studi
Hukum Tata Negara

Nirwana Halide. S.HI.. M.H.
NIP 19880106 201903 2 007

PRAKATA

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

اَلحَمْدُ لِلهِ رَبِّ الْعَلَمِيْنَ . وَالصَّلاَةُ وَ السَّلاَمُ عَلَى سَيِّدِ نَا مُحَمَّدٍ وَ عَلَى اَلِهِ وَ اَصْحَا اَجْمَعِيْنَ .

(اما بعد)

Puji syukur penulis pancatkan kepada Allah SWT yang telah menganugrahkan rahmat, hidayah, serta kekuatan lahir dan batin, sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Perlindungan Hukum Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022" setelah melalui proses panjang.

Shalawat dan salam kepada Nabi Muhammad SAW, kepada para keluarga, sahabat dan pengikut-pengikutnya. Skripsi ini disusun sebagai syarat yang harus diselesaikan, guna memeperoleh gelar sarjana pendidikan dalam bidang Hukum Tata Negara pada Intitut Islam Negeri (IAIN) Palopo. Penulisan skripsi ini dapat terselesaikan berkat bantuan, bimbingan serta dorongan dari banyak pihak walaupun penulisan skripsi ini masih jauh dari kata sempurna.

Terkhusus Penulis sampaikan terima kasih yang tulus kepada dua orang hebat dalam hidup saya, Ayahanda Muhammad Alfitri Lencing dan Ibunda Juriana, yang selalu memberikan semangat, dukungan dan inspirasi, sehingga penulis bisa sampai pada tahap di mana skripsi ini akhirnya selesai. Terima kasih atas pengorbanan dan kerja keras. Serta kakak saya Muh. Deni dan Adik saya Muh. Ari Syahbana yang telah membantu dan mendoakan. Semoga Allah SWT membalas segala kebaikan dan memudahkan jalan menuju kebahagiaan menuju dunia akhirat.

Sejak penyusunan proposal, penelitian, hingga selesainya skripsi ini, penulis telah banyak mendapat bantuan, motivasi dan bimbingan dari berbagai pihak. Oleh karena itu penulis menyampaikan ucapan terima kasih yang tulus dan tak terhingga kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rektor IAIN Palopo, Dr. Abbas Langaji, M.Ag. beserta Wakil Rektor I Bidang Akademik dan Pengembangan Kelembagaan, Dr. Munir Yusuf, M.Pd. Wakil Rektor II Bidang Administrasi Umum, Perencanaan dan Keuangnan Dr. Masruddin, S.S.,M.Hum, dan Wakil Rektor III Bidang Kemahasiswaan dan Kerjasama, Dr. Mustaming,S.Ag., M.HI..
2. Dekan Fakulas Syariah IAIN Palopo, Dr. Muhammad Tahmid Nur, M.Ag., beserta Bapak wakil Dekan I Bidang Akademik, Dr. Haris Kulle, Lc. M.Ag., Wakil Dekan II Bidang Administras Umum, Perencanaan dan Keuangan Ilham, S.Ag., M.A., dan Wakil Dekan III Bidang Kemahasiswaan dan Kerjasama Muh. Darwis S.Ag., M.Ag.
3. Ketua Program Studi Hukum Tata Negara IAIN Palopo, Nirwana Halide, S.HI., M.H. Sekertaris Program Studi Hukum Tata Negara Syamsuddin, S.HI., M.H beserta staf yang telah memberikan bimbingan, masukan dan membantu dalam penyelesaian skripsi.
4. Pembimbing I dan Pembimbing II, Dr. Rahmawati, M.Ag dan Firmansyah,S.Pd., S.H.,M.H. yang telah banyak memberi bimbingan, masukan dan mengarahkan dalam rangka penyelesaian skripsi ini.

5. Penguji I dan Penguji II, Dr. Muhammad Tahmid Nur, M.Ag dan Fitriani Jamaluddin yang telah banyak memberikan arahan untuk menyelesaian skripsi ini.
6. Penasehat Akademik, H. Hamza Hasan, Lc., M.Ag.
7. Seluruh Dosen dan staf pegawai IAIN Palopo yang telah mendidik penulis selama berada di IAIN Palopo dan memberikan bantuan dalam penyusunan skripsi ini.
8. Kepala Unit Perpustakaan, Abu Bakar S.Pd., M.Pd., beserta Karyawan dan Karyawati dalam ruang lingkup IAIN Palopo, yang telah banyak membantu, khususnya dalam mengumpulkan literatur yang berkaitan dengan pembahasan skripsi ini.
9. Kepada semua teman seperjuangan, mahasiswa Program Studi Hukum Tata Negara IAIN Palopo angkatan 2020 (khususnya kelas A), yang selama ini membantu dan selalu memberikan saran dalam penyusunan skripsi ini.
10. Asriani Jalil dan Adelia Sari Indra Utami selaku teman yang selalu membantu dan menyemangati dalam menyelesaikan skripsi penulis.
11. Pihak-pihak yang turut membantu dan terlibat dalam penulisan skripsi ini yang tidak sempat penulis tuliskan satu per satu.

Tiada balasan yang dapat diberikan penyusun, kecuali kepada Allah Swt penulis harapkan balasan dan semoga kerja keras ini bernilai pahala disisi-Nya. *Aamiin Ya Rabbal Alamin*

Palopo, Juni 2024

Penulis

Nur Alfiana Alfitri

PEDOMAN TRANSLITERASI ARAB DAN SINGKATAN

A. Transliterasi Arab-Latin

Daftar huruf bahasa Arab dan transliterasinya ke dalam huruf Latin dapat dilihat pada tabel berikut:

1. Konsonan

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	tidak dilambangkan	tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	ṡa	ṣ	es (dengan titik di atas)
ج	Jim	J	Je
ح	ḥa	ḥ	ha (dengan titik di bawah)
خ	Kha	K H	ka dan ha
د	Dal	D	De
ذ	Żal	Ż	zet (dengan titik di atas)
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	es dan ye
ص	ṣad	ṣ	es (dengan titik di bawah)
ض	ḍad	ḍ	de (dengan titik di bawah)
ط	ṭa	ṭ	te (dengan titik di bawah)
ظ	ẓa	ẓ	zet (dengan titik di bawah)
ع	‘ain	‘	apostrof terbalik
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Qi
ك	Kaf	K	Ka
ل	Lam	L	El

م	Mim	M	Em
ف	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
ء	Hamzah	’	Apostrof
ى	Ya	Y	Ye

Hamzah (ء) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apapun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda (’).

2. Vokal

Vokal bahasa Arab, seperti vokal bahasa Indonesia, terdiri atas vokal tunggal atau monoflog dan vokal rangkap atau diftong. Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin	Nama
اَ	*fatḥah*	A	A
اِ	*Kasrah*	I	I
اُ	*ḍammah*	U	U

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harakat dan huruf, transliterasinya berupa gabungan huruf, yaitu:

Tanda	Nama	Huruf Latin	Nama
ى ىَ	fatḥah dan yā’	Ai	a dan i
ى وَ	fatḥah dan wau	Au	a dan u

Contoh:

فَ ي كَ : *kaifa*

لَ وَ ه : *haula*

3. *Maddah*

Maddah atau vokal panjang yang lambagnya berupa harakat atau huruf transliterasinya berupa huruf dan tanda, yaitu:

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
.. ..ا|..ـَ..ـَ ى	*fatḥah* dan *alif* atau *yā'*	Ā	a dan garis di atas
ـِى	*kasrah* dan *yā''*	Ī	i dan garis di atas
ـُو ى	*ḍammah* dan *wau*	Ū	u dan garis di atas

Contoh:

تَ ماَ : *māta*
مَى رَ : *ramā*
قِيْلَ : *qīla*
تُ يَمُوْ : *yamūtu*

4. Tā' marbūṭah

Transliterasi untuk tā' marbūṭah ada dua, yaitu: tā' marbūṭah yang hidup atau mendapat harakat fatḥah, kasrah, dan ḍammah, transliterasinya adalah [t]. Sedangkan tā' marbūṭah yang mati atau mendapat harakat sukun, transliterasinya adalah [h]. Kalau pada kata yang berakhir dengan tā' marbūṭah di ikuti oleh kata yang menggunakan kata sandang al- serta bacaan kedua kata itu terpisah, maka tā' marbūṭah itu ditransliterasikan dengan ha (h).

Contoh:

لِ طْفَا الأ روْضَة : *rauḍah al-atf ā'l*
ضِلَة اَلْفَا يْنَة اَلْمَدِ : *al-maḍīnah al- fā'ḍilah*

5. اَلْحِكْمَة : *al-ḥikma***Syaddah (Tasydīd)**

Syaddah atau *tasydīd* yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda *tasydīd* (ـّ) dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda syaddah

Contoh:

رَبَّنَا : *rabbanā*
نَجَّيْنَا : *najjainā*
اَلْحَقّ : *al-haqq*
نُعِّمَ : *nu'ima*
عَدُوٌّ : *aduwwun*

Jika huruf ber-tasydid di akhir sebuah kata dan didahului oleh huruf kasrah (ىَ) maka ia ditransliterasi seperti huruf maddah menjadi ī.

Contoh:

عَلِيٌّ ::'Alī (bukan 'Aliyy atau 'Aly)
بِيُّ عَرَ ::'Arabī (bukan 'Arabiyy atau 'Araby)

6. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf (alif lam ma'rifah). Dalam pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa, al-, baik ketika ia diikuti oleh huruf syamsiyah maupun qamariyah. Kata sandang tidak mengikuti bunyi huruf langsung yang mengikutinya dan dihubungkan dengan garis mendatar (-).

Contoh:

اَلشَّمْسُ : al-syamsu (bukan asy-syamsu)
لةَ اَلزَّلْزَ : al-zalzalah (az-zalzalah)
اَلْفَلْسَفَة : al-falsafah
دُ اَلْبِلاَ : al-bilādu

7. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (‘) hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak melambangkan, karena dalam tulisan Arab ia berupa alif.

Contoh:

نَ وْ مُرُ تَأْ : ta'murūna

عُ اَلنَّوْ : al-nau’

ءٌ شَىْ : syai’un

تُ أُمِرْ : umirtu

8. Penulisan Kata Arab yang Lazim Digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, istilah atau kalimat yang belum dilakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang sudah lazim dan menjadi bagian dari perbendaharaan bahasa Indonesia, atau sering ditulis dalam tulisan bahasa Indonesia, atau lazim digunakan dalam dunia akademik tertentu, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya, kata al-Qur’an (dari al-Qur’ain), alhamdulillah dan munaqasyah. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka harus ditranslierasi secara utuh.

Contoh:

Syarḥ al-Arba’īn al-Nawāwī

Risālah fī Ri’āyah al-Maṣlaḥah

9. *Lafẓ al-Jalālah* (الله)

Kata “Allah” yang didahului partikel seperti huruf jarr dan huruf lainnya atau berkedudukan sebagai *muḍāf ilaih* (frasa nominal), ditransliterasi tanpa huruf hamzah.

Contoh :

دِيْنُ اللهِ : dīnullā

بِاللهِ : billāh

Adapun tā’ marbūṭah di akhir kata yang disandarkan kepada lafẓ al- jalālah, ditransliterasi dengan huruf [t].

Contoh:

هُمْ فِيْ رَحْمَةِ اللهِ : hum fī raḥmatillāh

10. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital (All Caps), dalam transliterasinya huruf-huruf tersebut dikenai ketentuan tentang penggunaan huruf kapital berdasarkan pedoman ejaan Bahasa Indonesia yang berlaku (EYD). Huruf kapital misalnya, digunakan untuk menuliskan huruf awal nama diri (orang, tempat, bulan) dan huruf pertama pada permulaan kalimat. Bila nama diri di dahului oleh kata sandang (al-), maka yang ditulis dengan huruf kapital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf kapital (Al-). Ketentuan yang sama juga berlaku untuk huruf awal dari judul referensi yang didahului oleh kata sandang al-, baik ketika ia ditulis dalam teks maupun dalam catatan rujukan (CK, DP, CDK, dan DR).

Contoh:

Wa mā Muḥammadun illā rasūl

Inna awwala baitin wuḍi'a linnāsi lallażī bi Bakkata mubārakan

Syahru Ramaḍān al-lażī unzila fīhi al-Qur'ān

Naṣr Hāmid Abū Zayd Al- Tūfī

Al-Maṣlaḥah fī al-Tasyrī' al-Islāmī

Jika nama resmi seseorang menggunakan kata Ibnu (anak dari) dan Abū (bapak dari) sebagai nama kedua terakhirnya, maka kedua nama terakhir itu harus disebutkan sebagai nama akhir dalam daftar pustaka atau daftar referensi.

Abū al-Walīd Muhammad ibn Rusyud, ditulis menjadi: Ibnu Rusyd, Abū alWalīd Muḥammad (bukan: Rusyd, Abū al-Walīd Muḥammad ibnu)
Naṣr Ḥāmid Abū Zaīd, ditulis menjadi: Abū Zaīd, Naṣr Ḥāmid (bukan: Zaīd, Naṣr Ḥamīd Abu)

Beberapa singkatan yang dibakukan adalah:

Swt.	= subhanahu wa ta 'ala
Saw.	= sallallahu 'alaihi wa sallam
a.s	= alaihi al-salam
Q.S	= Qur'an, Surah
H	= Hijrah
M	= Masehi
SM	= Sebelum Masehi
1.	= Lahir tahun (untuk orang yang masih hidup saja)
w.	= Wafat tahun
QS.../....:4	= QS al-Baqarah/2:4 atau QS Ali 'Imran

DAFTAR ISI

DAFTAR AYAT

DAFTAR ISTILAH

UUD	: Undang-Undang Dasar
UU ITE	: Undang-Undang Informasi dan Transaksi Elektronik
HAM	: Hak Asasi Manusia
EDI	: Electronic Data Interchange
KOMINFO	: Kementrian Informasi dan Informatika
PSE	: Penyelenggara Sistem Elektronik
BPJS	: Badan Pengawas Jaminan Sosial
BSI	: Bank Syariah Indonesia
SIM	: Subscriber Identity Module
PDN	: Pusat Data Nasional

ABSTRAK

Nur Alfiana Alfitri, 2024. "*Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022".* Program Studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo. Dibimbing oleh Rahmawati dan Firmansyah

Skripsi ini membahas tentang Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. Penelitian ini bertujuan untuk; mengetahui perlindungan hukum terhadap data pribadi di era digital; untuk mengetahui perlindungan hukum terhadap data pribadi di era digital berdasarkan undang-undang nomor 27 tahun 2022.

Jenis penelitian ini adalah penelitian hukum normatif dengan pendekatan penelitian yang digunakan adalah pendekatan perundang-undangan. Teknik pengumpulan data yang digunakan adalah studi kepustakaan dengan teknik analisis data yang digunakan adalah deskriptif kualitatif.

Hasil Penelitian ini menunjukkan bahwa Kemajuan Teknologi Informasi telah mengubah kehidupan manusia dalam berbagai aspek, termasuk dalam Pengelolaan Data Pribadi yang sangat rentan disalahgunakan. UU PDP bertujuan untuk memberikan perlindungan hukum dengan mengatur pengumpulan, pengolahan, dan penggunaan data pribadi, serta menetapkan sanksi bagi yang melakukan pelanggaran data. Sebelumnya Pengaturan mengenai perlindungan data pribadi tersebar dalam beberapa undang-undang sektoral, tetapi tidak secara khusus membahas perlindungan data pribadi. Kebocoran Data yang terjadi pada Tokopedia, KreditPlus, BPJS, SIM Card, dan BSI, ini menunjukkan kelemahan dalam sistem keamanan perangkat lunak dan kesalahan manusia sendiri. Perlunya sistem keamanan yang lebih kuat, seperti enkripsi data, autentikasi ganda, pembaruan perangkat lunak secara berkala dan memberikan edukasi terhadap masyarakat tentang pentingnya perlindungan data pribadi. UU PDP memberikan perlindungan hukum preventif dan represif. Akan tetapi UU PDP masih memerlukan peraturan tambahan seperti peraturan pemeritah dan lembaga independen khusus perlindungan data pribadi untuk memastikan implementasi undang-undang ini efektif.

Kata Kunci: Perlindungan Hukum, Data Pribadi, Era Digital

ABSTRACT

Nur Alfiana Alfitri, 2024. "Personal Data Protection in the Digital Age Based on Law Number 27 of 2022". Contitutional Law Study Program, Faculty of Sharia, Palopo State Islamic Institute. Supervised by Rahmawati and Firmansyah.

This thesis discusses the Protection of Personal Data in the Digital Age Based on Law Number 27 of 2022. This research aims to; find out the legal protection of personal data in the digital era; to find out the legal protection of personal data in the digital era based on law number 27 of 2022.

This type of research is normative legal research with the research approach used is a statutory approach. The data collection technique used is a literature study with the data analysis technique used is descriptive qualitative.

The results of this study indicate that advances in information technology have changed human life in various aspects, including in the management of personal data which is very vulnerable to misuse. The PDP Law aims to provide legal protection by regulating the collection, processing, and use of personal data, as well as establishing sanctions for those who commit data violations. Previously, regulations regarding personal data protection were scattered in several sectoral laws, but did not specifically discuss personal data protection. Data leaks that occurred in Tokopedia, KreditPlus, BPJS, SIM Card, and BSI, this shows weaknesses in software security systems and human error. The need for stronger security systems, such as data encryption, double authentication, regular software updates and educating the public about the importance of personal data protection. The PDP Law provides preventive and repressive legal protection. However, the PDP Law still requires additional regulations such as government regulations and independent institutions specialized in personal data protection to ensure effective implementation of this law.

Keywords: Legal Protection, Personal Data, Digital Era

BAB I

PENDAHULUAN

A. Latar Belakang

Era Digital merupakan suatu masa ketika teknologi informasi dan komunikasi menjadi bagian penting dalam kehidupan manusia. Di era ini informasi dapat diakses dan disebarkan dengan cepat melalui perangkat digital seperti komputer, smartphone dan tablet. Perkembangan teknologi yang pesat telah mengubah cara kita bekerja, berkomunikasi, dan berinteraksi dengan lingkungan sekitar. Era digital dimulai dengan hadirnya internet pada akhir abad ke-20, internet menjadi dasar utama munculnya berbagai inovasi teknologi yang belum pernah terpikirkan sebelumnya. Transformasi teknologi ini memudahkan akses informasi dan komunikasi antar individu serta organisasi seluruh dunia.[1] Namun dibalik segala kenyamanan dan keuntungan yang diberikan, teknologi juga dapat memberikan dampak negatif karena menjadi alat dalam melakukan tindak kejahatan dalam dunia maya.[2]

Salah satu dampak negatif dari kemajuan teknologi adalah pencurian data pribadi. Pencurian data pribadi merupakan kejahatan yang berbahaya karena dapat menjadi awal dari berbagai kejahatan lainnya di dunia maya. Kerugian yang di

[1] Telkom University "Transformasi Digital: Tren Dan Tantangan Di Era Teknologi Transformasi"https://bit.telkomuniversity.ac.id/transformasi-digital-tren-dan-tantangan-di-era-teknologi-informasi/ Di Akses Pada Tanggal 08 November 2024 Pukul 20.49

[2] Sevia Diah Pratiwi and Muhammad Irwan Padli Nasution, "Penegakan Hukum Terhadap Keamanan Data Privasi Pada Media Sosial Di Indonesia," *SAMMAJIVA : Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 3 (2023): 35–41.

dapatkan oleh korban pencurian data dapat berupa kerugian finansial, penipuan, penyalahgunaan identitas, dan pelanggaran privasi.[3]

Data pribadi sering dianggap sebagai bagian dari privasi. Privasi adalah hak dasar manusia yang sangat penting karena menyangkut otonomi dan kewenangan manusia privasi pada konsep awal perlindungannya disebut dengan hak untuk tidak di ganggu oleh orang lain "*The right to be alone*" jadi hak ini mengakui bahwa manusia menciptakan pembatasan dan melindungi dari gangguan yang tidak diinginkan dalam kehidupan kita.[4]

Hukum Islam sebagai kerangka Hukum Ilahi yang membimbing umat muslim dalam kehidupan sehari-hari memastikan tindakan mereka sesuai dengan kehendak Allah.[5] Islam memandang privasi sebagai sesuatu yang harus dihormati karena berkaitan dengan kerahasiaan seseorang.[6] Hal ini diatur dalam prinsip privasi sebagaimana yang dinyatakan dalam QS.An-Nur ayat 27:24

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ۚ ذَٰلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Artinya:" Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam

---

[3] Muhammad Triadi, "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital," *REUSAM: Jurnal Ilmu Hukum* 11, no. 1 (2023): 45, https://doi.org/10.29103/reusam.v11i1.10178.

[4] Sinta Dewi Rosadi, "*Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional"* Cet. 2 (Bandung: Refika Aditama, 2022)

[5] Nasya Tisfa Taudiyah, Rahmawati, Muhammad Nur Alam Muhajir, Andi Sukma Assad, Abdain, *" Harmonizing Islamic Law and Local Culture: A Study of The Mampatangpulo Tradition in Duri, Enrekang Regency" Jurnal Ilmiah Al-Syir'ah,* 22.1 (2024), pp. 74-75.

[6] Parida Angriani, "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif," *DIKTUM: Jurnal Syariah Dan Hukum* 19, no. 2 (2021): 149–65.

> kepada penghuninya. yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat"[7]

Ayat tersebut menekankan pentingnya adab atau etika dalam memasuki rumah orang lain. Allah melarang orang-orang yang beriman kepadanya memasuki rumah orang lain tanpa meminta izin dan mengucapkan salam terlebih dahulu kepada pemilik rumah. Hal ini untuk menghindari melihat sesuatu yang tidak pantas dilihat atau menggangu penghuni rumah hingga menimbulkan ketidaksenangan. Allah SWT berfirman "Sebelum meminta izin", yang artinya, hingga kalian mengetahui siapa yang ada di dalam rumah, apa yang terjadi di sana dan memperoleh izin. Sunnah juga menegaskan bahwa izin hanya diminta sebanyak tiga kali, tidak lebih.

Indonesia memiliki beberapa ketentuan mengenai perlindungan data pribadi yang secara umum tertuang dalam Undang-Undang Dasar 1945, yaitu Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman untuk berbuat atau tidk berbuat sesuatu yang yang merupakan hak asasi".[8] Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, seperti yang diuraikan di atas sangat berkaitan dengan perlindungan hak-hak pribadi.[9]

---

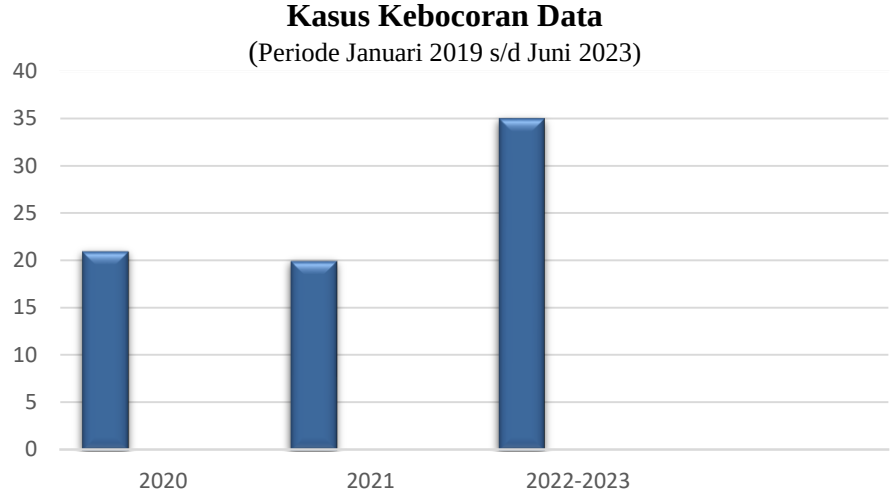
[7] Kementerian Agama RI, *Al-Qur'an dan Terjemahnya*, (Bogor: Unit Percetakan Al-Qur'an, 2018), h. 493.

[8] Upik Mutiara and Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari" 1, no. 1 (2020): 48.

[9] Sekaring Ayumeida Kusnadi And Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi Sekaring," *Tjyybjb.Ac.Cn* 27, No. 2 (2019): 58–66.

Kondisi di mana regulasi terkait perlindungan data pribadi tersebar di berbagai Undang-Undang dan peraturan pemerintah telah menciptakan ketidakpastian hukum dalam pelaksanaannya. Oleh karena itu, pemerintah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pada 10 September 2022.[10] Undang-Undang ini memberikan pengaturan yang komprehensif mengenai perlindungan data publik di Indonesia, termasuk mengatur hak-hak pemilik data pribadi dan menetapkan sanksi bagi penyelenggara sistem elektronik yang mengelola data pribadi dalam sistem mereka.[11]

Indonesia telah menghadapi beberapa kasus kebocoran data yang terjadi sebelum disahkannya undang-undang perlindungan data pribadi. Berikut grafik jumlah kasus kebocoran data yang terjadi di Indonesia:



[10] Anggianti Nurhana and Yana Indawati, "Perlindungan Hukum Atas Data Pribadi Pengguna SIM Card Telepon Seluler," *Amnesti: Jurnal Hukum* 5, no. 1 (2023): 66–82, https://doi.org/10.37729/amnesti.v5i1.2706.

[11] Menkominfo "RUU PDP Disahkan, Kominfo Awasi Tata Kelola Data Pribadi PSE – Ditjen Aptika 2022", diakses Oktober 5, 2022, https://aptika.kominfo.go.id/2022/09/menkominfo-uu-pdpdisahkan-kominfo-awasi-tata-kelola-data-pribadi-pse/.

Jumlah kasus kebocoran dugaan pelanggaran perlindungan data pribadi yang ditangani cenderung mengalami kenaikan. Pada tahun 2019 terdapat tiga kasus. Selanjunya berturut-turut adalah 21 kasus pada tahun 2020, 20 kasus pada tahun 2021, dan tahun 2022 sampai 2023 ada 35 kasus. [12]

Pentingnya perlindungan data pribadi di Indonesia semakin meningkat seiring dengan kemajuan teknologi, yang kerap memunculkan resiko kebocoran data akibat dugaan peretasan oleh para hacker di antaranya: pada 20 maret tahun 2020 tokopedia mengalami kebocoran data pribadi sebanyak 15 juta akun pengguna. Peretasan ini dilakukan oleh peretasan internasional yang menggunakan nama "*why so dank*". Tidak lama setelah insiden tokopedia, kembali terjadi kebocoran data yang dialami oleh kredit plus, sekitar 890.000 data nasabah kredit plus diperjualbelikan di situs raidforums. Selain itu pada tahun 2021 kebocoran data kembali terjadi pada situs badan penyelenggara jaminan sosial (BPJS) kesehatan. Data yang bocor mencakup informasi pribadi dari sekitar 279 juta warga negara Indonesia. Selanjutnya terjadi lagi pada tahun 2022, sebanyak 1,3 miliar data kartu SIM di Indonesia menjadi target kebocoran data dan dijual di forum breached.to. Pada tahun 2023 bank syariah indonesia juga menjadi target peretasan. Kelompok hacker lookbit berhasil mencuri sekitar 1,5 terabyte data dari BSI yang mencakup informasi pribadi nasabah dan karyawannya.[13] Data yang tidak dienskirpsi sangat rentan terhadap penyadapan atau penyalahgunaan untuk tujuan lain yang tidak sesuai dengan maksud pemberi

[12] Kompas.id "Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024", Diakses Pada Tanggal 02 November Pukul 09.15

[13] Lintasarta Cloudeka "10 Rangkuman Kasus Kebocoran dan di Indonesia dan di Dunia" https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/ Di Akses Pada Tanggal 15 Januari 2024 Pukul 20.21

informasi. Ini menunjukkan bahwa internet bukan tempat yang aman bagi seseorang yang mengharapkan privasinya dilindungi. [14]

Beberapa kasus kebocoran data tersebut menunjukkan perlindungan terhadap data pribadi masih perlu ditingkatkan. Karena perlindungan data menjadi kebutuhan masyarkat demi terciptanya keamanan dan kepercayaan terhadap penggunaan teknologi dan layanan digital. Dengan disahkannya Undang-Undang perlindungan data pribadi dapat mengurangi terjadinya lebih banyak korban kasus kebocoran data dan diharapkan mampu memberikan perlindungan hukum terhadap data pribadi warga negaranya.[15]

Berdasarkan latar belakang masalah yang telah diuraikan diatas penulis terarik untuk melakukan penelitian dengan judul " Perlindungan Terhadap Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022"

B. Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, maka akan dirumuskan pokok permasalahan dalam penelitian ini yaitu

1. Bagaimana Perlindungan Hukum Terhadap Data Pribadi di Era Digital?
2. Bagaimana Perlindungan Hukum Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022?

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini adalah

---

[14] Peter Mahmud Marzuki, *Pengantar Ilmu Hukum* (Jakarta: Kencana Prenada Media Group, 2008), Hlm 178

[15] Muhammad Yudistira and Ramadhan, *Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo*, *Unes Law Review*, vol. 5, 2023, https://doi.org/10.31933/unesrev.v5i4.

1. Untuk Mengetahui Perlindungan Hukum Terhadap Data Pribadi di Era Digital.
2. Untuk Mengetahui Perlindungan Hukum Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022.

D. Manfaat Penelitian

1. Manfaat Teoritis
    a) Penelitian ini dapat memberikan sumbangan dalam pengembangan teori hukum terkait perlindungan data pribadi.
    b) Hasil penelitian ini diharapkan bisa menjadi referensi dalam pengembang ilmu pengetahuan tentang perlindungan hukum terhadap data pribadi.
2. Manfaat Praktis
    a) Penelitian ini dapat membantu meningkatkan kesadaran masyarakat tentang pentingnya melindungi data pribadi. Dengan demikian, masyarakat dapat lebih waspada terhadap potensi penyalahgunaan data dan mengambil tindakan untuk melindungi privasi mereka.
    b) Memberikan gambaran mengenai perlindungan hukum berdasarkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi.

E. Kajian Penelitian Terdahulu yang Relevan

Penilitian terdahulu sangat dibutuhkan dalam suatu penelitian dan dengan adanya penelitian terdahulu ini dapat melihat kelebihan serta kekurangan antara peneliti sebelumnya dalam berbagai teori, konsep yang diungkapkan oleh penulis

dalam masalah yang berhubungan dengan penelitian. Penelitian terdahulu juga dapat mempermudah pembaca untuk melihat perbedaan dari persamaan teori yang digunakan oleh penulis dengan penulis yang lainnya dengan masalah yang sama. Penelitian terdahulu dapat berfungsi sebagai sumber inspirasi yang nantinya membantu pelaksanaan penelitian. Beberapa diantaranya adalah penelitian yang dilakukan oleh:

1) Muhammmad Fikri Mubarok, Universitas Nahdatul Ulama Indonesia, Jakarta, Indonesia Tahun 2021 dengan judul penelitian "Tinjauan Yuridis Perlindungan Hukum Terhadap Data Pribadi Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik" Metode Penelitian yang digunakan peneliti terdahulu yaitu jenis penelitian normatif dan pendekatan perundang-undangan. Dalam hasil penelitian menunjukkan model kebijakan untuk melindungi penyelenggara sistem elektronik dari kebocoran data pribadi atau penyalahgunaan data pribadi. Ini juga mencakup penegakan atau penyelesaian masalah melalui sistem hukum yang berlaku jika terjadi kebocoran atau penyalahgunaan data pribadi oleh penyelenggara sistem elektronik di Indonesia. Pelanggaran data pribadi di Indonesia sering terjadi karena tidak adanya peraturan hukum yang secara spesifik membahas tentang perlindungan hukum terhadap perlindungan data pribadi. Saat ini, Indonesia hanya memiliki beberapa peraturan perundang-undangan yang mengatur perlindungan data

pribadi, jadi perlu ada undang-undang yang komprehensif, jelas, dan tegas tentang penyalahgunaan data pribadi. [16]

Persamaan penelitian ini dengan penelitian terdahulu terdapat pada metode penelitian yang sama-sama menggunakan jenis penelitian normatif dan pendekatan melalui perundang-undangan. Sedangkan perbedaan dalam penelitian ini dengan penelitian terdahulu terdapat pada undang-undang yang digunakan peneliti terdahulu mengkaji undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik sedangkan peneliti selanjutnya menggunakan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi sebagai fokus dalam penelitian.

2) Aulia Akbar Navis, Universitas Islam Negeri Maulana Malik Ibrahim, Malang, Indonesia Tahun 2023. Dengan judul penelitian "Perlindungan Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 dan Persepektif Siyasah Syar'iyyah (Studi Dinas Komunikasi dan Informatika Kota Malang)". Hasil dari penelitian ini Pertama, Dinas komunikasi dan Informatika Kota Malang telah berupaya penuh dalam melindungi data pribadi masyarakat, dengan meningkatkan sistem keamanan firewall, sosialisasi dan penyebaran media online ataupun offline. Kedua, Dalam fiqh Siyasah, Dinas Komunikasi dan Informatika Kota Malang telah sesuai dengan ajaran-ajaran Islam dalam menjamin keamanan dan perlindungan data pribadi masyarakat. Pemerintah berupaya optimal melindungi data

[16] Muhammad Fikri Mubarok, "Tinjauan Yuridis Perlindungan Hukum Terhadap Data Pribadi Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", 2021.

pribadi dan mematuhi regulasi yang berlaku dan meningkatkan sistem keamanan Firewall, kemudian pemerintah dalam melindungi data pribadi masyarakat sesuai dengan ajaran Islam.

Persamaan yang ada dalam penelitian ini dengan penelitian terdahulu yaitu sama-sama membahas tentang perlindungan data pribadi berdasarkan undang-undang nomor 27 tahun 2022. Sedangkan perbedaan dalam penelitian ini yaitu peneliti terdahulu juga membahas perlindungan data pribadi menurut persepektif siyasah Syar'iyyah, sedangkan peneliti selanjutnya hanya membahas perlindungan data pribadi berdasarkan undang-undang nomor 27 tahun 2022 secara umum. [17]

3) Hanifan Nifari (Jurnal 2020), Universitas Indonesia tentang "Perlindungan Data Pribadi Sebagai Bagian dari Hak Aasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan di Negara Lain). Hasil penelitian menunjukkan bahwa perlindungan data pribadi sebagai bagian dari hak perlindungan diri yang diatur dalam pasal 28G ayat (1) Undang-Undang dasar negara republik indonesia tahun 1945 belum memiliki regulasi yang terintegrasi dalam satu undang-undang khusus. Urgensi pembentukan undang-undang khusus untuk perlindungan data pribadi sangat penting, mengingat maraknya penyalahgunaan data pribadi diluar tujuan awalnya, seperti praktik jual beli data secara komersial. Saat ini aturan terkait perlindungan data pribadi masih tersebar diberbagai peraturan perundang-undangan yang tidak secra

[17] Aulia Akbar Navis, "Perlindungan Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 dan Persepektif Siyasah Syar'iyyah (Studi Dinas Komunikasi dan Informatika Kota Malang)". 2023

khusus membahas hal tersebut. Pengaturan perlindungan data pribadi perlu disesuaikan dengan studi perbandingan dari negara-negara lain, sambil memperhatikan kondisi sosiologis indonesia. Penelitian ini membahas konsep umum perlindungan data pribadi, membandingkan regulasi di negara lain serta menganalisis hasil perbandingan tersebut untuk melihat kemungkinan penerapannya di indonesia.

Persamaan dalam penelitian ini sama-sama membahas terkait pengaturan dan perlindungan hukum terhadap data pribadi di indonesia. Sedangkan perbedaan yang ada dalam penelitian ini peneliti terdahulu lebih fokus membahas perlindungan data pribadi menggunakan metode perbandingan dengan negara-negara lain. Dalam penelitian ini tidak menggunakan undang-undang nomor 27 tahun 2022 sebagai rujukan utamannya.[18]

F. Metode Penelitian

1. Jenis dan Pendekatan Penelitian

a) Jenis Penelitian

Jenis penelitian yang digunakan penulis dalam penelitian ini adalah Penelitian Hukum Normatif atau disebut sebagai penelitian hukum murni, penelitian hukum positif dan penelitian hukum doktrinal. Penelitian hukum normatif merupakan penelitian hukum yang memfokuskan penelitian pada peraturan perundang-undangan yang

[18] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain," *Jurnal Hukum Dan Bisnis (Selisik)* 6, No. 1 (2020): 1–14, Https://Doi.Org/10.35814/Selisik.V6i1.1699.

tertulis (*Law in Books)* atau penelitian yang didasarkan pada kaidah atau norma hukum yang berlaku dimasyarakat. Penelitian Normatif bisa dikatakan sebagai penelitian kajian pustaka yang sumber datanya terdiri dari bahan hukum primer, sekunder dan tesier, dan sebagian besar datanya berasal dari Undang-Undang atau Peraturan-Peraturan yang tertulis dan berlaku dalam masyarakat.[19]

b) Pendekatan Penelitian

Pendekatan yang digunakan yaitu Pendekatan Perundang-Undangan (*Statute Approach*), ini dilakukan untuk memeriksa semua undang-undang dan peraturan yang terkait dengan masalah perlindungan data pribadi yaitu;[20]

1) Undang-Undang Nomor 10 tahun 1998 tentang Perbankan
2) Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
3) Undang-Undang Nomor 8 tahun tentang Perlindungan Konsumen
4) Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia
5) Undang-Undang Nomor 24 tahun 2008 tentang Keterbukaan Informasi Publik
6) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan
7) Undang -Undang Nomor 24 Tahun 2013 Tentang Perubahan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

[19] Muhammad Siddiq Armia ‘’Penentuan Metode & Pendekatan Penelitian’’’ (Lembaga Kajian Konstitusi Indonesia (LKKI) Fakultas Syariah dan Hukum Universitas Islam Negeri Ar-Raniry Banda Aceh, Agustus 2022) Hal. 8

[20] Sugiyono, *Metodologi Penelitian Kuantitatif, Kualitatif Dan R & D*, Cetakan 19 (Alfabeta Bandung, 2013).

8) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
9) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik
10) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
11) Undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi

1. Sumber Data Penelitian

a. Bahan Hukum Primer adalah bahan hukum yang mempunyai kekuatan hukum yang bersifat mengikat terdiri dari peraturan perundang-undangan yang terkait dengan objek penelitian.[21]
b. Bahan Hukum Sekunder adalah bahan hukum yang menjelaskan bahan hukum primer, seperti Buku-buku Hukum, hasil penelitian dari pakar hukum dan pendapat ahli bidang hukum. [22]
c. Bahan Hukum Tesier adalah bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer maupun bahan hukum sekunder, seperti kamus hukum dan kamus bahasa indonesia.

2. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan yaitu Studi Kepustakaan (*Library Research*) Teknik mengumpulkan data dengan mempelajari teori dari berbagai literatur yang berkaitan dengan topik

[21] Zainuddin Ali,"*Metode penelitian hukum*" Cet 1 (Jakarta Sinar Grafika 2019).
[22] Muhaimin,"*Merode Penelitian Hukum"* Cet 1 (NTB: Mataram, University Press, 2020),

penelitian. Pengumpulan data ini dilakukan dengan cara mencari dari berbagai sumber, seperti buku, jurnal, dan penelitian sebelumnya. Agar kebenaran dan gagasan dapat didukung, bahan pustaka yang dikumpulkan dari berbagai referensi harus dianalisis secara kritis.[23]

3. Teknik Analisis Data

Metode Analisis yang digunakan yaitu analisis deskriptif kualitatif merupakan analisis data yang tidak menggunakan angka melainkan memberikan gambaran-gambaran (deskripsi) dengan kata-kata yang diambil dari dokumen peraturan dan peraturan perundang-undangan. Analisis data kualitatif dalam penelitian ini dilakukan dengan model interaktif yaitu;

a. Reduksi Data *(Data Reduction)*. Dalam proses analisis, peneliti menggunakan reduksi data untuk membuat data lebih jelas, lebih ringkas, lebih fokus, dan menghilangkan hal-hal yang tidak penting.
b. Sajian Data *(Data Display)*. Peneliti berusaha menyajikan data dengan baik dan mudah di mengerti untuk mendapatkan pemahaman yang jelas tentang data, yang akan membantu mereka membuat kesimpulan.
c. Penarikan Kesimpulan *(Conclusion Drawing)*. Penelitian ini, setiap data telah diperiksa untuk keakuratan dan validitasnya sebelum

[23] Miza Nina Adlini et al., "Metode Penelitian Kualitatif Studi Pustaka," *Edumaspul: Jurnal Pendidikan* 6, no. 1 (2022): 974–80, https://doi.org/10.33487/edumaspul.v6i1.3394.

dipilih dan ditarik kesimpulan. Peneliti dapat sampai pada kesimpulan dengan model analisis interaktif.[24]

I. Definisi Istilah

Definisi Istilah digunakan untuk menghindari perbedaan pengertian terhadap istilah yang diguakan dalam penelitian ini, sehingga yang dimaksudkan menjadi jelas. Definisi istilah dalam hal ini sebagai berikut:

a. Perlindungan Hukum adalah upaya yang dilakukan pemerintah atau penguasa untuk melindungi hak-hak warga negara, dengan menggunakan peraturan-peraturan yang ada. Perlindungan hukum bertujuan agar masyarakat dapat menikmati hak-hak yang diberkn oleh hukum dan terhindar dari perbuatan sewenang-wenang.
b. Data Pribadi adalah Data perseorangan tertentu, yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiannya.
c. Era Digital adalah salah satu era atau zaman yang di dalamnya sudah memiliki kondisi perkembangan yang begitu maju hingga semua kegiatan penting bisa dilakukan secara digital.

[24] Subandi, "Qualitative Description as One Method in Performing Arts Study," *Harmonia*, no. 19 (2011): 173–79.

BAB II

TINJAUAN UMUM TENTANG PERLINDUNGAN DATA PRIBADI

A. Tinjaun Umum Perlindungan Data Pribadi

1. Pengertian Data Pribadi

Data pribadi merujuk pada informasi tunggal atau sekumpulan informasi, baik yang bersifat rahasia maupun yang diberikan oleh pemiliknya, yang dihimpun dalam suatu sistem untuk diproses sesuai dengan tujuan yang ditetapkan. Dalam perlindungan data pribadi, terdapat dua istilah yang sering digunakan, yakni "informasi pribadi" dan "data pribadi." Di Amerika Serikat, istilah yang dipakai adalah informasi pribadi (*personally identifiable information*), sedangkan di Eropa, digunakan istilah data pribadi (personal data). Regulasi yang berlaku di Indonesia saat ini mengadopsi terminologi data pribadi.

Pasal 2 (A) Data *Protection Directive* personal data menyatakan:

> *"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*[25]

Entitas yang dilindungi dalam mekanisme perlindungan data pribadi adalah "orang perorangan" (*natural person*), bukan "badan hukum" (*legal*

[25] Eka Martiana Wulansari, "Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Norm Dalam Perlindungan Terhadap Hak Atas Privasi Seseorang Di Indonesia," *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan* 7, no. 2 (2020): 265–89.

person).[26] Hak perlindungan data pribadi ini berasal dari hak atas kehidupan pribadi atau yang dikenal sebagai *the right to private life.* Konsep kehidupan pribadi berkaitan dengan manusia sebagai makhluk hidup, sehingga orang perorangan merupakan pemilik utama hak perlindungan data pribadi. Dalam hal perlindungan terhadap data pribadi, terdapat beberapa kategori subyek hukum yang harus diatur. Subyek hukum yang pertama adalah "Pengelola Data Pribadi" yaitu orang, badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang secara sendiri ataupun bersama-sama mengelola data pribadi. Subyek hukum lainnya adalah Pemroses Data Pribadi yaitu orang badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang melakukan pemrosesan data pribadi atas nama pengelola data.[27]

Data Pribadi menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik pada:

Pasal 1 ayat (1) menyatakan bahwa: "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannya".
Pasal 1 ayat (3) menyatakan "Bahwa pemilik data pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu".

[26] European Union Agency for Fundamental Rights & Council of Europe, *Handbook on European Data Protection Law, Publications Office of the European Union,* 2014, https://doi.org/10.2811/69915.

[27] Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018): 88–110, https://doi.org/10.25123/vej.2916.

Secara khusus, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.[28]

Data Pribadi menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang baru saja disahkan terdapat pada Pasal 1 Ayat (1) yang menyatakan bahwa:

> *"Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik"*.[29]

2. Prinsip Data Pribadi

Prinsip data pribadi menurut *Organizationfor Economic and Cooperation Development* (OECD) telah mengeluarkan standar dasar untuk perlindungan data pribadi yang dapat digunakan untuk membuat peraturan sebagai berikut;

a) Prinsip Pengumpulan Batasan *(Collection Limitation Principle)*. Ada batasan dalam pengumpulan data pribadi dan data yang diperoleh harus dengan cara yang sah dan adil, dengan sepengetahuan dan persetujuan subjek data;
b) Prinsip Kualitas Data *(Data Quality Principle)*. Data pribadi harus relevan dengan tujuan penggunaannya, tujuan tersebut, harus akurat, lengkap, dan selalu diperbarui;

---

[28] Muhammad Satria and Susilo Handoyo, "Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia," *Jurnal de Facto* 8, no. 2 (2022): 108–21, https://jurnal.pascasarjana.uniba-bpn.ac.id/index.php/jurnaldefacto/article/view/113.

[29] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Ditama Binbangkum – BPK RI, 016999,2022,1-50

c) Prinsip Tujuan Khusus *(Purpose Specification Principle)*. Tujuan pengumpulan data memastikan bahwa penggunaan data pribadi tidak melebihi batas atau tujuan yang telah ditetapkan dan disetujui oleh subjek data. Hal ini membatasi penggunaan data pribadi hanya untuk keperluan yang spesifik dan tidak menyalahgunakan data di luar tujuan awal pengumpulannya.;

d) Prinsip Penggunaan Batasan *(Use Limitation Principle)* Data pribadi tidak boleh diungkapkan, disediakan, atau digunakan untuk tujuan lain selain yang ditentukan dalam: a. dengan persetujuan subjek data; atau b. oleh otoritas hukum;

e) Prinsip Perlindungan Keamanan *(Security Safeguard Principle)*. Data pribadi harus dilindungi oleh perlindungan keamanan yang wajar terhadap risiko seperti kehilangan atau akses yang tidak sah, pemusnahan, penggunaan, modifikasi, atau pengungkapan data.[30]

f) Prinsip Keterbukaan *(Openness Principle)*. Ada kebijakan keterbukaan tentang pengembangan, praktik, dan undang-undang yang berkaitan dengan data pribadi. Untuk menentukan keberadaan, sifat, dan tujuan utama penggunaan data pribadi.

[30] Karo Karo, Rizky PP dan Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi Di Indonesia Persepektif Teori Keadilan Bermartabat*, Cet 1 (Penerbit Nusa Media Bandung, 2023).

g) Prinsip Partisipasi Individu *(Individual Participation Principle)* adalah untuk mengontrol atau mengkonfirmasi data dengan memberikan akses untuk menghapus, mengubah, dan memperbaiki data.[31]

h) Prinsip Akuntabilitas *(Accountability Principle)* Pengendali data bertanggung jawab penuh atas pengelolaan data pribadi sesuai dengan prinsip perlindungan data, baik dari segi hukum, etika, maupun kepentingan subjek data itu sendiri.[32]

B. Tinjauan Umum Hak Privasi sebagai hak asasi manusia

Hak privasi adalah salah satu aspek fundamental dari hak asasi manusia yang mendasar pada hakikat setiap individu. Hak ini harus dihormati, dipertahankan, dan dilindungi oleh semua pihak, termasuk individu, negara, hukum, dan pemerintah. Hak asasi manusia menghargai nilai-nilai yang melekat pada setiap orang, tanpa memandang latar belakang, tempat tinggal, penampilan, pemikiran, atau keyakinan mereka. Hak ini didasarkan pada prinsip-prinsip kesetaraan, martabat, dan saling menghormati, yang berlaku di berbagai budaya, agama, dan filosofi.[33]

Allan Westin dalam jurnal Sinta Dewi Rosadi mendefinisikan privasi sebagai hak individu, kelompok, atau lembaga untuk memutuskan apakah

---

[31] Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia Dan Malaysia," *Jurnal Cakrawala Hukum* 10, no. 2 (2019): 218–27, https://doi.org/10.26905/idjch.v10i2.3349.

[32] Muhammad Akbar Eka Pradana and Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative Journal of Social Science Research* 4 (2024): 3412–25, https://j-innovative.org/index.php/Innovative/article/view/13476/8935.

[33] Tika Widyaningsih and Suryaningsi Suryaningsi, "Kajian Perlindungan Hukum Terhadap Data Pribadi Digital Anak Sebagai Hak Atas Privasi Di Indonesia," *Nomos : Jurnal Penelitian Ilmu Hukum* 2, no. 3 (2022): 93–103, https://doi.org/10.56393/nomos.v1i5.582.

informasi tentang mereka akan dibagikan atau tidak kepada pihak lain.[34] Selain iu Julian Ines juga dalam jurnal Teguh Prasetyo and Jamalum Sinambela mendefinisikan privasi sebagai suatu kondisi ketika seseorang memiliki kontrol atas ranah keputusan privat.[35] Privasi pertama kali dikembangkan oleh Warren dan Brandeis, yang menulis sebuah jurnal ilmiah di Sekolah Hukum Universitas Harvard dengan judul *"The Right to Privacy"* atau hak untuk tidak diganggu. Dalam jurnal tersebut, Warren dan Brandeis menyatakan:

> *"Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal regocnition."*[36]

Privasi adalah hak untuk dibiarkan sendiri *(rights to be left alone),* adalah hak baru yang muncul akibat perkembangan teknologi, ekonomi, dan politik. Namun, hak ini belum sepenuhnya dilindungi, sehingga memerlukan pengakuan dan perlindungan hukum yang lebih baik.[37]

Warren dan Brandheis dalam jurnal Sekaring Ayumeida berpendapat bahwa privasi adalah sesuatu yang harus dihormati dan dilindungi karena melibatkan empat kepentingan utama. Pertama, Dalam menjalin hubungan dengan orang lain, seseorang perlu menyembunyikan sebagian aspek kehidupan pribadinya agar dapat mempertahankan posisinya pada tingkat tertentu. Kedua, setiap orang memerlukan waktu untuk menyendiri dalam hidupnya, sehingga

---

[34] Dewi Rosadi and Gumelar Pratama, "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia."

[35] Teguh Prasetyo and Jamalum Sinambela Sinambela, "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat," *Spektrum Hukum* 20, no. 1 (2023): 58, https://doi.org/10.56444/sh.v20i1.3663.

[36] Dhoni Martien, *Perlindungan Hukum Data Pribadi*, Cet 1 (Mitra Ilmu Makassar, 2023).

[37] Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia," *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 1, no. 1 (2019): 147–54, https://doi.org/10.21512/becossjournal.v1i1.6030.

privasi menjadi kebutuhan penting. Ketiga, Privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hak ini akan hilang apabila orang tersebut memublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi mencakup hak seseorang untuk menjaga kehidupan keluarganya, termasuk cara membangun pernikahan, keluarga, dan hubungan pribadi yang tidak boleh diketahui orang lain. Berdasarkan penjelasan di atas, setiap individu seharusnya memiliki hak untuk mendapatkan perlindungan dari berbagai gangguan atau upaya yang mencoba merusak dan menyalahgunakan hal-hal yang termasuk dalam ranah privasi mereka.[38]

Pendapat Warren dan Brandeis dalam jurnal Elfian dan Nabila penting karena untuk pertama kalinya privasi dipandang sebagai konsep hukum yang menuntut pengakuan dari negara dan pengadilan, sehingga individu dapat menikmati kehidupan mereka dengan lebih baik. Warren juga mencatat bahwa privasi tidak bersifat absolut dan memiliki batasan, yaitu:

1. Tidak melarang publikasi informasi pribadi untuk kepentingan umum.
2. Tidak ada perlindungan privasi tanpa adanya kerugian yang diderita.
3. Tidak ada privasi jika individu telah menyetujui penyebaran informasi pribadinya.
4. Perlindungan hukum diperlukan karena kerugian akibat pelanggaran privasi sulit diukur dan sering kali lebih dirasakan daripada kerugian fisik. Perlindungan hak atas privasi telah di atur diberbagai konvensi di dunia.

[38] Sekaring Ayumeida Kusnadi And Andy Usmina Wijaya, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi Sekaring," *Tjyybjb.Ac.Cn* 27, No. 2 (2019): 58–66.

Pada Pasal 12 *Universal Declaration of Human Rights* (UDHR) yag menyatakan bahwa:

> *" No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."* [39]

Pasal tersebut memberikan pengaturan yang luas mengenai privasi, meliputi: 1) *Physical Privacy* yaitu perlindungan privasi yang berkaitan dengan tempat tinggalnya; 2) *Decisional Privacy* yaitu perlindungan privasi terhadap hak untuk menentukan kehidupannya sendiri termasuk kehidupan keluarganya; 3) *Dignity* yaitu melindungi harga diri seseorang termasuk nama baik dan reputasi seseorang; 4) *Informational Privacy* yaitu privasi terhadap informasi artinya hak untuk menentukan cara seseorang melakukan dan menyimpan informasi pribadinya. UDHR merupakan instrumen perlindungan internasional yang mengatur hak asasi manusia secara komprehensif termasuk hak privasi.[40]

Setiap individu berhak mendapatkan perlindungan hukum dari gangguan atau pelanggaran terhadap hak atas privasi. Hak privasi juga melibattkan kemampuan seseorang untuk mengontrol siapa yang dapat mengakses informasi pribadi mereka dan bagaimana informasi tersebut digunakan. [41]

Hak privasi di Indonesia secara eksplisit diatur dalam konstitusi setelah amandemen tahun 2000, dengan penambahan sepuluh pasal baru dalam bab hak

---

[39] Wulansari, "Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Norm Dalam Perlindungan Terhadap Hak Atas Privasi Seseorang Di Indonesia."

[40] Elfian Fauzi and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Lex Renaissance* 7, no. 3 (2022): 445–61, https://doi.org/10.20885/jlr.vol7.iss3.art1.

[41] Fujiama Diapoldo Silalahi, "Keamanan Cyber (Cyber Security)," *Penerbit (Yayasan Prima Agus Teknik*, Semarang)

asasi manusia. Pengakuan terhadap hak privasi sebagai kebebasan dasar individu, termasuk perlindungan dari gangguan, tercermin dalam beberapa pasal yaitu:

> Pasal 28G Ayat (1) "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."
>
> Pasal 28H Ayat (4) "Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun".
>
> Pasal 28I Ayat (1) "Hak untuk hidup, hak untuk tidak disiksa, hak kemerdekaan pikiran dan hati nurani, hak beragama, hak untuk tidak diperbudak, hak untuk diakui sebagai pribadi dihadapan hukum, dan hak untuk tidak dituntut atas dasar hukum yang berlaku surut adalah hak asasi manusia yang tidak dapat dikurangi dalam keadaan apapun".
>
> Pasal 28J Ayat (2) Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis."[42]

Konstitusi Indonesia tidak secara langsung mengatur perlindungan data pribadi dalam UUD 1945. Meskipun UUD 1945 secara tegas menyebutkan perlindungan hak asasi manusia, privasi sebagai hal spesifik belum diatur secara rinci. Namun, UUD 1945 memberikan dasar hukum yang kuat dan mendasar untuk pengaturan lebih lanjut terkait pelaksanaan dan perlindungan privasi, termasuk data pribadi. [43]

[42] Undang-Undang Negara Republik Indonesia Tahun 1945

[43] Wahyudi Djafar & Asep Komarudin, *"Perlindungan Hak Atas Privasi Di Internet Beberapa Penjelasan Kunci"*, Elsam, 2014

Perlindungan hak atas privasi, selain diatur dalam UUD 1945, juga dirumuskan dalamm Undng-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia, dirumuskan dalam beberapa pasal sebgai berikut;

> Pasal 29 Ayat (1):" setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya."
>
> Pasal 30 "Setiap orang berhak atas rasa aman dan tenteram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu."
>
> Pasal 31 ayat (1) "Tempat kejadian siapapun tidak boleh diganggu."
>
> Pasal 31 Ayat (2) "Menginjak atau memasuki suatu pekarangan tempatkediaman atau memasuki suatu rumah bertentangan dengan kehendak orang yang mendiaminya, hanya diperbolehkan dalam hal-hal yang telah ditetapkan oleh undang-undang."
>
> Pasal 32 "Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan." [44]

Pasal-pasal dalam UU No. 39 Tahun 1999 secara efektif mengatur dan melindungi berbagai aspek hak privasi, mencakup perlindungan terhadap ruang pribadi seperti rumah, komunikasi, dan korespondensi. UU ini menetapkan bahwa perlindungan hak privasi harus didasarkan pada hukum atau perintah resmi, sehingga memberikan panduan untuk menjaga privasi dengan prinsip kehati-hatian dan memastikan hak individu terlindungi dari gangguan atau pelanggaran yang tidak sah.[45]

[44] Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia

[45] Wahyudi Djafar & Asep Komarudin, "Perlindungan Hak Atas Privasi Di Internet Beberapa Penjelasan Kunci." Elsam, 2014

C. Konsep Privasi dalam Persepektif Islam

Islam merupakan agama yang mengatur semua aspek dalam kehidupan manusia. Islam telah memberikan pedoman dalam berbagai bidang, termasuk hukum, sosial, politik dan berbagai bidang lainnya. Tujuan Hukum Islam adalah mewujudkan kemaslahatan bagi manusia dengan memenuhi kebutuhan primer (Dharuriyyah). Dharuriyah adalah kebutuhan dasar yang sangat penting dan tidak dapat diabaikan. Jika kebutuhan ini tidak terpenuhi, akan muncul kekacauan dan ketidakteraturan di berbagai aspek kehidupan. Islam menetapkan lima kebutuhan (Hifdz ad-Din); 2) Menjaga Jiwa (Hifdz an-Nasf); 3) Menjaga Akal (Hifdz Al-Aql); 4) Menjaga Keturunan (Hifdz-an Nasl); dan 5) Menjaga Harta Benda (Hifdz an-Mal).

Hifdz an-Nasf bertujuan untuk melindungi Hak Asasi Manusia atas kehidupan, kebebasan da rasa aman. Islam sangat memperhatikan Hak Aasi Manusia, terutama hak untuk hidup. Islam melarang tindakan bunuh diri diri dalam Surah An-Nisa ayat 29 menunjukkan penghargaan islam terhadap hak hidup. Sebaliknya siapapun menyelamatkan nyawa seseorang dapat dianggap seperti telah menyelamatkan seluruh kehidupan manusia, sebagaimana disebutkan dalam Surah Al-Maidah Ayat 32.[46]

Perlindungan terhadap hak asasi manusia juga tercermin dalam prinsip hukum Islam yang menekankan persamaan atau Egaliter (AL-Musawah). Prinsip ini ditegaskan dalam Al-Qur'an Surah Al-Hujurat ayat 13:

[46] Rohidin, *Pengantar Hukum Islam*, cetakan 1, vol. 53 (Yogyakarta: Lintang Rasi Aksara Books, 2016). Hlm 30

يٰٓاَيُّهَا النَّاسُ اِنَّا خَلَقْنٰكُمْ مِّنْ ذَكَرٍ وَّاُنْثٰى وَجَعَلْنٰكُمْ شُعُوْبًا وَّقَبَاۤىِٕلَ لِتَعَارَفُوْاۚ اِنَّ اَكْرَمَكُمْ عِنْدَ اللّٰهِ اَتْقٰىكُمْۗ اِنَّ اللّٰهَ عَلِيْمٌ خَبِيْرٌ

Artinya:"Hai manusia, sesungguhnya kami telamh menciptakan kamu dari seorang laki-laki dan perempuan. Kemudian, kami menjadikan kamu berbangsa-bangsa dan bersuku-suku agar kamu saling mengenal. Sesungguhnya yang paling mulia di antara kamu di sisi Allah adalah orang yang paling bertakwa. Sesungguhnya Allah Maha mengetahui lagi Maha Mengenal."

Kemuliaan Manusia tidak ditentukan oleh ras atau warna kulit, melainkan dari ketaqwaanya. Oleh karena itu, setiap manusia baik miskin maupun kaya pintar atau bodoh. Berhak mendapatkan perlakuan yang adil, baik di hadapan Tuhan ataupun di hadapan hukum. Islam menegaskan prinsip kesetaraan (*Egalite*) untuk memastikan bahwa semua individu diperlakukan setara tanpa memandang status dan latar belakang. Selain perlindungan terhadap hak-hak yang telah disebutkan di atas. Islam juga mencakup hak asasi manusia secara luas termasuk hak privasi.[47]

Islam menekankan pentingnya menjaga privasi terkait dengan rumah/kediaman. Rumah dianggap sebagai ruang pribadi yang tidak dapat di masuki oleh orang lain tanpa izin dari pemilik rumah. Hal ini dijelaskan dalam Al-Quran Surah An-Nur ayat 27:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ۚ ذَٰلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Artinya: " Wahai orang-orang yang beriman. Jangan memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam

[47] Rohidin, *Pengantar Hukum Islam*, cetakan 1, vol. 53 (Yogyakarta: Lintang Rasi Aksara Books, 2016). Hlm 27-28

kepada penghuninya demikian itu lebih baik bagimu agar kamu mengambil pelajaran"[48]

Ayat tersebut menggambarkan konsep privasi terkait rumah sebagai tempat tinggal, di mana izin atau Persetujuan *(Concest)* dari pemilik rumah sebagai pemegang hak privasi wajib diperoleh sebelum memasukinya. Masuk kerumah orang lain tanpa peretujuan pemiliknya tidak dibolehkan. Prinsip ini serupa dengan konsep persetujuan dalam pengelola data pribadi yang diatur dalam Pasal 22 UU PDP.

Nabi muhammad menjelaskan lebih lanjut dalam dalam Hadist Shahih Bukhari bahwa pelanggaran terhadap privasi dapat dikenanakan hukuman, sedangkan pemilik rumah tidak menanggung dosa akibatnnya. Hadist tersebut berbunyi:

وَبِإِسْنَادِهِ لَوْ اطَّلَعَ فِي بَيْتِكَ أَحَدٌ وَلَمْ تَأْذَنْ لَهُ خَذَفْتَهُ بِحَصَاةٍ فَفَقَأْتَ عَيْنَهُ مَا كَانَ عَلَيْكَ مِنْ جُنَاحٍ[49]

"Jika seseorang mengintip ke dalam rumahmu rumahmu padahal kamu tidak memebrinya izin, kemudian kamu melemparnya dengan batu sehigga membutakan matanya, kamu tidak mendapat dosa karenanya"(HR. Bukhari)

Dalam Hukum Isalm, Konsep privasi tempat tinggal memiliki peran penting dalam melindungi lima tujuan utama syariah (Maqasid Syariah) seperti agama, jiwa, akal, keturunan, dan harta. Tempat tinggal menjadi ruang bagu seseorang untuk beribadah tanpa gangguan, seperti saat sholat tahajjud, istikharah, berdoa atau intropeksi diri. Selain itu, rumah berfungsi sebagai perlindungan dari ancaman fisik maupun mental yang ada di luar.

[48] Angriani, "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif."

[49] Ilmu Islam "Kumpulan Hadis" https://ilmuislam.id/hadits Di Akses Pada Tanggal 09 November 2024 Pukul 21.15

Rumah juga menyediakan privasi yang mendukung aktivitas berpikir, belajar, dan membaca, sehingga menjaga akal. Tidak hanya itu rumah adalah tempat yang aman untuk menyimpan harta benda, membantu memastikan perlindungannya sesuai dengan tujuan syariah.[50]

D. Perlindungan Hukum

Perlindungan hukum dapat diartikan dari gabungan dua definisi, yaitu "perlindungan" dan "hukum". Menurut kamus besar bahasa indonesia (KBBI), perlindungan berarti tindakan atau upaya untuk melindungi. Sementara itu, hukum merujuk pada peraturan atau kebiasaan yang secara resmi dianggap mengikat yang disahkan oleh penguasa atau pemerintah. Perlindungan hukum adalah upaya yang dilakukan pemerintah untuk melindungi hak-hak, kebebasan dan kepentingan individu atau kelompok dalam masyarakat dengan sejumlah peraturan yang ada.[51]

Menurut Satjipto Rahardjo menjelaskan bahwa perlindungan hukum adalah memberikan pengayoman terhadap Hak Asasi Manusia yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh

---

[50] Skripsi Ramiz Afif Naufal, "Tanggung Jawab Pt Tokopedia Dalam Kasus" (Fakultas Hukum Universitas Islam Indonesia Yogyakarta, 2020), https://dspace.uii.ac.id/handle/123456789/26797.

[51] Hukum Online "Perlindungan Hukum: Pengertian, Unsur dan Contohnya" https://www.hukumonline.com/berita/a/perlindungan-hukum-lt61a8a59ce8062/ Diakses Pada Tanaggal 01 Agustus 2024 Pukul 20.19

aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun.[52]

Menurut Philipus M.Hadjon, perlindungan hukum diartikan sebagai tindakan melindungi atau memberikan pertolongan kepada subyek hukum dengan perangkat-perangkat hukum. Bila melihat pengertian perlindungan di atas maka dapat diketahui unsur-unsur dari perlindungan hukum, yaitu : subjek yang melindungi, objek yang akan dilindungi alat, instrumen maupun upaya yang digunakan untuk tercapainya perlindungan tersebut.[53]

Perlindungan hukum pada dasarnya merupakan suatu konsep yang Universal dari Negara hukum. Muchsin membedakan perlindungan hukum menjadi dua bagian, yaitu:[54]

1. Perlindungan hukum preventif adalah bentuk perlindungan yang diberikan oleh pemerintah untuk mencegah pelanggaran sebelum terjadi. Ini dilakukan melalui regulasi dan peraturan perundang-undangan yang dirancang untuk menghindari terjadinya tindakan melawan hukum.
2. Perlindungan hukum represif adalah perlindungan yang diterapkan setelah pelanggaran terjadi. Bentuk perlindungan ini melibatkan pemberian sanksi, seperti denda, penjara, atau hukuman tambahan, sebagai respons terhadap pelanggaran yang telah terjadi.[55]

---

[52] Sajipto Raharjo, *Ilmu Hukum*, (Bandung; PT Citra Aditya Bakti 2000) Hlm.74

[53] Philipus M. Hadjon, *Pengantar Hukum Administrasi Indonesia*, (Gajah Mada University Press,Yogyakarta 2011), Hlm 10.

[54] Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, (Surakarta, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, 2003) Hlm. 20

[55] Dhoni Martien, *Perlindungan Hukum Data Pribadi*, Cet 1 (Mitra Ilmu Makassar, 2023).

BAB III

PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DI ERA DIGITAL

A. Perlindungan Hukum Data Pribadi

Perkembangan Teknologi Informasi di Era Digital ini telah mengubah kehidupan manusia dalam berbagai aspek, termasuk dalam pengelolaan data pribadi. Data pribadi atau *personal data* didefinisikan sebagai "setiap informasi yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi (subjek data)." General Data Protection Regulation (GDPR) secara spesifik menetapkan cakupan data pribadi antara lain, nama, nomor identitas, data lokasi, *online identifier*, serta satu atau lebih karakteristik spesifik yang berkaitan dengan aspek fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial seseorang. Selain itu, GDPR juga mengakui bahwa data yang telah disamarkan (*pseudonymization*), tetapi tetap dapat mengidentifikasi individu jika dikombinasikan dengan informasi tambahan, termasuk dalam kategori data pribadi.[56]

Data pribadi merupakan aset berharga yang harus dilindungi karena memiliki nilai ekonomi yang tinggi dan dapat disalahgunakan jika jatuh ke tangan yang tidak bertanggung jawab.[57] Beberapa alasan data pribadi harus dilindungi yaitu:

1. Mencegah Pencurian Identitas

[56] Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia."

[57] Indah Rachma Cahyani, "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.3. No.12 (Desember 2022) Tema/Edisi : Hukum Dan Hak Asasi Manusia (Bulan Kedua Belas) Https://Jhlg.Rewangrencang.Com/" 3, no. 12 (2022): 1000–1010.

Kebocoran data pribadi membawa risiko besar, salah satunya adalah pencurian identitas. Jika pihak tak bertanggung jawab memperoleh informasi pribadi kita, mereka dapat berpura-pura menjadi kita untuk melakukan tindakan merugikan, seperti penipuan keuangan, pembukaan rekening bank, atau pengajuan pinjaman daring atas nama kita. Kasus pencurian identitas kerap sulit diselesaikan, berpotensi mencemarkan reputasi, serta menimbulkan berbagai permasalahan dan kerugian besar.

2. Menghindari Penipuan Online

   Pelaku kejahatan siber kerap menyalahgunakan data pribadi untuk melakukan penipuan daring. Informasi tersebut dapat dimanfaatkan untuk mengakses akun media sosial, email, hingga layanan perbankan digital. Dengan menjaga kerahasiaan data pribadi, kita dapat mencegah akses tidak sah ke akun serta meminimalkan risiko penipuan, antara lain dengan membuat kata sandi yang kuat dan mengaktifkan autentikasi dua faktor.

3. Menjaga Privasi dan Keamanan

   Data pribadi memiliki keterkaitan erat dengan kehidupan kita. Informasi seperti kata sandi akun, rekam medis, atau PIN ATM merupakan aspek privasi yang seharusnya tidak dibagikan kepada pihak yang tidak dikenal. Dengan menjaga kerahasiaan data pribadi, kita dapat melindungi privasi serta keamanan diri dari potensi penyalahgunaan oleh orang lain.

4. Menghindari penyalahgunaan data oleh pihak tidak bertanggung jawab

   Pihak tertentu, termasuk perusahaan, dapat memanfaatkan data pribadi kita untuk kepentingan mereka, seperti menjualnya tanpa izin,

melakukan pelecehan, atau pencemaran nama baik. Ketika data pribadi disalahgunakan, hal ini dapat menghambat aktivitas sehari-hari kita.

5. Hak memiliki privasi data pribadi

   Setiap orang berhak mendapatkan perlindungan dan menjaga kerahasiaan data pribadinya guna menghindari risiko atau kerugian yang tidak diharapkan. Oleh karena itu, pemberian, pemanfaatan, maupun penghapusan data pribadi sepenuhnya menjadi hak individu yang bersangkutan.[58]

Untuk itu diperlukan regulasi yang kuat dalam melindungi hak individu atas data pribadinya.[59] UU PDP disusun untuk memberikan perlindungan hukum terhadap data pribadi masyarakat di era digital ini. Undang-Undang ini mengatur berbagai hal terkait pengumpulan, pengelolaan, dan penggunaan data pribadi oleh pihak ketiga. Selain itu, UU PDP juga menetapkan sanksi tegas bagi pelaku usaha yang melanggar hak privasi data pribadi konsumen. Menurut Dirjen Aplikasi dan Informatika (Aptika), Semuel Abrijani Pangerapan, data pribadi adalah bagian dari hak asasi manusia dan privasi yang diakui dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia 1948. Undang-Undang PDP bertujuan untuk mengurangi pelanggaran privasi sekaligus meningkatkan kesadaran masyarakat agar lebih menjaga data pribadi mereka.[60]

---

[58] Antara News "Apa Itu Data Pribadi Dan Kenapa Harus Dilindungi" https://www.antaranews.com/berita/4397369/apa-itu-data-pribadi-dan-kenapa-harus-dilindungi Di Akses Pada Tanggal 02 Februari Tahun 2025 Pukul 20.30

[59] Jenda Mahuli, "Perlindungan Hukum Terhadap Data Pribadi Dalam Era Digital," *AFoSJ-LAS* 3, no. 4 (2023): 188–94, https://j-las.lemkomindo.org/index.php/AFoSJ-LAS/index.

[60] Chaterine Grace Gunadi et al., "Perlindungan Hukum Atas Kebocoran Data Pribadi," *Proceeding of Conference on Law and Social Studies* 4, no. 1 (2023): 1–14.

Sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, pengaturan mengenai perlindungan data pribadi sebelumnnya diatur dalam beberapa Undang-Undang di antaranya:[61]

1. Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan atas perubahan Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

   Undang-Undang Perbankan mengatur permasalahan terkait kerahasiaan bank, dengan berlandaskan prinsip kerahasiaan, yang mewajibkan bank untuk merahasiakan segala sesuatu yang berhubungan dengan data dan informasi mengenai nasabah, baik keadaan keuangannya maupun informasi yang bersifat pribadi. Dalam undang-undang perbankan nomor 10 tahun 1998 hak privasi dilindungi dengan diaturnya perihal bank. Pasal 1 ayat (28) UU Perbankan menyebutkan definisi dari Rahasia bank meliputi segala keterangan tentang penyimpan dan simpananya. Pasal 40 Ayat (1) UU Perbankan menyebutkan bahwa Bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal-hal tertentu yang dibolehkan. Dalam hal tersebut, dapat dketahui bahwa perlindungan nasabah bank juga tak hanya terkait dengan data keuangan, namun jga tak terbatas pada data privasi yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data privasi lain diluar data keuangan.[62]

2. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

---

[61] Erlina Maria Christin Sinaga, *''Formulasi Legislasi Perlindungan Data Pribad'''*, *Jurnal RechtVinding*, 9.2 (2020), pp. 237–56.

[62] Wahyudi Djafar, "Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap Urgensi Dan Kebutuhan Pembaruan," *Seminar Hukum Dalam Era Analisis Big Data*, no. 2013 (2019): 1–14, http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Pasal 18 ayat (1) diatur kewajiban penyelenggara telekomunikasi untuk mencatat atau merekam secara rinci pemakaian jasa telekomunikasi. Sedangkan pasal 22 telah menentukan tentang larangan akses ke jaringan dan/atau jasa komunikasi atau telekomunikasi secara tanpa hak,tidak sah, atau dengan manipulasi. Selain itu, letak perlindungan data pribadi dalam UU Telokomunikasi terdapat pada larangan terhadap penyadapan informasi yang disalurkan melalui jaringan telekomunikasi juga telah ditetapkan pada Pasal 40 UU Telekomunikasi. Sedangkan pasal 42 ayat (1) UU Telekomunikasi mewajibkan penyelenggara jasa telekomunikasi melalui jaringan dan/atau jasa telekomunikasi lain yang diselenggarakannya.[63]

3. Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia

Dalam Pasal 29 Ayat (1) Undang-Undang HAM 1999 diakui bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya. Hak privasi menjadi sangat penting dengan perkembangan masyarakat modern, dimana pertukaran serta perpindahan informasi dapat terjadi dengan cepat dan mudah. Tidak menutup kemungkinan terjadi pepindahan data ataupun informasi pribadi seseorang secara tidak sah dan dipergunakan tnpa seizin pemiliknya. Pasal 14 ayat (2) menyatakan bahwa setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia.

[63] Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Pasal 32 Undang-Undang HAM mengatur bahwa Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan. Pengaturan yang terdapat dalam pasal 14 ayat (2) serta pasal 32 Undang-Undang HAM di atas menunjukkan terdapatnya keseimbagan antara adanya hak untuk memperoleh, mencari, menyimpan sertaa menyampaikan informasi dengan hak atas diakuinya kerahasian dalam komunikasi, terutama yang berhubungan dengan informasi seseorang. Dapat disimpulkan bahwa jaminan diakuinya hak privasi seseorang dalam pasal 32 undang-undang HAM terutama adalah dalam perlindungan terhadap informasi serta data pribadi seseorang.[64]

4. Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Undang-Undang keterbukaan informasi publik, pada Pasal 1 ayat (1) mengatur definisi informasi bahwa:

> "Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik".

Selain itu, definisi informasi publik dapat dikeahui sebagai informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu

[64] Sinta Dewi Rosadi, "*Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional"* (Bandung: Refika Aditama, 2019)

badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik. Dari definisi di atas dapat diketahui bahwa badan publik sebagaimana yang diatur dalam undang-undang melakukan pengumpulan data dan informasi milik masyarakat yang dihimpun sedemikian rupa sesuai dengan perauran perundang-undangan yang berlaku.

Terhadap pengumpulan data tersebut juga diatur mengenai perlindungan dari data-data pribadi masyarakat. Badan publik diberi hak untuk tidak memberikan informasi publik dimana salah satunya informasi yang berkaitan dengan hak-hak pribadi. pengaturan seperti ini tentu dibuat dalam rangka menjaga perlndungan atas hak privasi, karena disamping hak untuk memeroleh informasi, hak privasi juga harus dilindungi.[65]

5. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan

Perlindungan terhadap riwayat kesehatan pasien terdapat dalam pasal 57 ayat (1) yang menyatakan bahwa Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. Selanjutnya pada pasal 57 ayat (2), diatur mengenai ketetntuan pengecualian atas rahasia kondisi kesehatan pribadi yang tidak berlaku dalam hal; a. perintah undang-undang; b.

[65] Undang-Undang Nomor 4 Tahun 2008 Tentang Keterbukaan Informasi Publik

perintah pengadilan; c.izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut.

Meskipun terdapat pengakuan hak pasien untuk mendapatkan perlindungan atas data pribadinya yang berupa riwayat kesehatan namun perlindungan data pribadi pasien tidak secara penuh diatur dalam undang-undang ini. Dalam undang-undang kesehatan tidak terdapat pengaturan sanksi ataupun hukuman bagi pelanggaran privasi yang dilakukan atas riwayat kesehatan pasien. Tidak terdapat pengaturan sanksi administrasi, perdata atau pidana, baik atas akses secara tidak sah maupun penyalahgunaan dari data pribadi pasien oleh pihak yang tidak berhak.[66]

6. Undang -Undang Nomor 24 Tahun 2013 Tentang Perubahan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

Pasal 1 ayat (22) UU Administrasi Pendudukan mendefinisikan bahwa Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiannya. Pasal 84 menentukan data pribadi penduduk yang harus dilindungi yaitu: a) keterangan tentang cacat fisik dan/atau mental; b) sidik jari; c) iris mata; d) tanda tangan dan e) elemen dta lainnya yang merupakan aib seseorang.

Selanjutnya, pada Pasal 85 UU Administrasi Kependudukan menemukan bahwa negara memiliki kewajiban untuk menyimpan dan memberikan perlindungan atas data pribadi penduduk tersebut. Data penduduk yang tersimpan di dalam database kependudukan dapat

[66] Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan

dimanfaatkan untuk berbagai kepentingan seperti dalam menganalisis dan erumuskan kebijakan kependudukan, menganalisis dan merumuskan perencanaan pembangunan, pengkajian ilmu pengetahuan.[67]

7. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sistem elektronik menurut pasal 1 ayat 5 Undang-Undang ITE 2008 adalah serakaian perangkat prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan atau menyebarkan informasi elektronik. Sedangkan yang dimaksud dengan informasi elektronik adalah sekumpulan data elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik *(electronic mail)*, telegram, *telex*, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Transaksi elektronik sebagaiamana yang dimaksdu dalam UU ITE adalah perbuatan hukum yang dilakuakan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya. UU ITE mengakui mengenai perlindungan data pribadi sebagai salah satu bagian dari hak privasi.

   Penjelasan pasal 26 ayat (1) UU ITE menegaskan bahwa:

[67] Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

> "Dalam pemanfaatan tekknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:
> a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
> b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
> c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Undang-Undang Nomor 19 Tahun 2016 rntang informasi dan transaksi elektronik menekankan pada persetujuan pemilik data dalam hal penggunaan data pribadi. pasal 26 ayat (1) Undang-undang Nomor 19 Tahun 2016 tentang informsi dan transaksi elektronik mengatur bahwa penggunaan setiap informasi yang berkaitan dengan data pribadi seseorang harus dilakukan oleh orang yang bersangkutan, dalam hal ini adalah pemilik data pribadi. selanjutnya, pada pasal 26 ayat (2) Undang-Undang Nomor 29 Tahun 2016 tentang informasi dn transaksi elektronik membuka peluang untuk mengajukan gugatan bagi setiap orang yang dilanggar haknya mengenai persetujuan pengguna data pribadi.

Pasal 26 ayat (3) dan (4) Undang-Undang Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik, telahh diatur suatu hak untuk penghapusan informasi yang juga disebut dengan hak untuk diupakan *(right to be forgotten).* Berikut bunyi pasalnya:

> "(3) Setiap Penyelenggara Sistem Elektronik Wajib Menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
> (4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yng sudah tidak relevan esuai dengan ketentuan peraturan perundang-undangan.

(5) Ketentuan Mengenai Tata Cara Penghapusan Informasi Elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah."

Selain itu, Undang-undang Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik juga mengatur mengenai larangan dalam perbuatan intersepsi atau penyadapn terhadap dan atau informasi elektronik. Sedangkan yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau jasa dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetic atau radio frekuensi.[68]

8. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem Elektronik (PSE) merupakan aturan turunan dari Undang-Undang informasi dan transaksi elektronik, yang mengatur lebih lanjut penyelenggara sistem dan transaksi elektronik. Dalam peraturan pemerintah ini, yang dimaksud dengan penyelenggara sistem elektronik adalah setiap orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem

[68] Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undng Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Elektronik. Dalam melakukan pemrosesan data wajib melaksanakan prinsip pelindungan Data Pribadi yang terdapat pada pasal 14 ayat (1) meliputi;

a. Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi;
b. Pemrosesan data pribadi dilakukan sesuai dengan tujuannya;
c. Pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi;
d. Pemrosesan data pribadi secara akurat, lengkap, tidak menyesatkan, mutakhir dapat dipertanggungjawabkan dan memperhatikan tujuan pemrosesan data pribadi;
e. Pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan data pribadi;
f. Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan
g. Pemrosesan data pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

Pada dasarnya pemrosesan data pribadi harus memenuhi ketentuan adanya persetujuan yang sah dari pemilik data tersebut. Maksudnya adalah persetujuan yang disampaikan secara eksplisit, tidak secara tersembunyi atau atas dasar kekhilafan, kelalaian, atau paksaan. Pasal 14 ayat (4) menjelaskan bahwa pemrosesan data pribadi harus memenuhi ketentuan yang diperlukan untuk:

a. Pemenuhan kewajiban perjanjian dalam hal pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan pemilik Data Pribadi pada saat akan melakukan perjanjian;
b. Pemenuhan kewajiban hukum dari pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
c. Pemenuhan pelindungan kepentingan yang sah (vital interest) pemilik Data Pribadi;
d. Pelaksanaan kewenangan pengendali data pribadi berdasarkan ketentuan peraturan perundang-undangan;
e. Pemenuhan kewajiban pengendali Data Pribadi dalam peJayanan publik untuk kepentingan umum; dan/atu
f. Pemenuhan kepentingan yang sah lainnya dari pengendali Data Pribadi dan/atau pemilik Data Pribadi.

Apabila terjadi kegagalan dalam perlindungan data pribadi yang di kelola Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut.

Pasal 15 Peraturan Pemerintah No. 71 Tahun 2019 secara rinci membahas hak dan kewajiban penyelenggara sistem elektronik yang memperoleh dan/atau memproses data pribadi mengenai penghapusan Informasi Elektronik dan/atau Dokumen Elektronik, termasuk data prbadi yang tidak relevan yang berada dibawah kendalinya atas permintaan orang yang bersangkutan melalui;

a. Penghapusan (*right to erasure*); dan
b. Pengeluaran dari daftar mesin pencari (*right tode listing*).

Dalam ketentuan Pasal 16 Peraturan Pemerintah Nomor 71 Tahun 2019 Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang dilakukan sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf a terdiri atas Data Pribadi yang:

a. Diperoleh dan diproses tanpa persetujuan pemilik Data Pribadi;
b. Telah ditarik persetujuannya oleh pemilik Data Pribadi;
c. Diperoleh dan diproses dengan cara melawan hukum;
d. Sudah tidak sesuai lagi dengan tujuan perolehan berdasarkan perjanjian dan/atau ketentuan peraturan perundang-undangan;
e. Penggunaannya telah melampaui waktu sesuai dengan perjanjian dan/atau ketentuan peraturan perundang-undangan; dan/atau
f. Ditampilkan oleh Penyelenggara Sistem Elektronik yang mengakibatkan kerugian bagi pemilik data pribadi.

Pasal 29 juga mengatur mengenai kewajiban Penyelenggara Sistem Elektronik wajib menyampaikan informasi kepada Pengguna Sistem Elektronik paling sedikit mengenai:

a. identitas Penyelenggara Sistem Elektronik
b. objek yang ditransaksikan;
c. kelaikan atau keamanan Sistem Elektronik;
d. tata cara penggunaan perangkat;
e. syarat kontrak;
f. prosedur mencapai kesepakatan;
g. jaminan privasi dan/atau pelindungan Data Pribadi; dan
h. nomor telepon pusat pengaduan.[69]

9. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Eektronik.

Pemenkominfo 20/2016 merupakan pengaturan lebih lanjut dari UU ITE yang mengatur khusunya terkait perlindungan data pribadi. privasi dalam peraturan menteri ini di nyatakan sebagai berikut:

"Kebebasan pemilik data pribadi untuk menyatakan atau tidak menyatakan rahasia data pribadinya, kecuali ditentukan lain sesuai dengan peraturan perundang-undangan"

Pasal 3 Peraturan menteri ini telah menyebutkan mengenai perlindungan data pribadi yang dilakukan pada proses a. perolehan dan pengumpulan; b). pengolahan dan penganalisisan; c. penyimpanan; d. penampilan,

[69] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik

pengumuman, pengiriman, penyebarluasan, dan/atau pembukan akses; dan e. pemusnahan.

Penyelenggara sistem elektronik dalam prosesnya wajib menyediakan formulir pesetujuan dalam bahasa indonesia untuk meminta persetujuan dari pemilik data pribadi diatur dalam Pasal 6. Permenkominfo 20/2016 dalam pasal 2 ayat (2) mengatur mengenai asas dalam perlindungan data yang baik yaitu:

a. Penghormatan terhadap Data Pribadi sebagai privasi;
b. Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan;
c. berdasarkan Persetujuan;
d. relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
e. kelayakan Sistem Elektronik yang digunakan;
f. iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi;
g. ketersediaan aturan internal pengelolaan perlindungan Data Pribadi;
h. tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna;
i. kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi; dan

j. keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.

Peraturan menteri nomor 20 tahun 2016 memuat beberapa pihak yang berperan dalam melindungi data pribadi. Pihak-piah tersebut antara lain:

a. Penyelenggara Sistem Elektronik, adalah adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendirisendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
b. Pengguna Sistem Elektronik, adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik.
c. Pemilik Data Pribadi, adalah individu yang padanya melekat Data Perseorangan Tertentu. Data Perseorangan Tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.
d. Menteri, adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

e. Direktur Jenderal, adalah direktur jenderal yang tugas dan fungsinya di bidang aplikasi informatika.

Permenkominfo juga mengatur mngenai hak dan kewajiban masing-masing pihak. Dalam hal pemilik data pribadi diatur pada pasal 26 yaitu:

a. Pemilik Data Pribadi berhak atas kerahasiaan Data Pribadinya;
b. mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri;
c. mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
d. mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan
e. meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.

Sedangkan kewajiban pengguna sistem elektronik diatur pada pasal 27 sebagai berikut:

a. menjaga kerahasiaan Data Pribadi yang diperoleh, dikumpulkan, diolah, dan dianalisisnya;
b. menggunakan Data Pribadi sesuai dengan kebutuhan Pengguna saja;
c. melindungi Data Pribadi beserta dokumen yang memuat Data Pribadi tersebut dari tindakan penyalahgunaan; dan
d. bertanggung jawab atas Data Pribadi yang terdapat dalam penguasaannya, baik penguasaan secara organisasi yang menjadi kewenangannya maupun perorangan, jika terjadi tindakan penyalahgunaan.

Terkait dengan kewajiban dari Penyelenggara Sistem Elektronik diatur pada pasal 28 Permenkominfo sebagai berikut:

a. melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan;
b. menajga kebenaran, keabsahan, kerahasiann, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi;
c. memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut:
    1) harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi;

2) dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya:

3) .harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut;

d. memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan;

e. menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya;

f. memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapatdigunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi;

g. memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;

h. memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya

yang secara khusus mengatur dimasing-masing Instansi Pengawas dan Pengatur Sektor untuk itu; dan

i. menyediakan narahubung (contact person) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pengelolaan Data Pribadinya.

Penyelenggara Sistem Elektronik wajib membuat kebijakan untuk mencegah terjadinya kegagalan dalam melindungi data pribadi. Kebijakan ini disusun dengan memperhatikan faktor-faktor seperti penerapan teknologi, ketersediaan sumber daya manusia, metode yang digunakan, biaya, dan juga harus sesuai dengan peraturan menteri serta undang-undang yang relevan.

Sedangkan dalam pasal 15 tentang hal penyimpanan data pribadi, informasi yang disimpan dalam sistem Elektronik wajib berupa data yang telah diverifikasi keakuratannya. Data tersebur harus diamankan dalam bentuk data terenkripsi. Penyimpanan data harus sesuai dengan peraturan perundang-undangan yang mengatur kewajiban erkait durasi penyimpnan data oleh instansi tertentu. Jika tidak ada aturan khusu yang mengatur, data pribadi wajib disimpan selama minimal 5 tahun.

Permenkominfo 20/2016 juga mengatur mekanisme penyelesaian sengketa terkait perlindungan data pribadi. Jika terjadi kegagalan dalam melindungi data pribadi, pihak yang dirugikan dapat mengajukan pengaduan kepada menteri. Pengaduan ini bertujuan untuk menyelesaikan masalah melalui musyawarah atau alternatif penyelesaian lainnya, adapun pengajuan pengaduan ini diatur dalam pasal 29 ayat (3) Permenkominfo 20/2016 yaitu:

a. Tidak dilakukannya pemberitahuan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi oleh Penyelenggara Sistem

Elektronik kepada Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lainnya yang terkait dengan Data Pribadi tersebut, baik yang berpotensi maupun tidak berpotensi menimbulkan kerugian; atau

b. Telah terjadinya kerugian bagi Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lainnya yang terkait dengan kegagalan perlindungan rahasia Data Pribadi tersebut, meskipun telah dilakukan pemberitahuan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi namun waktu pemberitahuannya yang terlambat.

Kewenangan penyelesaian sengketa data pribadi diserahkan oleh Menteri kepada Direktur Jenderal. Direktur Jenderal memiliki wewenang untuk membentuk panel khusus guna menangani sengketa data pribadi. Pengaduan harus diajukan paling lambat 30 hari kerja sejak pihak yang dirugikan mengetahui kerugian akibat kegagalan perlindungan data pribadi atau tidak menerima pemberitahuan mengenai kegagalan tersebut. Jika penyelesaian melalui musyawarah atau metode alternatif lainnya tidak berhasil, pemilik data pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan gugatan perdata terkait kegagalan dalam melindungi kerahasiaan data pribadi.

B. Kebocoran Data Pribadi di Era Digital

Data pribadi yang disimpan dalam sistem elektronik menjadi jejak digital yang tidak dapat dihapus, sehingga diperlukan perlindungan untuk mencegah kebocoran dan penyalahgunaan informasi tersebut. Namun, dalam praktiknya, sering terjadi kesalahan yang tidak disengaja karena sistem proteksi keamanan yang kurang memadai, membuka peluang bagi pihak yang tidak bertanggung jawab untuk mencuri, memperjualbelikan, atau memanfaatkan data pribadi untuk

tujuan ilegal.[70] Data pribadi mencakup informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Secara umum, data pribadi terbagi menjadi dua kategori:

1. Data Pribadi Umum Merupakan informasi dasar tentang seseorang, seperti:

a) Nama lengkap.
b) Alamat (domisili, tempat tinggal).
c) Tanggal dan tempat lahir.
d) Nomor telepon atau email.
e) Jenis kelamin.
f) Kewarganegaraan.
g) Status perkawinan.
h) Pekerjaan.
i) Pendidikan.

2. Data Pribadi Sensitif Merupakan informasi yang lebih bersifat rahasia dan memiliki potensi risiko lebih besar jika disalahgunakan, seperti:

a) Nomor identitas (KTP, paspor, SIM, NPWP).
b) Informasi keuangan (nomor rekening, kartu kredit, riwayat transaksi)
c) Data biometrik (sidik jari, retina mata, pengenalan wajah, suara).
d) Riwayat kesehatan (rekam medis, riwayat penyakit, hasil tes medis).
e) Keyakinan atau agama.
f) Pandangan politik.
g) Data lokasi (riwayat perjalanan, koordinat GPS).

[70] Aditama Candra Kusuma and Ayu Diah Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI : Jurnal Hukum* 5, no. 1 (2022): 46–63, https://doi.org/10.36441/supremasi.v5i1.721.

h) Informasi forensik atau genetika.[71]

Masalah Kebocoran Data yang sering terjadi di Indonesia yaitu:

1. Kebocoran data melalui *phishing*

   Kasus penyalahgunaan data pribadi ini tidak selalu dilakukan oleh peretas secara langsung. Berbeda dengan kebocoran data, phishing justru melibatkan tindakan dari pemilik data itu sendiri. Seorang pengguna menerima pesan melalui email, SMS, atau WhatsApp yang tampak berasal dari lembaga resmi, seperti institusi keuangan tempat ia menyimpan dana. Isi pesan tersebut sering kali meyakinkan, misalnya pengumuman sebagai pemenang hadiah undian. Karena merasa pesan itu valid, korban tanpa ragu membagikan informasi rekening dan data pribadinya. Tanpa disadari, ia telah menyerahkan informasi sensitif kepada penipu, yang kemudian menyalahgunakannya untuk mengakses rekening banknya. Selain itu, pesan semacam ini sering menyertakan tautan yang mengarahkan korban ke sebuah situs. Saat tautan diklik, ternyata situs tersebut merupakan alat bagi pelaku untuk mencuri data pribadi dari perangkat korban.[72]

2. Peretasan dan Spamming di Media Sosial

   Spamming di media sosial terjadi ketika seseorang membuat akun palsu atau menambahkan banyak teman dan pengikut. Dengan akun palsu

[71] Umsu "Jenis-Jenis Data Pribadi Menurut UU Perlindungan Data Pribadi" https://fahum.umsu.ac.id/info/jenis-jenis-data-pribadi-menurut-uu-perlindungan-data-pribadi/ Di Akses Pada Tanggal 23 Februari Tahun 2025 Pukul 20.41

[72] Vida Digital Identity "Penyalahgunaan Data Pribadi: Contoh Kasus Dan Kerugiannya" https://vida.id/id/blog/penyalahgunaan-data-Pribadi Di Akses Pada Tanggal 23 Februari Tahun 2025 Pukul 22.21

ini, pelaku dapat mengirimkan spam dalam jumlah besar, termasuk pesan berisi tautan berbahaya yang dapat menyebarkan malware-perangkat lunak berbahaya yang menyerang sistem dan perangkat pengguna. Malware merupakan istilah umum untuk berbagai jenis virus yang dapat menyusup ke komputer, ponsel, atau tablet guna mencuri data serta informasi pribadi. Selain itu, peretasan juga bisa digunakan untuk menyebarkan konten menyesatkan atau berita bohong (hoaks).

3. *Defacing* (Pembajakan Situs Web)

   Defacing adalah metode kejahatan siber yang melibatkan perubahan tampilan situs web sesuai keinginan pelaku. Jenis serangan ini sering digunakan untuk menampilkan tulisan provokatif atau gambar humor. Kejahatan ini menjadi salah satu bentuk serangan siber yang populer karena dampaknya langsung terlihat oleh publik.

4. Virus dan Trojan

   Virus komputer adalah program yang mampu mereplikasi dirinya sendiri dan menyebar dengan cara menyisipkan salinan ke dalam program atau dokumen lain. Sementara itu, Trojan merupakan jenis perangkat lunak berbahaya (malicious software) yang dapat merusak sistem atau jaringan. Tujuan utama Trojan adalah mengumpulkan informasi dari target, seperti kata sandi, aktivitas pengguna yang terekam dalam sistem log, serta data penting lainnya. Selain itu, Trojan juga memungkinkan

pelaku untuk mengendalikan target dengan mendapatkan hak akses ke sistem yang diserang.[73]

Adapun beberapa kasus kebocoran data yang terjadi dari tahun ke tahun di Indonesia

1. Kebocoran Data Tokopedia (2020)

   Seorang peretas internasional dengan nama samaran "*Why So Dank"* berhasil membobol tokopedia pada tanggal 17 april 2020. Berita peretasan ini tersebar di media sosial twitter, dengan akun @underthebreach yang mengungkapkan bahwa 15 juta akun pengguna tokopedia telah diretas. Namun setelah penyelidikan lebih lanjut jumlah akun yang diretas meningkat menjadi 91 juta akun pengguna serta 7 juta akun merchant. Pakar keamanan siber, Pratama Persadha menjelaskan bahwa peretas tersebut pertama kali mengunggah hasil retasannya di situs *dark web* bernama Raid Forums. Data pribadi seperti nama lengkap, tempat dan tanggal lahir, nomor telepon, jenis kelamin dan email dijual seharga US$5000 atau sekitar Rp 74 juta.[74] Kebocoran data tokopedia menandakan pentingnya peningkatan dalam keamanan siber, terutama di era digital yang terus berkembang. Kebocoran data ini juga menjadi peringatan bagi

[73] Skripsi Sriwulan "Tinjauan Yuridis Tindak Pidana Cyber Crie Di Indonesia" (Fakultas Syariah Institut Agama Islam Negeri Palopo 2023) http://repository.iainpalopo.ac.id/id/eprint/7312/

[74] Muhammad Fathur, "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data)," *Procceding: Call for Paper 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 2020, 43–60, http://jurnal.unissula.ac.id/index.php/PH/article/view/1476.

perusahaan untuk lebih serius dalam melindungi data pengguna serta mematuhi peraturan yang ada demi mencegah kebcoran data.

Peraturan Pemerintah nomor 71/2019 dalam Pasal 14 ayat (1) huruf e mengatur kewajiban PSE untuk menerapkan prinsip perlindungan data pribadi dalam proses pengelolaannya. Pasal ini menegaskan bahwa pemrosesan data pribadi harus dilakukan dengan menjaga keamanan data tersebut dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta perubahan atau perusakan yang tidak semestinya. Kebocoran data pribadi Tokopedia menunjukkan bahwa perusahaan gagal menerapkan prinsip perlindungan data pribadi dari akses dan pengungkapan yang tidak sah peretas berhasil mengakses data pribadi konsumen, yang kemudian dijual secara ilegal, sehingga data tersebut terungkap kepada pihak lain tanpa izin.

Pasal 14 ayat (5) PP 71/2019 mengatur kewajiban PSE untuk memberikan informasi jika terjadi kegagalan dalam melindungi data pribadi yang mereka kelola. Ketentuan ini juga menegaskan bahwa pemberitahuan tersebut harus disampaikan kepada konsumen. Wahyudi Djafar dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) menekankan bahwa Tokopedia sebagai PSE wajib memberitahukan konsumen terkait kegagalan dalam perlindungan data pribadi mereka.

Pasal 100 PP 71/2019 mengatur ketentuan yang apabila dilanggar dapat diberikan sanksi administratif. Pelanggaran terhadap Pasal 14 ayat (1) dan ayat (5), yang diduga dilakukan oleh Tokopedia, dapat

mengakibatkan perusahaan tersebut dikenakan sanksi administratif sebagaimana diatur dalam Pasal 100 PP 71/2019. Berdasarkan Pasal 100 ayat 2) sanksi administratif yang dapat dijatuhkan meliputi: a) teguran tertulis; b) denda administratif; c) penghentian sementara; d) pemutusan akses; dan/atau e) penghapusan dari daftar. Tokopedia dikenai denda administrasi sebesar 100.000.000.000.00 (Seratus Miliar Rupiah) dan penghentian kegiatan sementara sistem penyelenggara elektronik tokopedia. Adapun Pasal 100 ayat (5) menegaskan bahwa pemberian sanksi administratif tidak menghapus tanggung jawab pidana dan perdata.[75]

Untuk mencegah terjadinya kebocoran data yang berulang Tokopedia menyarankan kepada penggunanya untuk mengganti kata sandi akun dan mengaktifkan one time password (OTP) yang hanya dapat diakses oleh pemilik akun. Selain itu, disarankan untuk menggunakan kata sandi yang unik dan berbeda pada setiap akun media sosial maupun platform marketplace.

2. Kebocoran Data Kredit Plus (2020)

Kasus kebocoran data yang di alami kreditPlus pada agustus 2020 melibatkan informasi pribadi sekitar 890.000 data nasabah yang diduga telah dijual di forum online seperti Raid Forums. Kebocoran ini pertama kali dilaporkan oleh firma keamanan siber asal amerika serikat yaitu Cyble. Data yang bocor meliputi informasi sensitif seperti nama, alamat

[75] Putusan Nomor 235/Pdt.G/2020/PN.Jkt.Pst,"Tokopedia & Komunitas Konsumen Indonesia" Pengadilan Negeri Jakarta Pusat, 21 Oktober 2020

email, kata sandi, alamat rumah, nomor telepon, data pekerjaan dan informasi kartu keluarga. Lembaga riset siber indonesia CISSRec (*Communication & Information System Security Research Center*), melaporkan bahwa data berukuran 78 MB ini telah beredar di situs Raid Forums sejak 16 juli 2020.[76]

Kasus ini menungkapkan sistem keamanan kredit plus dianggap memiliki celah yang mempermudah akses bagi pihak yang tidak bertanggungjawab. ketidakmampuan untuk mendeteksi kebocoran sejak awal menunjukkan adanya kekurangan dalam pengawasan dan pengelolaan keamanan. KreditPlus segera mengambil langkah dengan menggunakan konsultan cyber security eksternal yang memiliki keahlian untuk melakukan investigasi menyeluruh terkait dugaan kebocoran data pelanggan. Kreditplus juga telah menerapkan prelindungan data finansial konsumen melalui fitur OTP yang hanya dapat diakses oleh pemilik akun. Mereka terus mengigatkan konsumen untuk menjaga kerhasiaan OTP dan kata sandi, termasuk tidak memberikannya kepada pihak lain, bahkan jika mengatasnamakan kredit plus. Selain itu, edukasi rutin telah dilakukan untuk meningkatkan kesadaran konsumen terkait keamanan data, seperti pentingnya mengganti kata sandi secara berkala.

3. Peretasan Terhadap Website BPJS Kesehatan (2021)

Situs badan penyelenggara jaminan sosial (BPJS) kesehatan mengalami peretasan, ini mengakibatkan kebocoran data pribadi dari 279

[76] Ditjen Aptika "Ratusan Ribu Data Bocor, Kominfo Minta Kreditplus Buka Suara" https://aptika.kominfo.go.id/2020/08/ratusan-ribu-data-bocor-kominfo-minta-kreditplus-buka-suara/ Di akses pada tanggal 25 september 2024, Pukul 12.49

juta warga negara Indonesia. Data tersebut dijual di forum online Raid Forums oleh pengguna yang bernama *"Kotz"*. Database yang mencakup informsi sensitif seperti nama, alamat, email, nomor telepon dan status pembayaran dijual dengan harga 0.15 bitcoin sekita Rp 84,4 juta. Hasil pemeriksaan oleh oleh kementrian komunikasi dan informasi (kominfo) serta otoritas terkait lainnya memastikan bahwa data tersebut sama yang dikelola oleh BPJS.[77]

Kebocoran data BPJS Kesehatan disebabkan oleh beberapa faktor yaitu Pertama, kurangnya kesadaran mengenai pentingnya keamanan data menjadi penyebab utama; jika pegawai BPJS Kesehatan tidak memahami betapa pentingnya menjaga kerahasiaan data pribadi peserta, risiko kebocoran data akan meningkat. Kedua, kekurangan investasi dalam sistem keamanan juga berkontribusi. Tanpa alokasi dana yang memadai untuk memperkuat sistem keamanan, kemungkinan kebocoran data menjadi lebih tinggi. Ketiga, minimnya pelatihan dan pemahaman terkait perlindungan data pribadi. Selain itu, adanya celah dalam sistem, seperti perangkat lunak yang tidak diperbarui, memungkinkan akses tidak sah ke server database meningkatkan risiko kebocoran data.

Saat itu indonesia belum memiliki undang-undang perlindungan data pribadi yang komprehensif. Hal ini meyebabkan kurangnya tanggung jawab dari instansi pemerintah dan swasta dalam melindungi data yang mereka kelola. Dengan disahkannya undang-undang perlindungan data

[77]Exabytes Indonesia "14 Kasus Cybercrime di Indonesia yang Menggemparkan Warganet" https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/ Di Akses Pada Tanggal 15 Agustus 2024 Pukul 23.20

pribadi ini pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan pelaksanaan prinsip perlindungan data pribadi.

4. Kebocoran Data Kartu SIM Prabayar (2022)

Bjorka kembali beraksi pada 31 Agustus 2022 dengan mengunggah sampel data di forum online Breached Forums, serta menawarkan untuk menjual sekitar 1,3 miliar data registrasi kartu SIM prabayar di Indonesia. Data tersebut mencakup nomor ponsel, nomor induk kependudukan (NIK) pelanggan, informasi mengenai operator seluler yang digunakan, dan tanggal registrasi kartu SIM. Bjorka mengklaim bahwa data yang dimilikinya berukuran 18 GB dalam kondisi terkomprsi dan 87 GB tanpa kompresi, dengan harga jual sebesar 50.000 dolar AS atau sekitar Rp 743 juta.[78]

Kementerian Komunikasi dan Informatika (Kominfo) bersama pihak terkait lainnya, seperti Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil), membantah bahwa kebocoran data tersebut berasal dari sistem mereka. Namun, data yang bocor memiliki kemiripan format dengan data yang dikumpulkan melalui proses registrasi kartu SIM via SMS, yang menunjukkan adanya potensi celah keamanan dalam sistem tersebut. Kebocoran ini membuka peluang penyalahgunaan data oleh pihak ketiga, termasuk spam, penipuan, dan phishing.

[78] CNN Indonesia "10 Kasus Kebocoran Data 2022: Brojka Rmai-Ramai Bantai" https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah Di Akses Pada Tanggal 16 Agustus Pukul 01.00

Pakar keamanan siber menyoroti kurangnya perlindungan data yang memadai, seperti minimnya penggunaan enkripsi dan autentikasi yang lemah dalam sistem SMS Gateway, sebagai salah satu faktor utama terjadinya kebocoran ini. Ahli teknologi informasi menekankan pentingnya penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) untuk memastikan bahwa penyelengara sistem elektronik memiliki kewajiban melindungi data pengguna. Tanpa regulasi yang ketat tidak ada jaminan akuntabilitas bagi pengelola data tersebut. Kominfo telah berkoordinasi dengan berbagai lembaga untuk menyelidiki insiden ini serta memperkuat sistem keamanan guna mencegah kebocoran serupa di masa mendatang. Pelanggaran kebocoran data pribadi pengguna SIM Card dapat dikenakan sanksi pidana berdasarkan undang-undang perlindungan data pribadi (PDP) dan undang-undang ITE.

5. Data nasabah Bank Syariah Indonesia (2023)

Pada 8 mei 2023, BSI mengalami gangguan layanan yang berlangsung lama, ini menyebabkan nasabah tidak bisa mengakses layanan mobile bangking, ATM dan teller. Awalnya pihak bank mengatakan bahwa ganggan tersebut disebabkan oleh pemeliharaan sistem. Namun setelah penyelidikan lebih lanjut, terungkap bahwa BSI menjadi target serangan ransomware yang menyebabkan pencurian data dalam jumlah besar. Kelompok hacker LockBit mengaku berhasil mencuri sekitar 1,5 terabyte data dari BSI yang mencakup informasi pribadi lebih dari 15 juta nasabah dan karyawan. Data yang di curi

meliputi nama, alamat, nomor rekening, saldo serta dokumen keuangan dan hukum. Serangan ini memicu kehawatiran serius terkait keamanan data nasabah dan potensi penyalahgunan informasi tersebut.[79]

Kebocoran data ini berisiko merusak kepercayaan terhadap nasabah, kebocoran ini bisa berdampak buruk pada loyalitas nasabah karena menurunnya kepercayaan terhadap keamanan bank. Adapun kerugian yang di alami nasabah akibat kebocoran data bank syariah Indonesia yaitu:

a) Informasi yang bocor, seprti identitas, nomor rekening atau data kontak, dapat digunakan untuk melakukan penipuan, pencurian identitas, atau tindakan kriminal lainnya.
b) Nasabah juga berisiko mengalami pencurian dana melalui transaksi tidak sah, terutma jikat data yang bocor mencakup informasi yang sensitif seperti PIN atau kartu kredit/debit.
c) Kebocoran data sering kali diikuti oleh gangguan operasional, yang dapat menyebabkan nasabah tidak dapat mengakses layanan perbankan, seperti penarikan, transfer, atau pembayaran tagihan.
d) Pihak yang mengakses data dapat mengancan untuk menyebarkan informasi sensitif jika tebusan tidak dibayarkan oleh nasbah atau pihak terkait.

Bank syariah indonesia, hingga kini belum mengakui adanya kebocoran data, juga enggan memberikan pemberitahuan tertulis kepada

[79] BeritaSatu.com *"Deretan Kasus Kebocoran Data yang Pernah Terjadi di Indonesia Selama 2023"* https://www.beritasatu.com/ototekno/2784168/deretan-kasus-kebocoran-data-yang-pernah-terjadi-di-indonesia-selama-2023 Di Akses Pada Tanggal 16 Agustus Pukul 01.37

pemilik data pribadi terkait serangan siber yang mengakibatkan peretasan data nasabah. Pakar keamanan siber Alfons Tanujaya menjelaskan bahwa jika gangguan bank berlangsung selama lebih dari empat jam, kemungkinan besar disebabkan oleh serangan ransomware pada sistem inti. Meskipun banyak media berupaya mendapatkan informasi lebih lanjut tentang serangan ransomware ini, BSI tidak memberikan tanggapan yang memadai. Kejadian ini menegaskan pentingnya memperkuat ketahanan terhadap serangan siber dalam layanan perbankan digital. Transformasi digital di sektor perbankan harus diserat kesiapan infrastruktur teknologi informasi yang mampu menjaga kepercayaan dan keamanan layanan.

Kasus kebocoran data seperti yang di alami oleh tokopedia, kredit plus, BPJS kesehatan, kartu SIM prabayar dan bank syariah indonesia, menunjukkan kurangnya kepatuhan terhadap standar keamanan data seperti penerapan enkripsi, autentifikasi, pengawasan ketat oleh lembaga serta kurangnya pembaharuan pada sistem keamanan perangkat lunak. Adapun faktor utama yang menjadi penyebab terjadinya kebocoran data yaitu Pertama *Human Eror*, kebocoran data juga dapat berasal dari kesalahan manusia sendiri. Seringkali seseorang tanpa sadar membagikan informasi pribadinya dengan mudah seperti di situs tidak resmi, media sosial, atau aplikasi dan lain sebagainya. Selain itu *human eror* juga dapat terjadi pada pihak pengembangan aplikasi atau perangkat, seperi kesalahan dalam pengiriman email dan kesalahan pemograman.

Kedua *Malware (Malicious Software)* adalah perangkat lunak yang berbahaya dirancang untuk merusak atau menyusup ke dalam sistem komputer. Tindakan ini dilakukan melalui email, unduhan dari internet, atau aplikasi yang sudah terinfeksi. Malware dapat merusak sistem komputer sekaligus membuka peluang bagi pencurian informasi perusahaan. Oleh karena itu penting untuk berhati-hati saat mengakses situs web mencurigakan atau membuka email dari pengirim yang tidak dikenal, karena kedua tindakan ini sering digunakan untuk menyebarkan malware yang dapat melemahkan keamanan dan meningkatkan resiko kebocoran data.

Ketiga *Social Engineering* atau manipulasi sosial adalah tindakan di mana pelaku memanipulasi psikologis target untuk memperoleh informasi yang diinginkan. Dalam kasus kebocoran data online, pelaku sering berpura-pura sebagai orang yang dikenal atau perwakilan dari lembaga yang dipercaya. Mereka meminta target mengunduh lampiran, atau memberikan informasi pribadi melalui berbagai platform. media yang paling sering digunakan meliputi SMS, Whatsapp, Telegram, Email dan panggilan telepon.[80]

Terkait dengan beberapa kasus kebocoran data yang terjadi, Undang-Undang PDP belum disahkan dan ada juga kasus kebocoran data yang terjadi pada masa transisi Undang-Undang PDP. Sebelumnya pengaturan mengenai perlindungan data tersebar dalam beberapa undang-undang, tetapi tidak secara spesifik mengatur tentang perlindungan data pribadi. Salah satu aturan yang secara spesifik mengatur hak pemilik data adalah Undang-Undang Nomor 11

[80] DetikInet "Waspada 7 Alasan Penyebab Kebocoran Data Sering Terjadi" https://inet.detik.com/security/d-6303662/waspadai-7-alasan-penyebab-kebocoran-data-sering-terjadi. Di Akses Pada Tanggal 18 November 2024 Pukul 22.55

Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang-Undang ITE mengatur berbagai jenis kejahatan yang dilakukan melalui media digital atau internet. Namun, aturan tentang pencurian data pribadi dalam Undang-Undang Nomor 19 Tahun 2016 (UU ITE) masih terbatas. Salah satu aturannya ada di Pasal 26 Ayat 1, yang menyebutkan bahwa,

"Kecuali diatur lain dalam peraturan perundang-undangan, penggunaan informasi pribadi seseorang melalui media elektronik harus mendapatkan izin dari pemilik data tersebut." Dan Pasal 26 Ayat 2 Undang-Undang Nomor 19 Tahun 2016 (UU ITE) menyatakan bahwa, "Setiap orang yang haknya dilanggar sebagaimana dimaksud dalam Ayat 1 berhak mengajukan gugatan atas kerugian yang terjadi sesuai dengan ketentuan dalam undang-undang ini."

Undang-undang ITE juga mengatur konsep *right to be forgotten* melalui pasal 26 ayat (3), yang memberikan hak kepada pemilik data untuk meminta penyelenggara sistem elektronik menghapus daa pribadi yang dianggap tidak relevan. Dalam Pasal 46 Ayat 2 dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur hukuman bagi pelaku pencurian data yaang menyatakan bahwa:

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 Ayat 2 dapat dipidana dengan penjara maksimal 7 tahun dan/atau denda hingga Rp700.000.000,00 (tujuh ratus juta rupiah)."

UU ITE juga secara jelas melarang akses data pribadi orang lain tanpa izin pemiliknya, karena data pribadi adalah bagian dari privasi yang harus dilindungi. Namun, UU ITE tidak mengatur tanggung jawab hukum bagi penyelenggara sistem elektronik yang gagal melindungi data pribadi korban dari kebocoran.[81]

[81] Triadi, "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital."

Kebocoran data dapat menyebabkan kerugian finansial, pencurian identitas, pelanggaran privasi serta hilangnya kepercayaan publik terhadap lembaga yang terlibat. Ketidakpastian tentang keamanan data dapat membuat publik ragu untuk mempercayakan informasi mereka kepada lembaga tersebut. Oleh karena itu, diperlukan perlindungan hukum yang memadai untuk menjaga keutuhan dan keamanan data pribadi. Dengan diberlakukannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi diharapkan dapat melindungi hak-hak dasar dan kebebasan warga negara terkait data pribadi, memperkuat perlindungan hukum terhadap data pribadi, serta memberikan kepastian hukum dalam kasus pelanggaran data pribadi. Meskipun sudah ada beberapa aturan sektoral yang secara mengatur perlindungan data pribadi, aturan tersebut masih belum sepenuhnya mampu memberikan perlindungan hukum yang maksimal dan kepastian hukum yang memadai.

BAB IV
PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022

A. Perlindungan Data Pribadi Berdasarkan Undang-Undang nomor 27 Tahun 2022 Tentang.

Indonesia saat ini sudah mempunyai regulasi yang khusus mengatur tentang perlindungan data pribadi. Pemerintah bersama DPR telah mengesahkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi pada 20 september 2022 dan undang-undang ini diberlakukan pada 17 Oktober 2022. UU PDP hadir sebagai upaya Indonesia untuk memenuhi standar internasional dalam perlindungan data pribadi, sejalan dengan regulasi seperti GDPR Uni Eropa. Dengan adanya aturan ini, Indonesia diharapkan lebih responsif menghadapi ancaman terhadap privasi warga serta mendorong ekosistem ekonomi digital yang lebih aman dan tepercaya.[82]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan berbagai pembaruan dalam regulasi perlindungan data di Indonesia. Berikut beberapa poin penting yang baru dibanding regulasi sebelumnya:

[82] LKPP "UU Perlindungan Data Pribadi Untuk Ekosistem Digital Yang Aman. Terpercaya, Dan Inklusif Di Bidang Pengadaan Barang/Jasa" https://www.lkpp.go.id/read/bu/uu-perlindungan-data-pribadi-untuk-ekosistem-digital-yang-aman-terpercaya-dan-inklusif-di-bidang-pengadaan-barang-jasa Di Akses Pada Tanggal 23 Februari Tahun 2025 Pukul 23.08

1. Hak Subjek Data

   Subjek data memiliki hak lebih kuat, termasuk hak untuk mengakses, mengoreksi, menghapus, dan menarik persetujuan atas pemrosesan data pribadinya.

2. Kewajiban Pengendali & Prosesor Data

   Pengendali data (pihak yang menentukan tujuan pemrosesan data) dan prosesor data (pihak yang memproses data atas nama pengendali) wajib menerapkan prinsip-prinsip perlindungan data yang ketat.

3. Kewajiban Laporan Kebocoran Data

   Dalam hal terjadi kebocoran data, pengendali data wajib melaporkan kepada otoritas dalam waktu 72 jam dan menginformasikan subjek data jika insiden tersebut berisiko tinggi bagi individu.

4. Sanksi Administratif & Pidana

   UU PDP memperkenalkan sanksi yang lebih tegas, termasuk:

   a) Denda administratif hingga 2% dari pendapatan tahunan bagi pelanggar.
   b) Pidana penjara hingga 6 tahun bagi pelaku penyalahgunaan data.
   c) Pidana denda hingga Rp6 miliar untuk pelanggaran serius.

5. Kewajiban Penunjukan Pejabat Perlindungan Data (DPO)

   Organisasi yang menangani data dalam skala besar atau data sensitif wajib menunjuk Data Protection Officer (DPO) untuk memastikan kepatuhan terhadap UU PDP.

6. Transfer Data ke Luar Negeri

Transfer data ke luar Indonesia hanya diperbolehkan jika negara tujuan memiliki tingkat perlindungan data yang setara atau lebih tinggi, atau ada persetujuan eksplisit dari subjek data.

UU PDP ini menandai era baru dalam perlindungan data di Indonesia, menyerupai regulasi global seperti GDPR di Uni Eropa, dengan fokus pada akuntabilitas dan hak individu atas data pribadinya.

Menurut Pasal 1 ayat (1) Undang-Undang Perlindungan Data Pribadi menyatakan bahwa:

> "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik."

Berdasarkan definisi tersebut, data pribadi merujuk pada informasi yang berkaitan dengan individu, baik secara tunggal maupun dalam kombinasi dengan data lain, yang memungkinkan identifikasi seseorang. Dengan demikian, data pribadi tidak terbatas pada identitas unik yang diberikan secara resmi, seperti KTP, nomor paspor, nomor SIM, atau foto. Namun, cakupannya lebih luas, mencakup segala jenis informasi yang dapat mengarah pada identifikasi individu, termasuk alamat IP dan data lokasi.

Pemerintah menegaskan pentingnya memberikan kepastian hukum untuk menjamin perlindungan data pribadi masyarakat. [83] Sebagaimana yang tertuang dalam pasal 1 ayat (2):

[83] Indriana Firdaus, 'Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan', *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 4.2 (2022), pp. 23-31, doi:10.52005/rechten.v4i2.98.

> "Perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi."

Pasal tersebut menyatakan bahwa data pribadi dilindungi oleh hukum sebagai jaminan hak dasar warga negara.

Pasal 2 ayat (1) Undang-Undang Perlindungan Data Pribadi berlaku untuk Setiap Orang, Badan Publik, dan Organisasi Internasional yang melakukan perbuatan hukum sebagaimana diatur dalam:

1. yang berada di wilayah hukum Negara Republik Indonesia; dan
2. di luar wilayah hukum Negara Republik Indonesia, yang memiliki akibat hukum:
    a) di wilayah hukum Negara Republik Indonesia; dan/atau
    b) bagi Subjek Data Pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia.

Pasal 2 ayat (1) menyatakan bahwa undang-undang ini berlaku untuk semua pihak, termasuk individu, perusahaan, badan publik, dan organisasi internasional, yang dikenal sebagai personal scope. Cakupannya sangat luas, tidak hanya terbatas pada wilayah tertentu (territorial scope) tetapi berlaku secara global, seperti yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Dengan demikian, Undang-Undang Pelindungan Data Pribadi mengadopsi prinsip extra territorial melalui asas yurisdiksi perlindungan, sehingga mengikat setiap individu, badan publik, atau organisasi internasional yang memproses data pribadi, baik di dalam wilayah hukum Indonesia maupun di luar negeri, selama menimbulkan dampak hukum bagi Indonesia.

Dalam melindungi dan menjamin hak Data Pribadi Undang-Undang ini memiliki 8 asas yang menjadi landasan utama Perlindungan Data Pribadi, seperti yang telah diatur dalam pasal 3:

a) perlindungan;
b) kepastian hukum;
c) kepentingan umum;
d) kemanfaatan;
e) kehati-hatian;
f) keseimbangan;
g) pertanggungjawaban; dan
h) kerahasiaan.

Undang-Undang PDP melindungi data pribadi masyarakat yang dapat terhubung secara otomatis dengan informasi lain, baik secara langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik. Data pribadi terbagi menjadi 2 yaitu data pribadi yang bersifat spesifik dan bersifat umum, sebgaimana yang diatur dalam pasal 4 undang-undang perlindungan data pribadi:

1. Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (l) huruf a meliputi:
   a) data dan informasi kesehatan;
   b) data biometrik;
   c) data genetika;
   d) catatan kejahatan;
   e) data anak;
   g) data keterangan pribadi; dan/ atau
   h) data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
2. Adapun data pribadi yang bersifat umum sebagaimana yang dimaksud pada ayat (3) yaitu:
   a) nama lengkap;
   b) jenis kelamin;
   c) kewarganegaraan;
   d) agama;
   e) status perkawinan dan/ atau;
   f) data pribadi yang dikombinasikan untuk mengidentifikasi seseorang

Pasal 5 Subjek data pribadi berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi. Undang-Undang Pelindungan Data Pribadi menegaskan pentingnya subjek data sebagai pihak yang memiliki kendali atas pengolahan data pribadinya. Kendali ini diatur

melalui hak-hak yang dimiliki oleh subjek data. UU ini lebih fokus pada perlindungan hak-hak subjek data dibandingkan kepada kewajibannya, karena data pribadi individu dikelola dalam sistem yang dioperasikan oleh pengendali data.

Pasal 12 Undang-Undang perlindungan data pribadi mengatur megenai penggugat dapat meminta gani rugi sebgaimana yang telah diatur dalam:

1. Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.
2. Ketentuan lebih lanjut mengenai pelanggaran pemrosesan Data Pribadi dan tata cara pengenaan ganti rugi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah."

Subjek data berhak mengajukan gugatan perdata untuk menuntut ganti rugi atas pelanggaran dalam pemrosesan data pribadi, dengan pengendali data pribadi memiliki tanggung jawab atas pelanggaran tersebut. Gugatan perdata dapat diajukan jika pengendali data terbukti melanggar prinsip-prinsip perlindungan data. Aturan lebih lanjut diatur dalam peraturan pemerintah.

Pasal 13 ayat (1) dan (2) menyatakan bahwa:

1. Subjek Data Pribadi berhak mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan struktur dan/ atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.
2. Subjek Data Pribadi berhak dan mengirimkan Data Pribadi tentang dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi berdasarkan Undang-Undang ini.
3. Ketentuan lebih lanjut mengenai hak Subjek Data Pribadi untuk menggunakan dan Data Pribadi sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Pemerintah.

Undang-undang perlindungan data pribadi mengatur mengenai pemrosesan data pribadi sebagaimana tercantum dalam pasal 16 yang menjadi prinsip utama dalam perlindungan data pribadi.

1. Pemrosesan Data Pribadi meliputi: pemrolehan dan pengumpulan;
   a) pengolahan dan penganalisisan;
   b) penyimpanan;
   c) perbaikan dan pembaruan;
   d) penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau
   e) penghapusan atau pemusnahan.
2. Pemrosesan data pribadi sebagaimana yang dimaksud pada ayat (1) dilakukan sesuai dengan prinsip perlindungan data pribadi meliputi;
   a) data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum dan transparan;
   b) pemrosesan data pribadi dilakukan sesuai dengan tujuannya;
   c) pemrosesan data pribadi dilakukan dengan menjamin hak subjek data pribadi;
   d) pemrosesan data pribadi dilakukan secara akurat, lengkaap, tidak menyesatkan, mutakhir dan dapat dipertanggungjawabkan.
   e) pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penghilangan data pribadi;
   f) pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan serta kegagalan pelindungan data pribadi;
   g) data pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan subjek data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
   h) pemrosesan Data Pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.
3. Ketentuan lebih lanjut mengenai pelaksanaan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah.

Pasal 16 telah mengatur dengan jelas tata cara pemrosesan data pribadi, tetapi seharusnya ada pembedaan antara pemrosesan data pribadi umum dan data pribadi yang bersifat spesifik. Selain data pribadi umum, perhatian khusus perlu diberikan pada kategori data pribadi tertentu yang sensitif, sehingga memerlukan tingkat perlindungan yang lebih tinggi.

Pasal 19 UU PDP mengatur tentang pengendali data pribadi dan prosesor data pribadi mencakup individu, badan publik, serta organisasi internasional. Pengendali data pribadi adalah pihak yang secara mandiri atau bersama-sama menentukan tujuan dan mengendalikan pengolahan data pribadi. Sedangkan prosesor data pribadi adalah pihak yang mengolah data pribadi atas nama pengendali, baik secara mandiri maupun bersama-sama.

Pasal 20 ayat (1) dan (2) Undang-Undang Perlindungan Data Pribadi menyatakan bahwa:

1. Pengendali Data Pribadi wajib memiliki dasar pemrosesan Data Pribadi.
2. Dasar pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi:
   a) persetujuan yang sah secara eksplisit dari subjek data prribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh pengendali data pribadi kepada subjek data pribadi;
   b) pemenuhan kewajiban perjanjian dalam hal subjek data pribadi merupakan salah satu pihak atau untuk memenuhi permintaan subjek data pribadi pada saat akan melakukan perjanjian;
   c) pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
   d) pemenuhan pelindungan kepentingan vital subjek data pribadi;
   e) pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan pengendali data pribadi berdasarkan peraturan perundang-undangan; dan/atau
   f) pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan,kebutuhan, dan keseimbangan kepentingan pengendali data pribadi dan hak subjek data pribadi.

Pasal 21 ayat (1) dalam hal pemrosesan data pribadi pengendali data pribadi wajib menyampaikan informasi mengenai:

a) legalitas dari pemrosesan data pribadi;
b) tujuan pemrosesan data Pribadi;
c) jenis dan relevansi data pribadi yang akan diproses;
d) jangka waktu retensi dokumen yang memuat data Pribadi;
e) rincian mengenai Informasi yang
f) jangka waktu pemrosesan data pribadi; dan
g) subjek data pribadi.

Pasal 21 ayat (2) dalam hal terdapat perubahan informasi sebagaimana dimaksud pada ayat (1) menyatakan bahwa:

> "Dalam hal terdapat perubahan Informasi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib memberitahukan kepada Subjek Data sebelum terjadi perubahan informasi."

Dari pasal tersebut dapat dilihat bahwa dalam pemrosesan data pribadi, pengendali data pribadi harus memperoleh persetujuan yang sah dari subjek data pribadi, serta wajib memberikan informasi mengenai tujuan-tujuan yang ingin dicapai dalam pemrosesan data pribadi tersebut.

Tata cara dan persyaratan pemrosesan terkait persetujuan pemrosesan data pribadi diatur dalam pasal 22:

1. Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau terekam.
2. Persetujuan sebagaimana dimaksud pada ayat (1) dapat disampaikan secara elektronik atau nonelektronik.
3. Persetejuan sebagaimana dimaksud pada ayat (1) mempunyai kekuatan hukum yang sama.
4. Dalam hal persetujuan sebagaimana dimaksud pada ayat (1) memuat tujuan lain, permintaan persetqjuan harus memenuhi ketentuan:
   a) dapat dibedakan secara jelas dengan hal lainnya;
   b) dibuat dengan forrnat yang dapat dipahami dan mudah diakses; dan
   c) menggunalan bahasa yang sederhana dan jelas.
5. Persetujuan yang tidak memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (4) dinyatakan batal demi hukum.

Pasal ini mensyaratkan bahwa pemrosesan data pribadi harus mengikuti prosedur persetujuan yang ditetapkan, yaitu harus dilakukan secara tertulis atau terekam, baik secara elektronik maupun non-elektronik, yang memiliki kekuatan hukum yang sama. Jika persetujuan tersebut mencakup tujuan lain, tujuan tersebut harus dibedakan secara jelas dari hal-hal lainnya. Apabila persetujuan tidak memenuhi ketentuan di atas, maka akan dianggap batal demi hukum.

Undang-Undang Perlindungan Data Pribadi juga mengatur tentang pemrosesan data pribadi anak yang telah diatur dalam pasal 25 menyatakan bahwa:

1. Pemrosesan Data Pribadi anak di lakukan secara khusus.
2. Pemrosesan Data Pribadi anak sebagaimana dimaksud pada ayat (1) wajib mendapat persetujuan dari orang tua anak dan/ atau wali anak sesuai dengan ketentuan peraturan perundang-undangan.

Berdasarkan Pasal 1 *Convention on the Rights of the Child (CRC),* Anak adalah seseorang yang berusia di bawah 18 tahun. Anak-anak lebih rentan dibandingkan orang dewasa karena mereka belum sepenuhnya memahami dampak jangka panjang dari menyetujui pengumpulan data pribadi mereka. Masalah privasi menjadi lebih penting ketika berhubungan dengan data anak, karena mereka lebih rentan secara kognitif, emosional, dan fisik.

Undang-undang perlindungan data pribadi juga secara khusus mengatur proses privasi anak penyadang disabilitas, sebgaiamana yang dinyatakan dalam pasal 26:

1. Pemrosesan Data Pribadi penyandang disabilitas diselenggarakan secara khusus.
2. Pemrosesan Data Pribadi penyandang disabilitas sebagaimana dimaksud pada ayat (1) dilakukan melalui komunikasi dengan menggunakan cara tertentu sesuai dengan ketentuan perundang-undangan.
3. Pemrosesan Data Pribadi penyandang disabilitas sebagaimana dimaksud pada ayat (2) wajib mendapat persetujuan dari penyandang disabilitas dan/atau wali penyandang disabilitas sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 22 menyebutkan bahwa penyandang disabilitas berhak atas perlindungan privasi terkait kehidupan pribadi, keluarga, tempat tinggal, korespondensi, serta bentuk komunikasi lainnya dari gangguan terhadap kehormatan dan reputasinya, serta berhak atas perlindungan hukum.

Dalam melakukan pemrosesan data pribadi, pengendali data pribadi diwajibkan untuk melindungi dan memastikan keamanan data pribadi, sesuai dengan ketentuan yang tercantum dalam Pasal 35 ayatmenyatakan bahwa:

"Pengendali Data Pribadi wajib melindungi dan memastikan kemanan Data Pribadi yang diprosesnya dengan melakukan:

1. penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang- undangan; dan
2. penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi."

Pasal 38 Pengendali Data Pribadi wajib melindungi Data Pribadi dari pemrosesan yang tidak sah. Pasal ini berkaitan dengan salah satu prinsip utama dalam UU PDP, yaitu pemrosesan data pribadi yang diatur dalam Pasal 16 ayat (2) huruf a. Prinsip ini menekankan bahwa pemrosesan harus dilakukan secara terbatas, spesifik, sah secara hukum, dan transparan. Semua proses tersebut wajib memenuhi dasar hukum yang sah. Oleh karena itu, pemrosesan data pribadi hanya diperbolehkan jika sesuai dengan legalitas sebagaimana diatur dalam Pasal 20 ayat (2). Pengendali data bertanggung jawab memastikan seluruh pemrosesan dilakukan secara legal. Jika dilakukan tanpa dasar hukum yang sah, akan dikenakan sanksi.

Pengendali data pribadi harus menghapus data pribadi yang sedang di prosesenya telah di atur dalam pasal 43:

1. pengendali data pribadi wajib menghapus data pribadi dalam hal;
   a) Data Pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi;
   b) subjek data pribadi telah melakukan penarikan kembali persetujuan pemrosesan data pribadi;
   c) terdapat permintaan dari subjek data pribadi; atau
   d) data pribadi diperoleh dan/atau diproses dengan cara melawan hukum.

Pasal ini menetapkan bahwa pengendali data wajib menghapus data pribadi, yang dikenal sebagai *The Right to be Forgotten.* Hak ini tidak bersifat mutlak dan hanya berlaku dalam kondisi tertentu, seperti ketika tujuan pemrosesan data sudah selesai dan data pribadi tidak diperlukan lagi. Penghapusan juga harus dilakukan jika subjek data mencabut persetujuan, mengajukan permintaan, atau jika data tersebut diproses secara melanggar hukum.

Jika terjadi kegagagalan perlindungan data pengendali data wajib menyampaikannya sebagaimana yang telah diatur dalam Pasal 46 menyatakan bahwa:

1. Dalam hal terjadi kegagalan Perlindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambar 3 × 24 jam kepada:
   a) subjek Data Pribadi; dan
   b) lembaga.
2. Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat:
   a) Data Pribadi yang terungkap;
   b) kapan dan bagaimana data pribadi terungkap; dan
   c) upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh Pegendali Data Pribadi.
3. Dalam hal tertentu, pengendali data pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan perlindungan data pribadi.

Pasal ini menerapkan prinsip akuntabilitas, yang mengharuskan pengendali data untuk memberikan pemberitahuan tertulis jika terjadi kegagalan dalam perlindungan data atau kebocoran data *(data breach).* Kewajiban ini dikenal dengan istilah pemberitahuan kebocoran data *(data breach notification).* Pemberitahuan tertulis disampaikan kepada subjek data pribadi dan Lembaga

Pengawas. Pemberitahuan tersebut mengatur hal-hal yang perlu dilaporkan baik kepada subjek data maupun kepada Lembaga Pengawas.

Undang-Undang Perlindungan Data Pribadi mengatur sanksi administrasi yang dikenakan apabila terjadi kegagalan dalam melindungi data pribadi. Sebagaimana yang telah diatur dalam Pasal 57 menyatakan bahwa:

1. Pelanggaran terhadap ketentuan Pasal 2O ayat (l), Pasal 21, Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (31, Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, Pasal 39 ayat (1), Pasal 40 ayat (1), Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1) dan ayat (3), Pasal 47, Pasal 48 ayat (l), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (l), Pasal 55 ayat (21, dan Pasal 56 ayat (2) sampai dengan ayat (4) dikenai sanksi administratif.
2. Sanksi administratif sebagaimana dimaksud pada ayat (l) berupa:
   a) peringatan tertulis;
   b) penghentian sementara kegiatan pemrosesan Data Pribadi;
   c) penghapusan atau pemusnahan Data Pribadi; dan/atau
   d) denda administratif.
3. Sanksi administratif berupa denda administratif sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari perrdapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.
4. Penjatuhan sanksi administratif sebagaimana dimaksud pada ayat (2) diberikan oleh lembaga.
5. Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif selagaimana dimaksud padaayat (3) diatur dalam Peraturan Pemerintah.

Pasal 57 mengatur 30 pasal terkait tanggung jawab pengendali data pribadi. Pelanggaran atas ketentuan tersebut dapat dijadikan dasar bagi subjek data untuk mengajukan tuntutan kepada lembaga. Selanjutnya, Lembaga Pengawas Pelindungan Data Pribadi akan memberikan sanksi administratif jika pelanggaran terbukti terjadi.

Undang-Undang Perlindungan Data Pribadi juga mengatur kelembagaan untuk melindungi dan mengawasi pelaksanaan pemrosesan data pribadi oleh pengendali dan prosesor data. Sebagaimana yang telah diatur dalam Pasal 58:

1. Pemerintah berperan dalam penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini.
2. Penyelenggaraan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga.
3. lembaga sebagaimana dimaksud pada ayat (2) ditetapkan oleh Presiden.
4. lembaga sebagaimana dimaksud pada ayat (2) bertanggung jawab kepada Presiden.
5. Ketentuan lebih lanjut mengenai lembaga sebagaimana dimalsud pada ayat (2) diatur dengan Peraturan Presiden.

Pasal 58 ayat (1) hingga ayat (5) UU Pelindungan Data Pribadi mengatur pelaksanaan pelindungan data pribadi secara kelembagaan. Ayat (1) menyebutkan bahwa pemerintah, sebagai bagian dari eksekutif, berperan dalam mewujudkan pelindungan data pribadi. Ayat (2) dan (3) selanjutnya menjelaskan bahwa pelindungan data pribadi dilaksanakan oleh sebuah lembaga yang pembentukannya ditetapkan oleh Presiden. Lembaga ini bertanggung jawab langsung kepada Presiden karena dibentuk berdasarkan keputusan Presiden. Dengan perannya dalam pelaksanaan pelindungan data pribadi di Indonesia, lembaga ini berfungsi sebagai lembaga pengawas.

Pasal 59 menyatakan bahwa lembaga sebagaimana dimaksud dalam Pasal 58 Ayat (2) melaksanakan:

a) perumusan dan penetapan kebijakan dan strategi Pelindungan Data Pribadi yang menjadi panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi;
b) pengawasan terhadap penyelenggaraan Pelindungan Data Pribadi;
c) penegakan hukum administratif terhadap pelanggaran Undang-Undang ini; dan
d) fasilitasi penyelesaian sengketa di luar pengadilan.

Pasal 59 menjelaskan secara lebih rinci peran utama Lembaga Pengawas Pelindungan Data Pribadi, termasuk merumuskan kebijakan dan strategi yang perlu diterapkan. Lembaga ini juga berfungsi sebagai panduan khusus bagi

pengendali dan prosesor data. Selain itu, lembaga ini bertugas mengawasi penerapan pelindungan data pribadi, baik pada instansi publik maupun swasta. Lembaga pengawas juga memiliki kewenangan untuk menegakkan hukum administratif terkait pelanggaran pada Pasal 57, yang mengatur sanksi atas pelanggaran kewajiban pengendali dan prosesor data pribadi.

Pasal 60 mengatur tentang wewenang lembaga sebagaiamana yang dimkasud pada pasal 58 ayat (2) menyatakan:

a) merumuskan dan menetapkan kebijakan di bidang Pelindungan Data Pribadi;
b) melakukan pengawasan terhadap kepatuhan Pengendali Data Pribadi;
c) menjatuhkan sanksi administratif atas pelanggaran Pelindungan Data Pribadi yang dilakukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi;
d) membantu aparat penegak hukum dalam penanganan dugaan tindak pidana Data Pribadi sebagaimana dimaksud dalam Undang-Undang ini;
e) bekerja sama dengan lembaga Pelindungan Data Pribadi negara lain dalam rangka penyelesaian dugaan pelanggaran Pelindungan Data Pribadi lintas negara;
f) melakukan penilaian terhadap pemenuhan persyaratan transfer Data Pribadi ke luar wilayah hukum Negara Republik Indonesia;
g) memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada Pengendali Data Pribadi dan/ atau Prosesor Data Pribadi;
h) melakukan publikasi hasil pelaksanaan pengawasan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
i) menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran Pelindungan Data Pribadi;
j) melakukan dan atas pengaduan, laporan, dan/atau hasil pengawasan terhadap dugaan terjadinya pelanggaran Pelindungan Data Pribadi;
k) memanggil dan menghadirkan Setiap Orang dan/ atau Badan Publik yang terkait dengan dugaan pelanggaran Pelindungan Data Pribadi;
l) meminta keterangan, data, Informasi, dan dokumen dari Setiap Orang dan/ atau Badan Publik terkait dugaan pelanggaran Pelindungan Data Pribadi;
m) memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaan pelanggaran Pelindungan Data Pribadi;
n) melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/ atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga; dan

o) meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa Pelindungan Data Pribadi.

Pasal 63 Undang-Undang Perlindungan Data Pribadi mengatur tentang partisipasi masyarakat dalam menjaga data pribadinya sebagaimana yang dinyatakan dalam Pasal (1) dan (2):

1. Masyarakat dapat berperan baik secara langsung maupun tidak langsung dalam mendukung terselenggaranya Pelindungan Data Pribadi.
2. Pelaksanaan peran sebagaimana dimaksud pada ayat (1) dapat dilakukan melalui pendidikan, pelatihan, advokasi, sosialisasi, dan/atau pengawasan sesuai dengan ketentuan peraturan perundang-undangan.

Penjelasan Pasal 63 Undang-Undang Pelindungan Data Pribadi ini memberikan kesempatan bagi semua pihak untuk berkontribusi dalam melindungi data pribadi. Kontribusi ini dapat berupa kegiatan sosialisasi dan edukasi yang membantu masyarakat memahami hak-haknya dan menjaga data pribadi, misalnya melalui pendidikan, pelatihan, dan advokasi. Sekolah mulai dari SD, SMP, SMA, hingga universitas bisa memasukkan topik perlindungan data pribadi ke dalam kurikulum. Selain itu, lembaga nonformal yang memenuhi syarat juga dapat menyelenggarakan berbagai pelatihan.

Undang-Undang Perlndungan Data Pribadi mengatur mengenai Penyelesaian Sengketa dan Hukum Acara dalam Pasal 64 yang menyatakan bahwa:

1. Penyelesaian sengketa Data Pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan.
2. Hukum acara yang berlaku dalam penyelesaian sengketa dan/ atau proses peradilan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan.
3. Alat bukti yang sah dalam Undang-Undang ini meliputi:
   a) alat bukti sebagaimana dimaksud dalam hukum acara; dan

b) alat bukti lain berupa informasi elelrtronik dan/ atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan.

4. Dalam hal diperlukan untuk melindungi Data Pribadi,proses persidangan dilakukan secara tertutup.

Undang-Undang Pelindungan Data Pribadi mengatur berbagai mekanisme penyelesaian sengketa, baik melalui jalur litigasi maupun nonlitigasi. Salah satunya adalah arbitrase, yang pelaksaanaan hukum acara dan pembuktiannya diatur sesuai dengan ketentuan undang-undang.

Pasal 65 mengatur tentang larangan dalam penggunaan data pribadi yang menyatakan bahwa:

1. Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
2. Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
3. Setiap orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.

Pasal 65 ayat (1), (2), dan (3) mengatur tindakan mengambil atau mengumpulkan data pribadi orang lain tanpa izin atau tanpa dasar hukum, mengungkapkan data pribadi milik orang lain, serta menggunakan data tersebut secara tidak sah, sebagai perbuatan melawan hukum. Aturan ini menjadi dasar hukum untuk mengajukan gugatan atas pelanggaran data pribadi.Ketentuan ini juga berkaitan dengan Pasal 1365 KUH Perdata (BW), yang menjelaskan unsur-unsur utama perbuatan melawan hukum.

Undang-Undang Perlindungan Data Pribadi mengatur larangan memalsukan data pribadi diatur dalam Pasal 66 yang menyatakan bahwa:

"Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain."

Pasal ini menegaskan larangan untuk membuat dan menggunakan data pribadi palsu. Ketentuan ini juga melarang tindakan phishing, yang dianggap sebagai pelanggaran hukum. Phishing didefinisikan sebagai penipuan yang dilakukan dengan cara memalsukan data untuk menipu korban. Tujuan utama phishing adalah mendapatkan informasi sensitif, seperti kata sandi atau data kartu kredit, dengan berpura-pura menjadi pihak atau perusahaan terpercaya melalui komunikasi elektronik resmi, seperti email atau pesan instan. Ketentuan ini juga mencantumkan adanya unsur kerugian bagi pihak lain, sehingga tindakan ini dapat dikenakan sanksi hukum baik secara perdata maupun pidana.

Terkait Kasus Pencurian Data Pribadi, pelaku dapat dikenakan sanksi pidana sebagaimana diatur dalam Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dengan ketentuan sebagai berikut::

Pasal 67:

1. “Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”
2. “Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).”
3. “Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima

miliar rupiah). Pasal 68 “Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 di pidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp 6.000.000.000,00 (enam miliar rupiah).”

Pasal 68:

“Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntrrngkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 .tipidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000. 000.000,00 (enam miliar rupiah).”

Pasal 69:

“Selain dijatuhi pidana ssfagaimana dimaksud dalam Pasal 67 dan Pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.”

Pasal 70:

1. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh Korporasi, pidana dapat dljatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/ atau Korporasi.
2. Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda.
3. Pidana denda yang dijatuhkan kepada Korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan.
5. Selain dijatuhi pidana denda sebagaimana dimaksud pada Ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:
   a) perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
   b) pembekuan seluruh atau sebagian usaha Korporasi;
   c) pelarangan permanen melakukan perbuatan tertentu;
   d) penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi;
   e) melaksanakan kewajiban yang telah dilalaikan;
   f) pembayaran ganti kerugian;
   g) pencabutan izin; dan/atau
   h) pembubaran Korporasi.

Berdasarkan ketentuan pasal-pasal yang disebutkan, tindak pidana pencurian data pribadi dapat dikenakan Pasal 67 Ayat (1) dan Ayat (3) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pelaku diancam dengan hukuman pidana maksimal lima tahun penjara

dan/atau denda hingga lima miliar rupiah. Selain itu, pelaku juga dapat dijatuhi hukuman tambahan, seperti perampasan keuntungan atau harta kekayaan yang diperoleh dari tindak pidana, serta kewajiban membayar ganti rugi.

Jika pencurian data dilakukan oleh korporasi, sanksi dalam Pasal 67 undang-undang tersebut dapat dikenakan kepada pengurus, pengendali, pemberi perintah, pemilik manfaat, atau korporasi itu sendiri (terutama pidana denda). Denda yang dijatuhkan kepada korporasi dapat mencapai sepuluh kali lipat dari batas maksimal denda yang diatur.

Korporasi juga dapat dijatuhi hukuman tambahan, seperti perampasan keuntungan atau harta kekayaan yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, pelarangan permanen atas tindakan tertentu, penutupan sebagian atau seluruh tempat usaha, pemenuhan kewajiban yang sebelumnya diabaikan, pembayaran ganti rugi, pencabutan izin, hingga pembubaran korporasi.

Data pribadi merupakan aset berharga atau komoditas penting di era big data dan ekonomi digital. Oleh karena itu, perlindungan data pribadi bertujuan untuk mengurangi pelanggaran privasi, mencegah penyalahgunaan data, dan meningkatkan kesadaran masyarakat agar lebih menjaga keamanan data pribadinya.[84]

[84] Jurnal Fakultas and Hukum Unsrat, "Jurnal Fakultas Hukum Unsrat Lex Privatum. Vol 13. No. 01. 2024" 13, no. 01 (2024): 1–17.

B. Kelebihan dan Kekurangan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribad

1. Kelebihan dalam Undang-Undang Perlindungan Data pribadi yaitu:

   a) UU PDP melindungi dan menjamin Hak Asasi Manusia terkait hak-hak individu dalam mengntrol data pribadinya.[85]

   b) UU PDP mengadopsi pengaturan yang sejalan dengan Perlindungan data pribadi yang berlaku di Uni Eropa, yaitu *General Data Protection Regulation* (GDPR). Beberapa hal yang diatur dalam GDPR juga diatur dalam UU PDP mencakup pengelola data (*Data Controller*), pemrosesan data (*Data Prosesor*) dan subjek data (*Data Subject Rights*).

   c) UU PDP mewajibkan pengolah data untuk transparan dalam pengelolaan data pribadi. Setiap individu berhak mengetahui data jenis data yang dikumpulkan, tujuan penggnaanya, serta pihak yang menerima data tersebut.[86]

   d) UU PDP menetapkan sanksi administratif dan pidana yang tegas bagi pelanggaran perlindungan data pribadi. Sanksi tersebut mencakup peringatan tertulis, ganti rugi, denda besar dan hukuman penjara bagi individu atau organisasi yang terbukti bertanggung jawab atas kebocoran data pribadi. Tujuan dari sanksi ini adalah memastikan

[85] Fauzi and Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi."

[86] Alza Gabriel, "Perlindungan Hukum Atas Data Pribadi Dalam Kasus Kebocoran Data Pusat Data Nasional Sementara (Pdns) Dalam Perspektif Hukum Pidana," *Seminar Nasional Hukum Dan Pancasila* 3 (2024): 18–26.

pengelola data bertanggung jawab dan serius dalam melindungi data pribadi yang mereka kelola.[87]

2. Kelemahan dalam Undang-Undang Perlindungan Data Pribadi yaitu:

a) Undang-Undang Perlindungan Data Pribadi juga mengatur tentang pemrosesan data pribadi terhadap anak dan penyandang disabilitas. Dalam ketentuan Pasal 25 dan 26 UU PDP mengatur bahwa pemrosesan data pribadi anak dan penyandang disabilitas harus diselenggarakan secara khusus dan wajib mendapat persetujuan orang tua dan/atau wali anak dalam penggunaanya. Akan tetapi pengaturan tentang data pribadi anak dan penyandang disabilita dalam UU PDP masih terbatas.

UU PDP belum memberikan penjelasan secara rinci mengenai bagaimana bentuk "Penyelenggaraan Khusus" yang dimaksud. Sehingga penyelenggara data pribadi seperti media sosial dan platform pendidikan kurang memiliki pedoman perlindungan hukum yang jelas dalam mengelola data nak. Selain itu, dalam UU PDP belum menetapkan batas usia yang jelas untuk menentukan siapa yang termasuk dalam kategori data anak. Hal ini penting untuk diperhatikan karena terdapat perbedaan pengertian 'usia anak' dalam berbagai peraturan perundang-undangan di Indonesia, seperti UU Perlindungan Anak, UU Perkawinan, dan KUH Perdata. Perbedaan tersebut dapat

[87] Danil Erlangga Mahameru et al., "Implementasi Undang-Undang Perlindungan Data" 5, no. 20 (2023): 115–31.

menyebabkan penafsiran yang beragam tentang batas usia anak, yang dapat disalahgunakan oleh berbagai pihak.[88]

b) Peraturan pelaksana UU PDP hingga saat ini belum selesai disusun atau disahkan.

UU PDP mengamanatkan pembentukan 10 peraturan pemerintah sebagai aturan pelaksana untuk melaksanakan perlindungan data pribadi di Indonesia. Ketentuan ini diatur dalam Pasal 10 ayat (2), Pasal 12 ayat (2), Pasal 13 ayat (3), Pasal 16 ayat (3), Pasal 34 ayat (3), Pasal 48 ayat (5), Pasal 54 ayat (3), Pasal 56 ayat (5), Pasal 57 ayat (5), dan Pasal 61. Namun, hingga satu tahun setelah disahkannya UU PDP, belum ada satu pun dari peraturan pemerintah yang diamanatkan tersebut diterbitkan. Ketiadaan aturan ini menciptakan ketidakpastian dan kekosongan hukum dalam perlindungan data pribadi di Indonesia. Lemahnya regulasi dan penegakan hukum membuat kejahatan terkait data pribadi semakin marak erjadi. Selain itu, tanpa peraturan pelaksana, ada risiko penafsiran yang salah terhadap UU PDP.

Dalam Pasal 12 ayat (1) UU PDP menyatakan bahwa pemilik data pribadi berhak meminta ganti rugi atau menggugat Pengendali Data yang melanggar hak mereka. Namun, UU ini tidak menjelaskan mekanisme gugatan, termasuk tata cara, prosedur, atau pengadilan yang berwenang menangani kasus perlindungan data pribadi. Aturan

[88] The Conversation "Panel ahli: UU Perlindungan Data Pribadi rentan makan korban dan belum jamin proteksi data yang kuat" https://theconversation.com/panel-ahli-uu-perlindungan-data-pribadi-rentan-makan-korban-dan-belum-jamin-proteksi-data-yang-kuat-191018 Di Akses Pada Pukul 25 November Pukul 22.27

mengenai hal ini direncanakan untuk diatur melalui peraturan pemerintah, tetapi hingga kini aturan tersebut belum diterbitkan. Tidak adanya peraturan pemerintah untuk mengatur mekanisme penegakan hukum terhadap pelanggaran data pribadi ini menciptakan kekosongan hukum dan ketidakpastian, terutama dalam hal prosedur ganti rugi dan pengajuan gugatan, yang pada akhirnya melemahkan perlindungan data pribadi di Indonesia.

c) Lembaga Independen Khusus untuk Perlindungan Data Pribadi belum dibentuk.

Pasal 58 UU PDP mengatur pembentukan lembaga untuk mengelola perlindungan data pribadi, yang bertanggung jawab langsung kepada Presiden. Lembaga tersebut memiliki 15 wewenang terkait penyelenggaraan perlindungan data pribadi. Pasal 61 UU PDP menyebutkan bahwa tata cara pelaksanaan wewenang lembaga ini akan diatur lebih lanjut dalam peraturan pemerintah. Namun, karena hingga saat ini belum ada peraturan pemerintah yang mengatur hal tersebut, pembentukan lembaga perlindungan data pribadi di Indonesia terhambat. Peran lembaga ini penting dalam menjaga keamanan data pribadi dan memastikan perlindungan data pribadi di Indonesia sesuai dengan standar yang ditetapkan oleh undang-undang, sehingga dapat meningkatkan kepercayaan masyarakat dalam penggunaan data pribadi di era digital. Selain itu lembaga tersebut juga diharapkan dapat bekerja sama dengan lembaga otoritas perlindungan data pribadi di

negara lain untuk meningkatkan kerjasama internasional dalam melindungi data pribadi. Ini penting untuk menjaga data pribadi pengguna, baik yang ada di Indonesia maupun di negara lain.

Pembentukan lembaga independen untuk perlindungan data pribadi tidak hanya merupakan mandat dari UU PDP, tetapi juga didorong oleh beberapa perjanjian internasional, seperti *Guidelines for the Regulation of Computerized Personal Data Files* 1990 (*UN GRCPDF*) dan *Asia Pacific Economic Cooperation* (*APEC) Privacy Framework*. Dalam *UN GRCPDF* 1990, salah satu syarat dasar perlindungan data pribadi di suatu negara adalah adanya lembaga pengawas yang independen. Sedangkan *APEC Privacy Framework*, yang merupakan pedoman privasi dari organisasi kerjasama negara-negara di kawasan Asia Pasifik *(APEC*), pertama kali dikeluarkan pada tahun 2004 dan diperbarui pada 2015. Dalam Pasal 10 *APEC Privacy Framework* dijelaskan bahwa untuk mencapai tujuan kerangka kerja ini, negara atau organisasi dapat meminta individu atau organisasi lain untuk mengumpulkan, menyimpan, menggunakan, memproses, mentransfer, atau mengungkapkan informasi pribadi atas nama mereka.

Salah Satu hambatan dalam melindungi data pribadi di Indonesia adalah belum terbentuknya lembaga independen yang khusus menangani perlindungan data pribadi. Padahal, pembentukan lembaga tersebut tidak hanya menjadi mandat dalam UU PDP, tetapi juga

didasarkan pada instrumen hukum internasional terkait privasi dan perlindungan data pribadi. Oleh karena itu, pemerintah perlu segera menerbitkan dan mengesahkan peraturan pemerintah mengenai pembentukan lembaga ini, agar lembaga independen perlindungan data pribadi di Indonesia dapat melaksanakan tugas serta wewenangnya. Selain itu, penting untuk diingat bahwa hukum tidak hanya berfungsi sebagai seperangkat aturan sosial, tetapi juga harus mencakup institusi dan mekanisme yang diperlukan agar dapat diterapkan secara efektif.[89]

C. Bentuk Perlindungan Hukum Undang-Undang Nomor 27 Tahun 2022

Perlindungan hukum adalah upaya melindungi subjek hukum melalui penerapan peraturan perundang-undangan yang dilengkapi dengan sanksi untuk menjamin pelaksanaannya. Subjek hukum mencakup individu maupun badan hukum. Perlindungan hukum terbagi menjadi dua jenis: preventif dan represif. Perlindungan hukum preventif diberikan oleh pemerintah untuk mencegah terjadinya pelanggaran, diatur dalam peraturan perundang-undangan yang berfungsi memberikan panduan dalam menjalankan kewajiban. Sementara itu, perlindungan hukum represif adalah langkah terakhir berupa pemberian sanksi, seperti denda, penjara, atau hukuman tambahan, yang diterapkan setelah terjadi pelanggaran atau sengketa.[90] Undang-Undang Perlindungan Data Pribadi memberikan perlindungan hukum:

[89] Bella Christine and Christine S.T. Kansil, "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 9 (2023): 16331–39, https://doi.org/10.36418/syntax-literate.v7i9.13936.

[90] Refaldy Braif, Carundeng, Anna S. Wahongan, Presly Prayogo, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan

1. Perlindungan Hukum Preventif berupa:
    a. Dalam pemrosesan data pribadi pengendali data harus meminta pesetujuan yang sah kepada subjek data untuk menghindari penggunaan data tanpa izin.
    b. Memberikan hak kepada subjek data untuk mengakses, memperbarui, menghapus dan menarik persetujuan atas pemrosesan data dalam melindungi privasi mereka.
    c. Mewajibkan pengelola data untuk melaporkan setiap kejadian kebocoran data kepada lembaga terkait dan subjek data untuk mencegah dampak yang lebih luas dari kebocoran data ini.
    d. Memberikan penyuluhan dan edukasi dalam masyarakat untuk meningkatkan pemahaman tentang pentingnya melindungi data pribadi dan cara-cara untum menjaga keaamanannya, penyuluhan ini dapat dilakukan melalui media massa, seminar, serta materi edukasi di sekolah
2. Perlindungan Hukum Represif berupa:
    a. Sanksi Administrasi

        Pengendali dan prosesor data pribadi dapat dikenakan sanksi administratif untuk pelanggaran terhadap ketentuan pasal dalam UU PDP. Sanksi-sanksi Administrasi tersebut berupa;

        1) Peringatan tertulis;
        2) Penghentian sementara kegiatan pemrosesan data pribadi;
        3) Penghapusan atau pemusnahan data pribadi; dan/atau

---

Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik," *Lex Privatum* 10, no. 1 (2022): 188–98, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/38083.

4) Denda administrasi;

Sanksi administrasi berupa denda administrasi sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.[91] Adapun kasus kebocoran data pribadi yang dikenakan sanksi administrasi dalam UU PDP yaitu:

a) Kasus kebocoran data Tokopedia dan BPJS Kesehatan

Dalam undang-undang perlindungan data pribadi, pengendali data pribadi diwajibkan bertanggungjawab atas pengolahan data pribadi dan harus dapat menunjukkan akuntabilitas dalam mematuhi prinsip perlindungan data pribadi. Salah satu prinsip yang harus di penuhi dalam pemrosesan data pribadi adalah menjaga keamanan data pribadi dari akses dan pengungkapan yang tidak sah, penyalahgunaan, perusakan, atau penghapusan data pribadi. Pengendali data pribadi tokopedia dan BPJS wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi. Pelanggaran terhadap ketentuan pasal 46 ayat (1) dan (3) sebagaimana disebut diatas dikenai sanksi administrasi berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi,

[91] Undang-Undang nomor 27 tahun 2022 tentang perlindungan data pribadi pasal 57

penghapusan atau pemusnahan data pribadi, dan/atau denda administrasi

b. Sanksi pidana

UU PDP dalam ketentuan pidananya, mengatur mengenai sanksi pidana bagi setiap orang yang melanggar ketentuan UU PDP, begitu juga sanksi bagi korporasi yang menjadi pengendali dan prosesor data pribadi. Sanksi pidana yang dapat dikenakan tersebut dapat berupa pidana penjara, pidana denda serta juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Sebagaimana yang diatur dalam Pasal 67:[92]

1. Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
2. Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
3. Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

[92] Beni Kharisma Arrasuli and Khairul Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES Journal of Swara Justisia* 7, no. 2 (2023): 369, https://doi.org/10.31933/ujsj.v7i2.351.

Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda. Pidana denda yang dijatuhkan kepada Korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan. Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:

a) perampasan keuntungan dan atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
b) pembekuan seluruh atau sebagian usaha Korporasi;
c) pelarangan permanen melakukan perbuatan tertentu;
d) penutupan seluruh atau sebagian tempat usaha dan atau kegiatan Korporasi;
e) melaksanakan kewajiban yang telah dilalaikan;
f) pembayaran ganti kerugian;
g) pencabutan izin; dan
h) pembubaran Korporasi.

Adapun kasus kebocoran data yang dikenakan sanksi pidana dalam UU PDP yaitu:

1) Kebocoran data SIM card

   Kebocoran data pribadi pengguna SIM Card dapat dikenakan sanksi pidana berdasarkan undang-undang perlindungan data pribadi (PDP). Sebagaimana yang diatur dalam Pasal 67 ayat (1) dan (3) UU PDP mengatur tentang pencurian data pribadi (identity theft). Pasal 67 ayat (1) menyatakan bahwa

> “Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah) dan dapat dijerat dengan ancaman pidana penjara maksimal 5 tahun dan/atau pidana denda maksimal Rp 5 miliar. Sedangkan Pasal 65 ayat (3) menyatakan bahwa “Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).

c. Sanksi Perdata

Undang-Undang Perlindungan Data Pribadi (UU PDP) tidak secara spesifik mengatur hal tersebut. Dalam Pasal 12 UU PDP memberikan hak kepada subjek Data Pribadi untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Undang-undang PDP memberikan kewenang kepada peraturan pemerintah untuk mengatur prosesnya. Setidaknya pelanggaran terhadap perlindungan data pribadi dapat digugat sebagai perbuatan melawan hukum atas dasar kesalahan

berdasarkan ketentuan undang-undang. Dalam hal ini Pasal 1365 KUHPerdata yang mengaturnya:

> ”Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut”, maupun atas dasar ketidakpatutan atau ketidakhati-hatian sebagaimana Pasal 1366 KUHPerdata "setiap orang bertanggung jawab tidak hanya atas perbuatanya tetapi juga kelalaianya dan kurang hati-hati”.[93]

Tindakan dikategorikan sebagai Perbuatan Melawan Hukum apabila memenuhi unsur berikut :

1. Ada perbuatan
2. Terbukti melawan hukum
3. Adanya kesalahan
4. Kerugian
5. Terdapat hubungan sebab-akibat antara tindakan yang dilakukan dan munculnya kerugian.

Adapun kasus kebocoran data pribadi yang dikenakan sanksi perdata dalam UU PDP yaitu;

a) Kredit plus

Kesalahan yang dilakukan kredit plus terjadi akibat kelalaiannya dalam memenuhi kewajiban menjaga kerahasiaan data pribadi nasabah. Kreditplus memperlihatkan bahwa peneglolaan, pengawasan dan penyimpnan data nasabahnya tidak dilakukan dengan baik dan aman, sehingga data pribadi nasabah

[93] Taufik Hidayat Telaumbanua, Deasy Soeikromo, and Delasnova S. S. Lumintang, “Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif,” *Jurnal Fakultas Hukum Unsrat Lex Privatum* 13, no. 1 (2024): 11.

diretas oleh pihak luar. Karen kelalaian dalam menjaga kerahasian data tersebut. Kredit plus dianggap melakukan perbuatan melawan hukum sesuai dengan pasal 1366 KUHPerdata.

Bentuk tanggung jawab yang diterapkan oleh kredit plus adalah tanggung jawab *presumption liability*, di mana beban pembuktian terletak pada nasabah yang mengalami kebocoran data. Hal ini disebabkan oleh kesulitan dalam melakukan pembuktian ketika terjadi sengketa antara nasabah dan perusahaan atau badan hukum. Dengan demikian, nasabah harus dapat membuktikan bahwa kebocoran data tidak disebabkan oleh tindakan dirinya, baik secara langsung maupun tidak langsung, tetapi lebih kepada dugaan kelalaian dalam melindungi data pribadi nasabah serta ketidakpatuhan dalam memberikan pemberitahuan tertulis sesuai prosedur yang berlaku di Kredit Plus, dengan tetap memperhatikan ketentuan peraturan perundang-undangan. Hal ini sejalan dengan Pasal 15 UU ITE yang secara implisit mengatur model tanggung jawab tersebu.

“Pasal 15

1) Sistem penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.
2) Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya.
3) Ketentuan sebagaimana dimkasud dalam (2) tidak berlaku dalam hal dpat dibuktikan erjadinya keadaan memaksa,

kesalahan, dan atau kelalaian pihak pengguna sistem elektronik".[94]

b) Kebocoran data Bank Syariah Indonesia

Jika terjadi kebocoran data, BSI wajib bertanggung jawab dan mengambil langkah-langkah perbaikan serta pencegahan di masa kini dan masa depan. Otoritas Jasa Keuangan (OJK) telah mengeluarkan peraturan nomor 12/PJOK.03/2018 mengenai penyelenggaraan layanan perbankan digital oleh bank umum. Peraturan ini memastikan bahwa bank memiliki infrastruktur dan manajemen teknologi informasi yang memadai serta menerapkan prinsip perlindungan nasabah.

Pasal 4 UU No. 8 Tahun 1999 tentang Perlindungan Konsumen, nasabah berhak untuk dilindungi, dan pihak pengelola bank wajib melindungi serta bertanggung jawab atas perlindungan tersebut. Sebelum berlakunya UU Perlindungan Data Pribadi (UU PDP), pengaturan mengenai perlindungan data nasabah telah diatur dalam UU No. 10 Tahun 1998 yang merupakan perubahan atas UU No. 7/1992 tentang Perbankan. Peraturan ini kemudian diperbarui dengan UU No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. UU Perbankan mengatur kewajiban bank untuk menjaga kerahasiaan data nasabah, sejalan dengan ketentuan OJK dalam Surat Edaran No. 14/SEOJK.07/2014

[94] Felicia Edbert and Moody Rizqy Syailendra Putra, "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi Pada Perusahaan Pengelola Jasa Keuangan Berbasis IT," *Unes Law Review* 6, no. 2 (2023): 5966–77.

tentang kerahasiaan dan keamanan data konsumen. Di dalamnya diatur bahwa pelaku usaha jasa keuangan, termasuk BSI wajib melindungi data pribadi konsumen dan tidak boleh membagikannya kepada pihak ketiga tanpa persetujuan.

Kasus kebocoran data kredit plus dan bank syariah indonesia dalam undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi, melanggar ketetuan Pasal 12 ayat (1) jelas menyatakan bahwa setiap individu sebagai pemilik data pribadi berhak untuk mengajukan gugatan perdata dan menuntut ganti rugi atas pelanggaran dan kerugian baik material maupun non material sebagai akibat pemrosesan, pengolahan, penyimpanan data pribadi nasabah. Tuntutan dalam perbuatan melawan hukum dinilai berdasarkan kerugian, kemampuan, dan kondisi para pihak dengan mengacu pada Pasal 1365 KUHPerdata, di antaranya;

1) Tuntuntan ganti rugi dalam bentuk uang, yang didasari atas kerugian material dan/atau kerugian non material;
2) Tuntutan untuk mengembalikan keadaan ke semula/natura;
3) Tuntutan untuk menyatakan bahwa perbuatan yang dilakukan dikategorikan sebagai perbuatan melawan hukum;
4) Melarang untuk melakukan suatu perbuatan;
5) Memusnahkan dan/atau menghentikan sesuatu yang dilakukan atau diadakan secara melawan hukum; dan

6) Tuntutan kepada tergugat untuk mengumumkan keputusan atau sesuatu atau sistem yang telah diperbaiki oleh tergugat.[95]

Dengan adanya sanksi hukum dalam undang-undang ini dapat memperkuat perlindungan hukum atas data pribadi warga negara serta memberikan hukuman bagi yang melanggar. Hukuman pidana berupa penjara dan denda dalam jumlah besar dimaksudkan untuk memberikan efek jera kepada pihak-pihak yang menyalahgunakan data pribadi. Undang-Undang Perlindungan Data Pribadi, diharapkan dapat melindungi hak-hak dasar serta kebebasan warga negara terkait perlindungan data pribadi dan memberikan kepastian hukum jika terjadi pelanggaran dalam penggunaan data pribadi.

[95] M A Moegni Djojodirjo, Perbuatan Melawan Hukum, Cetakan Kedua, Jakarta : Pradnya Paramita, 1979,hlm. 102.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil pembahasan penulis mengenai Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 maka dapat ditarik kesimpulan sebagai berikut:

1. Perkembangan Teknologi Informasi di Era Digital ini telah mengubah kehidupan manusia dalam berbagai aspek, termasuk dalam pengelolaan data pribadi. Data Pribadi merupakan aset berharga yang harus dilindungi dalam era digital ini. Penyalahgunaan data pribadi dapat menimbulkan dampak serius seperti penipuan, pencurian identitas dan pelanggaran privasi. Oleh karena itu dibutuhkan regulasi yang kuat dalam melindungi data pribadi. UU PDP disusun untuk memberikan perlindungan hukum terhadap data pribadi masyarakat di era digital ini. UU ini mengatur pengumpulan, pengelolaan, dan penggunaan data pribadi serta menetapkan sanksi bagi pelanggaran data pribadi. Sebelumnya, pengaturan terkait perlindungan data pribadi tersebar dalam berbagai undang-undang sektoral tetapi tidak mengatur secara khusus mengenai perlindungan data pribadi. Kasus kebocoran data yang terjadi di Indonesia, seperti kasus Tokopedia, Kredit Plus, BPJS Kesehatan, registrasi kartu SIM, dan Bank Syariah Indonesia ini disebabkan oleh kelemahan dalam sistem keamanan perangkat lunak dan dari kesalahan manusia sendiri. kebocoran data ini menunjukkan perlunya sistem keamanan yang lebih kuat, seperti enkripsi

data, autentikasi ganda, dan pembaruan perangkat lunak secara berkala. Dengan diterapkannya UU PDP, diharapkan terjadi peningkatan dalam keamanan data pribadi, kepatuhan terhadap standar keamanan, serta pemulihan kepercayaan publik terhadap pengelolaan data. Meskipun sudah ada beberapa aturan sektoral yang secara mengatur perlindungan data pribadi, aturan tersebut masih belum sepenuhnya mampu memberikan perlindungan hukum yang maksimal dan kepastian hukum yang memadai

2. Indonesia saat ini sudah mempunyai regulasi yang khusus mengatur tentang perlindungan data pribadi. Pemerintah bersama DPR telah mengesahkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi pada 20 september 2022 dan undang-undang ini diberlakukan pada 17 Oktober 2022. Undang-Undang ini menetapkan hak dan subjek data pribadi, kewajiban bagi pengendali data untuk melindungi data pribadi, mengatur prosedur pemrosesan data, dan mengharuskan pemberitahuan jika terjadi kebocoran data. Undang-Undang PDP memberikan perlindungan hukum preventif dan represif dalam melindungi data pribadi. Perlindungan Hukum Preventif bertujuan untuk mencegah terjadinya pelanggaran dengan memberi kewajiban kepada pengendali data untuk meminta persetujuan subjek data dalam memproses data pribadinya, memberikan hak kepada subjek data untuk mengakses dan memperbarui datanya, mewajibkan pengendali data untuk melaporkan dan memberi tahu jika terjadi kebocoran data serta memberikan penyuluhan dan edukasi tentang pentingnya melindungi data pribadi dalam masyarakat. Adapun

perlindungan hukum represif yang diberikan sebagai upaya terakhir jika sudah terjadi pelanggaran atau sengketa, dapat berupa sanksi administrasi, pidana, dan perdata bagi pelanggaran terhadap data pribadi. Sanksi administrasi yang diberikan dalam UU PDP meliputi peringatan tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data, ganti kerugian atau denda administrasi. Sanksi pidana meliputi penjra 5 tahun dan denda hingga Rp 5 miliar, dengan ketentuan khusus korporasi, dapat dikenakan denda 10 kali lipat dan sanksi tambahan seperti pembekuan usaha dan pembubaran. Sanksi perdata memberikan hak kepada subjek data untuk menggugat pelaku berdasarkan Pasal 1365 dan 1366 KUHPerdata untuk memperoleh ganti rugi atas tindakan melawan hukum. Undang-undang perlindungan data pribadi memberikan kerangka hukum yang kompherensif dalam menjamin hak dan keamanan data pribadi. Akan tetapi peraturan pemeritah dan lembaga independen khusus perlindungan data pribadi masih diperlukan untuk memastikan implementasi undang-undang ini efektif.

B. Saran

1. Bagi pengguna atau pemilik data pribadi, seharusnya pada zaman sekarang kita harus dapat bertindak untuk lebih teliti dan hati-hati terutama saat menggunakan sistem elektronik yang berkaitan dengn data ptibadi. Berbagai macam informasi yang kita lepaskan saat menggunakan sistem elektronik secara online, yang awalnya hal tersebut merupakan hal yng sangat privasi tetapi setelah berada di tangan yang salah bisa saja menjadi

sesuatu yang tidak bisa disebut sebagai privasi dan dapat merugikan pemilik data pribadi tersebut.

2. Pemerintah sebaiknya segera mengupayakan menyusun peraturan turunan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi dalam bentuk Peraturan Pemerintah, serta membentuk lembaga independen khusus dalam menangani perlindungan data pribadi. Untuk memastikan implementasi yang efektif dan perlindungn hukum yang maksimal terhadap data pribadi masyarakat.

DAFTAR PUSTAKA

Buku

Al-Qur'an dan Terjemahnya, Kementerian Agama RI Bogor: Unit Percetakan Al-Qur'an, 2018

Armia, Muhammad Siddiq. "Penentuan Metode Pendekatan Penelitian Hukum."2002

Az-Zhuaili Wahbah. *Tafsir Al-Wasith, Surah An-Nur*, cet 1, Jakarta: Gema Insani

Djojodirjo, MA Moegni, and Perbuatan Melawan Hukum. "Cetakan Pertama." *Jakarta: Pradnya Paramita*, 1979.

Fujiama Diapoldo Silalahi, 'Keamanan Cyber (Cyber Security)', *Penerbit Yayasan Prima Agus Teknik*, 2002

Guntara, Bima. "Cybercrime Penghinaan dan Pencemaran Nama Baik Melalui Dunia Maya." CV.Pena Persada 2020.

Hadjon, Philipus M., and Pengantar Hukum Administrasi Indonesia, Yogyakarta.

Karo Karo, Rizky P.P and Teguh Prasetyo. *Pengaturan perlindungan data pribadi di Indonesia: perspektif teori keadilan bermartabat*. Nusa Media. 2023

Martien Dhoni, Perlindungan Hukum Data Pribadi Makassar: Mitra Ilmu, 2023

Marzuki, Peter Mahmud, *Pengantar ilmu hukum*. Prenada Media, 2021.

Muchsin, Muchsin. "Perlindungan dan Kepastian Hukum bagi Investor di Indonesia." *Universitas Sebelas Maret* 2003.

Muhaimin,"Metode Penelitian Hukum" NTB: Mataram, University Press, Juni 2020,

Rahardjo, Satjipto. *Ilmu hukum*. Citra Aditya Bakti, 2002

Rahmadi, "Pengantar metodologi penelitian." Antasri Press Banjarmasin, 2011.

Rohidin, R. "Pengantar Hukum Islam: Dari Semenanjung Arabia Hingga Indonesia (M. Nasrudin, Ed.). Yogyakarta: Lintang Rasi Aksara Books." 2016,

Rosadi, Sinta Dewi. *Cyber law: aspek data privasi menurut hukum internasional, regional, dan nasional*. Refika Aditama, 2015.

Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika, 2023.

Sabian Usman, "*Dasar-Dasar Sosiologi", Yogyakarta:Pustaka Belajar, 2009*

Sihombing, Agustinus. *Hukum Perlindungan Konsumen*. CV. Azka Pustaka, 2023.

Sugiyono, "Metode Penelitian Kuantitatif Kualitatif Dan R & D Cetakan 17." *Bandung: CV Alfabeta*, 2015.

Jurnal

Adlini, Miza Nina, et al. "Metode penelitian kualitatif studi pustaka." Jurnal Edumaspul 6.1 (2022)

Anugerah, Fiqqih, and Tantimin Tantimin. "Pencurian Data Pribadi di Internet dalam Perspektif Kriminologi." *Jurnal Komunikasi Hukum (JKH)* 8.1 (2022)

Arrasuli, Beni Kharisma, and Khairul Fahmi. "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi." *UNES Journal of Swara Justisia* 7.2 (2023)

Baiq, Parida Angriani. "Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif." *DIKTUM: Jurnal Syariah dan Hukum* 19.2, 2021

Carundeng, Refaldy Braif. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik." *Lex Privatum* 10.1 (2022).

Christine, Bella, and Christine ST Kansil. "Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Syntax Literate; Jurnal Ilmiah Indonesia* 7.9 (2022)

Djafar, Wahyudi, and Asep Komarudin. "Perlindungan Privasi di Internet: Beberapa Penjelasan Kunci." *Seri Internet dan HAM, Jakarta: ELSAM* (2014).

Djafar, Wahyudi. "Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan." *Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*.

DM, Mohd Yusuf, et al. "Tinjauan Yuridis Faktor-Faktor Yang Mempengaruhi Efetivitas Penegakan Hukum Di Masyarakat." *JPIn: Jurnal Pendidik Indonesia* 5.2 (2022)

Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen." *National Conference on Law Studies (NCOLS)*. Vol. 2. No. 1. 2020.

Fauzy, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7.3 (2022)

Gabriel, Alza. "Perlindungan Hukum Atas Data Pribadi Dalam Kasus Kebocoran Data Pusat Data Nasional Sementara (Pdns) Dalam Perspektif Hukum Pidana." *Seminar Nasional-Hukum dan Pancasila*. Vol. 3. No. 3. 2024.

Gunadi, Chaterine Grace, et al. "Perlindungan Hukum Atas Kebocoran Data Pribadi." *Proceeding of Conference on Law and Social Studies*. Vol. 4. No. 1. 2023.

Hisbulloh, Moh Hamzah. "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi." *Jurnal Hukum* 37.2 (2021)

Indriana Firdaus, 'Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan', Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia, 4.2 (2022), pp. 23-31, doi:10.52005/rechten.v4i2.98.

Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2.1 (2021)

Kusuma, Aditama Candra, and Ayu Diah Rahmani. "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)." *SUPREMASI: Jurnal Hukum* 5.1 (2022)

Mutiara, Upik, and Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies* 1.1, 2020

Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7.1. 2020

Nurhana, Anggianti, and Yana Indawati. "Perlindungan Hukum atas Data Pribadi Pengguna SIM Card Telepon Seluler." *Amnesti: Jurnal Hukum* 5.1 (2023)

Orlando, Galih. "Efektivitas Hukum dan Fungsi Hukum di Indonesia." *Tarbiyah bil Qalam: Jurnal Pendidikan Agama dan Sains* 6.1 (2022).

Pradana, Muhammad Akbar Eka, and Horadin Saragih. "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya." *Innovative: Journal Of Social Science Research* 4.4 (2024)

Prasetyo, Teguh, and Jamalum Sinambela Sinambela. "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat." *Spektrum Hukum* 20.1 (2023)

Pratiwi, Sevia Diah, and Muhammad Irwan Padli Nasution. "Penegakan Hukum Terhadap Keamanan Data Privasi Pada Media Sosial Di Indonesia." *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen* 1.3 2023

Prianto, Yuwono, Nabila Annisa Fuzain, and Afif Farhan. "Kendala Penegakan Hukum Terhadap Cyber Crime Pada Masa Pandemi Covid-19." *Prosiding SENAPENMAS* (2021)

Prihatin, Lilik, Muhammad Achwan, and Citra Candra Dewi. "Kajian Yuridis Regulasi Perlindungan Hukum Terhadap Penyalahgunaan Data Privasi dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *UNES Law Review* 5.4 (2023)

Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com)." *Borneo Law Review* 5.1 (2021)

Rizal, Muhammad Saiful. "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia." *Jurnal Cakrawala Hukum* 10.2 (2019)

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4.1 2018

Satria, Muhammad, and Susilo Handoyo. "Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia." *Journal de Facto* 8.2. 2022

Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9.2 (2020)

Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia." *Jurnal Analisis Hukum* 6.1 (2023)

Telaumbanua, Taufik Hidayat. "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif." *Lex Privatum* 13.1. 2024.

Triadi, Muhammad. "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital." Reusam: Jurnal Ilmu Hukum 11.1. 2023.

Widyaningsih, Tika, and Suryaningsi. "Kajian Perlindungan Hukum Terhadap Data Pribadi Digital Anak Sebagai Hak Atas Privasi di Indonesia." *Nomos: Jurnal Penelitian Ilmu Hukum* 2.3. 2022.

Wulansari, Eka Martiana. "Konsep Perlindungan Data Pribadi sebagai Aspek Fundamental Norm dalam Perlindungan terhadap Hak atas Privasi Seseorang di Indonesia." Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan 7.2 (2020)

Yamin, Ahmad Fachri, et al. "Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi." Meraja journal 7.2 (2024): 138-155.

Yudistira, Muhammad, and Ramadani Ramadani. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO." UNES Law Review 5.4..2023

Yuniarti, Siti. "Perlindungan hukum data pribadi di Indonesia." *Business Economic, Communication, and Social Sciences Journal (Becoss)* 1.1 (2019)

Zahwani, Syfa Tasya, and Muhammad Irwan Padli Nasution. "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital." *Journal of Sharia Economics Scholar (JoSES)* 2.2 (2024).

Skripsi

Navis, Aulia Akbar. *Perlindungan data pribadi menurut undang-undang nomor 27 tahun 2022 dan perspektif Siyasah Syar'iyyah: studi di Dinas Komunikasi dan Informatika Kota Malang*. Diss. Universitas Islam Negeri Maulana Malik Ibrahim, 2023.

Mubarok, Muhammad Fikri. *Tinjauan Yuridis Perlindungan Hukum Terhadap Data Pribadi Berdasarkanundang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Diss. Unusia, 2021.

Naufal, Ramiz Afif. "*Tanggung Jawab PT Tokopedia dalam Kasus Kebocoran Data Pribadi Pengguna.*" (2020).

Peraturan Undang-Undang

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Eektronik

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik

Undang -Undang Nomor 24 Tahun 2013 Tentang Perubahan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

Undang-Undang Nomor 10 tahun 1998 tentang Perbankan

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 24 tahun 2008 tentang Keterbukaan Informasi Publik

Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi
Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia
Undang-Undang Nomor 8 tahun tentang Perlindungan Konsumen

Website

https://app.cnnindonesia.com/https://www.cnnindonesia.com/teknologi/20240702104538-192-1116574/data-diklaim-dari-pdn-2021-2024-dijual-rp198-m-di-forum-gelap
https://bit.telkomuniversity.ac.id/transformasi-digital-tren-dan-tantangan-di-era-teknologi-informasi/
https://ilmuislam.id/hadits Di Akses Pada Tanggal 09 November
https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data yang-terjadi-
https://www.beritasatu.com/ototekno/2784168/deretan-kasus-kebocoran-data-yang-pernah-terjadi-di-indonesia-selama-2023
https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/
https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-banta
https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/
https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=2

DAFTAR RIWAYAT HIDUP

Nur Alfiana Alfitri, lahir di palopo pada tanggal 15 juni 2002. Penulis merupakan anak kedua dari tiga bersaudara dari pasangan seorang ayah bernama Muh. Alfitri Lencing dn Ibu Juriana. Saat ini penulis bertempat tinggal di Jl. Salutete, Kelurahan Pentojangan, Kecamatan Telluwanua Kota Palopo. Pendidikan Dasar penulis dimulai pada tahun 2008 dan diselesaikan pada tahun 2014 di SDN 486 Salutete. Kemudian, di tahun yang sama menempuh pendidikan di SMP 9 Palopo hingga 2017. Pada tahun 2017 melanjutkan pendidikan di MAN Palopo. Pada saat menempuh pendidikan di MAN, penulis aktif mengikuti kegiatan ekstrakulikuler PMR (Palang Merah Remaja). Setelah lulus SMA di tahun 2020, penulis melanjutkan pendidikan yang ditekuni yaitu di Program studi Hukum Tata Negara Fakultas Syari'ah Institusi Agama Islam Negeri (IAIN) Palopo.

Contract person penulis: *nuralfianaalfitri@gmail.com*