

KEPASTIAN HUKUM PIDANA TERHADAP KEBOCORAN DATA PRIBADI PADA MARKETPLACE

Skripsi

*Diajukan Untuk Memenuhi Salah Satu Syarat Guna Memperoleh Gelar
Sarjana Hukum (S.H) pada Program Studi Hukum Tata Negara (Siyasah)
Fakultas Syariah Universitas Islam Negeri Palopo*



Diajukan Oleh:

SIDAR SAPUTRI
20 0302 0108

**PROGRAM STUDI HUKUM TATA NEGARA (SIYASAH)
FAKULTAS SYARIAH
UNIVERSITAS ISLAM NEGERI PALOPO
2025**

KEPASTIAN HUKUM PIDANA TERHADAP KEBOCORAN DATA PRIBADI PADA MARKETPLACE

Skripsi

*Diajukan Untuk Memenuhi Salah Satu Syarat Guna Memperoleh Gelar
Sarjana Hukum (S.H) pada Program Studi Hukum Tata Negara (Siyasah)
Fakultas Syariah Universitas Islam Negeri Palopo*



Diajukan Oleh:

SIDAR SAPUTRI
20 0302 0108

Pembimbing:

1. **Dr. H. Firman Muhammad Arif, Lc., M.HI.**
2. **Fitriani Jamaluddin, S.H., M.H.**

**PROGRAM STUDI HUKUM TATA NEGARA (SIYASAH)
FAKULTAS SYARIAH
UNIVERSITAS ISLAM NEGERI PALOPO
2025**

HALAMAN PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini :

Nama	: Sidar Saputri
NIM	: 20 0302 0108
Fakultas	: Syariah
Program Studi	: Hukum Tata Negara (Siyasah)

Menyatakan dengan sebenarnya dengan :

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

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

Demikian pernyataan ini di buat untuk dipergunakan sebagaimana mestinya.

Palopo, 25 Agustus 2025

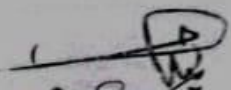

Sidar Saputri
NIM. 2003020108

HALAMAN PENGESAHAN

Skripsi berjudul "*Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace* " yang ditulis oleh *Sidar Saputri*, Nomor Induk Mahasiswa (NIM) 20 0302 0108, mahasiswa Program Studi Hukum Tata Negara (siyasah) Fakultas Syariah Universitas Islam Negeri Palopo, yang dimunaqasyahkan pada hari *Senin, 29 September 2025*, bertepatan dengan *7 Rabi'ul Akhir 1447 H*, dan telah diperbaiki sesuai cacatan dan permintaan Tim Penguji, dan diterima sebagai syarat meraih gelar Sarjana Hukum (S.H).

Palopo, 06 Oktober 2025

TIM PENGUJI

1. Dr. Muhammad Tahmid Nur, M.Ag.	Ketua Sidang	()
2. Dr. Fasiha, S.E.I., M.E.I.	Sekretaris Sidang	()
3. Ilham, S.Ag., M.A	Penguji I	()
4. Firmansyah, S.Pd., S.H., M.H.	Penguji II	()
5. Dr. H. Firman Muhammad Arif, Lc., M.HI.	Pembimbing I	()
6. Fitriani Jamaluddin, S.H., M.H	Pembimbing II	()

Mengetahui:

a.n Rektor UIN Palopo
Dekan Fakultas Syariah



Ketua Program Studi
Hukum Tata Negara (siyasah)



PRAKATA

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ وَالصَّلَاةُ وَالسَّلَامُ عَلَى أَشْرَفِ الْأَنْبِيَاءِ وَالْمُرْسَلِينَ سَيِّدِنَا مُحَمَّدٍ
وَعَلَى آلِهِ وَأَصْحَابِهِ أَجْمَعِينَ أَمَّا بَعْدُ

Alhamdulillah segala puji dan syukur penulis panjatkan kepada Allah Swt yang telah menganugerahkan rahmat, hidayah, dan karunia-Nya, serta kekuatan lahir batin, sehingga peneliti dapat menyelesaikan penulisan skripsi ini dengan judul **“Kepastian Hukum Pidana terhadap Kebocoran Data Pribadi pada *Marketplace*”** setelah melalui proses yang panjang.

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

Terkhusus kepada kedua orang tua saya tercinta Bapak Ridwan dan Ibu Sinar. sosok yang luar biasa hebat, dua orang yang sangat berjasa dalam hidup saya, yang selalu mengusahakan anak pertamanya ini menempuh pendidikan setinggi-tingginya. Dua orang yang selalu menjadi sumber semangat terkuat dalam menghadapi kerasnya kehidupan, yang selama ini merawat, membesarkan, mendidik, serta terus menerus memberikan kasih dengan penuh cinta, dukungan, motivasi, serta doa yang tulus demi pendidikan penulis. Terimakasih telah

berjuang demi kehidupan penulis. Terimakasih atas kasih sayang tanpa batas yang tak pernah lekang oleh waktu, atas kesabaran dan pengorbanan yang selalu mengiringi perjalanan hidup saya, terimakasih telah menjadi sumber kekuatan dan inspirasi, serta pelita yang tak pernah padam dalam setiap langkah yang saya tempuh. Terakhir, terimakasih atas segala hal yang kalian berikan yang tak terhitung jumlahnya. Untuk adik saya Syahrul terimakasih atas dukungan dan selama ini membantu mendoakanku. Semoga Allah SWT, mengumpulkan kita semua dalam surganya kelak. Serta penulis menyampaikan ucapan terimakasih yang tak terhingga dengan penuh ketulusan hati dan keikhlasan, kepada:

1. Rektor IAIN Palopo Bapak Dr. Abbas Langaji, M.Ag., beserta Wakil Rektor I Bapak Dr. Munir Yusuf, M.Pd. Wakil Rektor II Bapak Dr. Masruddin, S.S., M.Hum. dan Wakil Rektor III Bapak Dr. Takdir, S.H.,M.H.
2. Dekan Fakultas Syariah Bapak Dr. Muhammad Tahmid Nur, M.Ag. beserta Wakil Dekan I Ibu Dr. Fasiha, S.E.I.,M.E.I. Wakil Dekan II Bapak Muh. Akbar, S.H.,M.H. dan Wakil Dekan III Bapak Muh. Darwis, S.Ag., M.Ag. Fakultas Syariah IAIN Palopo
3. Ketua Program Studi Hukum Tata Negara (Siyasah) IAIN Palopo Ibu Nirwana Halide, S.HI.,M.H. dan Sekretaris Prodi Hukum Tata Negara Bapak Firmansyah, S.Pd.,S.H.,M.H beserta staf yang telah membantu dan mengarahkan dalam penyelesaian skripsi.
4. Pembimbing I skripsi tugas akhir Bapak Dr. H. Firman Muhammad Arif, Lc., M.HI. dan Pembimbing II Ibu Fitriani Jamaluddin, S.H., M.H. yang telah memberikan bimbingan, masukan dan mengarahkan dalam rangka

penyelesaian skripsi.

5. Penguji I Bapak Ilham, S.Ag., M.A dan Penguji II Bapak Firmasyah, S.Pd., S.H.,M.H yang telah banyak memberi arahan untuk menyelesaikan skripsi ini.
6. Dosen Penasehat Akademik Ibu Dr.Dirah Nurmila Siliwadi, S.KM., M.H.
7. Seluruh Dosen beserta seluruh staf pegawai UIN Palopo yang telah mendidik penulis selama berada di UIN Palopo dan memberikan bantuan dalam penyusunan skripsi ini.
8. Kepala Unit Perpustakaan Bapak Zainuddin S.,S.E.,M.Ak. beserta Karyawan dan Karyawati dalam ruang lingkup UIN Palopo, yang telah banyak membantu, khususnya dalam mengumpulkan literatur yang berkaitan dengan pembahasan skripsi ini.
9. Kepada sahabat-sahabatku, Mayumi Fabrianti Pajar, Beby Zahara Mattaja, Elsiana Anwar, Rabiatul adawiah, Ayu Andira dan Imelia. Terimakasih atas semangat yang tidak pernah putus, dukungan, nasehat, serta motivasi yang kalian berikan. Terimakasih karena selalu ada untuk mendengarkan keluhan kesah dan menjadi tempat berbagi cerita, sehingga penulis dapat menyelesaikan skripsi ini.
10. Teman seperjuangan yakni Tendry Nuraden, Siti Nursyifahun Linnas, Frihartini Ro'ren, Helmalia Hermadi, Andi Wahida Mahmud, dan seluruh mahasiswa Program Studi Hukum Tata Negara (Siyasah) IAIN Palopo angkatan 2020 yang selama ini membantu dan selalu memberikan saran dalam penyusunan skripsi ini.

11. Teman-teman KKN Desa Bone Pute Kecamatan Burau Kabupaten Luwu Timur Angkatan tahun 2023 yang selama ini membantu, mendukung dan selalu memberikan saran dalam penyusunan skripsi.

12. Terakhir, untuk diri saya sendiri, seorang anak sulung berusia 23 tahun. Terimakasih sudah bertahan sejauh ini. Terimakasih sudah memilih berusaha dan merayakan diri sendiri sampai titik ini, walaupun kadang merasa putus asa atas apa yang diusahakan dan belum berhasil, namun terimakasih karena memutuskan untuk tidak menyerah sesulit apapun proses penyelesaian skripsi ini dan telah menyelesaikan sebaik dan semaksimal mungkin, ini merupakan pencapaian yang patut dirayakan untuk diri sendiri.

Terimakasih kepada semua pihak yang telah membantu, membimbing dan mendukung selama penulisan skripsi ini. Mudah-mudahan bernilai ibadah dan mendapatkan pahala dari Allah Swt. Aamiin.

Palopo, 18 Februari 2025

Penulis



Sidar Saputri

PEDOMAN TRANSLITERASI ARAB-LATIN DAN SINGKATAN

A. Transliterasi Arab-Latin

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

1. Konsonon

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	-	-
ب	Ba	B	Be
ت	Ta	T	Te
ث	Ṣa [“]	Ṣ	es (dengan titik di atas)
ج	Jim	J	Je
ح	Ḥa [“]	Ḥ	ha (dengan titik di bawah)
خ	Kha	Kh	ka dan ha
د	Dal	D	De
ذ	Ẓal	Z	zet (dengan titik di atas)
ر	Ra	R	Er
ز	Zal	Ẓ	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	Za	Z	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	Ei
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
ء	Hamzah	“	Apostrof
ي	Ya	Y	Ye

Hamzah (ء) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apa pun. 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 monoftong dan vokal rangkap atau diftong. Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harakat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin	Nama
َ	<i>Fathah</i>	A	A
ِ	<i>Kasrah</i>	I	I
ُ	<i>Dammah</i>	U	U

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

Tanda	Nama	Huruf Latin	Nama
اِي	<i>Fathah dan yā''</i>	Ai	a dan i
او	<i>Fathah dan wau</i>	Au	a dan u

Contoh:

كَيْفَ *Kaifa*
 حَوْلَ *Haula*

3. Maddah

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

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
أ.....ى	<i>fathah</i> dan <i>alif</i> atau <i>yā</i> ''	Ā	Adan garis diatas
يِ	<i>Kasrah</i> dan <i>yā</i> '''	Ī	Idan garis diatas
وُ	<i>Dammah</i> dan <i>wau</i>	Ū	Udan garis diatas

Contoh :

مَاتَ	<i>Māta</i>
رَمَى	<i>Ramā</i>
قِيلَ	<i>Qīla</i>
يَمُوتُ	<i>Yamūtu</i>

4. Ta marbūṭah

Alih aksara untuk ta marbūṭah (ة atau ة) ada dua, yaitu: ta marbūṭah yang hidup atau mendapat harakat *fathah*, *kasrah*, dan *dammah* dengan t sedangkan ta marbūṭah yang mati atau mendapat harkat sukun dengan h.

Kalau pada kata yang berakhir dengan ta marbūṭah diikuti oleh kata yang menggunakan kata sandang al- serta bacaan kedua kata itu terpisah, ta marbūṭah itu dialihaksarakan dengan h.

الأَطْفَالِ رَوْضَةَ	<i>Rauḍah al-atfāl</i>
الْفَاضِلَةُ الْمَدِينَةِ	<i>Al-madīnah al-fāḍilah</i>
الْحِكْمَةُ	<i>Al-ḥikmah</i>

5. Syaddah (Tasydid)

Syaddah atau tasydid yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda tasydid (ّ), dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda syaddah.

رَبَّنَا *Rabbanā*

جَيْنَانَا *Najjainā*

الْحَقُّ *Al-Ḥaqq*

الْحَجُّ *Al-Ḥajj*

نُعَمُّ *Nu‘ima*

عَدُوُّ *‘Aduww*

Jika huruf ي bertasydid di akhir sebuah kata dan didahului oleh huruf kasrah (ِ), ia dialihaksarakan seperti huruf maddah ī.

Contoh:

عَلِيٌّ *‘Alī*

بِيْعَر *‘Arabī*

6. Kata Sandang

Kata sandang dalam abjad Arab dilambangkan dengan huruf ال (*alif ma‘arifah*). Dalam pedoman alih aksara ini, kata sandang dialihaksarakan biasa, al-, baik ketika ia diikuti oleh huruf *syamsiah* maupun huruf *qamariah*. Kata sandang tidak mengikuti bunyi huruf langsung yang mengikutinya.

sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan garis mendatar (-).

Contoh:

الشَّمْسُ	<i>Al-Syamsu</i> (bukan <i>asy-syamsu</i>)
الزَّلْزَلَةُ	<i>Al-Zalزالah</i> (bukan <i>az-</i>
الْفَلْسَفَةُ	<i>Al-Falsafah</i>
الْبِلَادُ	<i>Al-Bilād</i>

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 dilambangkan, karena dalam tulisan ~~Arab~~ **Arab** berupa alif.

تَأْمُرُونَ	<i>Ta'murūna</i>
النَّوْءُ	<i>An-Nau'</i>
سَيِّءٌ	<i>Syai'un</i>
أَمْرٌ	<i>Umirtu</i>

8. Penulisan Kata Arab yang Lazim Digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, kalimat yang belum dibakukan dalam bahasa Indonesia. Kata, istilah atau yang sudah lazim dan menjadi bagian dari perbendaharaan bahasa

sering ditulis dalam tulisan bahasa Indonesia, atau lazim digunakan dalam akademik tertentu, tidak lagi ditulis menurut cara transliterasi di atas. kata al-Qur'an (dari al-Qur'a>n), alhamdulillah, dan munaqasyah. Namun, kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka ditransliterasi secara utuh.

Contoh:

- Fī Zilāl al-Qur'ān,
- Al-Sunnah qabl al-tadwīn, dan
- Al-'Ibārāt bi 'umūm al-lafz lā bi khuṣūṣ al-sabab.

9. Lafz al-Jalālah (الله)

Lafz al-jalālah (lafal kemuliaan) “Allah” (الله) yang didahului partikel seperti huruf jarr dan huruf lainnya atau berkedudukan sebagai muḍāf ilaih (frasa nominal), dialihaksarakan tanpa huruf hamzah (hamzah wasal).

Contoh:

الله دِينُ *Dīnullāh*

بِالله *Billāh*

Adapun ta marbutah di akhir kata yang disandarkan kepada *lafz al-* dialihaksarakan dengan huruf *t*.

Contoh:

ال رَحْمَةِ فِي هُمْ *Hum fī rahmatillāh*

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 didahului 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).

- *Wa mā Muḥammadun illā rasūl*
- *Inna awwala baitin wuḍi‘a linnāsi lallaẓī bi Bakkata mubārakan*
- *Syahru Ramaḍān al-laẓī unzila fīh al-Qur’ān*
- *Naṣīr al-Dīn al-Ṭūsī*
- *Abū Naṣr al-Farābī*
- *Al-Gazālī*
- *Al-Munqiz min al-Ḍalāl*

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

Abū al-Walid Muhammad ibn Rusyad, ditulis menjadi: Ibnu Rusyd, Abū al-Walid Muhammad (bukan: Rusyd, Abū al-Walid Muhammad Ibnu)

Naṣr Hāmid Abū Zaīd, ditulis menjadi: Abū Zaīd, Naṣr Hāmid (bukan: Zaīd, Naṣr Hāmid Abū)

B. Daftar Singkatan

Beberapa singkatan yang dibakukan adalah:

swt	= <i>subḥānahū wa ta'' ālā</i>
saw	= <i>ṣallallāhu'alaihi wa salām</i>
a.s	= <i>alaihi al-salām</i>
H	=Hijrah
M	=Masehi
SM	=Sebelum Masehi
1	= Lahir tahun (untuk orang yang masih hidup saja)
W	=Wafat Tahun
QS.../...:8	= QS al-Maidah/5: 8 atau QS Ād „Dzāriyāt /51: 56
HR	=Hadis Riwayat

DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	ii
HALAMAN PERNYATAAN KEASLIAN.....	iii
PRAKATA.....	iv
PEDOMAN TRANSLITERASI ARAB-LATIN DAN SINGKATAN	viii
DAFTAR ISI.....	xvii
DAFTAR AYAT.....	xix
DAFTAR HADIS	xx
DAFTAR GAMBAR.....	xxi
ABSTRAK	xxii
BAB I PENDAHULUAN.....	1
A. Latar Belakang	1
B. Rumusan Masalah	9
C. Tujuan Penelitian	9
D. Manfaat Penelitian	9
E. Penelitian Terdahulu yang Relevan	10
F. Kajian Pustaka.....	13
G. Kerangka Pikir	18
H. Metode Penelitian.....	19
BAB II DATA PERLINDUNGAN PRIBADI DI INDONESIA	22
A. Ruang Lingkup Perlindungan Data Pribadi	22
B. Kasus Kebocoran Data Pribadi	42

BAB III KEPASTIAN HUKUM PERLINDUNGAN DATA PRIBADI	
DI INDONESIA	61
A. Teori Kepastian Hukum	61
B. Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen	63
C. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).....	66
D. Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.....	70
E. Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.....	72
BAB IV TINJAUAN FIKHI JINAYAH TERHADAP KEBOCORAN DATA PRIBADI	78
A. Kajian Fikih Jinayah Terkait Perlindungan Data Pribadi	78
BAB V PENUTUP	86
A. Kesimpulan	86
B. Saran.....	87
DAFTAR PUSTAKA.....	89

DAFTAR AYAT

Kutipan Q.S An-Nisa/4:58.....	6
-------------------------------	---

DAFTAR HADIS

Hadis 1 Hadis tentang Hak Kekayaan	6
--	---

DAFTAR GAMBAR

Gambar 1.1 Jumlah Kasus Kebocoran Data Pribadi	4
Gambar 1.2 Kerangka Pikir.....	20
Gambar 2.1 Negara Dengan Kebocoran Data Terbesar 2020-2024	28
Gambar 2.2 Jumlah <i>Marketplace</i> dengan Pengunjung Terbanyak Tahun 2023	30
Gambar 2.3 Syarat dan Ketentuan Aplikasi <i>Marketplace Shopee</i>	42

ABSTRAK

Sidar Saputri, 2025, “Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi pada *Marketplace*”. Skripsi Program Studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo. Dibimbing oleh Dr. H. Firman Muhammad Arif dan Fitriani Jamaluddin.

Skripsi ini membahas tentang Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi pada *Marketplace*. Yang bertujuan untuk mengetahui, 1) fakta dan data tentang penerapan Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi setelah diundangkan sampai sekarang, 2) kepastian hukum pidana terhadap kebocoran data pribadi, 3) tinjauan fiqhi jinayah terhadap kebocoran data pribadi. Jenis penelitian yang digunakan adalah penelitian hukum normatif dengan melalui pendekatan perundang-undangan (*statute approach*). Pengumpulan data yang digunakan dalam penelitian ini yaitu mengumpulkan informasi serta data dengan bantuan berbagai macam material seperti, buku referensi, hasil penelitian terdahulu yang sejenis, artikel, catatan, serta berbagai jurnal yang berkaitan dengan penelitian. Hasil penelitian menunjukkan bahwa kebocoran data pribadi pada marketplace masih sering terjadi, seperti kasus Tokopedia dan Facebook, meskipun regulasi khusus telah disahkan melalui Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kendala utama terdapat pada lemahnya pemahaman masyarakat, minimnya regulasi turunan, serta keterbatasan kapasitas aparat penegak hukum. Sanksi pidana yang diatur, baik berupa pidana penjara maupun denda, dimaksudkan untuk memberikan efek jera, namun implementasinya masih belum optimal. Dari perspektif fikih jinayah, kebocoran data pribadi dipandang sebagai bentuk pelanggaran terhadap hak milik dan amanah, sehingga pelaku dapat dikenai sanksi "ta'zīr" sesuai tingkat kerugian yang ditimbulkan. Penelitian ini menyimpulkan bahwa perlindungan hukum pidana terhadap kebocoran data pribadi di marketplace membutuhkan konsistensi penegakan, penguatan regulasi, serta peningkatan literasi digital masyarakat. Dengan demikian, hukum nasional dan prinsip fikih jinayah dapat berjalan seiring dalam menjaga keamanan data pribadi di era digital.

Kata Kunci : Hukum Pidana, Data Pribadi, *Marketplace*

ABSTRACT

Sidar Saputri, 2025, "Legal Certainty in Criminal Law Regarding Personal Data Breach in Marketplaces." Undergraduate Thesis, Constitutional Law Study Program, Faculty of Sharia, State Islamic Institute of Palopo. Supervised by Dr. H. Firman Muhammad Arif and Fitriani Jamaluddin.

This thesis discusses the certainty of criminal law on personal data leaks in the marketplace. Which aims to find out, 1) facts and data on the application of Law Number 27 of 2022 concerning Protection of Personal Data After being enacted until now, 2) Criminal Legal Certainty of Personal Data Leaks, 3) Jinayah Fiqhi Review of Personal Data Leaks. The type of research used is normative legal research through the statute approach (statute approach). Data collection used in this study is to collect information and data with the help of various kinds of materials such as reference books, previous research results, articles, notes, and various journals related to research. The results showed that the leakage of personal data in the marketplace still often occurred, such as the case of Tokopedia and Facebook, although special regulations have been passed through Law No. 27 of 2022 concerning Protection of Personal Data. The main obstacles are in the weak understanding of the community, the lack of derivative regulations, and the limited capacity of law enforcement officials. Criminal sanctions regulated, both in the form of imprisonment or fines, are intended to provide a deterrent effect, but the implementation is still not optimal. From the perspective of Jinayah Jinayah, leakage of personal data is seen as a form of violation of property rights and trust, so that the perpetrators can be subject to "ta'zīr" sanctions according to the level of losses caused. This study concluded that the protection of criminal law against leakage of personal data in the marketplace requires consistency of enforcement, strengthening regulations, and increasing digital literacy of the community. Thus, national law and principles of Jinayah fiqh can run in hand in hand in maintaining the security of personal data in the digital age.

Keywords : Criminal Law, Personal Data, *Marketplace*

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan belanja online atau biasa disebut *E-Commerce* melalui aplikasi *marketplace* di Indonesia saat ini berkembang semakin pesat. Hal ini dilihat dari banyaknya pengguna yang memulai bisnisnya dari media sosial, yang mana perkembangan ini tidak lepas dari pengaruh teknologi yang semakin maju. *Multi-peran* internet dalam dunia *online-shop* memberikan kemudahan bagi konsumen dalam melakukan jual beli dikarenakan dengan belanja online konsumen dapat dengan mudah, cepat berbelanja dimana dan kapan saja melalui aplikasi *marketplace* tanpa tatap muka. Perilaku aplikasi ini yang bervariasi dan beragam memberikan penawaran yang menggiurkan dengan berbagai model gambar dengan desain yang menarik, tawaran harga fantastik dengan diskon yang luar biasa, dan mudah dijangkau melalui *smartphone*, maka *marketplace online-shop* memanjakan penggunanya dengan penawaran-penawaran yang terbaik untuk menarik para konsumen dalam berbelanja.¹

Salah satu dampak yang harus diperhatikan dalam penggunaan aplikasi *marketplace* sendiri yaitu kebocoran data pribadi individu. Kebocoran data adalah suatu kejadian dimana informasi sensitif yang bersifat rahasia seperti nama, nomor telepon, alamat, usia, agama, dan data akun (*username* dan *password*) secara tidak sengaja diungkapkan oleh pihak yang tidak berwenang. Hal ini dapat terjadi dari

¹ G Harwida et al., "Edukasi Mahasiswa Dalam Kapabilitas Belanja Online Melalui Marketplace," *Journal.Unublitar.Ac.Id* 7, no. 2 (2023): 266–74, http://journal.unublitar.ac.id/pendidikan/index.php/Riset_Konseptual/article/view/713.

beberapa faktor yaitu serangan *siber* seperti peretasan, keamanan dalam sistem lemah, dimana dampak yang terjadi dari kebocoran data ini sangat merugikan, termasuk dalam hal finansial, dan kerusakan reputasi.

Aturan tentang Perlindungan Data Pribadi (PDP) saat ini diatur dalam Undang-Undang Nomor 27 tahun 2022. Data pribadi adalah setiap data seseorang baik yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik.² Data pribadi dibagi dalam dua jenis. Pertama, data pribadi bersifat umum seperti nama, jenis kelamin, kewarganegaraan, agama, atau data yang di kombinasikan untuk mengidentifikasi seseorang. Kedua, data pribadi yang bersifat spesifik, yang meliputi data informasi kesehatan, data genetika, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya yang sesuai dengan ketentuan undang-undang. Informasi data seseorang merupakan hal yang sangat rahasia sehingga dalam penggunaannya diperlukan kehati-hatian agar seseorang tidak dapat menyalahgunakannya. Keamanan data pribadi konsumen sangatlah berpengaruh terhadap berbelanja online, hal ini dapat menjamin integritas, kerahasiaan, otentifikasi dan tanpa pencatatan transaksi yang dapat merugikan konsumen.³

² Kementerian komunikasi dan informasi, Bersama lindungi data pribadi di platform digital, Diakses pada 3 Agustus, kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel#:~:text=Data%20pribadi%2C%20dalam%20RUU%20PDP,sistem%20elektronik%20dan%20fatau%20nonelektronik.

³ Almira Putri Aryani, Liana Endah Susanti, "Pentingnya perlindungan data pribadi konsumen dalam transaksi online pada marketplace terhadap kepuasan konsumen", Ahmad Dahlan Legal Perspective, Volume 02, (2022).

Perlindungan data pribadi hadir dalam tata kelola hukum seperti perangkat hukum berwujud regulasi dan aksi dari struktur hukum yang mengawasi jika terjadi adanya ketimpangan. Akan tetapi regulasi yang ada tentang perlindungan data pribadi bersifat sektoral sehingga kebocoran data pribadi sering terjadi dan terus berulang.⁴ Perlindungan data pribadi sangat penting karena dapat dilihat dari beberapa aspek yaitu, mengenai privasi individu, pencegahan penyalahgunaan identitas, keamanan finansial, dan kepercayaan publik. Perlindungan data pribadi bukan hanya tanggung jawab individu, tetapi juga organisasi dan Pemerintah untuk memastikan data tersebut dijaga dengan aman dan digunakan secara etis. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan hukum terhadap data pribadi karena merupakan bagian dari hak asasi manusia dan wajib dilindungi.

Aturan tentang Perlindungan Data Pribadi memang sudah ada, namun kasus kebocoran data pribadi tersebut masih marak terjadi, dimana pada Mei 2020, sekitar 91 juta pengguna akun Tokopedia bocor dan diperjualbelikan di forum gelap, data tersebut yang bocor meliputi informasi pribadi seperti, nama, nomor telepon, email, dan kata sandi yang telah diubah. contoh kasusnya yakni yang terjadi pada aplikasi facebook *marketplace* dimana seorang pengguna forum *hacker* membocorkan 200 ribu data nomor ponsel, Alamat email, dan informasi pribadi lainnya yang di publikasikan di forum *hacker* dark web.⁵ Kebocoran tersebut menimbulkan resiko serius bagi para pengguna, terutama

⁴ Muhammad Saifullah Chania Firman Muhammad Arif, "Aktualisasi standar penalaran filosofis dalam perlindungan data pribadi," *Jurnal Studi Islam* Vol. 11. No.1 (2022).

⁵ Iskandar, "200 Ribu Data Pengguna Facebook Bocor Di Forum Hacker," *Liputan6*, 2024, <https://www.liputan6.com/tekno/read/5528128/200-ribu-data-pengguna-facebook-marketplace-bocor-di-forum-hacker>.

dalam hal acaman *phising*⁶ dan potensi pencurian identitas. Namun hingga saat ini *meta*, perusahaan induk facebook, belum memberikan tanggapan resmi terkait kebocoran tersebut. Hal ini menambah kekhawatiran para pengguna, mengingat bahwa ini bukan kali pertama Facebook mengalami masalah kebocoran data besar-besaran. Para ahli keamanan *siber* menyarankan pengguna untuk lebih waspada, misalnya dengan menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan berhati-hati terhadap email atau pesan yang mencurigakan yang mungkin merupakan upaya *phishing*.⁷

Berdasarkan data kemenkominfo, jumlah kasus perlindungan data pribadi yang ditangani cenderung mengalami kenaikan. Hal ini dapat dilihat dari Januari sampai 14 Mei 2024, yang mana mayoritas jenis pelanggaran tersebut berupa kebocoran data pribadi.⁸ Berikut jumlah peningkatan kasus yang terjadi pada kebocoran data pribadi:



Gambar 1.1 Jumlah kasus kebocoran data pribadi (2020-2024)

⁶ *Phising* merupakan kejahatan online berupa penipuan yang dilakukan dengan menyamar sebagai orang terpercaya untuk mencuri informasi pengguna.

⁷ CNN Indonesia, "200 Ribu Data Pengguna Facebook Marketplace Bocor Di Forum Hacker," 2024, <https://www.cnnindonesia.com/teknologi/20240215145425-192-1063044/200-ribu-data-pengguna-facebook-marketplace-bocor-di-forum-hacker>.

⁸ Mediana, "Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024," KOMPAS, 2024, <https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024>.

Dari grafik diatas memperlihatkan bahwa jumlah kasus kebocoran data pribadi di Indonesia mengalami peningkatan yang signifikan. Peningkatan ini menunjukkan adanya kelemahan mendasar dalam tata kelola perlindungan data pribadi, baik pada tingkat regulasi, pengawasan, maupun penerapan sistem keamanan oleh penyelenggara sistem elektronik. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah disahkan, kenyataannya regulasi ini belum sepenuhnya mampu menekan laju kasus kebocoran data. Hal tersebut dapat dilihat dari masih terbatasnya aturan turunan yang lebih teknis, kurangnya kapasitas aparat penegak hukum dalam menangani kejahatan siber, serta lemahnya kesadaran masyarakat dalam menjaga keamanan data pribadinya.

Peningkatan jumlah kasus juga mengindikasikan bahwa sektor privat, khususnya platform digital dan marketplace, belum memiliki standar keamanan yang memadai untuk melindungi data pengguna. Banyak perusahaan hanya memandang perlindungan data sebagai kewajiban administratif, bukan sebagai bagian dari tanggung jawab etis dan hukum yang fundamental.⁹ Akibatnya, kasus kebocoran data terus berulang dan menimbulkan kerugian finansial maupun non-finansial bagi masyarakat.

Undang-undang memberikan dasar hukum yang jelas bagi pengendali data pribadi untuk memproses data pribadi sesuai dengan prinsip perlindungan data pribadi. Perlindungan data pribadi harus dilaksanakan sesuai dengan prinsip

⁹ Deri Dahuri, "Pemerintah Harus Libatkan Stakeholder Dalam Buat Regulasi Perlindungan Data Pribadi," MediaIndonesia, 2022, <https://mediaindonesia.com/teknologi/522236/pemerintah-harus-libatkan-stakeholder-dalam-buat-regulasi-perlindungan-data-pribadi>.

perlindungan data pribadi yaitu kejelasan, kepastian, keterbukaan, penggunaan, kinerja, pengumpulan, persetujuan penggunaan data pribadi, pemrosesan data pribadi, keamanan data pribadi, penghapusan atau penghancuran data pribadi, dan akuntabilitas pengendali data pribadi.¹⁰ Dalam Undang-Undang Nomor 1 Tahun 2024 tentang informasi dan transaksi elektronik (ITE) dijelaskan bahwa undang-undang ini mengatur tentang pengelolaan informasi dan transaksi elektronik di Indonesia yang berisi mengenai berbagai aspek terkait dengan transaksi elektronik, seperti informasi, dokumen, tanda tangan elektronik, sertifikasi elektronik, transaksi elektronik, nama dokumen, hak kekayaan intelektual, perlindungan hak pribadi, perbuatan yang dilarang, penyelesaian sengketa, peran pemerintah dan masyarakat, penyidikan, ketentuan pidana, serta ketentuan peralihan. Dalam transaksi jual online atau media online jika terjadi suatu sengketa maupun tindak pidana penipuan akan sulit untuk melakukan eksekusi. Apabila penjual menggunakan data palsu, maka dapat dikenakan tindak pidana penipuan berdasarkan pasal 378 KUHP tentang penipuan dan pasal 28 ayat (1) undang-undang informasi transaksi elektronik.¹¹

Dalam Al-Quran, tindakan pencurian data pribadi atau hak oranglain adalah tindakan yang dilarang oleh Allah SWT karena melanggar prinsip-prinsip syariah seperti perlindungan harta, amanah, serta larangan melakukan kezaliman dan pencurian. Tindakan tersebut tidak hanya melanggar manusia, tetapi juga

¹⁰ Achmad Bachtiyar, Implikasi Hukum Pidana Dalam Perlindungan Data Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Skripsi, Sekolah Tinggi Ilmu Hukum BIAK-PAPUA, 2023),vii

¹¹ Komang Pande Angga Tridipta, I yoman Sujana Dan Ni Made Puspasutari Ujjianti, "Perlindungan Hukum Terhadap Pelanggar Privasi Konsumen Dalam Jual Beli Online," *Jurnal Analogi Hukum*, Vol 2 (3) (2020), 356-360.

melanggar hukum Allah yang mengatur hubungan manusia dengan harta dan privasi oranglain. QS.An-Nisa (4):58 Allah SWT Berfirman:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۚ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا

Terjemahnya:

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat."¹²

Dalam Islam, harta dapat dilihat sebagai amanah yang harus dijaga dan dipertanggungjawabkan dengan baik. Dalam konteks data pribadi, data tersebut dapat dianggap sebagai bagian dari hak kekayaan individu yang harus dilindungi oleh pihak yang diberi amanah:

أَدِّ الْأَمَانَةَ إِلَىٰ مَنْ اتَّيَمَّنَكَ وَلَا تَخُنْ مَنْ خَانَكَ

Artinya:

“Tunaikanlah amanah kepada orang yang mempercayaimu dan jangan engkau mengkhianati orang yang mengkhianatimu!”(HR.Tirmidzi).¹³

Secara garis besar dalam UU PDP (Perlindungan Data Pribadi) Nomor 27 tahun 2022 terdapat dua sanksi hukum yaitu sanksi administratif dan sanksi pidana. Ketetapan hukum pidana yang diatur dalam undang-undang yaitu pertama, dikenakan denda maksimal 4 hingga 6 miliar, kedua penjara maksimal 4

¹² Kementrian Agama RI, Al-Qur'an dan Terjemahnya, QS. An-Nisa [4]:58, <https://quran.kemenag.go.id/quran/per-ayat/surah/4?from=58&to=176>.

¹³ Wakalahmu, “Hadis Tentang Amanah Dalam Islam,” 2021, <https://wakalahmu.com/artikel/dunia-islam/hadits-tentang-amanah-dalam-islam>.

hingga 6 tahun.¹⁴ Dalam pasal 69 undang-undang perlindungan data pribadi mengatur mengenai pidana tambahan untuk pemalsuan data pribadi selain pidana sebagaimana dimaksud dalam pasal 67 dan pasal 68 pelaku pemalsuan data pribadi dapat dijatuhi sanksi pidana berupa biaya ganti rugi.

Kepastian hukum diberikan untuk jaminan keamanan dan kenyamanan dalam hal data pribadi, sehingga ketika terjadi kasus penyalahgunaan data pribadi maka kita sudah mengetahui hal-hal apa saja yang harus dilakukan.¹⁵ Namun, penerapan hukum pidana dalam kasus kebocoran data pribadi di Indonesia meskipun sudah memiliki undang-undang tersendiri yang disahkan pada tahun 2022, implementasinya masih dalam tahap awal, yang mana peraturan hukum ini masih memerlukan turunan yang lebih rinci untuk memastikan penegakan yang efektif, terlebih dalam penegakan hukum yang lemah karena kurangnya kapasitas dan keahlian aparat penegak hukum dalam menangani kejahatan *siber* termasuk dalam halnya kebocoran data, dan juga dampak dari kebocoran data pribadi tersebut dapat menyebabkan kerugian yang besar bagi individu.¹⁶

Perkembangan teknologi yang cepat seringkali membuat hukum tertinggal. Dengan adanya penerapan hukum pidana yang jelas dan tegas, perusahaan *e-commerce* dan konsumen harus memiliki pedoman yang jelas dalam mengatasi pembocoran data pribadi dan menegakkan hukum. Selain itu, platform *e-commerce* juga perlu memiliki kebijakan privasi yang jelas dan transparansi,

¹⁴ Doni, "Mengetahui Sanksi Pelanggaran Data Pribadi," *Kementerian Komunikasi Dan Informasi*, September 24, 2022, <https://www.kominfo.go.id/content/detail/44680/mengetahui-sanksi-pelanggaran-data-pribadi/0/artikel>.

¹⁵ Fitriani Jamaluddin et al., "perlindungan data pribadi pengguna dompet digital ovo" 6, no. 1 (2021): 37–41.

¹⁶ Fransiscus Xaverius Watkat Et Al., "Perlindungan data pribadi melalui penerapan" 5, no. 1 (2024).

termasuk pernyataan privasi yang tersedia dengan jelas untuk melindungi data pribadi konsumen. Berdasarkan pemaparan diatas, maka penulis tertarik melakukan penelitian tentang Kepastian hukum pidana terhadap kebocoran data pribadi pada marketplace.

B. Rumusan Masalah

1. Bagaimana fakta tentang kebocoran data pribadi di *platform marketplace* ?
2. Bagaimana kepastian hukum pidana terhadap kebocoran data pribadi?
3. Bagaimana Tinjauan Fiqhi Jinayah terhadap Penanganan Kebocoran Data Pribadi?

C. Tujuan Penelitian

Tujuan penelitian merupakan gambaran tentang arah yang akan dituju dalam melakukan penelitian. Setelah menentukan rumusan masalah dalam penelitian, maka tujuan penelitian tersebut diatas adalah sebagai berikut:

1. Untuk mengetahui bagaimana fakta tentang kebocoran data pribadi di *platform marketplace*.
2. Untuk mengetahui bagaimana kepastian hukum pidana terhadap kebocoran data pribadi.
3. Untuk mengetahui Bagaimana Tinjauan Fiqhi Jinayah terhadap Penanganan Kebocoran Data Pribadi

D. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini di harapkan dapat memberikan sumbangan pemikiran dan pemahaman mengenai fenomena pembocoran data pribadi pada *marketplace*, dan

dari penelitian ini juga diharapkan dapat menambah wawasan dan informasi yang lebih konkrit bagi usaha pembaharuan di bidang hukum pidana.

2. Manfaat Praktis

Manfaat praktisnya adalah dapat memberikan kontribusi penuh kepada masyarakat dalam memahami pembocoran data pribadi pada *marketplace* dalam dunia digital.

3. Manfaat Akademis

Penelitian ini merupakan salah satu syarat untuk menyelesaikan studi program strata 1 (SI) pada program studi Hukum Tata Negara Fakultas Syariah Institut Agama Islam Negeri Palopo.

E. Penelitian Terdahulu yang Relevan

1. Penelitian terdahulu yang berjudul "Tinjauan yuridis terhadap efektivitas penanganan kejahatan *siber* terkait pencurian data pribadi menurut undang-undang no. 27 tahun 2022 oleh kominfo". Oleh Muhammad Yudistira dan Ramadani Tahun 2023. Penelitian tersebut bertujuan untuk melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik (PSE), seperti kementerian komunikasi dan informatika (KOMINFO), serta mencegah kejahatan yang dilakukan oleh suatu individu yang tidak bertanggung jawab. Kebutuhan untuk mengatasi masalah kebocoran data menjadi fokus utama yang harus segera diatasi dengan solusi yang pasti dan aman. Dengan berlakunya undang-undang perlindungan data pribadi ini diharapkan dapat menjadi solusi efektif dalam menangani masalah kebocoran data pribadi yang

sering terjadi di Indonesia.¹⁷ Adapun perbedaan penelitian ini dengan penelitian terdahulu yaitu penelitian ini berfokus terhadap kepastian hukum pidana terhadap kasus-kasus kebocoran data pribadi yang terjadi di platform marketplace.

2. Penelitian terdahulu yang berjudul “Kebijakan hukum pidana terhadap pengaturan pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi”. Oleh Adik Nur Luthiya, Benni Irawan, dan Rena Yulia dari Universitas Sultan Ageng Tirtayasa Tahun 2021. Penelitian tersebut merupakan penelitian yang dilakukan secara konseptual, kebijakan hukum pidana yang saat ini digunakan untuk menanggulangi kasus pencurian data pribadi dapat dilihat dari pasal 362 dan pasal 363 ayat (1) undang-undang hukum pidana (KUHP) dan pasal 30 jo, pasal 46 dan pasal 32 jo. Pasal 48 undang-undang nomor 19 tahun 2016 perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Sedangkan kebijakan hukum pidana terhadap pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi di masa yang akan datang dapat ditemukan dalam RUU KUHP 2019 dan RUU PDP 2020.¹⁸ Adapun perbedaan penelitian ini dengan penelitian yang terdahulu yaitu penelitian ini lebih spesifik terhadap hukum pidana terkait kebocoran data pribadi yang terjadi di

¹⁷ Muhammad Yudistira and 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, no. 4 (2023): 3803, <https://doi.org/https://doi.org/10.31933/unesrev.v5i4>.

¹⁸ Adik Nur Luthiya, Benny Irawan, & Rena Yulia, “Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi dan Informasi, *jurnal hukum pidana & kriminologi*, Vol 02 No 02 Edisi Oktober 2021 (hlm. 14-29).

marketplace dan menitikberatkan hukum pidana ketika data pribadi pengguna yang disimpan oleh *marketplace* mengalami kebocoran.

3. Penelitian terdahulu yang berjudul “Perlindungan konsumen terhadap kebocoran data pada jasa keuangan di indonesia”. Oleh Andri Soemitra dan Adlina dari Universitas Islam Negeri Sumatera Utara tahun 2022. Penelitian tersebut membahas mengenai kebocoran data pada jasa keuangan di indonesia tidak terlepas dari 2 faktor:

1. faktor konsumen, perilaku konsumen dalam melakukan transaksi pinjaman online, memberikan data pribadi seperti KTP, nomor handphone, nomor kartu kredit, dan sebagainya.
2. Faktor kebocoran dari pihak pelaku jasa keuangan dengan cara menjual data konsumen, memberikan data pada pihak ketiga dan sistem aplikasi data yang mudah di retas oleh *hacker*.

Penelitian tersebut menggunakan pendekatan penelitian kualitatif dengan melakukan studi literatur dari 26 paper terindeks yang relevan. Hasil penelitian sarana perlindungan hukum tersebut ada dua, yaitu sarana perlindungan hukum preventif dan sarana perlindungan hukum represif.¹⁹ Adapun perbedaan penelitian ini dengan penelitian terdahulu yaitu penelitian ini lebih berfokus pada proses hukum dan sanksi pidana yang dikenakan pelanggar pelaku pembocoran data pribadi.

¹⁹ Andri Soemitra dan Adlina, “Perlindungan kosumen terhadap kebocoran data terhadap pada jasa keuangan di indonesia”, 288.

F. Kajian Pustaka

1. Kajian tentang Kebocoran Data

Data adalah bentuk jamak dari datum, berasal dari bahasa latin yang berarti “sesuatu yang diberikan”. Data terbentuk dari karakter berupa angka, simbol khusus ataupun *alphabet* yang disusun untuk diolah dalam bentuk struktur data, file, dan *database*.²⁰ Kebocoran data merupakan informasi sensitif yang secara tidak sengaja diunggah atau diakses tanpa izin oleh pelaku yang tidak bertanggungjawab, dimana ancaman ini muncul melalui *website*, email, *hard drive*, dan laptop.²¹ Kebocoran data terjadi apabila informasi seseorang seperti nama, alamat, nomor identitas, keuangan, atau informasi sensitif lainnya terungkap ke internet oleh pihak yang tidak bertanggung jawab yang diakses tanpa izin. Informasi data yang bocor dapat menyebabkan konsekuensi yang parah bagi individu yang menyebabkan kerusakan reputasi, kerugian finansial, dan implikasi hukum. Kebocoran data sangat erat hubungannya dengan pembobolan data, yang mana ketika data seorang terekspos dengan sengaja ke internet atau situs yang tidak aman, maka seorang *peretas* dapat mengakses informasi pribadi untuk melakukan pembobolan data, karena kurangnya kesadaran dan pemahaman terhadap penyebaran data sensitif seperti memasukkan nomor telepon di aplikasi dan situs yang tidak aman, hal ini menjadi salah satu faktor terjadinya kebocoran data, sistem yang tidak terupdate atau memiliki celah keamanan dapat di

²⁰ Uni Sabadina, “Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online,” *Jurnal Lex Renaissance* 6, no. 4 (2021): 799–814, <https://doi.org/10.20885/jlr.vol6.iss4.art11>.

²¹ Abdul Muid ardiyansyah, M, “Tinjauan Yuridis Tindak Pidana Terhadap Kebocoran Data Pribadi Pengguna Perdagangan Elektronik,” 2023, 1–14, <https://www.ncbi.nlm.nih.gov/books/NBK558907/>.

eksploitasi oleh pihak yang tidak bertanggungjawab. Adapun dampak negatif dari kebocoran data yaitu:

1. Kerugian finansial dimana pencurian identitas dan penipuan bisa mengakibatkan kerugian uang.
2. Kerugian reputasi baik individu maupun perusahaan dapat kehilangan kepercayaan publik akibat kebocoran data.
3. Individu yang mengalami data pribadinya bocor dapat mengalami stres akibat ketidakpastian tentang bagaimana data tersebut akan digunakan.

Dalam mencegah kebocoran data pribadi diperlukan beberapa hal sebagai berikut:

1. Penerapan teknologi dan keamanan
2. Pelatihan dan kesadaran
3. Audit dan pengawasan berkala
4. Kebijakan privasi yang lebih ketat

Dalam mencegah kebocoran data pribadi belanja online terdapat pada keamanan informasi dan keuangan yang dimiliki oleh para konsumen. Penjahat siber menggunakan teknik seperti peretasan dan pencurian data identitas untuk mendapatkan akses tidak sah ke data sensitif, selain itu produk palsu, deskripsi produk yang tidak akurat atau sesuai, pengiriman yang lambat juga menjadi kekhawatiran para konsumen dalam menciptakan pengalaman belanja yang tidak baik.²² Berikut beberapa resiko tersebut:

²² Kemendikbud, diakses pada (7 Juli 2024), <https://lldikti5.kemdikbud.go.id/home/detailpost/kepercayaan-dan-risiko-belanja-online>.

a. Pencurian identitas

Pencurian identitas merupakan tindakan kejahatan yang diambil dan penyalahgunaan informasi seseorang tanpa izin, yang bertujuan untuk mendapatkan keuntungan ilegal dan merugikan orang lain. Informasi pribadi yang dicuri merupakan data-data sensitif, seperti nama, alamat, nomor identitas, dan informasi finansial.²³

b. Phising

Dalam era digital yang semakin maju sekarang ini kita sering kali mendapatkan penipuan.²⁴ *Phising* merupakan salah satu kejahatan siber di dunia digital dimana penyerang menyamar sebagai seseorang yang terpercaya untuk mencuri informasi pengguna. Pelaku *phising* biasanya menggunakan email atau situs web palsu yang meniru toko online untuk melakukan kejahatannya.

c. Data breach

Istilah data *breach* sering di kaitkan dengan serangan *cyber* (*cyber attack*). Hal ini dikarenakan sebagian besar data *breach* terjadi karena peretasan atau serangan *malware*. Data *breach* adalah insiden keamanan ketika data pribadi pengguna diakses tanpa adanya izin.²⁵ Kebocoran data pada platform *e-commerce* atau situs *web* dapat menyebabkan informasi pribadi bocor ke publik atau di jual di pasar gelap.

²³ Rani Pilo, "Pencurian Identitas: Ancaman Terbesar Yang Harus Diwaspadai," Aplikasi Servis Pesona, 2023, <https://aplikas.com/blog/pencurian-identitas/>.

²⁴ Diskominfo, Awas tindakan phising! Ini dia langkah-langkah agar tidak terkena pesan berisi link phising, diakses pada (18 juli 2024), <https://kominform.kotabogor.go.id/index.php/post/single/897>.

²⁵ Sindo News, Mengenal perbedaan data breach, security breach, dan data leakage, diakses pada (18 juli 2024), <https://tekno.sindonews.com/read/501844/207/mengenal-perbedaan-data-breach-security-breach-dan-data-leakage-162808611>.

d. Transaksi tidak sah

Transaksi ini terkait mengenai informasi kartu kredit atau rekening bank yang di curi dan dapat digunakan untuk melakukan transaksi tidak sah atau penarikan dana tanpa izin.

Untuk mengurangi resiko diatas, ada beberapa langkah yang dapat diambil:

1. Menggunakan situs yang terpercaya
2. Menggunakan koneksi yang aman
3. Menggunakan metode pembayaran yang aman
4. Memperbarui kata sandi secara berkala
5. Memantau transaksi keuangan.

2. Kajian tentang Hukum Pidana

Hukum pidana adalah bagian dari hukum publik yang mengatur tindak pidana, pelaku tindak pidana, serta sanksi yang dapat di kenakan terhadap pelaku tindak pidana. Dalam hukum pidana indonesia, KUHP merupakan pokok dari peraturan perundang-undangan yang mengatur mengenai hukum pidana berupa pelanggaran dan kejahatan.²⁶ Hukum pidana memiliki tujuan dan proses sanksi yang merupakan dari pelaksanaan proses pidana dalam menjalankan sistem peradilan.²⁷ Pengertian hukum pidana menurut beberapa ahli yaitu:

1. Prof.Van Hamel

Hukum pidana yaitu semua dasar-dasar dan aturan-aturan yang dianut oleh suatu negara dalam menjalankan ketertiban hukum, melarang apa yang

²⁶ Besse Muqita Rijal Mentari, Sanksi pidana pembunuhan dalam kitab undang-undang hukum pidana dan hukum islam, Jurnal ilmiah hukum, Sekolah Tinggi Ilmu Hukum Lamadukelleng Sengkang, Vol 23 no 1, (Mei 2020), hlm 3.

²⁷ Kurniawan Tri Wibowo, dan Warih Anjari, Hukum pidana materil, (Jakarta Timur : Prenada Media, 2022), hal.12.

bertentangan dengan hukum dan mengenakan suatu nestapa bagi yang melanggar larangan-larangan tersebut.

2. Prof.Simons

Hukum pidana yaitu kesemua perintah-perintah dan larangan-larangan yang diadakan oleh negara yang diancam dengan suatu pidana, barangsiapa yang tidak menaatinya, maka aturan-aturan tersebut menentukan syarat-syarat bagi akibat hukum untuk di jatuhi hukuman yang harus dijalankan.

3. Prof. Pompe

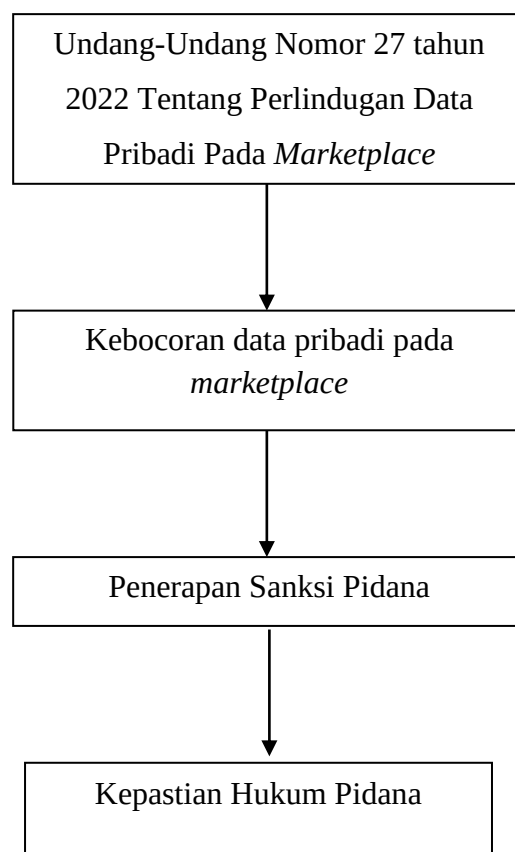
Hukum pidana yaitu semua aturan-aturan hukum yang menentukan terhadap perbuatan-perbuatan apa seharusnya dijatuhi pidana dan apakah macamnya pidana itu.²⁸

Beberapa pengertian hukum pidana diatas dapat disimpulkan bahwa hukum pidana ialah keseluruhan aturan-aturan dan larangan-larangan yang jika dilanggar akan di kenakan sanksi bagi yang melakukan perbuatan pelanggaran tersebut. Sanksi pidana merupakan hukuman yang di jatuhkan oleh hakim kepada orang-orang yang telah melanggar undang-undang hukum pidana. Sanksi pidana bertujuan untuk memberikan efek jera kepada pelaku pelanggaran agar mereka merasakan akibat perbuatannya. Dalam konteks hukum pidana terhadap pembocoran data pribadi, tindak pidana pencurian data pribadi yang sengaja atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain dapat mengakibatkan kerugian maka akan dikenakan pidana penjara 5 tahun atau pidana denda paling banyak 5

²⁸ Ayu Efridadewi ,Modul hukum pidana, (Tanjungpinang-Kepulauan Riau, Universitas maritim raja ali haji,2020),hal 1.

miliar (pasal 67 ayat 1), tindak pidana yang sengaja dan melawan hukum yang mengungkapkan data pribadi yang bukan miliknya dipidana penjara 4 tahun atau denda paling banyak 4 miliar (Pasal 67 ayat 2), tindak pidana yang sengaja membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain dapat mengakibatkan kerugian bagi oranglain dipidana penjara 6 tahun atau denda paling bayak 6 miliar (Pasal 68 UU PDP).²⁹ Sanksi pidana yang diberikan dalam undang-undang no.27 tahun 2022 bertujuan untuk menegakkan kepatuhan, melindungi hak-hak individu, dan mencegah penyalahgunaan data pribadi.

G. Kerangka Pikir



Gambar 1.2 Kerangka Pikir

²⁹ “Tindak Pidana Dalam UU PDP Dan Sanksinya,” kementrian pendayagunaan aparatur negara dan reformasi birokrasi, 2023, <https://sippn.menpan.go.id/berita/59933/rumah-tahanan-negara-kelas-iib-pelaihari/4-tindak-pidana-dalam-uu-pdp-dan-sanksinya>.

Keterangan:

Penelitian yang dilakukan oleh penulis berjudul Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace. Dalam penelitian yang dilakukan peneliti, bertujuan untuk mengetahui bagaimana aturan dalam Undang-Undang nomor 27 tahun 2022 tentang perlindungan data pribadi, kemudian kebocoran data yang terjadi pada *marketplace*, lalu bagaimana penerapan sanksi pidana terhadap pelaku pembocoran data pada *marketplace*, kemudian kepastian hukum pidana dalam pembocoran data pada *marketplace*.

H. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan melalui pendekatan perundang-undangan (*statute approach*). Penelitian hukum normatif atau melalui pendekatan perundang-undangan adalah pendekatan yang dilakukan dengan mengkaji semua peraturan perundang-undangan dan regulasi yang bersangkutan dengan isu hukum yang ditangani.³⁰ Penelitian ini terdiri dari asas-asas hukum, sistematika hukum, taraf sinkronisasi vertikal dan horizontal, perbandingan hukum, dan sejarah hukum.³¹ Penelitian kepustakaan tidak hanya di baca dan dicatat saja, namun mencatat serta mengolah bahan penelitian.³²

³⁰ Manotar Tampubolon, "Metode Penelitian Metode Penelitian," *Metode Penelitian Kualitatif* 3, no. 17 (2023): 43, [http://repository.unpas.ac.id/30547/5/BAB III.pdf](http://repository.unpas.ac.id/30547/5/BAB%20III.pdf).

³¹ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu tinjauan singkat*, cet. Keduabelas, Rajawali Pers, Jakarta, 2010, hlm 14.

³² Stie Dewantara, *Metode Penelitian, Jenis dan sifat penelitian*.

2.Sumber Data

Sumber data yang digunakan dalam penelitian ini adalah sumber data sekunder. Sumber data sekunder adalah data yang telah dikumpulkan oleh pihak lain dan diperoleh secara tidak langsung dari objek penelitian yang dilakukan secara tertulis maupun lisan yang bisa didapatkan melalui media perantara seperti artikel, buku, skripsi, jurnal, laporan, dan majalah sesuai dengan permasalahan yang akan diteliti. Kemudian data sekunder dalam penelitian ini untuk mendukung data penelitian yang spesifik.³³

3.Teknik Pengumpulan Data

Data yang digunakan dalam penelitian ini adalah jenis penelitian kepustakaan dimana penelitian ini dilakukan dengan cara mengumpulkan informasi serta data dengan bantuan berbagai macam material seperti, buku referensi, hasil penelitian terdahulu yang sejenis, artikel, catatan, serta berbagai jurnal yang berkaitan dengan penelitian ini. Kegiatan ini dilakukan secara sistematis, mengumpulkan, mengolah, dan menyimpulkan data relevan yang mencakup gambaran yang luas sehingga data tersebut dapat ditarik kesimpulan. Pengumpulan data ini dilakukan dengan metode *survey book* atau *library research*.

³³ Bonifasius Tambunan dan Jhon Feliks Simajuntak , Analisis pelaksanaan kas kecil (*Petty Cash*) pada PT Deli Jaya Samudera, Journal Of Economics And Business, Vol 03 (01 September 2021), hlm 44.

4. Teknik Analisis Data

Analisis data merupakan langkah dalam mengolah serta mengidentifikasi dan mengorganisir data pada pola-pola tertentu. Teknik analisis data bertujuan untuk mendapatkan pemahaman yang lebih dalam tentang data yang dianalisis dan mengambil keputusan informasi yang ditemukan serta menyeleksi apa yang penting dan di pahami dalam menggambarkan kesimpulan data tersebut. Dalam proses analisis data melibatkan beberapa tahap pengumpulan data, penyusunan data, pengolahan data serta pembuatan laporan hasil.

BAB II

DATA TERKAIT PERLINDUNGAN DATA PRIBADI DI INDOESIA

A. Ruang Lingkup Perlindungan Data Pribadi

Data pribadi adalah setiap data seseorang baik yang teridentifikasi dan/atau diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik maupun non elektronik.³⁴ Informasi dalam data pribadi mencakup nama lengkap, alamat, nomor ponsel, tanggal lahir, nomor identitas (seperti KTP, atau paspor), data biometrik, data genetika, informasi kesehatan, data keuangan pribadi, dan sebagainya.³⁵ Secara umum, ruang lingkup pengaturan dalam Undang-Undang PDP mencakup beberapa aspek penting, antara lain: definisi dan klasifikasi data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, prinsip-prinsip pemrosesan data, mekanisme pengawasan, serta ketentuan sanksi administratif dan pidana. Menurut Undang-Undang Nomor 27 tahun 2022 tentang perlindungan data pribadi (UU PDP), data pribadi dikategorikan dalam dua jenis yaitu data pribadi umum, dan data pribadi spesifik.

Data pribadi umum merupakan jenis data yang umumnya dapat diidentifikasi oleh beberapa orang. Dalam Bab III pasal 4 ayat (1) huruf b Undang-Undang Nomor 27 Tahun 2022 data pribadi umum meliputi:

³⁴ Kominfo, “Bersama Lindungi Data Pribadi Di Platform Digital,” Diskominfo, 2020, <https://diskominfo.kotawaringinbaratkab.go.id/page/detail/bersama-lindungi-data-pribadi-di-platform-digital>.

³⁵ Nibras Nada Nailufar Tari Oktaviani, “UU Perlindungan Data Pribadi: Jenis Data Dan Sanksi Pidananya,” Kompas.com, 2023, <https://nasional.kompas.com/read/2023/07/19/00150061/uu-perlindungan-data-pribadi--jenis-data-dan-sanksi-pidananya?>

- a) Nama lengkap
- b) Jenis kelamin
- c) Kewarganegaraan
- d) Agama
- e) Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Data pribadi spesifik merupakan jenis data yang mencakup data informasi dan kesehatan yang jika diproses dapat mengakibatkan dampak yang lebih besar bagi individu yang terkait dengan data tersebut. Dalam Bab III pasal 4 ayat (1) huruf a Undang-Undang Nomor 27 Tahun 2022 data pribadi spesifik meliputi:

- a) Data dan informasi kesehatan
- b) Data biometrik
- c) Data genetika
- d) Pandangan politik
- e) Catatan kejahatan
- f) Data anak
- g) Data keuangan pribadi
- h) Data lain yang sesuai dengan peraturan perundang-undangan.³⁶

Dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur larangan-larangan dalam penggunaan data pribadi, dimana hal ini terdapat dalam pasal 65 Undang-undang perlindungan data pribadi dengan tegas melarang:

- 1) Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk

³⁶ Mauliana Yuniarti, "Bab Ii Tinjauan Umum Tentang Data Pribadi 1.1," 2022, 14–22.

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) Menggunakan data pribadi yang bukan miliknya secara melawan hukum.³⁷

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan tonggak penting dalam sistem hukum Indonesia yang secara khusus mengatur mengenai tata kelola data pribadi. Kehadiran Undang-Undang ini bertujuan untuk menjamin perlindungan hak setiap individu atas data pribadinya, serta menciptakan kepastian hukum bagi semua pihak yang melakukan pemrosesan data, baik dalam lingkup publik maupun privat. Dalam pelaksanaannya, Undang-Undang Perlindungan Data Pribadi berlaku untuk setiap orang, badan publik, dan badan privat yang memproses data pribadi secara *elektronik* maupun *non-elektronik*.

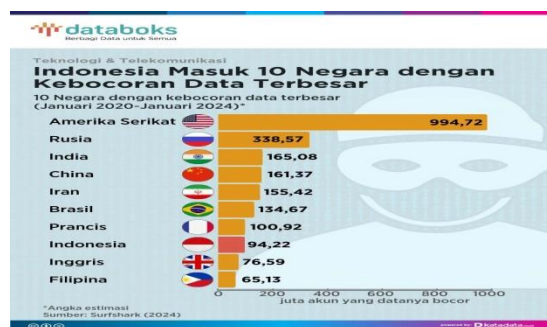
Dalam konteks hubungan antarnegara, Undang-Undang Perlindungan Data Pribadi juga mengatur transfer data pribadi lintas batas wilayah hukum (*cross-border data transfer*), yang harus dilakukan dengan jaminan perlindungan setara di negara tujuan. Ketentuan ini menunjukkan bahwa ruang lingkup Undang-Undang PDP juga bersifat *transnasional*, mengingat pemrosesan data saat ini tidak lagi terbatas secara geografis. Oleh karena itu, pengaturan dalam Undang-Undang Perlindungan Data Pribadi berusaha menyeimbangkan kepentingan

³⁷ Info Hukum, "Jenis-Jenis Data Pribadi Menurut UU Perlindungan Data Pribadi," InfoHukum, 2025, <https://fahum.umsu.ac.id/info/jenis-jenis-data-pribadi-menurut-uu-perlindungan-data-pribadi/>.

perlindungan individu dengan kebutuhan pertumbuhan ekonomi digital yang mengandalkan pengelolaan data secara lintas batas.

Ruang lingkup Undang-Undang Perlindungan Data Pribadi mencakup tidak hanya aspek teknis pengelolaan data pribadi, tetapi juga dimensi etik, sosial, dan ekonomi dari pemanfaatan data. Undang-Undang ini menjadi kerangka hukum utama yang diperlukan dalam menciptakan ekosistem digital yang aman, adil, dan berkelanjutan, serta sejalan dengan standar perlindungan data internasional seperti *General Data Protection Regulation* (GDPR) di Uni Eropa.³⁸

Perusahaan *virtual private network* (VPN) asal Belanda, selama Januari 2020-Januari 2024 ada sekitar 3,96 miliar akun digital yang mengalami kebocoran data. Indonesia menjadi salah satu negara dengan kebocoran data terbanyak ke-8 di dunia dengan estimasi 94,22 juta akun bocor.³⁹ Berikut jumlah negara dengan kebocoran data terbesar:



Gambar 2.1 Negara dengan kebocoran data terbesar 2020-2024

³⁸ Bp Lawyers, “UU PDP Berlaku, Ini Isi Pengaturan Perlindungan Data Pribadi Di Indonesia,” Bp Lawyers Counselor At Law, 2022.

³⁹ Adi Ahdiat, “Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar,” Databoks, 2024, <https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>.

Gambar diatas menunjukkan bahwa Indonesia berada pada peringkat ke-8 dengan tingkat kebocoran data tertinggi secara global. Tercatat sekitar 94,22 juta pengguna akun di Indonesia mengalami kebocoran data. Kebocoran ini sebagian besar terjadi melalui platform digital yang memiliki sistem keamanan lemah atau belum menerapkan *enkripsi end-to-end*. Dengan perkembangan teknologi digital saat ini peningkatan penggunaan berbagai *platform media social*, layanan *e commerce* dan lain sebagainya. Kemajuan teknologi ini tidak diimbangi dengan sistem perlindungan data yang memadai. Sehingga banyak *platform* digital masih mengabaikan standar keamanan yang ketat, dimana hal ini membuka celah bagi peretas untuk mengakses informasi pribadi pengguna. Kondisi ini menjadi semakin mengkhawatirkan ketika data yang bocor mencakup informasi sensitif seperti alamat *email*, nomor telepon, hingga data finansial.

Perlindungan data pribadi menjadi hal yang sangat penting untuk diterapkan dalam era digital saat ini. Pemerintah berperan penting dalam melindungi data pribadi dengan Undang-Undang Perlindungan Data Pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah peraturan baru yang mengatur bagaimana data pribadi harus dilindungi dan diproses di Indonesia.

Langkah ini penting untuk menjamin privasi dan hak-hak individu dalam hal pengumpulan, penggunaan, dan pembagian data pribadi. Undang-Undang ini membatasi bagaimana data pribadi harus ditangani dan dilindungi, termasuk catatan, persetujuan, akses, keamanan, penyalahgunaan, hukum, dan lembaga

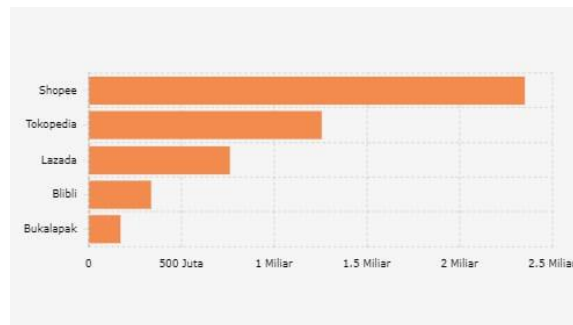
otoritas.⁴⁰ Perlindungan data pribadi merupakan upaya pemerintah untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi dari akses, penggunaan, atau pengungkapan yang tidak sah.

E-commerce telah menjadi salah satu sektor paling dinamis dalam dunia digital, dengan *marketplace* sebagai induk dalam pertumbuhan industri ini. Setiap hari, jutaan pengguna mengunjungi berbagai *platform marketplace* untuk mencari, membandingkan, dan membeli produk yang mereka butuhkan. Dengan semakin meningkatnya pengguna internet maka perubahan pola belanja konsumen juga berubah, persaingan antar *marketplace* dalam menarik pengunjung terbanyak pun semakin ketat. Faktor seperti kenyamanan, variasi produk, harga kompetitif, serta strategi pemasaran yang inovatif menjadi kunci utama dalam menarik perhatian pengguna dan mempertahankan loyalitas pelanggan.

Kategori *marketplace* shopee merupakan situs yang kunjungannya terbanyak di indonesia sepanjang tahun 2023. Januari-Desember 2023, secara kumulatif situs Shopee meraih sekitar 2,3 miliar kunjungan, jauh melampaui para pesaingnya.⁴¹ Berikut data kunjungan situs *mrketplace* terbanyak sepanjang tahun 2023:

⁴⁰ John F. Mariani, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *Of Social Science Research* 3 (2020): 176–176, <https://doi.org/10.5040/9781635577068-0537>.

⁴¹ Adi Ahdiat, "5 E-Commerce Dengan Pengunjung Terbanyak Sepanjang 2023," Databoks, 2023, <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3c9132bd3836eff/5-e-commerce-dengan-pengunjung-terbanyak-sepanjang-2023>.



Gambar 2.2 Jumlah *Marketplace* dengan Pengunjung terbanyak Tahun 2023

Perkembangan ekonomi digital di Indonesia mendorong pertumbuhan berbagai platform marketplace yang kini menjadi bagian penting dalam sektor perdagangan elektronik. Marketplace berperan sebagai perantara antara penjual dan pembeli secara daring, dengan karakteristik dan model bisnis yang beragam. Hingga saat ini, terdapat sejumlah marketplace yang aktif beroperasi di Indonesia,⁴² diantaranya:

1) Bukalapak

Bukalapak didirikan pada tahun 2010 oleh Achmad Zaky, Nugroho Herucahyono, dan Muhammad fajrin Rasyid sebagai lokapasar untuk memfasilitasi para pelaku usaha kecil menengah. Platform digital ini memenuhi transaksi elektronik dengan menyediakan metode pembayaran yang praktis serta harga kompetitif dengan berbagai promo menarik.⁴³

⁴² Mutiara Hapiz et al., “Analisis Kebijakan Pengembangan UMKM Digital Di Indonesia: Tantangan Dan Peluang,” *Jurnal Ilmiah Multidisiplin* 3, no. 5 (2025): 36–44, <https://doi.org/10.5281/zenodo.15538100>.

⁴³ Amry Nur Hidayat, “Perjalanan Bukalapak, Dari IPO Pasar Modal Terbesar Indonesia Hingga Jadi Fokus Jual Pulsa,” *Warta Ekonomi.co.id*, 2025, <https://wartaekonomi.co.id/read554564/perjalanan-bukalapak-dari-ipo-pasar-modal-terbesar-indonesia-hingga-jadi-fokus-jual-pulsa>.

2) Tokopedia

Tokopedia didirikan pada tahun 2009 oleh William Tanuwijaya dan Leontinus Alpha Edison sebagai ekonomi digital ekonomi digital dengan memotivasi masyarakat Indonesia untuk mulai berjualan secara online, yang dilakukan dengan membangun platform yang memungkinkan setiap orang dapat memulai dan menemukan apapun, dan dimanapun. Platform digital ini menjual berbagai macam produk seperti kebutuhan rumah tangga, fashion, makanan dan minuman, serta produk digital. Selain itu, Tokopedia juga menyediakan layanan seperti tiket perjalanan, layanan finansial, dan donasi.⁴⁴

3) Shopee

Shopee Indonesia resmi diperkenalkan kepada publik pada Desember 2015, dibawah bendera PT. Shopee Internasional Indonesia. tujuan didirikannya Shopee Indonesia adalah, karena percaya pada kekuatan transformatif dari teknologi yang bisa mengubah dunia menjadi lebih baik, melalui platform yang menghubungkan penjual dengan pembeli dalam satu komunitas. *Mobile platform* pertama di Asia Tenggara yang menawarkan berbagai fitur seperti *shopeepay*, *spaylater*, serta transaksi jual beli online yang menyenangkan, serta berbagai kebutuhan dengan harga terbaik.⁴⁵

⁴⁴ Ayu Rifka Sitoresmi, "Profil PT Tokopedia Dan Perjalanan Bisnisnya, Perusahaan Perdagangan Elektronik Di Indonesia," Liputan6.com, 2023, <https://www.liputan6.com/hot/read/5183788/profil-pt-tokopedia-dan-perjalanan-bisnisnya-perusahaan-perdagangan-elektronik-di-indonesia>.

⁴⁵ Kumparan, "Profil Perusahaan Shopee Sebagai Aplikasi Belanja Online Asia," Kumparan.com, 2022, <https://kumparan.com/berita-terkini/profil-perusahaan-shopee-sebagai-aplikasi-belanja-online-asia-1y5jwp8MoSo/1>.

4) Lazada

Lazada merupakan perusahaan *e-commerce* Asia Tenggara yang didirikan pada tahun 2012 oleh Rocket Internet, sebuah perusahaan inkubator teknologi dari Jerman. Awalnya, Lazada didirikan sebagai "*Amazon of Southeast Asia*" dengan model bisnis menjual produk langsung dari gudang mereka, tetapi kemudian berubah menjadi marketplace yang memungkinkan pihak ketiga menjual produk mereka. Pada tahun 2016, Alibaba Group mengakuisisi saham mayoritas di Lazada, memperkuat posisinya di pasar *e-commerce*. Platform digital ini menyediakan layanan jual beli online bagi penjual dan pembeli. Penjual dapat mendaftar dan menjual produk mereka melalui Seller Center, sementara pembeli dapat menelusuri, memilih, dan membeli produk yang diinginkan.⁴⁶

5) Blibli

Blibli Didirikan pada tahun 2011 blibli dikenal sebagai salah satu mal online terbesar di Indonesia dengan komitmen memberikan pengalaman berbelanja yang nyaman dan aman. Platform digital yang menyediakan berbagai macam produk seperti elektronik, fashion, aksesoris, kecantikan, dan lain sebagainya.⁴⁷

Perkembangan *marketplace* digital sebagai sarana transaksi daring telah membawa perubahan besar dalam pola konsumsi masyarakat. Dibalik kemudahan yang ditawarkan, penggunaan marketplace menuntut konsumen untuk

⁴⁶ Tempo, "Cerita Di Balik Mulai Beroperasinya Lazada 11 Tahun Lalu," Tempo.co, 2023, https://www.tempo.co/ekonomi/cerita-di-balik-mulai-beroperasinya-lazada-11-tahun-lalu-204670#goog_rewarded.

⁴⁷ Elga Nurmutia, "Profil Blibli, Perusahaan E-Commerce Milik Grup Djarum Yang Tercatat Di BEI," Liputan6.com, 2023, <https://www.liputan6.com/saham/read/5232245/profil-blibli-perusahaan-e-commerce-milik-grup-djarum-yang-tercatat-di-bei>.

menyerahkan berbagai data pribadi seperti nama lengkap, alamat rumah, nomor telepon, informasi rekening bank, hingga riwayat pembelian.⁴⁸

Data-data ini menjadi aset penting bagi penyedia layanan untuk keperluan analisis pasar, personalisasi layanan, dan peningkatan sistem keamanan. Namun, di sisi lain, data pribadi pengguna sangat rentan terhadap penyalahgunaan, baik oleh pihak internal maupun eksternal. Dalam konteks ini, hubungan antara marketplace dan data pribadi menjadi sangat erat dan kompleks, karena aktivitas jual beli tidak hanya menyangkut aspek ekonomi, tetapi juga menyangkut perlindungan hak individu atas privasi.

Pengelolaan data dalam ekosistem *marketplace* harus memperhatikan prinsip transparansi, persetujuan yang sah, serta tanggung jawab hukum atas keamanan informasi, agar tidak bertentangan dengan hak dasar pengguna maupun nilai-nilai etika dan hukum yang berlaku, termasuk dalam perspektif fikih Islam.

Layanan seperti *Shopee PayLater* mengharuskan pengguna untuk mengunggah data pribadi, termasuk Kartu Tanda Penduduk (KTP), sebagai bagian dari proses verifikasi identitas sebelum dapat menggunakan fasilitas kredit tersebut. Penggunaan KTP ini bertujuan untuk memastikan keabsahan identitas pemohon serta mencegah penyalahgunaan layanan oleh pihak yang tidak berwenang.⁴⁹ Namun, hal ini juga menimbulkan potensi risiko kebocoran data apabila pihak penyedia layanan tidak memiliki sistem keamanan data yang

⁴⁸ K S Dewi, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Pembelian Barang Di Marketplace" 7, no. 1 (2022): 64–70, http://eprints.unmas.ac.id/id/eprint/1527/%0Ahttp://eprints.unmas.ac.id/id/eprint/1527/2/1522_FH_watermark-15-27.pdf.

⁴⁹ Anisa Prasetya Putri Kartini, "Cara Daftar Shopee Paylater Beserta Syaratnya," *Tempo*, 2023, <https://www.tempo.co/ekonomi/cara-daftar-shopee-paylater-beserta-syaratnya-124266>.

memadai. Oleh karena itu, penyelenggara layanan seperti *Shopee PayLater* memiliki tanggung jawab besar untuk melindungi data pribadi pengguna sesuai dengan prinsip-prinsip perlindungan data dan regulasi yang berlaku, seperti yang diatur dalam Undang-Undang Perlindungan Data Pribadi di Indonesia.

Perkembangan teknologi informasi yang pesat telah mendorong peningkatan penggunaan data pribadi dalam berbagai aktivitas elektronik, termasuk transaksi digital dan layanan daring. Dalam konteks tersebut, perlindungan terhadap data pribadi menjadi hal yang esensial untuk menjamin hak privasi setiap individu. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, memuat ketentuan mengenai pentingnya perlindungan data pribadi dalam sistem elektronik.⁵⁰ Melalui ketentuan tersebut, UU ITE menegaskan bahwa setiap orang berhak atas perlindungan data pribadi, serta memiliki kendali atas pengumpulan, pemrosesan, dan penyebaran informasi pribadi miliknya.

Ruang lingkup perlindungan ini menjadi dasar hukum awal sebelum diterbitkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang secara lebih komprehensif mengatur pengelolaan data pribadi di Indonesia. *Cyber law* merupakan aspek hukum yang ruang lingkungannya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya. Sementara, ruang lingkup *cyber law* sendiri meliputi hak cipta, hak merek,

⁵⁰ Ridho Sadillah Ahmad, Dyah Ayu Puspaningtyas, and Muhammad Nur Karim Al Ismariy, "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital," *The Juris* 9, no. 1 (2025): 15–23, <https://doi.org/10.56301/juris.v9i1.1307>.

pencemaran nama baik, penistaan, penghinaan, transaksi elektronik, pengaturan sumber daya internet, keamanan pribadi, kehati-hatian, kejahatan *IT*, pembuktian, penyelidikan, pencurian lewat internet, perlindungan konsumen dan pemanfaatan internet dalam keseharian. Dimana *cyber law* ini juga berkaitan dengan upaya pencegahan dan penanganan tindak pidana serta menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan elektronik, termasuk kejahatan pencucian uang dan kejahatan terorisme.⁵¹

Mencegah maraknya berbagai kejahatan dan pelanggaran hukum dalam pemanfaatan teknologi. Undang-Undang No.19 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) disusun sebagai upaya untuk memberikan kepastian hukum dalam pemanfaatan teknologi informasi, serta untuk mencegah dan menanggulangi berbagai bentuk penyalahgunaan teknologi yang dapat merugikan individu maupun institusi.

Perkembangan pesat teknologi informasi di era digital saat ini membawa dampak yang signifikan terhadap berbagai sektor kehidupan, namun disisi lain menimbulkan tantangan serius dalam hal pelanggaran hukum, seperti pencurian data, penyebaran informasi palsu, hingga tindak pidana *siber* lainnya. Oleh karena itu, keberadaan regulasi yang mengatur transaksi elektronik menjadi sangat penting sebagai landasan hukum dalam mengatur aktivitas masyarakat di ruang digital.

⁵¹ News, “Aspek Dan Perbuatan Hukum Dalam Undang-Undang ITE,” Sip Law Firm, 2023, <https://siplawfirm.id/aspek-dan-perbuatan-hukum-dalam-undang-undang-ite/?lang=id>.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) memberikan pengaturan lebih lanjut terkait dengan aktivitas elektronik, termasuk transaksi daring, dokumen elektronik, serta perlindungan terhadap informasi dan data pribadi. Kehadiran undang-undang tersebut tidak hanya menjadi instrumen hukum dalam menanggulangi kejahatan di ruang digital, tetapi juga berperan penting dalam membentuk tata kelola teknologi informasi yang transparan dan akuntabel.

Negara melalui perangkat hukumnya berupaya untuk menyeimbangkan antara kebebasan berekspresi di dunia maya dan perlindungan terhadap kepentingan umum, termasuk perlindungan terhadap hak kekayaan intelektual dan keamanan informasi. Upaya ini tampak dari hadirnya berbagai regulasi yang mengatur ruang digital, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi. Regulasi tersebut tidak hanya berfungsi sebagai sarana pembatasan, melainkan juga sebagai instrumen untuk menciptakan keteraturan dan kepastian hukum dalam pemanfaatan teknologi informasi.⁵²

Implementasi dari Undang-Undang ITE menuntut adanya sinergi antara pemerintah, penegak hukum, pelaku industri, serta masyarakat sebagai pengguna teknologi informasi. Efektivitas penegakan hukum sangat bergantung pada pemahaman yang komprehensif terhadap substansi hukum itu sendiri, serta kemampuan untuk mengadaptasi peraturan yang ada dengan dinamika perkembangan teknologi yang begitu cepat. Oleh karena itu, diperlukan pula

⁵² Fachrul Razi, Hadi Tuasikal, and Dwi Pratiwi Markus, "Implementation and Challenges of the Personal Data Protection Law in Indonesia," *Jurnal Indonesia Sosial Teknologi* 5, no. 12 (2024): 6015–21, <https://doi.org/10.59141/jist.v5i12.1285>.

pembaruan regulasi secara berkala agar tetap relevan dengan kebutuhan masyarakat digital dan tidak tertinggal oleh kemajuan zaman.

Undang-Undang ITE mencakup beberapa aspek diantaranya:

1) Informasi Elektronik

Informasi Elektronik Merupakan satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI)*, surat elektronik (*electronic mail*), *telegram*, *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. (Pasal 1 ayat (1)).⁵³ Hal ini menunjukkan bahwa informasi elektronik mencakup berbagai bentuk representasi data yang tersimpan atau ditransmisikan secara digital, yang memiliki makna dan dapat digunakan dalam komunikasi maupun transaksi elektronik.

Ruang lingkup informasi elektronik sangat luas dan mencakup seluruh elemen yang dapat diinterpretasikan dalam sistem informasi digital, baik dalam bentuk teks, suara, gambar, maupun simbol digital lainnya. Hal ini menunjukkan bahwa informasi elektronik tidak terbatas pada data yang bersifat administratif atau formal, tetapi juga meliputi berbagai bentuk ekspresi digital yang memiliki nilai hukum dan sosial dalam interaksi daring.

⁵³ Moh. Faishol Hassanuddin, "UU Informasi Dan Transaksi Elektronik, Aspek Hukum Dan Pembuktiannya," Mahkamah Agung Republik Indonesia Pengadilan Tinggi Agama Samarinda, 2023, <https://pta-samarinda.go.id/artikel-pengadilan/1949-uu-informasi-dan-transaksi-elektronik-aspek-hukum-dan-pembuktiannya-oleh-dr-drs-h-moh-faishol-hasanuddin-s-h-m-h>.

2) Transaksi Elektronik

Transaksi Elektronik Merupakan perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya, dengan mencakup definisi, jenis, dan prosedur transaksi elektronik. (Pasal 1 ayat (2)).⁵⁴ Transaksi elektronik memiliki kekuatan hukum yang sama dengan transaksi konvensional selama memenuhi unsur-unsur legalitas sebagaimana ditetapkan dalam peraturan perundang-undangan. Dalam konteks Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), transaksi elektronik tidak hanya terbatas pada aktivitas jual beli daring, tetapi juga mencakup berbagai bentuk interaksi hukum lainnya seperti perjanjian, pembayaran, pengiriman dokumen elektronik, hingga pertukaran data secara digital antar pihak yang berwenang.

Pengakuan hukum sangat penting terhadap transaksi elektronik karena terletak pada kemampuannya untuk memberikan kepastian hukum ditengah perkembangan teknologi informasi yang pesat. Melalui pengaturan tersebut, negara memberikan landasan hukum yang kuat bagi pelaku usaha, konsumen, serta lembaga pemerintahan dalam menjalankan aktivitasnya secara efisien dan aman di ruang digital. Selain itu, keberadaan ketentuan mengenai prosedur dan validitas transaksi elektronik juga menjadi dasar dalam menjamin integritas dan keabsahan data yang digunakan selama proses transaksi berlangsung.

3) Teknologi Informasi

Teknologi Informasi merupakan suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, meng-analisis, dan/atau

⁵⁴ Abdul Halim Barkatullah, *Hukum Transaksi Elektronik (Sebagai Panduan Dalam Menghadapi Era Digital Bisnis e-Commerce Di Indonesia)*, n.d.

menyebarkan informasi. (Pasal 1 ayat (3)). Teknologi Informasi merujuk pada istilah penggunaan komputer, perangkat lunak, jaringan, dan infrastruktur telekomunikasi. Tujuan dari Teknologi Informasi sendiri untuk menyediakan solusi yang efektif dalam mengelola informasi yang dilakukan dengan cepat, akurat dan aman, serta dapat membantu pengambilan keputusan berdasarkan data yang valid.

4) Dokumen Elektronik

Dokumen Elektronik merupakan setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.⁵⁵ (Pasal 1 ayat (4)).

Dokumen elektronik memiliki kedudukan hukum yang setara dengan dokumen fisik, selama memenuhi unsur keabsahan dan keautentikan sebagaimana diatur dalam peraturan perundang-undangan. Dokumen elektronik tidak hanya terbatas pada bentuk teks, tetapi juga mencakup elemen multimedia seperti suara, gambar, dan simbol digital yang dapat diproses atau dimaknai oleh sistem elektronik maupun manusia. Dengan demikian, dokumen elektronik memiliki fleksibilitas bentuk dan fungsi yang luas, serta mampu menggantikan dokumen konvensional dalam berbagai aktivitas administrasi dan transaksi.

⁵⁵ Syahrul Ibad et al., “Pengembangan Pelayanan Publik Melalui E-Government (Studi Pada Layanan Smartcity Kabupaten Situbondo),” *Jurnal Administrasi Publik* 6, no. 2 (2020): 201–26.

Penggunaan dokumen elektronik semakin penting dalam era digital, terutama dalam mendukung efisiensi proses bisnis, pelayanan publik, dan komunikasi resmi antar lembaga. *Validitas* Hukum Dokumen Elektronik yang dijamin oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memberikan dasar legal yang kuat bagi penggunaannya diberbagai sektor.⁵⁶ Hal ini memungkinkan lembaga pemerintahan, perusahaan, dan individu untuk melakukan pertukaran informasi secara cepat, aman, dan dapat dipertanggungjawabkan secara hukum, asalkan dokumen tersebut disusun dan dikelola dengan memenuhi prinsip integritas, *autentikasi*, dan *non-repudiation*.

Dari penjelasan diatas dapat disimpulkan bahwa ruang lingkup materi yang diatur dalam Undang-Undang ITE sangatlah luas dan saling berkaitan dengan bidang hukum yang lainnya, misalnya hukum telekomunikasi, hukum penyiaran, hukum kontrak atau perjanjian, hukum administrasi, hukum bisnis atau perdagangan, hukum perdata, dan hukum pidana, baik secara nasional maupun dalam lingkup dunia Internasioal, serta berbagai peraturan Perundang-Undangan lainnya.

Ruang lingkup global dari aktivitas elektronik juga menuntut adanya harmonisasi antara Undang-Undang ITE dengan ketentuan hukum internasional, seperti konvensi tentang kejahatan *siber* (*cybercrime*), perlindungan data lintas negara, dan standar keamanan informasi internasional. Dalam konteks ini, Undang-Undang ITE memiliki peran strategis sebagai dasar hukum nasional yang mendukung posisi Indonesia dalam dunia global, khususnya dalam kerja sama

⁵⁶ Astri Aprilianti, "Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi," *Begawan Abioso* 15, no. 1 (2025): 41–50, <https://doi.org/10.37893/abioso.v15i1.1002>.

internasional terkait dengan penanggulangan kejahatan *siber*, perlindungan konsumen digital, dan penguatan tata kelola data. Dengan demikian, keberadaan Undang-Undang ITE menjadi sangat penting dalam mendukung transformasi digital nasional, baik dari sisi regulasi maupun implementasi teknis.⁵⁷ Untuk mewujudkan sistem hukum digital yang responsif dan berkeadilan, dibutuhkan sinergi antarsektor serta pembaruan regulasi secara berkala agar mampu mengantisipasi perkembangan teknologi yang semakin kompleks.

Era digital saat ini semakin berkembang pesat, perlindungan terhadap data pribadi menjadi isu yang sangat krusial, terutama seiring dengan meningkatnya pemrosesan data melalui berbagai platform elektronik. Untuk menjawab tantangan ini, Indonesia telah mengesahkan dua regulasi utama yang berkaitan dengan tata kelola informasi elektronik dan data pribadi, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kedua undang-undang ini memiliki peran strategis dalam membentuk kerangka hukum nasional terkait aktivitas digital dan pengelolaan data pribadi.

Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik terdapat perbedaan mendasar dalam ruang lingkupnya dari sisi fokus pengaturan, Undang-Undang Perlindungan Data Pribadi secara khusus mengatur mengenai perlindungan data pribadi individu, mulai dari proses

⁵⁷ Martini Idris, Meirina Nurlani, and Serlika Aprita, "Pengaturan Dan Penegakan Hukum Kejahatan Dunia Maya (Cyber Crime): Harmonisasi Revisi Undang-Undang ITE Dan KUHP," *Lex Lata : Jurnal Ilmiah Ilmu Hukum* 6, no. 3 (2024): 396–411, <https://doi.org/10.28946/lexl.v6i3.4266>.

pengumpulan hingga penghapusan data, sedangkan Undang-Undang Informasi Teknologi Elektronik memiliki cakupan yang lebih luas namun tidak spesifik, karena berfokus pada transaksi elektronik, informasi digital, serta tindak pidana *siber*. Dalam hal ini, perlindungan data dalam UU ITE hanya disebut secara terbatas, seperti dalam Pasal 26 yang mengatur persyaratan persetujuan penggunaan data pribadi.

Cakupan data dari Undang-Undang Perlindungan Data Pribadi secara eksplisit membedakan antara data pribadi umum dan data pribadi spesifik, seperti data kesehatan, biometrik, dan finansial. Hal ini tidak ditemukan dalam Undang-Undang Informasi Teknologi Elektronik yang tidak memberikan klasifikasi khusus terhadap jenis data pribadi. Selanjutnya, dari segi prinsip dan kewajiban, Undang-Undang Perlindungan Data Pribadi menetapkan prinsip-prinsip yang komprehensif seperti kejelasan tujuan, dasar persetujuan, keamanan, serta akuntabilitas dalam pemrosesan data pribadi.

Undang-Undang perlindungan data pribadi mewajibkan pengendali data untuk melaporkan insiden kebocoran serta menunjuk pejabat pelindung data. Sebaliknya, Undang-Undang Informasi Teknologi Elektronik tidak secara rinci mengatur prinsip-prinsip tersebut dan lebih berfokus pada peran penyelenggara sistem elektronik dalam konteks hukum umum. Perbedaan lain yang signifikan terletak pada aspek sanksi dan penegakan hukum. Undang-Undang Perlindungan Data Pribadi memuat ketentuan sanksi yang lebih berat dan terstruktur, baik dalam bentuk sanksi pidana (dengan ancaman penjara hingga 6 tahun) maupun

sanksi administratif seperti denda hingga dua persen dari pendapatan tahunan.⁵⁸ Sebaliknya, Undang-Undang ITE hanya memberikan sanksi pidana umum terhadap pelanggaran privasi dan kejahatan siber, tanpa pengaturan khusus terkait kebocoran data pribadi.⁵⁹ Penerapan, Undang-Undang Perlindungan Data pribadi memiliki jangkauan yang lebih luas karena berlaku untuk seluruh entitas publik dan privat, baik yang menggunakan sistem elektronik maupun non-elektronik, serta mencakup pengaturan transfer data lintas negara. Sementara itu, Undang-Undang ITE terbatas pada aktivitas yang berlangsung dalam sistem elektronik saja, dan tidak mengatur mekanisme transfer data lintas yurisdiksi.

Perspektif dari kedudukan hukum dilihat bahwa, Undang-Undang Perlindungan Data Pribadi dapat dikategorikan sebagai *lex specialis* terhadap isu perlindungan data pribadi, yang mengesampingkan ketentuan dalam Undang-Undang Informasi Teknologi Elektronik apabila terjadi tumpang tindih norma.

Undang-Undang ITE, sebagai *lex generalis*, tetap relevan sebagai dasar hukum awal yang mengatur informasi elektronik secara umum, namun peranannya dalam hal perlindungan data pribadi kini telah dilengkapi dan diperjelas oleh kehadiran Undang-Undang Perlindungan Data Pribadi.⁶⁰ Hal ini menegaskan pentingnya harmonisasi antara kedua undang-undang tersebut dalam

⁵⁸ Mochamad Januar Rizki, "Ancaman Sanksi Administratif Hingga Pidana Dalam UU Pelindungan Data Pribadi," Hukum Online.com, 2022, <https://www.hukumonline.com/berita/a/ancaman-sanksi-administratif-hingga-pidana-dalam-uu-pelindungan-data-pribadi-lt633c69ce2de5c?>

⁵⁹ Desmon Trisandi and Ahmad Sofian, "Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber Indonesia," *Syntax Literate; Jurnal Ilmiah Indonesia* 9, no. 2 (2024): 728–37, <https://doi.org/10.36418/syntax-literate.v9i2.15198>.

⁶⁰ Elyasa Yahya Saputri, "Regulasi Hukum Dalam Melindungi Data Pribadi," Radarmagelang.id, 2025, https://radarmagelang.jawapos.com/artikel-ilmiah/686176164/regulasi-hukum-dalam-melindungi-data-pribadi?#google_vignette.

menciptakan sistem perlindungan data yang komprehensif dan adaptif terhadap dinamika teknologi informasi.

B. Kasus Kebocoran Data Pribadi

Beberapa tahun terakhir, sejumlah platform marketplace di Indonesia tercatat mengalami insiden kebocoran data pribadi pengguna. Salah satu kasus terbesar terjadi pada Tokopedia pada Mei 2020, ketika lebih dari 91 juta data akun pengguna diduga bocor dan diperjualbelikan di forum daring. Data yang bocor meliputi nama lengkap, alamat email, nomor telepon, tanggal lahir, jenis kelamin, serta kata sandi yang telah di-hash. Bentuk kebocoran ini menunjukkan adanya peretasan terhadap sistem basis data internal yang kemudian dimanfaatkan oleh pihak ketiga untuk menyebarkan atau memperdagangkan informasi tersebut.⁶¹

Model kebocoran data pada kasus Tokopedia termasuk dalam kategori peretasan sistem basis data internal (*data breach*). Dalam hal ini, pelaku kejahatan siber (*hacker*) berhasil menembus sistem keamanan database Tokopedia dan menyalin data pengguna yang tersimpan, termasuk nama, email, nomor telepon, tanggal lahir, dan kata sandi yang telah di-hash. Setelah data diambil, informasi tersebut kemudian diperjualbelikan di forum online atau *dark web*. Dimana bentuk penipuannya seperti:

1. Phising: Pelaku menggunakan data yang bocor untuk membuat email, SMS, atau pesan palsu yang seolah-olah berasal dari Tokopedia atau institusi resmi lainnya.

⁶¹ Cyberthreat.id, “91 Juta Data Pengguna Tokopedia Diduga Bocor Dan Diperjualbelikan,” 2020.

2. *Social Engineering*: Pelaku mengaku dari layanan Tokopedia dan meminta OTP dengan alasan keamanan, padahal untuk membajak akun atau mencuri uang korban.
3. *Credential Stuffing*: Data berisi email dan password yang di-*hash*, jika pelaku berhasil mendekripsi hash-nya atau korban menggunakan kata sandi yang sama di berbagai platform, pelaku bisa mencoba login ke akun media sosial, e-wallet, hingga perbankan korban.

Dalam kasus Tokopedia jenis penipuan yang digunakan oleh pelaku yaitu:

1. Penipuan Identitas: Data pribadi digunakan untuk membuat akun palsu, mengajukan pinjaman online, atau tindakan kriminal atas nama korban.
2. Penipuan Finansial: Pelaku mencuri uang korban lewat akses akun e-commerce, e-wallet, atau akun perbankan digital.
3. Penipuan berbasis OTP atau login palsu: Memanfaatkan kepercayaan korban untuk mendapatkan kode rahasia, lalu menyalahgunakannya.

Marketplace atau biasa disebut dengan belanja online menjadi bagian yang tidak terpisahkan dari kehidupan masyarakat dalam memenuhi kebutuhan konsumsi dan perdagangan. Namun, dibalik kemudahan yang ditawarkan, terdapat risiko yang signifikan terhadap keamanan dan privasi data pribadi pengguna.

Salah satu isu paling krusial yang muncul adalah kebocoran data pribadi, dimana informasi sensitif milik konsumen disalahgunakan, diperjualbelikan, atau tersebar tanpa izin. Fenomena ini tidak hanya menimbulkan kerugian secara individu, tetapi juga merusak kepercayaan publik terhadap penyelenggara sistem

elektronik. Berikut gambar syarat dan ketentuan layanan dalam aplikasi marketplace shopee:

3. Penggunaan Layanan

3.1 Anda setuju bahwa Anda hanya akan menggunakan Layanan untuk tujuan mengajukan permohonan untuk mendapatkan Fasilitas Pendanaan, menerima Fasilitas Pendanaan dari Pemberi Dana sebagaimana disetujui dalam Perjanjian Fasilitas Pendanaan, dan tujuan lain yang diperbolehkan oleh peraturan perundang-undangan yang berlaku.

3.2 Dalam rangka penyediaan Layanan oleh Pemberi Dana melalui LDN, Anda mengakui dan menyetujui bahwa LDN berperan sebagai perantara yang mempertemukan Pemberi Dana dan Penerima Dana untuk tujuan pemberian Fasilitas Pendanaan.

3.3 Untuk menggunakan Layanan, Anda wajib melakukan pendaftaran dalam Platform Shopee atau platform lainnya sebagaimana tersedia, memberikan data pribadi sesuai ketentuan yang disyaratkan dalam halaman pendaftaran dan melakukan pengkinian data pribadi sesuai dengan ketentuan Peraturan Yang Berlaku.

3.4 Dalam rangka memenuhi Peraturan Yang Berlaku atau sebagaimana dianggap diperlukan oleh LDN, Pemberi Pinjaman dan/atau pihak ketiga yang bekerja sama dengan LDN, termasuk namun tidak terbatas pada pihak ketiga Penyelenggara Sertifikasi Elektronik (PSE-E), berhak untuk melaksanakan credit scoring, customer due diligence dan/atau tindakan lain untuk memeriksa kelayakan Anda sebagai calon Penerima Pinjaman untuk mendapatkan Fasilitas Pinjaman dan memenuhi kewajiban pelunasan Fasilitas Pinjaman. Untuk menghindari keraguan, Pemberi Dana atau LDN dapat bekerja sama dengan pihak ketiga penyedia layanan penerbitan sertifikat elektronik dan tanda tangan elektronik yang diperlukan sehubungan dengan Layanan termasuk untuk hal-hal yang disebutkan pada kalimat sebelumnya. Untuk keperluan tersebut dan tanpa mengurangi sifat umum dari ketentuan di atas ataupun ketentuan lainnya dalam Syarat dan Ketentuan Layanan ini, Anda menyetujui hal-hal berikut ini:

(a) Ketentuan PT Indonesia Digital Identity ("VIDA")

1. Sehubungan dengan verifikasi identitas untuk tujuan menggunakan Layanan, data pribadi Anda berupa data demografi dan/atau biometrik akan diperiksa kesesuaiannya, oleh PT Indonesia Digital Identity (VIDA) sebagai mitra LDN, dengan data yang tercatat pada sistem nasional pemerintahan yang berhak mengeluarkan identitas tersebut. Apabila data pribadi Anda diverifikasi kesesuaiannya, maka VIDA sebagai Penyelenggara Sertifikasi Elektronik tersertifikasi oleh

Gambar 2.3 Syarat dan Ketentuan Aplikasi Marketplace Shoope

Proses pendaftaran pada layanan *marketplace* umumnya mengharuskan pengguna untuk memberikan data pribadi seperti nama lengkap, alamat, nomor telepon, alamat email, hingga informasi keuangan. Data ini tidak hanya digunakan oleh pihak penyelenggara *platform*, tetapi juga berpotensi dibagikan kepada pihak ketiga yang terafiliasi, seperti mitra logistik, penyedia layanan pembayaran, atau pihak pemasaran, sesuai dengan kebijakan privasi yang disetujui pengguna.⁶² Dalam hal ini, pengguna secara tidak langsung memberikan hak kepada pihak-pihak tersebut untuk mengakses dan memproses data pribadinya, yang bisa menimbulkan risiko apabila tidak dikelola dengan transparan dan bertanggung jawab. Beberapa contoh kasus yang dapat dilihat dari kebocoran data yang terjadi di *e-commerce*:

⁶² Kadek Dio Ramadi Natha., I Nyoman Putu Budiarta., and Ni Gusti Ketut Sri Astiti, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada Perdagangan Elektronik Lokapasar (Marketplace)," *Jurnal Preferensi Hukum* 3, no. 1 (2022): 143–48.

1. *platform Tokopedia*. Dimana pada tahun 2020 Tokopedia dilaporkan mengalami peretasan yang jumlahnya diperkirakan sekitar 91 juta akun dan 7 juta akun merchant. Pelaku menjual data tersebut di *darkweb*, berupa User ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor handphone, dan *password*. Hal ini menimbulkan kekhawatiran yang serius terhadap perlindungan data pribadi di sektoral *e-commerce*.

Kasus ini menjadi perhatian publik luas dan menimbulkan pertanyaan tentang kesiapan penyelenggara sistem elektronik (PSE) dalam menjaga keamanan data pengguna. Dalam konteks hukum, saat itu belum terdapat Undang-Undang Perlindungan Data Pribadi (UU PDP) yang secara khusus mengatur mekanisme dan kewajiban perlindungan data pribadi. Penanganan kasus ini lebih banyak merujuk pada Pasal 26 UU ITE, yang mewajibkan persetujuan dari pemilik data untuk setiap penggunaan data pribadi, namun tidak mengatur secara komprehensif tentang tanggung jawab penyelenggara sistem elektronik terhadap insiden kebocoran data.⁶³

2. Kasus kebocoran data pribadi pada *platform Marketplace* Lazada di Singapura pada Oktober 2022. Anak perusahaan Alibaba Group ini mengalami insiden kebocoran data yang melibatkan 1,1 juta akun pelanggan RedMart, yang merupakan bagian dari Lazada. Data yang bocor termasuk nama lengkap, alamat pengiriman, nomor telepon, dan sebagian informasi kartu pembayaran. Tidak seperti di Indonesia saat kasus Tokopedia terjadi, Singapura telah memiliki

⁶³ Aditya Jaya Iswara, "Data 91 Juta Pengguna Tokopedia Diduga Bocor, Media Asing Ikut Soroti," Kompas.com, 2020, <https://www.kompas.com/global/read/2020/05/03/133257970/data-91-juta-pengguna-tokopedia-diduga-bocor-media-asing-ikut-soroti?page=all>.

kerangka hukum yang komprehensif dalam bentuk Personal Data Protection Act (PDPA) sejak tahun 2012. Berdasarkan PDPA, perusahaan pengendali data diharuskan untuk menerapkan langkah-langkah keamanan yang memadai, dan wajib melaporkan insiden pelanggaran data kepada otoritas dalam waktu maksimal 72 jam setelah diketahui. Lazada kemudian mengonfirmasi pelanggaran tersebut, menghentikan sementara layanan RedMart, dan bekerja sama dengan otoritas perlindungan data untuk mitigasi lebih lanjut.⁶⁴

3. Kasus lainnya yang terjadi yaitu pada kasus aktris Luna Maya yang mengaku ditipu oleh salah seorang oknum tidak bertanggungjawab yang mengaku sebagai *Customer Service* salah satu layanan operator *telepon*. Akibatnya Luna Maya kehilangan uang senilai 1,9 juta. Kejadian tersebut bermula ketika Luna Maya ditelpon oleh orang tersebut dan menawarkan untuk menukarkan poin yang dimiliki oleh Luna dilayanan operator tersebut. Dari penukaran poin tersebut, Luna akan mendapatkan layanan telepon gratis selama 3 bulan. Oknum tersebut kemudian menawarkan Luna untuk menukarkan sisa poinnya dengan uang senilai Rp800 ribu.⁶⁵

Dari kasus Luna Maya tersebut dapat disimpulkan bahwa modus *social engineering* masih marak digunakan untuk mengecoh korban dengan berpura-pura menjadi pihak resmi, dalam hal ini customer service e-wallet. Oknum tersebut biasanya memancing korban untuk memberikan kode *OTP*, *password*, atau

⁶⁴ CNN Indonesia, "Lazada Konfirmasi Peretasan 1,1 Juta Akun RedMart," CNN Indonesia, 2022, <https://www.cnnindonesia.com/teknologi/20201031103811-185-564335/lazada-konfirmasi-peretasan-11-juta-akun-redmart>.

⁶⁵ CNN Indonesia, "Luna Maya Jadi Korban Penipuan, Rugi Rp1,9 Juta," CNN Indonesia, 2022, <https://www.cnnindonesia.com/hiburan/20220202123717-234-754031/luna-maya-jadi-korban-penipuan-rugi-rp19-juta>.

bahkan akses ke akun pribadi, dengan dalih verifikasi akun atau adanya transaksi mencurigakan. Padahal, informasi tersebut bersifat sangat rahasia dan tidak seharusnya diminta oleh pihak resmi melalui telepon atau pesan singkat. Dalam hal ini jika mendapatkan telepon dari nomor tidak dikenal yang mengaku sebagai customer service *E-wallet* manapun ada baiknya kita harus berhati-hati dalam menggunakan layanan keuangan elektronik.

Perlindungan data pribadi di Indonesia saat ini diatur dalam Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mengatur asas, jenis data pribadi, hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali data pribadi, kelembagaan, sanksi administratif, sanksi pidana dan banyak hal lainnya.

Tujuan utama dari perlindungan data pribadi adalah untuk melindungi hak konstitusional subjek data pribadi. Undang-undang ini memberikan landasan hukum yang kuat untuk memberikan keamanan atas data pribadi berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Undang-Undang Nomor 27 Tahun 2022 juga menetapkan bahwa pengendali data pribadi wajib melindungi data yang mereka kelola dan transfer data pribadi ke pihak lain dalam wilayah hukum Indonesia, hal ini mencakup pengaturan mengenai berbagai jenis data pribadi seperti data kesehatan, data biometrik, data genetika, dan data keuangan pribadi. Pengendali data pribadi memiliki kewajiban untuk memberikan salinan data pribadi secara gratis kepada subjek data pribadi, kecuali untuk kondisi tertentu yang memerlukan biaya.

Undang-Undang Nomor 27 Tahun 2022, selain kewajiban untuk melindungi data pribadi, memberikan hak kepada subjek data pribadi, undang-undang ini juga untuk mengetahui tujuan dan keabsahan pengumpulan data oleh pengendali data. Subjek data berhak untuk mendapatkan informasi mengenai pihak yang menerima data pribadi mereka dan lamanya data tersebut disimpan. Hal ini bertujuan untuk memberikan transparansi dan akuntabilitas dalam pengelolaan data, sehingga mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Singapura, Korea Selatan, dan Indonesia telah menerapkan undang-undang perlindungan data pribadi yang mencakup serangkaian informasi diluar rincian data pribadi umum seperti nama lengkap, nomor registrasi nasional, informasi kontak, data biometrik, dan foto. Kategori data lainnya mencakup informasi sensitif, yang memerlukan pemrosesan khusus untuk memastikan keamanan dan perlindungan karena potensi dampaknya terhadap individu jika salah ditangani atau diungkapkan. Ada pula informasi yang disamarkan (*Pseudonymized Information*), yang diproses sedemikian rupa sehingga individu tidak dapat diidentifikasi tanpa informasi tambahan, sehingga mengurangi risiko akses tidak sah atau penyalahgunaan. Jenis data ini dapat digunakan untuk analisis statistik, penelitian ilmiah, pengarsipan, dan tujuan lainnya tanpa persetujuan eksplisit dari subjek data.⁶⁶

⁶⁶ Sukarso Lailatul Badriah, Dwiyanto Indiahono, "Akuntabilitas Dalam Kebijakan Perlindungan," *Inovasi Kebijakan* 8 (2023): 89–102.

Regulasi Perlindungan Data Umum atau *General Data Protection Regulation* (GDPR) yang diberlakukan di Uni Eropa menjadi acuan global dalam perlindungan data pribadi. Latar belakang pembentukan GDPR berakar dari kebutuhan akan harmonisasi regulasi perlindungan data di seluruh negara Eropa dan respons terhadap perkembangan teknologi digital yang semakin kompleks.

GDPR memiliki ruang lingkup pengaturan yang sangat komprehensif, mencakup tidak hanya proses pengumpulan dan pengolahan data, tetapi juga mekanisme penegakan hukum yang ketat. Hak-hak subjek data dalam GDPR lebih rinci, termasuk hak untuk dipulihkan (*right to be forgotten*), hak portabilitas data, dan hak untuk mendapatkan pemberitahuan dalam waktu 3x24 jam jika terjadi pelanggaran data. Salah satu instrumen penting dalam implementasi perlindungan data adalah *Register of Processing Activities* (ROPA).

ROPA merupakan dokumentasi komprehensif yang berisi seluruh informasi atau aktivitas pemrosesan data yang dilakukan oleh suatu organisasi. Dalam hal ini ROPA memastikan kepatuhan terhadap peraturan perlindungan data.⁶⁷ Definisi dan tujuan ROPA adalah untuk menciptakan transparansi dan akuntabilitas dalam pengelolaan data pribadi. Unsur-unsur yang harus dicantumkan dalam ROPA meliputi identitas pengendali dan pemroses data, tujuan pemrosesan, kategori data yang diproses, basis hukum pemrosesan, serta periode retensi data. Manfaat ROPA tidak hanya sebatas dokumentasi, tetapi juga sebagai alat untuk memastikan kepatuhan terhadap regulasi perlindungan data dan

⁶⁷ Ferinda K Fachri, "Mengenal ROPA, Catatan Aktivitas Pengolahan Data Pribadi," Hukum Online.com, 2023, <https://www.hukumonline.com/berita/a/mengenal-ropa--catatan-aktivitas-pengolahan-data-pribadi-lt651dafcd8038d/>.

memfasilitasi audit internal maupun eksternal.⁶⁸ Melalui pembahasan komprehensif ini, dapat dipahami bahwa perlindungan data pribadi bukanlah sekadar isu teknis, melainkan refleksi dari penghormatan terhadap hak asasi manusia di era digital.⁶⁹

Prinsip akuntabilitas adalah inti dari perlindungan data pribadi sebagaimana tercantum dalam Pasal 5 *GDPR*. Pengendali data pribadi berkewajiban untuk mempertanggungjawabkan dan menunjukkan kepatuhan terhadap enam prinsip perlindungan data lainnya. Ini berarti akuntabilitas mempengaruhi dan memastikan harus terpenuhinya semua prinsip perlindungan data pribadi. Oleh karena itu, sebagai regulasi acuan Undang-Undang Perlindungan Data Pribadi, prinsip-prinsip *GDPR* diintegrasikan ke dalam pasal-pasal UU PDP.

Prinsip akuntabilitas memastikan bahwa pengendali data pribadi harus memenuhi prinsip-prinsip perlindungan data pribadi lainnya dan mampu menunjukkan kepatuhan tersebut kepada pemilik data yang diproses. Prinsip ini diyakini akan memberikan perlindungan dan kepastian hukum yang lebih baik bagi perlindungan data pribadi di Indonesia. Hal ini sesuai dengan teori-teori hukum tentang asas/prinsip, teori hukum tentang perlindungan hukum, dan teori hukum tentang kepastian hukum, yang semuanya menekankan pentingnya

⁶⁸ Yahya Ziqra, Mahmul Siregar, and Jelly Leviza, "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online," *Iuris Studia: Jurnal Kajian Hukum* 2 (2021): 330–36, <https://doi.org/10.55357/is.v2i2.146>.

⁶⁹ Ahmad M Ramli et al., "Perlindungan Data Pribadi Di Indonesia Melalui Mekanisme Register of Processing Activities (ROPA): Studi Komparatif Antara UU PDP Dengan GDPR" 2 (2024): 274–83.

kerangka hukum yang jelas, adil, dan konsisten untuk melindungi hak-hak individu.⁷⁰

Pengendali dan Pemroses harus bertanggung jawab atas cara mereka memproses data pribadi dan mematuhi prinsip-prinsip lainnya. Pasal 5 (2) GDPR menyatakan, “Pengendali harus bertanggung jawab, dan mampu menunjukkan kepatuhan terhadap, pengendali data. Akuntabilitas dibagi menjadi dua bagian:

- 1) Tanggung jawab atas kepatuhan: Menjadi proaktif dan sistematis tentang perlindungan data pribadi.
- 2) Menunjukkan kepatuhan: Menunjukkan bukti dan pembenaran atas langkah-langkah yang telah diambil organisasi untuk mematuhi GDPR.⁷¹

Hukum perlindungan data pribadi pada prinsipnya berfokus pada upaya perlindungan dan kemudahan terhadap pengumpulan dan penggunaan data pribadi, sedangkan hukum keamanan siber membahas mengenai tindak kriminal yang terjadi melalui sistem dan infrastruktur komputer.⁷² Dalam dunia digital keamanan *siber* menjadi salah satu hal yang harus diperhatikan dan dijaga karena merupakan sebuah aset yang harus dilindungi untuk menjaga rahasia dagang dari akses yang tidak sah, dimana jika terjadi pelanggaran tersebut dapat berdampak besar pada keuangan perusahaan dan juga hilangnya suatu kepercayaan pelanggan.

⁷⁰ 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, no. 4 (2024): 3412–25.

⁷¹ Robert Healey, “GDPR Dan Prinsip Akuntabilitas,” FORMITI, 2020, <https://www.lexology.com/library/detail.aspx?g=34144a92-3aa2-4c75-b1c3-346be0719117>.

⁷² Rendy Pratama Putra et al., “Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi,” *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 2898–2905, <https://j-innovative.org/index.php/Innovative/article/view/6662>.

Salah satu bentuk dari perlindungan Hak Asasi Manusia adalah perlindungan terhadap data pribadi seseorang, salah satu contohnya terdapat pada negara lain, hal tersebut telah diakui oleh HAM yaitu dalam Piagam HAM Eropa dan Deklarasi HAM ASEAN. Deklarasi Universal HAM yang terbentuk pada tahun 1948 pada akhirnya mengakui hak untuk melindungi data pribadi sebagai HAM setelah melalui proses *evolusi* yang panjang, dimana hak tersebut terbentuk dari persilangan antara hak atas informasi dan hak atas privasi.⁷³

Data pribadi sejatinya merupakan informasi nyata dan otentik yang melekat pada seseorang sehingga dapat mengidentifikasi orang tersebut. Pentingnya perlindungan data pribadi adalah untuk memastikan bahwa data pribadi yang dikumpulkan oleh individu digunakan sesuai dengan tujuan pengumpulannya, sehingga dapat menghindari penyalahgunaan data.

Transparansi dan akuntabilitas juga krusial, dimana konsumen berhak mendapatkan informasi yang jelas tentang bagaimana data mereka dikumpulkan dan digunakan, serta perusahaan juga bertanggung jawab atas pengelolaannya. Konsumen juga harus diberitahu dan memberikan persetujuan sebelum data mereka diproses, serta diberikan akses serta hak untuk memperbaiki data yang dimilikinya.⁷⁴

⁷³ Rosihan Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia," *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36, <https://doi.org/10.59188/jurnalsostech.v2i5.336>.

⁷⁴ Yuyut Prayuti, "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di Indonesia," *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13, <https://doi.org/10.22225/juinhum.5.1.8482.903-913>.

Undang-Undang Perlindungan Data Pribadi di Indonesia dirancang untuk memberikan perlindungan hukum secara menyeluruh bagi data pribadi di Indonesia, dimana undang-undang ini mengatur segala aspek yang terkait mengenai pengumpulan, pengolahan, dan pemanfaatan data pribadi oleh pihak ketiga. Lebih lanjut, Undang-Undang perlindungan data pribadi memberlakukan sanksi bagi pelaku usaha yang melanggar hak privasi data pribadi konsumen sebagai bentuk penegakan hukum yang tegas, disamping itu UU PDP memberikan hak penuh kepada konsumen sebagai pengendali penuh terhadap informasi data mereka.⁷⁵

Dalam Undang-Undang Perlindungan Data Pribadi (PDP) menegaskan bahwa UU PDP harus dipahami secara konteks hukum yang terkait dengan perlindungan data pribadi. Oleh karena itu, UU PDP dalam tatanan hukum merupakan Undang-Undang yang bersifat khusus, sehingga adanya norma lain yang disebutkan dalam aturan pasal-pasalanya secara hukum harus merujuk pada ketentuan dalam Undang-Undang lain yang mengatur secara khusus, termasuk dalam perkara Undang-Undang yang mengatur tentang pertahanan dan keamanan nasional.⁷⁶

Penerapan Undang-undang perlindungan data pribadi saat ini, pemerintah berharap dapat meminimalisir adanya kebocoran data yang selama ini kerap menghantui perusahaan teknologi di Indonesia. UU PDP mencakup berbagai aspek penting yang sebelumnya diabaikan dalam regulasi terkait data di

⁷⁵ 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.

⁷⁶ Sri Pujiarti, “Pemerintah: UU Perlindungan Data Pribadi Beri Perlindungan Hukum,” *Humas MKRI*, 2023, <https://www.mkri.id/index.php?page=web.Berita&id=18915>.

Indonesia, undang-undang ini mengatur segala sesuatu mulai dari bagaimana data dikumpulkan, disimpan, diproses, hingga dihapus, dimana undang-undang ini memberikan hak kepada individu untuk meminta akses, koreksi, bahkan penghapusan data pribadi mereka jika diperlukan.⁷⁷

Perlindungan hukum merupakan suatu hal yang dilindungi sebagai subyek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan adanya sanksi yang diberikan. Tujuan dari perlindungan hukum yaitu untuk memastikan bahwa setiap orang memiliki akses yang sama terhadap keadilan, mendapatkan perlakuan yang adil, dan dijamin hak-haknya oleh hukum. Perlindungan hukum dapat dibedakan menjadi dua, yaitu perlindungan hukum preventif dan represif.⁷⁸

Perlindungan hukum preventif memberikan subyek hukum kesempatan untuk mengajukan keberatan atau pendapat sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Perlindungan hukum yang preventif bertujuan untuk mencegah terjadinya permasalahan atau sengketa. Perlindungan hukum yang represif bertujuan untuk menyelesaikan permasalahan atau sengketa yang timbul. Perlindungan hukum terhadap tindakan pemerintah yang bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia.

⁷⁷ Dwitri Waluyo, "Era Baru Perlindungan Data Pribadi," INDONESIA.GO.ID Portal Informasi Indonesia, 2024, <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>.

⁷⁸ Erna Priliyasi, "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia)," *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79.

Konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia merupakan prinsip fundamental dalam hukum dan keadilan yang diarahkan kepada pembatasan-pembatasan dan peletakan kewajiban masyarakat dan pemerintah. Perlindungan hak asasi manusia juga mencakup upaya untuk memastikan bahwa setiap individu dapat menikmati hak-haknya tanpa diskriminasi. Pentingnya menekankan sikap menghargai dalam perlindungan hak asasi manusia di mana semua individu, tanpa memandang latar belakang, berhak mendapatkan perlindungan yang sama.⁷⁹

Pengakuan dan perlindungan HAM merupakan tanggung jawab bersama antara negara, masyarakat, dan komunitas internasional. diperlukan hukum yang kuat, lembaga yang efektif, serta kesadaran masyarakat untuk memastikan bahwa hak-hak fundamental ini benar-benar dihormati dan dilindungi di seluruh dunia.

Indonesia, sebelum adanya Undang-Undang Perlindungan Data Pribadi tidak memiliki payung hukum khusus yang mengatur mengenai perlindungan data pribadi. Perlindungan data hanya diatur secara keseluruhan dalam beberapa peraturan seperti UU ITE, dan peraturan sektoral. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memang menjadi salah satu dasar hukum yang mengatur perlindungan data, namun cakupannya terbatas dan lebih fokus pada transaksi elektronik. Selain itu, beberapa sektor seperti perbankan, kesehatan, dan telekomunikasi memiliki peraturan sektoral yang mengatur perlindungan data, namun hal ini menimbulkan ketidak konsistenan dalam penerapannya. Akibatnya,

⁷⁹ D I Era and Revolusi Industri, "UNIVERSITAS NEGERI MEDAN DALAM MEREALISASIKAN HAK ASASI WARGA NEGARA" XII (2023): 93–103.

masyarakat seringkali merasa kurang terlindungi karena tidak adanya standar yang jelas dan menyeluruh.

Dengan banyaknya kasus kebocoran data yang terjadi tanpa adanya sanksi yang tegas terhadap pelaku. Hal ini menimbulkan kekhawatiran di kalangan masyarakat, terutama di era digital dimana pertukaran data terjadi secara masif. Selain itu, ketiadaan regulasi yang komprehensif juga menghambat Indonesia dalam menjalin kerja sama internasional, terutama dengan negara-negara yang telah memiliki standar ketat dalam perlindungan data pribadi seperti Uni Eropa dengan General Data Protection Regulation (GDPR)-nya.⁸⁰

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) merupakan langkah penting Indonesia dalam mengatur dan melindungi hak individu atas data pribadi. Undang-undang ini disahkan untuk merespons tantangan era digital yang semakin kompleks, dimana penyalahgunaan data pribadi menjadi masalah serius.⁸¹ Dengan adanya Undang-Undang ini, Indonesia memiliki payung hukum yang jelas untuk mengatur pengumpulan, penyimpanan, dan penggunaan data pribadi oleh berbagai pihak, baik pemerintah maupun swasta. Hal ini diharapkan dapat meningkatkan kepercayaan masyarakat dalam bertransaksi digital dan mengurangi risiko kebocoran data. Dengan demikian, Indonesia dapat menciptakan ekosistem digital yang lebih aman dan terpercaya, serta sejajar dengan negara-negara lain yang telah memiliki regulasi serupa.

⁸⁰ Mitraberdaya, "Perbedaan GDPR Dan Regulasi Indonesia," Mitra Berdaya Optima, 2024, <https://mitraberdaya.id/id/news-information/perbedaan-gdpr-dan-regulasi-indonesia>.

⁸¹ Arffudin Dasep Suryanto, Slamet Riyanto, "Tentang Perlindungan Data Pribadi Dalam Industri Ritel " Tinjauan Terhadap Kepatuhan Dan Dampaknya Pada Konsumen," *Veritas* 10, no. 1 (2022): 121–35.

Salah satu aspek penting dalam UU PDP adalah penegakan sanksi terhadap pelanggaran. Undang-undang ini mengatur sanksi administratif, dan pidana bagi pihak yang melanggar ketentuan perlindungan data pribadi. Misalnya, sanksi pidana dapat mencapai hukuman penjara hingga 6 tahun dan denda hingga Rp72 miliar bagi pelaku yang dengan sengaja menyalahgunakan data pribadi. Adanya sanksi yang tegas ini diharapkan dapat menjadi efek jera bagi pelaku dan mendorong kepatuhan terhadap aturan yang berlaku.⁸²

Penerapan UU PDP juga menuntut kesiapan dari berbagai sektor, termasuk pemerintah, perusahaan, dan masyarakat. Perusahaan-perusahaan yang mengelola data pribadi, seperti platform *e-commerce*, *fintech*, dan media sosial, harus menyesuaikan sistem mereka dengan standar yang ditetapkan dalam undang-undang, mereka diwajibkan untuk memiliki sistem keamanan data yang memadai, melakukan audit secara berkala, dan melaporkan setiap insiden kebocoran data kepada otoritas yang berwenang. Hal ini memerlukan investasi dan komitmen yang besar dari para pelaku bisnis.

Secara keseluruhan, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan langkah progresif Indonesia dalam menghadapi tantangan digitalisasi. Dengan adanya undang-undang ini, diharapkan dapat tercipta ekosistem digital yang lebih aman dan terpercaya. Namun, keberhasilan penerapannya sangat bergantung pada komitmen semua pemangku kepentingan, mulai dari pemerintah, pelaku bisnis, hingga masyarakat umum. Tanpa kolaborasi yang baik, tujuan utama undang-undang ini untuk melindungi

⁸² Jurnal Pengabdian and Kepada Masyarakat, “Edukasi Terkait Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Bagi Masyarakat Desa Lubang Buaya” 3 (2024): 106–13.

data pribadi masyarakat mungkin akan sulit tercapai. Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) telah menunjukkan perkembangan yang signifikan sejak disahkan.

Data dari Kementerian Komunikasi dan Informatika (Kominfo) menunjukkan bahwa hingga akhir tahun 2023, lebih dari 60% perusahaan teknologi dan fintech di Indonesia telah melakukan penyesuaian sistem untuk mematuhi ketentuan UU PDP. Hal ini mencerminkan keseriusan pelaku bisnis dalam menghadapi regulasi baru ini. Grafik pertumbuhan kepatuhan perusahaan terhadap UU PDP menunjukkan peningkatan dari 20% pada kuartal pertama 2023 menjadi 60% pada kuartal keempat tahun yang sama.⁸³

Secara keseluruhan, data dan grafik pada penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menunjukkan kemajuan yang signifikan, meskipun masih terdapat tantangan yang perlu diatasi. Peningkatan kepatuhan perusahaan, kesadaran masyarakat, dan penegakan hukum menjadi indikator positif dalam implementasi UU PDP. Namun, upaya lebih lanjut diperlukan untuk meningkatkan kapasitas SDM, infrastruktur keamanan data, dan kolaborasi antar pemangku kepentingan. Dengan demikian, tujuan utama UU PDP untuk melindungi data pribadi masyarakat dapat tercapai secara optimal. Dalam Undang-Undang nomor 27 tahun 2022, untuk memastikan implementasi efektif dari Undang-Undang ini, pemerintah melakukan berbagai upaya antara lain:

⁸³ ANTARA News, “Dirjen Aptika Pastikan UU PDP Sudah Berlaku Sepenuhnya,” 2024, <https://www.antaranews.com/berita/4404977/dirjen-aptika-pastikan-uu-pdp-sudah-berlaku-sepenuhnya>.

a) Sosialisasi dan Edukasi

dalam hal ini Pemerintah, melalui Kementerian Komunikasi dan Informatika (Kominfo), aktif mengadakan sosialisasi dan edukasi kepada masyarakat serta pelaku industri mengenai pentingnya perlindungan data pribadi dan kewajiban yang diatur dalam UU PDP. Langkah ini bertujuan meningkatkan kesadaran dan pemahaman semua pihak terkait.

b) Penunjukan Pejabat Pelindungan Data

Undang-Undang Perlindungan Data Pribadi (PDP) mewajibkan perusahaan yang memproses data pribadi untuk menunjuk pejabat khusus yang bertanggung jawab atas perlindungan data. Hal ini memastikan adanya pengawasan internal yang ketat terhadap pengelolaan data pribadi.

c) Penyusunan Regulasi Turunan

Pemerintah sedang menyusun peraturan pelaksana sebagai panduan teknis bagi implementasi UU PDP. Regulasi ini akan memberikan detail lebih lanjut mengenai prosedur dan standar yang harus dipatuhi oleh pengendali dan prosesor data.

d) Pengawasan dan Penegakan Hukum

Memastikan kepatuhan terhadap UU PDP, pemerintah akan membentuk lembaga pengawas independen yang memiliki kewenangan untuk mengawasi, menerima aduan, serta menjatuhkan sanksi administratif bagi pelanggar. Sanksi dapat berupa denda hingga 2% dari pendapatan tahunan perusahaan.

e) Kerja Sama Internasional

Menyadari sifat lintas batas dari data digital, pemerintah menjalin kerja sama dengan negara lain dan organisasi internasional untuk harmonisasi standar perlindungan data dan penegakan hukum terkait.

f) Partisipasi Masyarakat

Undang-Undang Perlindungan Data Pribadi mendorong peran aktif masyarakat dalam perlindungan data pribadi melalui pendidikan, pelatihan, advokasi, dan pengawasan. Partisipasi ini diharapkan dapat memperkuat budaya perlindungan data di Indonesia.

Dari beberapa upaya tersebut, pemerintah berkomitmen untuk menciptakan ekosistem digital yang aman dan terpercaya, serta memastikan hak-hak privasi warga negara terlindungi dengan baik. Salah satu langkah signifikan yang diambil adalah pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada September 2022. Undang-Undang ini menjadi landasan hukum dalam tata kelola data pribadi di Indonesia, dimana dalam hal ini pemerintah mampu memberikan perlindungan hak fundamental bagi setiap warga negara, dan memperkuat kewenangan pemerintah dalam memantau pihak yang memproses data pribadi.⁸⁴

⁸⁴ Wahyudi Djafar, "Pengesahan RUU Perlindungan Data Pribadi: 'Terancam' Menjadi Macan Kertas," Lembaga Studi & Advokasi Masyarakat, 2022.

BAB III

KEPASTIAN HUKUM PERLINDUNGAN DATA PRIBADI di INDONESIA

A. Teori Kepastian Hukum

Teori kepastian hukum merupakan konsep fundamental dalam ilmu hukum yang menekankan pentingnya kejelasan, konsistensi, dan prediktabilitas dalam peraturan hukum. Kepastian hukum memastikan bahwa hukum berfungsi sebagai pedoman yang dapat diandalkan oleh masyarakat dalam berperilaku dan mengambil keputusan.⁸⁵

Teori kepastian hukum menjadi salah satu tujuan hukum yang dapat dikatakan dari upaya untuk mewujudkan suatu keadilan. Dalam teori kepastian hukum dijelaskan mengenai jaminan hukum itu sendiri akan ditegakkan dan dijalankan, bahwa yang berhak akan memperoleh haknya. Teori ini juga menjelaskan bahwa kepastian hukum merupakan perlindungan yang sah terhadap kesewenang-wenangan.⁸⁶ Dalam konteks kebocoran data pribadi pada platform marketplace, penerapan teori ini menjadi krusial untuk melindungi hak-hak konsumen dan memastikan tanggung jawab penyedia layanan. Kebocoran data pribadi di platform *marketplace* telah menjadi isu serius di Indonesia. Kasus-kasus seperti peretasan data pengguna menimbulkan kekhawatiran mengenai

⁸⁵ Ismail Roni Andriyanto, Dhody Ananta Rivandi W, “Kepastian Hukum Prosedur Penggantian Kerugian Pemegang Hak Atas Tanah Yang Terdampak ProyekJala Tol” 4, no. 5 (2022): 1291–1310.

⁸⁶ Pandu, “Pengertian Kepastian Hukum Secara Umum Dan Pendapat Para Ahli,” Gramedia Blog, accessed February 23, 2025, https://www.gramedia.com/literasi/pengertian-kepastian-hukum/?srsltid=AfmBOor8tlvkldIuvyXM07AD3SsBfheCj8_9FxbRBFRXHXZxHJ5VruaP.

perkembangan perlindungan hukum yang tersedia bagi konsumen, tanpa kepastian hukum yang memadai, konsumen rentan terhadap penyalahgunaan data pribadi mereka, sementara pelaku usaha mungkin tidak memiliki panduan yang jelas mengenai kewajiban mereka dalam melindungi data tersebut.

Penerapan teori kepastian hukum dalam konteks perlindungan data pribadi juga berkaitan dengan penegakan hukum yang efektif. Tanpa penegakan yang konsisten dan tegas, aturan yang ada tidak akan memiliki daya guna. Oleh karena itu, aparat penegak hukum harus dibekali dengan pemahaman yang mendalam mengenai UU PDP dan dilengkapi dengan sumber daya yang memadai untuk menangani kasus-kasus kebocoran data.

Secara keseluruhan, penerapan teori kepastian hukum dalam konteks kebocoran data pribadi pada platform marketplace merupakan upaya komprehensif yang melibatkan pembentukan regulasi yang jelas, penegakan hukum yang konsisten, edukasi kepada masyarakat, dan kerjasama antara berbagai pemangku kepentingan. Dengan pendekatan ini, diharapkan perlindungan data pribadi di Indonesia dapat terwujud secara efektif, memberikan rasa aman bagi konsumen, dan mendorong pertumbuhan ekonomi digital yang sehat.

Penegakan hukum yang konsisten juga menjadi kunci dalam menjamin kepastian hukum. Tanpa penegakan hukum yang tegas, pelanggaran terhadap perlindungan data pribadi cenderung diabaikan, yang pada gilirannya dapat merugikan konsumen dan melemahkan kepercayaan publik terhadap platform marketplace. Edukasi kepada masyarakat mengenai hak-hak mereka terkait data pribadi dan bagaimana melindunginya juga sangat penting. Dengan pemahaman

yang baik, konsumen dapat lebih waspada dan proaktif dalam menjaga informasi pribadi mereka saat bertransaksi di platform marketplace.

Kerjasama antara pemerintah, pelaku usaha, dan masyarakat diperlukan untuk menciptakan ekosistem digital yang aman. Pemerintah perlu menyediakan regulasi yang jelas dan mekanisme penegakan hukum yang efektif, sementara pelaku usaha harus memastikan kepatuhan terhadap standar keamanan data. Masyarakat juga harus berperan aktif dalam melindungi data pribadi mereka. Dengan pendekatan yang komprehensif ini, diharapkan perlindungan data pribadi di Indonesia dapat terwujud secara efektif, memberikan rasa aman bagi konsumen, dan mendorong pertumbuhan ekonomi digital yang sehat. Kepastian hukum yang terjamin akan meningkatkan kepercayaan publik terhadap platform marketplace, yang pada akhirnya akan menguntungkan semua pihak yang terlibat.

B. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-Undang Nomor 8 Tahun 1999 disahkan dengan tujuan melindungi hak-hak konsumen di Indonesia dari praktik bisnis yang merugikan atau tidak adil. Meskipun pada saat undang-undang ini disusun belum ada konsep yang jelas mengenai "data pribadi" seperti dalam Undang-Undang PDP, namun beberapa pasalnya dapat dimaknai sebagai dasar perlindungan atas informasi pribadi konsumen, terutama dalam konteks kepercayaan, keamanan transaksi, dan kewajiban pelaku usaha.⁸⁷ Dalam praktiknya, informasi pribadi seperti nama, alamat, nomor telepon, atau bahkan riwayat transaksi konsumen, menjadi bagian yang tidak terpisahkan dalam layanan digital modern dan sangat rentan terhadap

⁸⁷ Ririn Nur Aisyah et al., "Efektivitas Uu No. 8 Tahun 1999 Dalam Melindungi Data Pribadi Konsumen Di Sektor E-Commerce," *Jurnal Moralita : Jurnal Pendidikan Pancasila Dan Kewarganegaraan* 6, no. 1 (2025): 9–18, <https://doi.org/10.36985/v7dfhf27>.

penyalahgunaan apabila tidak dilindungi secara memadai. Pasal 62 memberikan sanksi pidana kepada pelaku usaha yang melanggar ketentuan Undang-Undang Perlindungan Konsumen, termasuk denda atau pidana penjara. Jika pelanggaran terhadap data pribadi menyebabkan kerugian pada konsumen, sanksi ini dapat diterapkan apabila terbukti bahwa pelaku usaha melanggar kewajiban informatif dan kehati-hatian.⁸⁸

Relevansi Undang-Undang Perlindungan Konsumen dengan Undang-Undang Perlindungan Data Pribadi yaitu walaupun tidak secara jelas membahas mengenai perlindungan data pribadi, Undang-Undang Perlindungan Konsumen menjadi dasar penting sebelum hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Banyak prinsip di dalamnya, seperti hak atas informasi, kewajiban pelaku usaha, dan hak untuk mendapatkan ganti rugi, merupakan elemen penting yang juga diadopsi dalam regulasi data pribadi. Dengan demikian, Undang-Undang ini tetap relevan dalam konteks perlindungan data konsumen di Indonesia.

Kehadiran Undang-Undang Perlindungan Data Pribadi memperkuat dan memperjelas prinsip-prinsip didalamnya dengan memberikan definisi yang lebih tegas mengenai data pribadi serta menetapkan mekanisme yang lebih rinci terkait pengumpulan, penyimpanan, pemrosesan, dan penghapusan data. Namun, Undang-Undang Perlindungan Konsumen tetap menjadi acuan penting dalam situasi dimana pelanggaran data berkaitan langsung dengan hubungan konsumen dan pelaku usaha, terutama dalam sektor perdagangan barang dan jasa. Sinergi

⁸⁸ 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>.

antara kedua undang-undang ini menciptakan kerangka hukum yang lebih komprehensif untuk melindungi konsumen di era digital, sekaligus mendorong pelaku usaha untuk lebih bertanggung jawab dalam mengelola informasi pelanggan. Dalam praktiknya, penerapan kedua undang-undang ini secara bersamaan memungkinkan adanya penegakan hukum yang lebih efektif, baik melalui mekanisme administratif, perdata, maupun pidana.

Undang-Undang Perlindungan Konsumen memberikan jalur penyelesaian sengketa dan kompensasi atas kerugian konsumen, sementara Undang-Undang Perlindungan Data Pribadi menetapkan standar teknis dan prosedural yang harus dipatuhi oleh pelaku usaha dalam mengelola data pribadi. Dengan demikian, keduanya saling melengkapi dan membentuk ekosistem perlindungan yang lebih kuat bagi masyarakat dalam menghadapi tantangan digital yang semakin kompleks.

Integrasi prinsip-prinsip perlindungan data pribadi dalam konteks perlindungan konsumen juga mendorong transparansi dalam praktik bisnis serta memperkuat kepercayaan publik terhadap layanan digital. Konsumen semakin menyadari pentingnya kendali atas informasi pribadi mereka, dan keberadaan kedua undang-undang ini memberi dasar hukum bagi mereka untuk menuntut hak tersebut. Di sisi lain, pelaku usaha yang mematuhi ketentuan perlindungan data tidak hanya menghindari sanksi, tetapi juga membangun reputasi positif dan loyalitas pelanggan. Dengan demikian, perlindungan data pribadi bukan sekadar kewajiban hukum, melainkan juga strategi bisnis yang berkelanjutan dalam era ekonomi digital.

Penerapan prinsip perlindungan data pribadi oleh pelaku usaha mencerminkan komitmen terhadap transparansi, akuntabilitas, dan etika dalam pengelolaan informasi konsumen. Hal ini sejalan dengan meningkatnya kesadaran masyarakat terhadap pentingnya privasi di era digital, dimana konsumen cenderung lebih mempercayai perusahaan yang secara aktif menjaga keamanan data pribadi mereka. Kepatuhan terhadap regulasi perlindungan data pribadi juga dapat meningkatkan kepercayaan investor dan mitra bisnis, terutama dalam skala global, dimana standar perlindungan data menjadi salah satu indikator penting dalam evaluasi tata kelola perusahaan. Dalam konteks ini, perlindungan data tidak hanya dilihat sebagai beban regulasi, melainkan sebagai bagian integral dari praktik bisnis yang bertanggung jawab dan berorientasi jangka panjang. Hal ini menunjukkan bahwa terdapat korelasi yang kuat antara pemenuhan aspek hukum dan pencapaian tujuan bisnis yang berkelanjutan.

C. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan UU Nomor 19 Tahun 2016, merupakan *cyber law* pertama di Indonesia dan mengatur tentang berbagai aspek, termasuk definisi informasi elektronik, transaksi elektronik, penyelenggara sistem elektronik, dan sanksi bagi pelanggaran.⁸⁹

⁸⁹ Nyoman Gede Antaguna and Anak Agung Sagung Laksmi Dewi, "Pembatasan Kebebasan Berpendapat Dan Bereksprei Di Sosial Media Berdasarkan Peraturan Perundang-Undangan Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE)," *Kertha Wicaksana* 17, no. 2 (2023): 138–46.

Tujuan utama dari undang-undang ini adalah untuk memberikan landasan hukum bagi penggunaan teknologi informasi, khususnya internet, serta transaksi elektronik yang berkembang di masyarakat. Perlindungan terhadap data pribadi menjadi salah satu bagian penting dari UU ini, meskipun tidak secara jelas menjadi fokus utama.

Pasal 26 merupakan pasal utama dalam UU ITE yang secara langsung menyentuh isu perlindungan data pribadi:

(1) Menyebutkan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Hal ini menegaskan prinsip dasar perlindungan data pribadi harus ada persetujuan yang jelas dari pemilik data.

Pasal 26 Undang-Undang ITE memberikan dasar hukum terhadap perlindungan privasi digital. Meskipun tidak secara jelas menggunakan istilah "data pribadi", makna pasal ini mencakup perlindungan terhadap informasi pribadi dalam bentuk digital. Dalam konteks saat ini, mencakup nama, alamat, nomor identitas, email, dan data lain yang dapat mengidentifikasi individu. tindakan mendistribusikan, menyampaikan informasi, atau membuat diaksesnya informasi pribadi tanpa persetujuan dianggap sebagai pelanggaran terhadap hak privasi. Hal ini mencakup penyebaran informasi pribadi seseorang tanpa izin di *media sosial* atau dalam transaksi digital.

Undang-Undang Informasi Teknologi Elektronik meskipun tidak memberikan sanksi pidana langsung atas pelanggaran terhadap Pasal 26 ayat (1), korban dapat menempuh jalur hukum perdata berdasarkan prinsip ganti rugi.

Namun, dalam praktiknya, dalam pasal ini digunakan dalam aduan terhadap pelanggaran etika digital dan perlindungan konsumen. Undang-Undang ITE kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016, yang memperkuat perlindungan privasi dan memperjelas beberapa pasal, termasuk Pasal 26.⁹⁰

(2) Bahwa setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan di bawah kendalinya atas permintaan seseorang berdasarkan putusan pengadilan. Ini menjadi dasar penting dalam kasus pencemaran nama baik, penyebaran konten pribadi, atau penyebaran data pribadi yang merugikan.

Undang-Undang ITE mewajibkan Penyelenggara Sistem Elektronik untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi yang mereka kelola. Hal ini ditegaskan lebih lanjut dalam peraturan turunannya, seperti PP 71 Tahun 2019 dan Permenkominfo No. 20 Tahun 2016, yang menjelaskan tata cara pengelolaan dan penyimpanan data pribadi oleh penyelenggara sistem elektronik. Walaupun Undang-Undang ITE telah memberikan dasar awal perlindungan data pribadi, regulasinya masih bersifat umum dan sektoral. Oleh karena itu, Undang-Undang ITE dianggap sebagai cikal bakal atau dasar hukum awal yang kemudian diperluas dan diperjelas oleh UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mengatur secara komprehensif tentang pengumpulan, pemrosesan, penyimpanan, dan penghapusan data pribadi.⁹¹

⁹⁰ Fadhilah Nuraini Rustam, "Sanksi Pidana Penyalahgunaan Informasi/Dokumen Elektronik Konsumen," Dalimunthe Tampubolon, 2020.

⁹¹ Jeane Neltje Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU NO.27 TAHUN 2022" 1, no. 3 (2023): 145–53.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016, merupakan salah satu instrumen hukum utama yang mengatur aktivitas dalam ruang digital di Indonesia. Undang-Undang ITE mencakup berbagai aspek, seperti pengakuan terhadap dokumen elektronik, transaksi daring, serta perlindungan terhadap informasi pribadi. Salah satu pasal yang relevan dengan perlindungan data pribadi adalah Pasal 26 ayat (1), yang menyatakan bahwa penggunaan informasi pribadi melalui media elektronik harus dilakukan atas persetujuan dari orang yang bersangkutan. Ketentuan ini menunjukkan adanya pengakuan awal terhadap pentingnya hak subjek data, meskipun dalam bentuk yang masih umum dan belum sistematis.⁹²

Dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Indonesia memasuki era baru dalam perlindungan data pribadi yang lebih komprehensif dan terarah. Undang-Undang PDP mengatur secara rinci mengenai prinsip-prinsip pemrosesan data, hak-hak subjek data, tanggung jawab pengendali dan prosesor data, serta mekanisme pengawasan dan sanksi atas pelanggaran. Dalam hal ini, Undang-Undang PDP menjadi *lex specialis* atau hukum khusus yang secara spesifik mengatur perlindungan data pribadi di Indonesia. Keberadaan Undang-Undang ini melengkapi kekosongan norma yang sebelumnya belum diatur secara mendalam dalam Undang-Undang ITE.

⁹² Leonardo Latsiano Dade, Caecilia J.J Waha, and Nurhikmah Nachrawy, "Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia" 13, no. 3 (2024): 9.

Meskipun demikian, Undang-Undang ITE tetap memiliki relevansi dan kedudukan penting dalam sistem hukum digital Indonesia. Undang-Undang ITE berfungsi sebagai kerangka hukum umum (*lex generalis*) yang mengatur berbagai bentuk interaksi elektronik dan transaksi digital, sementara Undang-Undang PDP hadir sebagai pengaturan yang lebih khusus terkait data pribadi. Kedua undang-undang ini bersifat saling melengkapi dan dapat diimplementasikan secara sinergis. Dengan demikian, dalam era digital saat ini, perlindungan terhadap data pribadi dan keamanan informasi membutuhkan pendekatan yang holistik melalui integrasi norma dari kedua undang-undang tersebut, guna menjamin hak-hak digital warga negara secara maksimal.

D. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (beserta perubahan melalui UU Nomor 24 Tahun 2013)

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (beserta perubahan melalui UU Nomor 24 Tahun 2013) dibuat untuk menyelenggarakan tertib administrasi kependudukan secara nasional. Tujuannya adalah untuk menjamin hak-hak konstitusional warga negara dalam bidang administrasi kependudukan, termasuk perlindungan terhadap data pribadi dalam dokumen kependudukan. Data seperti Nomor Induk Kependudukan (NIK), nama lengkap, tempat dan tanggal lahir, jenis kelamin, alamat, hingga *biometrik* (sidik jari, iris mata) termasuk kategori data pribadi yang dikumpulkan dan dikelola oleh negara.⁹³

⁹³ Anak Agung et al., “Perlindungan Hukum Subyek Data Pribadi Khususnya Nomor Induk Kependudukan Pada Kartu Tanda Penduduk Ketika Terjadi Peretasan” 12, no. 11 (2024): 2881–91.

Sistem informasi dan administrasi kependudukan, perlindungan data pribadi penduduk, sanksi administratif dan sanksi pidana terkait administrasi kependudukan. Setiap Penduduk wajib melaporkan Peristiwa Kependudukan dan peristiwa penting yang dialaminya kepada Instansi Pelaksana dengan memenuhi persyaratan yang diperlukan dalam Pendaftaran Penduduk dan Pencatatan Sipil.

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan menyebutkan bahwa data pribadi menjadi bagian yang tak terpisahkan dari sistem administrasi kependudukan. Informasi yang dikumpulkan oleh Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) bersifat sangat sensitif dan memiliki potensi besar untuk disalahgunakan jika tidak dilindungi secara ketat. Oleh karena itu, pengaturan perlindungan data pribadi dalam Undang-Undang ini sangat penting sebagai bagian dari perlindungan hak asasi warga negara. Dalam Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (beserta perubahan melalui UU Nomor 24 Tahun 2013) yang terkait dengan Perlindungan Data Pribadi terdapat dalam pasal 58 membahas mengenai Pengelolaan Data Kependudukan, Pasal 79A (dari UU No. 24 Tahun 2013 membahas mengenai Perlindungan dan Kerahasiaan Pribadi, Pasal 84A mengenai Acaman Pidana atas Penyalahgunaan Data dalam pasal ini menegaskan bahwa pelanggaran terhadap perlindungan data kependudukan sebagaimana dimaksud dalam pasal 79A dapat dikenai sanksi pidana.⁹⁴

⁹⁴ Johny Hinonaung, Kezia Lembong and Harly Stanly Muaja, “Ketentuan Pidana Di Bidang Administrasi Kependudukan Menurut Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan,” *Lex Privatum* 8, no. 32 (2020): 73–92, http://hpj.journals.pnu.ac.ir/article_6498.html.

Pasal 94 dalam Undang-Undang Nomor 23 Tahun 2006 Administrasi Kependudukan (beserta perubahan melalui UU Nomor 24 Tahun 2013) menyatakan bahwa setiap orang yang dengan sengaja memerintahkan, memfasilitasi, atau melakukan manipulasi data kependudukan atau elemen data penduduk dapat dikenai pidana penjara paling lama enam tahun dan/atau denda paling banyak sebesar Rp75.000.000,00.⁹⁵ Lebih lanjut, Pasal 95A mengatur ancaman pidana terhadap setiap orang yang menyebarluaskan data kependudukan atau data pribadi tanpa hak, dengan ancaman pidana penjara paling lama dua tahun dan/atau denda paling banyak Rp25.000.000,00. Sanksi ini ditujukan sebagai bentuk perlindungan hukum terhadap privasi warga negara, khususnya dalam konteks digitalisasi data seperti KTP elektronik (e-KTP) yang menyimpan informasi biometrik.

E. Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik diterbitkan sebagai respons terhadap meningkatnya pemrosesan data pribadi secara digital di Indonesia, seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi.⁹⁶ Regulasi ini menjadi salah satu peraturan spesifik

⁹⁵ Victoria Sengkey, Said Aneke-R, and Deizen Rompas, "Penyidikan Terhadap Tindak Pidana Di Bidang Administrasi Kependudukan Berdasarkan Undang-Undang No. 24 Tahun 2013 Tentang Administrasi Kependudukan," *Lex Privatum* XI, no. 5 (2023): 1–8.

⁹⁶ kosworo wenderline, "Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan Dan Kepastian Hukum" 7, no. 2 (2022): 86–103.

pertama yang secara eksplisit mengatur prinsip-prinsip perlindungan data pribadi dalam sistem elektronik. Tujuannya untuk memberikan kepastian hukum bagi pemilik data, serta mengatur tanggung jawab pengendali/pengelola data dalam melindungi hak-hak individu.

Pasal 2 menjelaskan bahwa peraturan ini berlaku bagi penyelenggara sistem elektronik (PSE), baik publik maupun privat, yang melakukan pemrosesan data pribadi dalam sistem elektronik. Hal ini mencakup instansi pemerintah, perusahaan teknologi, layanan keuangan, *e-commerce*, hingga Perusahaan yang baru berdiri untuk mengelola data pengguna. Dengan demikian, ruang lingkungannya sangat luas dan mencakup hampir seluruh sektor yang mengandalkan teknologi informasi.

Pasal 3 dalam prinsip Perlindungan Data Pribadi menegaskan delapan prinsip utama dalam pengelolaan data pribadi, antara lain kejelasan tujuan, persetujuan dari subjek data, relevansi, keamanan, akurasi, dan batasan penyimpanan. Prinsip-prinsip ini mencerminkan standar internasional perlindungan data, dan menjadi dasar etis serta hukum bagi PSE dalam mengelola informasi pribadi pengguna.

Pasal 6 menyatakan bahwa data pribadi hanya boleh dikumpulkan dengan persetujuan yang jelas dari pemilik data. Pasal 7 menambahkan bahwa PSE wajib memberikan informasi lengkap mengenai tujuan, jangka waktu, dan penggunaan data sebelum persetujuan diberikan. Hal ini memastikan bahwa pengguna mengetahui hak dan risiko sebelum memberikan data mereka.

Pasal 26 hingga 30 mengatur hak subjek data untuk mengakses, memperbaiki, menarik kembali persetujuan, hingga menghapus data pribadi yang telah diberikan. Ini memberikan kendali langsung kepada individu atas informasi yang dimiliki oleh pihak ketiga, sejalan dengan konsep "*data ownership*". Dengan demikian, subjek data tidak hanya diposisikan sebagai objek dari pengumpulan data, tetapi juga sebagai pemilik sah atas informasi pribadinya yang berhak untuk menentukan bagaimana data tersebut digunakan, disimpan, atau dibagikan.

Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, tidak secara langsung diatur mengenai sanksi pidana. Undang-Undang ini lebih menitikberatkan pada pengaturan teknis dan administratif mengenai pengelolaan data pribadi oleh Penyelenggara Sistem Elektronik (PSE), seperti kewajiban memperoleh persetujuan subjek data, prinsip kehati-hatian dalam pengolahan data, dan pengamanan sistem. Sanksi yang diatur dalam Permenkominfo No. 20 Tahun 2016 bersifat administratif, sebagaimana disebutkan dalam Pasal 36, yaitu dapat berupa peringatan tertulis, denda administratif, penghentian sementara, hingga pemblokiran akses sistem elektronik, apabila PSE terbukti melanggar ketentuan mengenai perlindungan data pribadi. Meskipun tidak memuat ketentuan pidana secara eksplisit, pelanggaran berat terhadap perlindungan data pribadi yang diatur dalam Permenkominfo ini tetap dapat dijerat sanksi pidana melalui peraturan perundang-undangan lainnya, seperti Pasal 26 ayat (1) UU ITE, atau ketentuan pidana dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur secara lebih tegas mengenai sanksi pidana terhadap

pelanggaran data pribadi. Oleh karena itu, Permenkominfo No. 20 Tahun 2016 berperan sebagai norma pelengkap yang menjembatani kekosongan aturan teknis sebelum lahirnya Undang-Undang Perlindungan Data Pribadi, namun tidak memuat sanksi pidana tersendiri di dalamnya.

Dari hasil penelusuran kepustakaan Undang-Undang yang telah dibahas diatas dapat dibahas bahwa meskipun Indonesia telah memiliki berbagai perangkat hukum yang mengatur mengenai perlindungan data pribadi, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan yang terbaru Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), realitas penegakan sanksi pidana atas kebocoran data pribadi masih sangat terbatas.

Berdasarkan data yang disampaikan dalam penelitian ini, dari banyaknya kasus kebocoran data pribadi yang terjadi, hanya sebagian kecil yang ditindaklanjuti melalui proses hukum pidana. Hal ini menunjukkan bahwa meskipun terdapat landasan normatif untuk penjatuhan sanksi pidana, implementasinya belum memberikan kepastian hukum yang efektif dan menyeluruh bagi korban pelanggaran data pribadi. UU ITE sebenarnya telah lebih awal memberikan ketentuan pidana terhadap perbuatan melawan hukum dalam bentuk akses ilegal terhadap sistem elektronik atau penyebaran data pribadi tanpa persetujuan. Namun, setelah hadirnya Undang-Undang Perlindungan Data Pribadi, fokus kebijakan cenderung mengarah pada penegakan sanksi administratif. Undang-Undang Perlindungan Data Pribadi secara substansial lebih banyak mengatur mekanisme administratif, seperti teguran tertulis, penghentian

sementara layanan, atau denda administratif sebesar maksimal 2% dari pendapatan tahunan pengendali data, dan tidak secara komprehensif menekankan penegakan sanksi pidana. Ketimpangan ini menimbulkan pertanyaan kritis mengenai efektivitas perlindungan hukum yang diberikan.

Sanksi administratif yang bersifat institusional dan korporatif dinilai tidak cukup memberikan efek jera terhadap pelaku, baik individu maupun badan usaha, karena denda yang dijatuhkan dapat dianggap sebagai biaya operasional semata. Padahal, Undang-Undang Perlindungan Data Pribadi juga mengandung ketentuan pidana sebagaimana diatur dalam Pasal 67 dan 68, yang memuat ancaman pidana penjara hingga 6 tahun bagi individu yang dengan sengaja menyebarluaskan, memalsukan, atau menyalahgunakan data pribadi.⁹⁷ Namun lemahnya penegakan hukum, kurangnya kapasitas aparat, serta belum adanya preseden kasus yang tegas menimbulkan kesan bahwa pendekatan pidana dalam pelanggaran data pribadi masih bersifat simbolis.⁹⁸ Oleh karena itu, perlu adanya upaya penegakan hukum pidana yang lebih konsisten dan sistematis untuk memastikan bahwa hak atas perlindungan data pribadi benar-benar dihormati, serta agar keberadaan UU PDP tidak hanya menjadi norma hukum tertulis semata, melainkan juga menjadi instrumen efektif dalam menjamin keadilan bagi korban kebocoran data.

Dalam era digital seperti saat ini, perkembangan teknologi informasi telah memunculkan bentuk-bentuk kejahatan baru, termasuk pelanggaran terhadap perlindungan data pribadi. Oleh karena itu, penerapan asas-asas hukum pidana

⁹⁷ Widhia Arum Wibawana, "Isi UU Perlindungan Data Pribadi: Larangan, Sanksi Dan Jenis Data," Detiknews, 2022.

⁹⁸ M Rafifnafia Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia," *Kertha Patrika* 43, no. 1 (2021): 93, <https://doi.org/10.24843/kp.2021.v43.i01.p07>.

menjadi relevan dalam menjawab tantangan penegakan hukum terhadap kebocoran data pribadi sebagai bentuk kejahatan modern. Kebocoran data pribadi merupakan tantangan serius dalam era digital. Untuk menanggulangnya, asas-asas hukum pidana seperti legalitas, kepastian hukum, dan keadilan harus diterapkan secara nyata dalam penegakan hukum agar pelaku dapat diproses dan hak korban terlindungi.

BAB IV

TINJAUAN FIQHI JINAYAH TERHADAP KEBOCORAN DATA PRIBADI

A. Kajian Fikih Jinayah Terkait Perlindungan Data Pribadi

Perlindungan data pribadi dalam perspektif fikih jinayah merupakan perlindungan data pribadi yang dapat dikaitkan dengan konsep *hifz al-‘ird* (menjaga kehormatan) dan *hifz al-nafs* (menjaga jiwa), yang merupakan bagian dari *maqāṣid al-syarī‘ah*. Data pribadi merupakan bagian dari kehormatan individu yang wajib dijaga agar tidak disalahgunakan atau disebarluaskan tanpa izin.⁹⁹ Dalam konteks ini, tindakan membocorkan atau menyalahgunakan data pribadi dapat dikategorikan sebagai bentuk pelanggaran terhadap hak-hak individu yang dilindungi syariat.

Fikih jinayah, sebagai cabang ilmu fikih yang membahas tindak pidana dan sanksinya dalam Islam, memberikan landasan normatif bahwa setiap bentuk pelanggaran terhadap kehormatan dan privasi seseorang dapat dikenakan sanksi, baik dalam bentuk *ta‘zīr* maupun *ḥudūd*, tergantung pada kadar kerusakan yang ditimbulkan.¹⁰⁰ Oleh karena itu, penting untuk meninjau ulang kebijakan dan regulasi perlindungan data pribadi dalam kerangka fikih jinayah guna menjamin bahwa perlindungan hak individu sejalan dengan nilai-nilai keadilan dalam Islam, bagian dari tanggung jawab negara dalam menjaga kemaslahatan rakyat dan mencegah kemudharatan.

⁹⁹ Eriska Laila Nisau, “ANALISIS MAQĀSID AL-SHARĪAH TERHADAP PERLINDUNGAN HUKUM DATA PRIBADI MENURUT UNDANG-UNDANG NOMOR 27 TAHUN 2022,” *Skripsi* 87, no. 1,2 (2023): 149–200.

¹⁰⁰ Utpy Asifae et al., “Penerapan Kaidah Fiqhiyyah Terhadap Kejahatan Siber Dalam Hukum Jinayah,” *Jurnal Ilmu Hukum* 2, no. 1 (2024): 134–39.

Data pribadi seperti nama, alamat, nomor identitas, rekam medis, dan aktivitas daring termasuk dalam kategori informasi yang menyangkut kehormatan individu (*'ird*), yang dalam Islam sangat dijaga. Maka, segala bentuk penyalahgunaan data tersebut dapat dikategorikan sebagai pelanggaran terhadap hak-hak individu yang dilindungi oleh syariat.¹⁰¹ Pelanggaran terhadap informasi pribadi tersebut tidak hanya menimbulkan kerugian secara materiil, tetapi juga dapat mengakibatkan rusaknya reputasi, rasa aman, dan martabat seseorang. Dalam fikih jinayah, bentuk pelanggaran semacam ini dipandang sebagai tindak kejahatan terhadap kehormatan (*jināyah 'alā al-'ird*), yang dapat dikenai sanksi berupa *ta'zīr* sesuai dengan tingkat kerusakan yang ditimbulkan.

Prinsip dasar ini merujuk pada tujuan utama syariat Islam (*maqāṣid al-syarī'ah*), khususnya dalam menjaga kehormatan dan privasi individu dari segala bentuk tindakan yang merugikan.¹⁰² Oleh karena itu, dalam konteks modern, pelanggaran data pribadi harus dipahami tidak semata sebagai pelanggaran administratif, tetapi juga sebagai pelanggaran moral dan agama yang berdampak langsung terhadap stabilitas sosial dan perlindungan hak asasi manusia menurut pandangan Islam.

Ayat-ayat Al-Qur'an seperti QS. Al-Hujurat ayat 12 yang melarang *tajassus* (memata-matai), serta hadis-hadis yang menegaskan pentingnya menjaga rahasia orang lain, menunjukkan bahwa syariat mengakui dan melindungi hak atas

¹⁰¹ Muhammad Taufik and Fatimah Zahara, "Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)," *Jurnal Ilmu Hukum, Humaniora Dan Politik* 4, no. 6 (2024): 2378–92, <https://doi.org/10.38035/jihhp.v4i6.2744>.

¹⁰² Sudarti, "Perlindungan Data Pribadi Perspektif Sadd Dzari'ah," *Artikula.id*, 2022.

privasi.¹⁰³ Negara sebagai representasi otoritas dalam fikih jinayah memiliki legitimasi syar‘i untuk menetapkan kebijakan dan regulasi yang bertujuan melindungi data pribadi masyarakat.¹⁰⁴ Tindakan ini tidak hanya sejalan dengan prinsip siyāsah shar‘iyyah, tetapi juga merupakan bentuk nyata dari pelaksanaan tugas wilāyah dalam menjaga kemaslahatan umat.

Negara dituntut untuk tidak sekadar bersikap pasif, melainkan aktif dalam menyediakan sistem dan mekanisme perlindungan data yang mampu menjamin rasa aman bagi warga negara, baik dalam ranah sosial, ekonomi, maupun digital. Dalam hal ini, prinsip maṣlaḥah mursalah menjadi landasan penting yang membolehkan pemerintah merumuskan kebijakan baru yang belum secara eksplisit diatur dalam nas, namun sangat diperlukan dalam menjawab tantangan zaman modern.

Perlindungan data pribadi juga dapat dikaitkan dengan konsep *ta‘zīr* dalam hukum pidana Islam, dimana negara memiliki wewenang untuk menjatuhkan sanksi terhadap pihak-pihak yang terbukti menyalahgunakan atau membocorkan informasi pribadi individu tanpa izin yang sah. Sanksi ini bersifat fleksibel dan disesuaikan dengan tingkat kerusakan yang ditimbulkan, dengan tujuan untuk memberikan efek jera serta menjaga stabilitas sosial.¹⁰⁵ Kewajiban melindungi data pribadi tidak hanya berada di tangan negara, tetapi juga menjadi

¹⁰³ Andi Tri Saputra, “Konsep Intelijen Dan Penafsiran Kontekstualitas Terhadap Q.S Al-Hujarat Ayat 12 (Aplikasi Metode Penafsiran Kontekstualis Abdullah Saeed,” *Nun: Jurnal Studi Alquran Dan Tafsir Di Nusantara* 5, no. 2 (2020): 93–125, <https://doi.org/10.32495/nun.v5i2.92>.

¹⁰⁴ Mustafid, “Etika Pemerintahan Berbasis Fiqih Siyasah Di Era Digital,” *Jurnal Hukum Islam Dan Sosial*, 2024.

¹⁰⁵ Maulana Fikran, “Tinjauan Hukum Pidana Islam Terhadap Cyber Crime Dalam Bentuk Pencurian Data Pribadi,” *Legitimasi: Jurnal Hukum Pidana Dan Politik Hukum* 10, no. 2 (2021): 7.

tanggung jawab individu dan lembaga yang mengelola data. Dalam Islam, setiap individu wajib menjaga amanah dan tidak boleh menyalahgunakan informasi yang dipercayakan kepadanya. Lembaga publik maupun swasta dituntut untuk bertindak jujur dan bertanggung jawab dalam pengelolaan data pribadi. Pengkhianatan terhadap amanah ini dapat dikenai sanksi ta'zīr oleh pemerintah sebagai bentuk pelaksanaan hukum Islam yang kontekstual dan responsif terhadap perkembangan zaman.¹⁰⁶

Pertanggungjawaban pidana dalam fikih jinayah merupakan prinsip dasar yang menegaskan bahwa setiap perbuatan yang menimbulkan kerugian bagi orang lain, baik dilakukan secara sengaja maupun karena kelalaian, harus ditanggung oleh pelakunya. Dalam konteks kebocoran data pribadi pada marketplace, pertanggungjawaban pidana tidak hanya diarahkan kepada pelaku kejahatan digital yang secara aktif melakukan peretasan, tetapi juga dapat dikenakan kepada pihak penyedia layanan yang lalai dalam menjaga keamanan data pengguna yang merupakan amanah.

Pelaku eksternal yang dengan sengaja meretas sistem, mencuri, atau menyebarkan data pribadi pengguna jelas melakukan tindak jarimah ta'zir, karena ia telah melanggar hak orang lain dan menimbulkan kerugian baik secara materiil maupun immateriil. Sedangkan pihak platform marketplace dapat dimintai pertanggungjawaban apabila terbukti lalai dalam menjaga keamanan sistem. Kelalaian tersebut dapat dianggap sebagai pelanggaran terhadap amanah, karena marketplace berkewajiban menjaga kerahasiaan dan keamanan data yang

¹⁰⁶ Akhir Nazli Khatami and Arifuddin Muda Harahap, "Penyalahgunaan KTP Masyarakat Untuk Pinjaman Dana PNM Mekaar Perspektif Sadd Adz- Zari ' Ah Di Kota Tanjungbalai," *Ad-Deenar: Jurnal Ekonomi Dan Bisnis Islam*, 2023, 343–54.

dipercayakan oleh penggunanya. Dalam perspektif fikih jinayah, kedua pihak ini memiliki kadar tanggung jawab yang berbeda: hacker dihukum karena melakukan tindakan kejahatan aktif, sedangkan marketplace dapat dikenai ta'zir dalam bentuk sanksi administratif atau kewajiban ganti rugi (dhaman) bila terbukti lalai. Dengan demikian, hukum Islam tidak hanya menjerat pelaku utama, tetapi juga menuntut pihak yang lalai menjalankan kewajibannya untuk ikut bertanggung jawab, demi menjaga maslahat umum dan mencegah kerugian yang lebih luas.

Tantangan dalam perlindungan data pribadi di era digital tidaklah ringan. Keterbatasan infrastruktur keamanan digital, rendahnya kesadaran masyarakat akan pentingnya privasi, serta cepatnya perkembangan teknologi menjadi hambatan serius.¹⁰⁷ Oleh karena itu, diperlukan pendekatan holistik yang tidak hanya mengandalkan regulasi, tetapi juga edukasi publik dan pembinaan etika digital. Dalam hal ini, fikih jinayah memberikan kerangka normatif yang dapat menjadi pijakan dalam menyusun kebijakan dan strategi perlindungan data pribadi secara adil dan berkelanjutan.

Fikih jinayah tidak hanya menawarkan pendekatan represif dalam bentuk sanksi, tetapi juga mengedepankan nilai-nilai preventif yang berbasis pada kesadaran moral dan tanggung jawab sosial. Dalam kerangka ini, setiap individu dituntut untuk menjaga amanah informasi yang dimiliki, sebagaimana ditegaskan dalam prinsip syariat bahwa segala bentuk hak milik, termasuk data pribadi, harus dihormati dan dijaga dari perbuatan aniaya (*ẓulm*). Oleh karena itu, penguatan kesadaran akan nilai-nilai etika Islam, seperti kejujuran (*ṣidq*), tanggung jawab

¹⁰⁷ Fitra Ashari, "APJII Tingkatkan Kesadaran Masyarakat Akan Isu Keamanan Siber," Antara.News, 2023.

(amānah), dan kehati-hatian (*taharruz*), menjadi fondasi penting dalam menciptakan budaya digital yang sehat. Integrasi antara regulasi positif dan prinsip-prinsip fikih jinayah akan memperkuat upaya perlindungan data pribadi secara komprehensif, yang tidak hanya mengandalkan sistem, tetapi juga membangun karakter dan kesadaran kolektif umat.¹⁰⁸ Dalam menanamkan pemahaman bahwa menjaga data pribadi merupakan bagian dari pelaksanaan ajaran Islam yang menyeluruh.

Konsep hisbah dalam Islam, yakni pengawasan moral dan sosial, juga dapat dihidupkan kembali sebagai mekanisme pengontrol internal dalam masyarakat, dimana setiap anggota masyarakat memiliki peran untuk saling menasihati dan mencegah kemungkaran, termasuk dalam ranah digital. Dengan demikian, perlindungan data pribadi tidak hanya menjadi tanggung jawab negara melalui perangkat hukum formal, melainkan juga menjadi bagian dari tanggung jawab kolektif umat Islam dalam menjaga kehormatan sesama dan mewujudkan keadilan sosial.

Kebocoran data pribadi dalam platform marketplace dari perspektif fikih jinayah sebagai bentuk pelanggaran atas hak milik (*al-ḥaqq al-mālī*) yang berdampak pada kerugian pengguna secara langsung. Dalam fikih, platform marketplace bertindak sebagai pihak yang memegang amanah (*musta'man*) atas data pengguna, sehingga apabila terjadi kebocoran data yang menyebabkan kerugian materiil seperti hilangnya saldo atau akses keuangan, maka platform dapat dikenai tanggung jawab atas kelalaiannya. Berdasarkan kaidah “*al-ḍamān bi*

¹⁰⁸ Eryna Syahadatina Badar, Ahmad Fauzi, and Ahya Jazuli, “Kebijakan Pelindungan Data Pribadi Undang-Undang Nomor 27 Tahun 2022 Dalam Prespektif Hukum Positif Dan Hukum Islam,” *Hukum Islam* 23, no. 1 (2023): 61, <https://doi.org/10.24014/jhi.v23i1.20465>.

al-tafrīt” (tanggung jawab disebabkan kelalaian), maka pihak penyedia layanan berkewajiban mengganti kerugian yang timbul apabila terbukti gagal menjaga data dengan layak. Dalam hal ini, korban tidak dapat dipidana karena pada dasarnya ia adalah pihak yang dirugikan, kecuali ditemukan unsur kesengajaan atau kelalaian berat yang dapat dibuktikan secara hukum.

Hukum positif Indonesia dalam, perlindungan terhadap data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memuat sanksi administratif, hingga pidana terhadap penyelenggara sistem elektronik yang lalai atau menyalahgunakan data pribadi. Selain itu, UU ITE dan Permenkominfo No. 20 Tahun 2016 turut memperkuat landasan hukum bagi perlindungan data di ranah digital. Namun demikian, dalam praktiknya, penegakan hukum terhadap kasus kebocoran data masih tergolong lemah dan belum memberikan efek jera terhadap pelaku maupun platform. Sanksi yang dapat dikenakan terhadap platform meliputi teguran administratif, denda, pembatasan akses sistem, bahkan penutupan layanan sebagaimana diatur dalam Pasal 51 UU PDP. Dalam kerangka fiqih jinayah, penanganan kebocoran data harus memenuhi tiga asas penting, yakni asas keadilan (al-‘adālah), asas kepastian hukum (al-yaqīn), dan asas kemanfaatan (al-maṣlaḥah). Asas keadilan menuntut agar korban memperoleh perlindungan dan kompensasi secara layak, sementara asas kepastian menegaskan bahwa regulasi harus ditegakkan dengan jelas dan tidak tebang pilih. Sedangkan asas kemanfaatan mengarahkan bahwa upaya perlindungan data tidak hanya menguntungkan korporasi, tetapi juga memberi manfaat sebesar-besarnya bagi keamanan digital masyarakat. Oleh karena itu,

solusi konkret yang dapat diterapkan meliputi penguatan sistem enkripsi, penerapan autentikasi ganda (2FA), audit keamanan rutin, serta peningkatan edukasi digital kepada masyarakat. Di sisi pemerintah, penguatan otoritas pengawas data, serta penegakan sanksi yang tegas terhadap pelanggaran harus dijalankan secara konsisten. Langkah-langkah ini diharapkan dapat mencegah terjadinya kebocoran data serupa di masa mendatang dan mewujudkan ekosistem digital yang aman, adil, dan terpercaya sesuai prinsip hukum Islam dan sistem hukum nasional.

BAB V

PENUTUP

A. Kesimpulan

1. Kebocoran data pribadi di *platform marketplace* merupakan fenomena yang marak terjadi di Indonesia, ditandai dengan meningkatnya jumlah kasus dalam beberapa tahun terakhir. Kasus-kasus tersebut menunjukkan lemahnya sistem keamanan data serta kurangnya kesadaran pengguna dalam menjaga kerahasiaan informasi pribadi. Hal ini berdampak pada kerugian finansial, kerugian reputasi, hingga potensi penyalahgunaan identitas. Kondisi tersebut menegaskan bahwa perlindungan data pribadi menjadi kebutuhan mendesak dalam ekosistem digital. Tanpa adanya sistem keamanan yang kuat serta regulasi yang efektif, kebocoran data akan terus berulang dan merugikan banyak pihak. Oleh karena itu, diperlukan sinergi antara pemerintah sebagai regulator, penyelenggara *marketplace* sebagai pengelola data, dan masyarakat sebagai pengguna, agar tercipta lingkungan digital yang aman, terpercaya, serta sejalan dengan prinsip kepastian hukum dan perlindungan hak asasi manusia.

2. Perlindungan hukum terhadap kebocoran data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang ITE dan peraturan sektoral lainnya. Meskipun demikian, implementasi kepastian hukum pidana masih menghadapi kendala, seperti terbatasnya pemahaman aparat penegak hukum, kurangnya regulasi turunan, serta lemahnya mekanisme penegakan hukum. Hal ini mengakibatkan perlindungan

hukum belum sepenuhnya optimal dalam memberikan rasa aman bagi pengguna marketplace. Aparat penegak hukum memerlukan peningkatan kapasitas dalam bidang kejahatan siber, sementara pemerintah harus segera menyusun peraturan pelaksana yang lebih rinci agar Undang-Undang Perlindungan Data Pribadi dapat berjalan sesuai tujuan. Selain itu, dibutuhkan koordinasi yang kuat antara lembaga negara, penyelenggara sistem elektronik, dan masyarakat untuk menciptakan ekosistem digital yang aman. Tanpa langkah konkret tersebut, kepastian hukum pidana hanya akan bersifat normatif dan belum mampu memberikan perlindungan nyata bagi korban kebocoran data pribadi.

3. Dalam perspektif fikih jinayah, kebocoran data pribadi dapat dikategorikan sebagai jarimah ta'zir, karena merupakan perbuatan yang melanggar hak individu dan menimbulkan kerugian. Pertanggungjawaban pidana tidak hanya dibebankan kepada peretas sebagai pelaku aktif, tetapi juga kepada pengelola marketplace apabila terbukti lalai menjaga keamanan data. Dengan demikian, fikih jinayah memberikan legitimasi bagi negara untuk menetapkan sanksi pidana maupun administratif guna menjaga kemaslahatan umum serta menegakkan prinsip perlindungan terhadap harta (hifz al-mal) dan kehormatan (hifz al-'irdh).

B. Saran

1. Diperlukan penguatan regulasi turunan dari Undang-Undang Perlindungan Data Pribadi, khususnya terkait mekanisme penegakan hukum, standar keamanan data, serta tata cara pemberian ganti rugi bagi korban. Pemerintah juga perlu meningkatkan literasi digital dan menyelenggarakan sosialisasi secara masif agar masyarakat memahami hak-haknya dalam perlindungan data pribadi. Masyarakat

harus didorong untuk berpartisipasi aktif dalam perlindungan data pribadi melalui pendidikan, pelatihan, dan advokasi, sehingga budaya perlindungan data dapat terbangun dengan baik di Indonesia.

2. Pengelola marketplace harus meningkatkan standar keamanan siber dengan teknologi yang lebih mutakhir, melakukan audit sistem secara berkala, serta menyediakan kebijakan privasi yang transparan. Selain itu, perlu adanya mekanisme pertanggungjawaban yang jelas, termasuk pemberian kompensasi bagi pengguna yang dirugikan akibat kebocoran data pribadi.

3. Masyarakat sebagai subjek data diharapkan lebih berhati-hati dalam memberikan informasi pribadi pada layanan digital. Kesadaran untuk menggunakan kata sandi yang kuat, mengaktifkan autentikasi ganda, dan memantau aktivitas akun secara berkala menjadi langkah preventif yang penting untuk meminimalisasi risiko kebocoran data.

DAFTAR PUSTAKA

- Aryani, A. P., & Susanti, L. E. (2022). Pentingnya perlindungan data pribadi konsumen dalam transaksi online pada marketplace terhadap kepuasan konsumen. *Ahmad Dahlan Legal Perspective*, 2(1), 20-29.
- Azhari, S. P. (2022). Kemudahan Penggunaan, Resiko, dan Kepercayaan Konsumen Terhadap Repurchase Intention pada Situs Belanja Online Shopee. *JURNAL ADMINISTRASI BISNIS*, 12(2), 132-138.
- Bahtiyar, A., Anwar, I., & Aziz, M. F. (2023). Implikasi Hukum Pidana Dalam Perlindungan Data Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
- Dewantara, Stie. Metode Penelitian, Jenis dan sifat penelitian. <http://repository.stiedewantara.ac.id/1868/5/BAB%20III.pdf>
- Diskominfo. Awas tindakan phising! Ini dia langkah-langkah agar tidak terkena pesan berisi link phising, <https://kominfo.kotabogor.go.id/index.php/post/single/897>.
- Efritadewi, A. (2020). Modul Hukum Pidana. *Tanjungpinang–Kepulauan Riau, Universitas Maritim Raja Ali Haji*.
- Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. *Ganesha Law Review*, 5(1), 39-57.
- Frahyanti, F., Syafi'i, M. A., & Devi, H. S. (2024). Analisis faktor-faktor konsumen dalam memilih belanja di online store daripada offline store. *Sahmiyya: Jurnal Ekonomi dan Bisnis*, 42-49.
- Kautsar, T. R. (2022). Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi (Doctoral dissertation, UIN Ar-Raniry).
- Kemendikbud. Kepercayaan dan risiko belanja online. <https://lldikti5.kemdikbud.go.id/home/detailpost/kepercayaan-dan-risiko-belanja-online>, diakses pada 7 juli 2024
- Kementrian komunikasi dan informasi. Bersama lindungi data pribadi di platform digital.
- Lubis, S. N. (2022). Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara (Doctoral dissertation, Universitas Hasanuddin).
- Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan

- Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana Dan Kriminologi*, 2(2), 14-29.
- Mentari, B. M. R. (2020). Saksi Pidana Pembunuhan Dalam Kitab Undang-Undang Hukum Pidana Dengan Hukum Islam. *Al-Ishlah: Jurnal Ilmiah Hukum*, 23(1), 1-38.
- Muin, I. (2023). Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. *Journal Law And Justice*, 1(2).
- News, Sindo. Mengenal perbedaan data breach, security breach, dan data leakage. <https://tekno.sindonews.com/read/501844/207/mengenal-perbedaan-data-breach-security-breach-dan-data-leakage-162808611>.
- Soekonto, Soerjono., & Mamudji, Sri. Penelitian Hukum Normatif: Suatu tinjauan singkat. *Rajawali Pers, Jakarta*.
- Soemitra, A. (2022). Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia. *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, 5(1), 288-303.
- Tambunan, B. H., & Simanjuntak, J. F. (2021). Analisis Pelaksanaan Kas Kecil (Petty Cash) Pada Pt Deli Jaya Samudera. *Journal of Economic and Business*, 3(1), 41-48.
- Tridipta, K. P. A., Sujana, I. N., & Ujianti, N. M. P. (2020). Perlindungan Hukum Terhadap Pelanggar Privasi Konsumen Dalam Jual Beli Online. *Jurnal Analogi Hukum*, 2(3), 356-360.
- Wantiknas. Jenis-jenis data pribadi menurut uu pdp. <http://www.wantiknas.go.id/id/berita/jenis-jenis-data-pribadi-menurut-uu-pdp-ini-rincianny>.
- Wibowo, K. T., SH, M., & Warih Anjari, S. H. (2022). *Hukum pidana materiil*. Prenada Media.
- Yuniarti, Mauliana. Tinjauan umum tentang data pribadi, 15.
- Agung, Anak, Sagung Devi, Utami Jayanti, Fakultas Hukum Universitas, Dewa Ayu, Dian Sawitri, Fakultas Hukum, and Universitas Udayana. "Perlindungan Hukum Subyek Data Pribadi Khususnya Nomor Induk Kependudukan Pada Kartu Tanda Penduduk Ketika Terjadi Peretasan" 12, no. 11 (2024): 2881–91.
- Ahdiat, Adi. "5 E-Commerce Dengan Pengunjung Terbanyak Sepanjang 2023." Databoks, 2023. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/3c9132bd3836eff/5-e-commerce-dengan->

pengunjung-terbanyak-sepanjang-2023.

———. “Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar.” Databoks, 2024. <https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>.

Antaguna, Nyoman Gede, and Anak Agung Sagung Laksmi Dewi. “Pembatasan Kebebasan Berpendapat Dan Berekspresi Di Sosial Media Berdasarkan Peraturan Perundang-Undangan Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE).” *Kertha Wicaksana* 17, no. 2 (2023): 138–46.

ANTARA News. “Dirjen Aptika Pastikan UU PDP Sudah Berlaku Sepenuhnya,” 2024. <https://www.antaranews.com/berita/4404977/dirjen-aptika-pastikan-uu-pdp-sudah-berlaku-sepenuhnya>.

Aprilianti, Astri. “Efektivitas Dan Implementasi Undang-Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siber Di Indonesia: Tantangan Dan Solusi.” *Begawan Abioso* 15, no. 1 (2025): 41–50. <https://doi.org/10.37893/abioso.v15i1.1002>.

ardiyansyah, M, Abdul Muid. “TINJAUAN YURIDIS TINDAK PIDANA TERHADAP KEBOCORAN DATA PRIBADI PENGGUNA PERDAGANGAN ELEKTRONIK,” 2023, 1–14. <https://www.ncbi.nlm.nih.gov/books/NBK558907/>.

Arrasuli, Beni Kharisma, 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>.

Ashari, Fitra. “APJII Tingkatkan Kesadaran Masyarakat Akan Isu Keamanan Siber.” *Antara.News*, 2023.

Asifae, Utpy, Tiara Rizki Amaniar, Jesica Anastasya, Irwandi, and Lisnawati. “Penerapan Kaidah Fiqhiyyah Terhadap Kejahatan Siber Dalam Hukum Jinayah.” *Jurnal Ilmu Hukum* 2, no. 1 (2024): 134–39.

Badar, Eryna Syahadatina, Ahmad Fauzi, and Ahya Jazuli. “Kebijakan Pelindungan Data Pribadi Undang-Undang Nomor 27 Tahun 2022 Dalam Prespektif Hukum Positif Dan Hukum Islam.” *Hukum Islam* 23, no. 1 (2023): 61. <https://doi.org/10.24014/jhi.v23i1.20465>.

Barkatullah, Abdul Halim. *Hukum Transaksi Elektronik (Sebagai Panduan Dalam Menghadapi Era Digital Bisnis e-Commerce Di Indonesia)*, n.d.

- Cyberthreat.id. "91 Juta Data Pengguna Tokopedia Diduga Bocor Dan Diperjualbelikan," 2020.
- Dade, Leonardo Latsiano, Caecilia J.J Waha, and Nurhikmah Nachrawy. "Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia" 13, no. 3 (2024): 9.
- Dahuri, Deri. "Pemerintah Harus Libatkan Stakeholder Dalam Buat Regulasi Perlindungan Data Pribadi." *MediaIndonesia*, 2022. <https://mediaindonesia.com/teknologi/522236/pemerintah-harus-libatkan-stakeholder-dalam-buat-regulasi-perlindungan-data-pribadi>.
- Dasep Suryanto, Slamet Riyanto, Arffudin. "Tentang Perlindungan Data Pribadi Dalam Industri Ritel " Tinjauan Terhadap Kepatuhan Dan Dampaknya Pada Konsumen." *Veritas* 10, no. 1 (2022): 121–35.
- Dewi, K S. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Pembelian Barang Di MarketPlace" 7, no. 1 (2022): 64–70. http://eprints.unmas.ac.id/id/eprint/1527/%0Ahttp://eprints.unmas.ac.id/id/eprint/1527/2/1522_FH_watermark-15-27.pdf.
- Djafar, Wahyudi. "Pengesahan RUU Pelindungan Data Pribadi: 'Terancam' Menjadi Macan Kertas." *Lembaga Studi & Advokasi Masyarakat*, 2022.
- Doni. "Mengenal Sanksi Pelanggar Data Pribadi." *Kementrian Komunikasi Dan Informasi*, September 24, 2022. <https://www.kominfo.go.id/content/detail/44680/mengenal-sanksi-pelanggar-data-pribadi/0/artikel>.
- Dr. Drs. H. Moh. Faishol Hassanuddin, S.H., M.H. "UU Informasi Dan Transaksi Elektronik, Aspek Hukum Dan Pembuktiannya." *Mahkamah Agung Republik Indonesia Pengadilan Tinggi Agama Samarinda*, 2023. <https://pta-samarinda.go.id/artikel-pengadilan/1949-uu-informasi-dan-transaksi-elektronik-aspek-hukum-dan-pembuktiannya-oleh-dr-drs-h-moh-faishol-hasanuddin-s-h-m-h>.
- Era, D I, and Revolusi Industri. "UNIVERSITAS NEGERI MEDAN DALAM MEREALISASIKAN HAK ASASI WARGA NEGARA" XII (2023): 93–103.
- Fachri, Ferinda K. "Mengenal ROPA, Catatan Aktivitas Pengolahan Data Pribadi." *Hukum Online.com*, 2023. <https://www.hukumonline.com/berita/a/mengenal-ropa--catatan-aktivitas-pengolahan-data-pribadi-lt651dafcd8038d/>.
- Firman Muhammad Arif, Muhammad Saifullah Chania. "AKTUALISASI STANDAR PENALARAN FILOSOFIS DALAM PERLINDUNGAN

DATA PRIBADI.” *Jurnal Studi Islam* Vol. 11. N (2022).

Gunadi, Chaterine Grace, Danishel Subiran, Elena Philomena Lee, Lauren Angel Gunawan, and Nicole Baretta. “Perlindungan Hukum Atas Kebocoran Data Pribadi.” *Proceeding of Conference on Law and Social Studies* 4, no. 1 (2023): 1–14.

Hapiz, Mutiara, Livia Pijar Septia, Dwi Aprilianti, Dwi Aprilianto, Isda Maulida, Fadil Muhammad, Amanda Shaafia, Muhammad Hilman Maulana, and Dian Herdiana. “Analisis Kebijakan Pengembangan UMKM Digital Di Indonesia: Tantangan Dan Peluang.” *Jurnal Ilmiah Multidisiplin* 3, no. 5 (2025): 36–44. <https://doi.org/10.5281/zenodo.15538100>.

Harwida, G, E Novilia, S Hadi, Y Tertibi, N Arqom, F Eka, and ... “Edukasi Mahasiswa Dalam Kapabilitas Belanja Online Melalui Marketplace.” *Journal.Unublitar.Ac.Id* 7, no. 2 (2023): 266–74. http://journal.unublitar.ac.id/pendidikan/index.php/Riset_Konseptual/article/view/713.

Healey, Robert. “GDPR Dan Prinsip Akuntabilitas.” FORMITI, 2020. <https://www.lexology.com/library/detail.aspx?g=34144a92-3aa2-4c75-b1c3-346be0719117>.

Hertianto, M Rafifnafia. “Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia.” *Kertha Patrika* 43, no. 1 (2021): 93. <https://doi.org/10.24843/kp.2021.v43.i01.p07>.

Hidayat, Amry Nur. “Perjalanan Bukalapak, Dari IPO Pasar Modal Terbesar Indonesia Hingga Jadi Fokus Jual Pulsa.” *Warta Ekonomi.co.id*, 2025. <https://wartaekonomi.co.id/read554564/perjalanan-bukalapak-dari-ipo-pasar-modal-terbesar-indonesia-hingga-jadi-fokus-jual-pulsa>.

Hinonaung, Kezia Lembong, Johny, and Harly Stanly Muaja. “Ketentuan Pidana Di Bidang Administrasi Kepedudukan Menurut Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.” *Lex Privatum* 8, no. 32 (2020): 73–92. http://hpj.journals.pnu.ac.ir/article_6498.html.

Ibad, Syahrul, Yona Wahyu Lolita, Program Studi, Teknologi Informasi, and Universitas Ibrahimy. “Pengembangan Pelayanan Publik Melalui E-Government (Studi Pada Layanan Smartcity Kabupaten Situbondo).” *Jurnal Administrasi Publik* 6, no. 2 (2020): 201–26.

Indonesia, CNN. “200 Ribu Data Pengguna Facebook Marketplace Bocor Di Forum Hacker,” 2024. <https://www.cnnindonesia.com/teknologi/20240215145425-192-1063044/200-ribu-data-pengguna-facebook-marketplace-bocor-di-forum->

hacker.

———. “Lazada Konfirmasi Peretasan 1,1 Juta Akun RedMart.” CNN Indonesia, 2022. <https://www.cnnindonesia.com/teknologi/20201031103811-185-564335/lazada-konfirmasi-peretasan-11-juta-akun-redmart>.

———. “Luna Maya Jadi Korban Penipuan, Rugi Rp1,9 Juta.” CNN Indonesia, 2022. <https://www.cnnindonesia.com/hiburan/20220202123717-234-754031/luna-maya-jadi-korban-penipuan-rugi-rp19-juta>.

Info Hukum. “Jenis-Jenis Data Pribadi Menurut UU Perlindungan Data Pribadi.” InfoHukum, 2025. <https://fahum.umsu.ac.id/info/jenis-jenis-data-pribadi-menurut-uu-perlindungan-data-pribadi/>.

Iskandar. “200 Ribu Data Penggua Facebook Bocor Di Forum Hacker.” Liputan6, 2024. <https://www.liputan6.com/tekno/read/5528128/200-ribu-data-pengguna-facebook-marketplace-bocor-di-forum-hacker>.

Iswara, Aditya Jaya. “Data 91 Juta Pengguna Tokopedia Diduga Bocor, Media Asing Ikut Soroti.” Kompas.com, 2020. <https://www.kompas.com/global/read/2020/05/03/133257970/data-91-juta-pengguna-tokopedia-diduga-bocor-media-asing-ikut-soroti?page=all>.

Jamaluddin, Fitriani, Muhammad Ashabul Kahfi, Ekonomi Syariah, Fakultas Syariah, Iain Palopo, Ekonomi Syariah, Fakultas Syariah, et al. “PERLINDUNGAN DATA PRIBADI PENGGUNA DOMPET DIGITAL OVO” 6, no. 1 (2021): 37–41.

Kartini, Anisa Prasetya Putri. “Cara Daftar Shopee Paylater Beserta Syaratnya.” Tempo, 2023. <https://www.tempo.co/ekonomi/cara-daftar-shopee-paylater-beserta-syaratnya-124266>.

kementrian pendayagunaan aparatur negara dan reformasi birokrasi. “Tindak Pidana Dalam UU PDP Dan Sanksinya,” 2023. <https://sippn.menpan.go.id/berita/59933/rumah-tahanan-negara-kelas-iib-pelaihari/4-tindak-pidana-dalam-uu-pdp-dan-sanksinya>.

Khatami, Akhir Nazli, and Arifuddin Muda Harahap. “Penyalahgunaan KTP Masyarakat Untuk Pinjaman Dana PNM Mekaar Perspektif Sadd Adz-Zari ’ Ah Di Kota Tanjungbalai.” *Ad-Deenar: Jurnal Ekonomi Dan Bisnis Islam*, 2023, 343–54.

Kominfo. “Bersama Lindungi Data Pribadi Di Platform Digital.” Diskominfo, 2020. <https://diskominfo.kotawaringinbaratkab.go.id/page/detail/bersama-lindungi-data-pribadi-di-platform-digital>.

kosworo wenderline. “Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan Dan

Kepastian Hukum” 7, no. 2 (2022): 86–103.

Kumparan. “Profil Perusahaan Shopee Sebagai Aplikasi Belanja Online Asia.” Kumparan.com, 2022. <https://kumparan.com/berita-terkini/profil-perusahaan-shopee-sebagai-aplikasi-belanja-online-asia-1y5jwp8MoSo/1>.

Lailatul Badriah, Dwiyanto Indiahono, Sukarso. “Akuntabilitas Dalam Kebijakan Perlindungan.” *Inovasi Kebijakan* 8 (2023): 89–102.

Lawyers, Bp. “UU PDP Berlaku, Ini Isi Pengaturan Perlindungan Data Pribadi Di Indonesia.” Bp Lawyers Counselor At Law, 2022.

Luthfi, Rosihan. “Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia.” *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36. <https://doi.org/10.59188/jurnalsostech.v2i5.336>.

Mariani, John F. “Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia.” *Of Social Science Research* 3 (2020): 176–176. <https://doi.org/10.5040/9781635577068-0537>.

Martini Idris, Meirina Nurlani, and Serlika Aprita. “Pengaturan Dan Penegakan Hukum Kejahatan Dunia Maya (Cyber Crime): Harmonisasi Revisi Undang-Undang ITE Dan KUHP.” *Lex Lata : Jurnal Ilmiah Ilmu Hukum* 6, no. 3 (2024): 396–411. <https://doi.org/10.28946/lexl.v6i3.4266>.

Maulana Fikran. “Tinjauan Hukum Pidana Islam Terhadap Cyber Crime Dalam Bentuk Pencurian Data Pribadi.” *Legitimasi: Jurnal Hukum Pidana Dan Politik Hukum* 10, no. 2 (2021): 7.

Mediana. “Kemenkominfo Tangani 111 Kasus Kebocoran Data Pribadi Sepanjang 2019-2024.” KOMPAS, 2024. <https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024>.

Mitraberdaya. “Perbedaan GDPR Dan Regulasi Indonesia.” Mitra Berdaya Optima, 2024. <https://mitraberdaya.id/id/news-information/perbedaan-gdpr-dan-regulasi-indonesia>.

Muhammad Taufik, and Fatimah Zahara. “Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook).” *Jurnal Ilmu Hukum, Humaniora Dan Politik* 4, no. 6 (2024): 2378–92. <https://doi.org/10.38035/jihhp.v4i6.2744>.

Mustafid. “Etika Pemerintahan Berbasis Fiqih Siyasah Di Era Digital.” *Jurnal Hukum Islam Dan Sosial*, 2024.

- Natha., Kadek Dio Ramadi, I Nyoman Putu Budiarta., and Ni Gusti Ketut Sri Astiti. "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada Perdagangan Elektronik Lokapasar (Marketplace)." *Jurnal Preferensi Hukum* 3, no. 1 (2022): 143–48.
- News. "Aspek Dan Perbuatan Hukum Dalam Undang-Undang ITE." Sip Law Firm, 2023. <https://siplawfirm.id/aspek-dan-perbuatan-hukum-dalam-undang-undang-ite/?lang=id>.
- Nisau, Eriska Laila. "ANALISIS MAQĀSĪD AL- SHARĪAH TERHADAP PERLINDUNGAN HUKUM DATA PRIBADI MENURUT UNDANG-UNDANG NOMOR 27 TAHUN 2022." *Skripsi* 87, no. 1,2 (2023): 149–200.
- Nurmutia, Elga. "Profil Blibli, Perusahaan E-Commerce Milik Grup Djarum Yang Tercatat Di BEI." *Liputan6.com*, 2023. <https://www.liputan6.com/saham/read/5232245/profil-blibli-perusahaan-e-commerce-milik-grup-djarum-yang-tercatat-di-bei>.
- Pengabdian, Jurnal, and Kepada Masyarakat. "Edukasi Terkait Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Bagi Masyarakat Desa Lubang Buaya" 3 (2024): 106–13.
- Pilo, Rani. "Pencurian Identitas: Ancaman Terbesar Yang Harus Diwaspadai." *Aplikas Servis Pesona*, 2023. <https://aplikas.com/blog/pencurian-identitas/>.
- 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, no. 4 (2024): 3412–25.
- Pratama Putra, Rendy, Hendi Saputra, Hukum Perlindungan Privasi Yusuf Daeng, Nasri Linra, Atan Darham, Derry Handrianto, Risky Risandy Sianturi, and Denny Martin. "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi." *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 2898–2905. <https://j-innovative.org/index.php/Innovative/article/view/6662>.
- Priliasari, Erna. "PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA (Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia)." *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79.

- Pujianti, Sri. "Pemerintah: UU Perlindungan Data Pribadi Beri Perlindungan Hukum." Humas MKRI, 2023. <https://www.mkri.id/index.php?page=web.Berita&id=18915>.
- Ramli, Ahmad M, Tasya Safiranita Ramli, Fakultas Hukum, and Universitas Padjadjaran. "Perlindungan Data Pribadi Di Indonesia Melalui Mekanisme Register of Processing Activities (ROPA): Studi Komparatif Antara UU PDP Dengan GDPR" 2 (2024): 274–83.
- Razi, Fachrul, Hadi Tuasikal, and Dwi Pratiwi Markus. "Implementation and Challenges of the Personal Data Protection Law in Indonesia." *Jurnal Indonesia Sosial Teknologi* 5, no. 12 (2024): 6015–21. <https://doi.org/10.59141/jist.v5i12.1285>.
- Ririn Nur Aisyah, Hana Khalidah, Surya Putri Nazrina, Johan Silalahi, and Dhini Aulia. "Efektivitas Uu No. 8 Tahun 1999 Dalam Melindungi Data Pribadi Konsumen Di Sektor E-Commerce." *Jurnal Moralita : Jurnal Pendidikan Pancasila Dan Kewarganegaraan* 6, no. 1 (2025): 9–18. <https://doi.org/10.36985/v7dfhf27>.
- Rizki, Mochamad Januar. "Ancaman Sanksi Administratif Hingga Pidana Dalam UU Pelindungan Data Pribadi." Hukum Online.com, 2022. <https://www.hukumonline.com/berita/a/ancaman-sanksi-administratif-hingga-pidana-dalam-uu-pelindungan-data-pribadi-lt633c69ce2de5c?>
- Rustam, Fadhilah Nuraini. "Sanksi Pidana Penyalahgunaan Informasi/Dokumen Elektronik Konsumen." Dalimunthe Tampubolon, 2020.
- Sabadina, Uni. "Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online." *Jurnal Lex Renaissance* 6, no. 4 (2021): 799–814. <https://doi.org/10.20885/jlr.vol6.iss4.art11>.
- Sadillah Ahmad, Ridho, Dyah Ayu Puspaningtyas, and Muhammad Nur Karim Al Ismariy. "Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital." *The Juris* 9, no. 1 (2025): 15–23. <https://doi.org/10.56301/juris.v9i1.1307>.
- Saly, Jeane Neltje, Halena Artamevia, Kendelif Kheista, Barnabas Juni, Saputra Gulo, Evellyn Abigael Rhemrev, and Michelle Christie. "Analisis Perlindungan Data Pribadi Terkait UU NO.27 TAHUN 2022" 1, no. 3 (2023): 145–53.
- Saputra, Andi Tri. "Konsep Intelijen Dan Penafsiran Kontekstualitas Terhadap Q.S Al-Hujarat Ayat 12 (Aplikasi Metode Penafsiran Kontekstualis Abdullah Saeed." *Nun: Jurnal Studi Alquran Dan Tafsir Di Nusantara* 5, no. 2 (2020): 93–125. <https://doi.org/10.32495/nun.v5i2.92>.

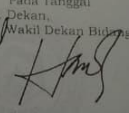
- Saputri, Elyasa Yahya. "Regulasi Hukum Dalam Melindungi Data Pribadi." Radarmagelang.id, 2025. https://radarmagelang.jawapos.com/artikel-ilmiah/686176164/regulasi-hukum-dalam-melindungi-data-pribadi?#google_vignette.
- Sengkey, Victoria, Said Aneke-R, and Deizen Rompas. "Penyidikan Terhadap Tindak Pidana Di Bidang Administrasi Kependudukan Berdasarkan Undang-Undang No. 24 Tahun 2013 Tentang Administrasi Kependudukan." *Lex Privatum* XI, no. 5 (2023): 1–8.
- Sitoresmi, Ayu Rifka. "Profil PT Tokopedia Dan Perjalanan Bisnisnya, Perusahaan Perdagangan Elektronik Di Indonesia." Liputan6.com, 2023. <https://www.liputan6.com/hot/read/5183788/profil-pt-tokopedia-dan-perjalanan-bisnisnya-perusahaan-perdagangan-elektronik-di-indonesia>.
- Sudarti. "Perlindungan Data Pribadi Perspektif Sadd Dzari'ah." Artikula.id, 2022.
- Tampubolon, Manotar. "Metode Penelitian Metode Penelitian." *Metode Penelitian Kualitatif* 3, no. 17 (2023): 43. [http://repository.unpas.ac.id/30547/5/BAB III.pdf](http://repository.unpas.ac.id/30547/5/BAB%20III.pdf).
- Tari Oktaviani, Nibras Nada Nailufar. "UU Perlindungan Data Pribadi: Jenis Data Dan Sanksi Pidananya." Kompas.com, 2023. <https://nasional.kompas.com/read/2023/07/19/00150061/uu-perlindungan-data-pribadi--jenis-data-dan-sanksi-pidananya?>
- Tempo. "Cerita Di Balik Mulai Beroperasinya Lazada 11 Tahun Lalu." Tempo.co, 2023. https://www.tempo.co/ekonomi/cerita-di-balik-mulai-beroperasinya-lazada-11-tahun-lalu-204670#goog_rewarded.
- Trisandi, Desmon, and Ahmad Sofian. "Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber Indonesia." *Syntax Literate ; Jurnal Ilmiah Indonesia* 9, no. 2 (2024): 728–37. <https://doi.org/10.36418/syntax-literate.v9i2.15198>.
- Wakalahmu. "Hadis Tentang Amanah Dalam Islam," 2021. <https://wakalahmu.com/artikel/dunia-islam/hadits-tentang-amanah-dalam-islam>.
- Waluyo, Dwitri. "Era Baru Perlindungan Data Pribadi." INDONESIA.GO.ID Portal Informasi Indonesia, 2024. <https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1>.
- Watkot, Fransiscus Xaverius, Muhammad Toha Ingratubun, Adelia Apriyanti, and Data Pribadi. "PERLINDUNGAN DATA PRIBADI MELALUI PENERAPAN" 5, no. 1 (2024).

- Wibawana, Widhia Arum. "Isi UU Perlindungan Data Pribadi: Larangan, Sanksi Dan Jenis Data." Detiknews, 2022.
- Yudistira, Muhammad, and 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, no. 4 (2023): 3803. <https://doi.org/https://doi.org/10.31933/unesrev.v5i4>.
- Yuniarti, Mauliana. "Bab Ii Tinjauan Umum Tentang Data Pribadi 1.1," 2022, 14–22.
- Yuyut Prayuti. "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di Indonesia." *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13. <https://doi.org/10.22225/juinhum.5.1.8482.903-913>.
- Ziqra, Yahya, Mahmul Siregar, and Jelly Leviza. "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online." *Iuris Studia: Jurnal Kajian Hukum* 2 (2021): 330–36. <https://doi.org/10.55357/is.v2i2.146>.

Lampiran 1 Surat Keputusan (SK)


KEPUTUSAN DEKAN FAKULTAS SYARIAH INSTITUT AGAMA ISLAM NEGERI PALOPO
NOMOR 176 TAHUN 2024
TENTANG
PENGANGKATAN TIM DOSEN PEMBIMBING DAN PENGUJI SEMINAR PROPOSAL, SEMINAR HASIL
DAN UJIAN MUNAQASYAH MAHASISWA FAKULTAS SYARIAH IAIN PALOPO TAHUN 2024
DENGAN RAHMAT TUHAN YANG MAHA ESA
DEKAN FAKULTAS SYARIAH INSTITUT AGAMA ISLAM NEGERI PALOPO,

Menimbang	a. bahwa demi kelancaran proses pengujian seminar proposal, seminar hasil dan ujian munaqasyah bagi mahasiswa Program Strata Satu (S1), maka dipandang perlu dibentuk Tim Dosen Pembimbing dan Penguji Seminar Proposal, Seminar Hasil dan Ujian Munaqasyah;
	b. bahwa untuk menjamin terlaksananya tugas Tim Dosen Pembimbing dan Penguji Seminar Proposal, Seminar Hasil dan Ujian Munaqasyah sebagaimana dimaksud dalam butir a di atas, maka perlu ditetapkan melalui Surat Keputusan Dekan;
Mengingat	1. Undang-Undang RI Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional;
	2. Undang-Undang RI Nomor 12 Tahun 2012 tentang Pendidikan Tinggi;
	3. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan dan Pengelolaan Perguruan Tinggi;
	4. Peraturan Presiden RI Nomor 141 Tahun 2014 tentang Perubahan STAIN Palopo Menjadi IAIN Palopo;
	5. Peraturan Menteri Agama RI Nomor 5 Tahun 2015 tentang Organisasi dan Tata Kerja IAIN Palopo.
	MEMUTUSKAN :
Menetapkan	KEPUTUSAN DEKAN FAKULTAS SYARIAH IAIN PALOPO TENTANG PENGANGKATAN TIM DOSEN PEMBIMBING DAN PENGUJI SEMINAR PROPOSAL, SEMINAR HASIL DAN UJIAN MUNAQASYAH MAHASISWA PROGRAM STRATA SATU (S1) FAKULTAS SYARIAH INSTITUT AGAMA ISLAM NEGERI PALOPO
KESATU	Mengangkat mereka yang tersebut namanya pada lampiran Surat Keputusan ini sebagaimana yang tersebut pada alinea pertama huruf (a) di atas,
KEDUA	Tugas Tim Dosen Pembimbing dan Penguji Seminar Proposal, Seminar Hasil dan Ujian Munaqasyah adalah : mengoreksi, mengarahkan, menilai/mengevaluasi dan menguji kompetensi dan kemampuan mahasiswa berdasarkan skripsi yang diajukan serta memberi dan menyampaikan hasil keputusan atas pelaksanaan ujian skripsi mahasiswa berdasarkan pertimbangan tingkat penguasaan dan kualitas penulisan karya ilmiah dalam bentuk skripsi;
KETIGA	Segala biaya yang timbul sebagai akibat ditetapkannya Surat Keputusan ini dibebankan kepada DIPA BLU IAIN Palopo Tahun 2024;
KEEMPAT	Surat Keputusan ini berlaku sejak tanggal ditetapkannya dan berakhir setelah kegiatan pengujian munaqasyah selesai, dan akan diadakan perbaikan seperlunya jika terdapat kekeliruan didalamnya;
KELIMA	Surat Keputusan ini disampaikan kepada yang bersangkutan untuk dilaksanakan sebagaimana mestinya.

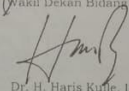
Ditetapkan di : Palopo
Pada Tanggal : 20 Juli 2024
an. Dekan,
Wakil Dekan Bidang Akademik

Dr. H. Haris Kulle, Lc., M. Ag.
NIP 197006232005011003

PERAN : KEPUTUSAN DEKAN FAKULTAS SYARIAH IAIN PALOPO
AMOR : 176 TAHUN 2024
TENTANG : PENGANGKATAN TIM DOSEN PEMBIMBING DAN PENGUJI SEMINAR PROPOSAL,
SEMINAR HASIL DAN UJIAN MUNAQASYAH MAHASISWA INSTITUT AGAMA ISLAM
NEGERI PALOPO TAHUN 2024

- I. Nama Mahasiswa : Sidar Saputri
NIM : 20030201108
Fakultas : Syariah
Program Studi : Hukum Tata Negara (Siyasah)
- II. Judul Skripsi : "Eksistensi Hukum Pidana Dalam Pembocoran Data Pribadi Pada Belanja Online".
- III. Tim Dosen Penguji :
1. Ketua Sidang : Dr. Muhammad Tahmid Nur, M.Ag.
2. Sekretaris Sidang : Dr. H. Haris Kulle, Lc., M.Ag.
1. Penguji I : Ilham, S. Ag., M. Ag.
2. Penguji II : Muhammad Yassir Akbar Ramadhani S. H., M. H.
1. Pembimbing I / Penguji : Dr. H. Firman Muhammad Arif, Lc., M. Hl.
2. Pembimbing II / Penguji : Fitriani Jamaluddin, S. H., M. H.

Palopo, 03 Juni 2024

an. Dekan,
Wakil Dekan Bidang Akademik


Dr. H. Haris Kulle, Lc., M. Ag.
NIP 197006232005011003

Lampiran 2 Halaman Persetujuan Pembimbing

HALAMAN PERSETUJUAN PEMBIMBING

Setelah menelaah dengan seksama skripsi berjudul :

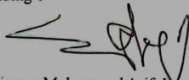
Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace
yang ditulis oleh :

Nama : Sidar Saputri
NIM : 2003020108
Fakultas : Syariah
Program Studi : Hukum Tata Negara (Siyasah)

Menyatakan bahwa skripsi tersebut telah memenuhi syarat-syarat akademik dan layak untuk diajukan pada ujian/*munaqasyah*.

Demikian persetujuan ini dibuat untuk proses selanjutnya.

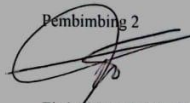
Pembimbing 1



Dr. H. Firman Muhammad Arif, Lc., M.HI

NIP. 197702012011011002

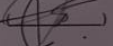
Pembimbing 2



Fitriani Jamaluddin, S.H., M.H

NIP. 199204162018012003

Lampiran 3 Berita Acara

		KEMENTERIAN AGAMA REPUBLIK INDONESIA UNIVERSITAS ISLAM NEGERI PALOPO FAKULTAS SYARIAH Kampus 1 Jalan Agatis Kel. Balandi Kec. Bara Kota Palopo Sulawesi Selatan 91914 Email: fakultas syariah@uinpalopo.ac.id - Website: www.syariah.uinpalopo.ac.id
BERITA ACARA		
Pada hari ini Kamis, 28 Agustus 2025 telah dilaksanakan Seminar Hasil Penelitian Skripsi mahasiswa atas:		
Nama	: Sidar Saputri	
NIM	: 2003020108	
Prodi	: Hukum Tata Negara	
Judul Skripsi	: Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace.	
Pembimbing I	: Dr. H. Firman Muhammad Arif, Lc., M.Hl.	
Pembimbing II	: Fitriani Jamaluddin, S.H., M.H.	
Penguji I	: Ilham, S.Ag., M.A.	
Penguji II	: M. Yassir Akbar Ramadhani, S.H., M.H.	
Demikian berita acara ini dibuat untuk digunakan sebagaimana mestinya.		
 Dekan,  Muhammad Tahmid Nur		

Lampiran 4 Nota Dinas Tim Penguji

Ilham, S.Ag., M.A.
Firmansyah, S.Pd., S.H., M.H.
Dr. H. Firman Muhammad Arif, Lc., M.HI
Fitriani Jamaluddin, S.H., M.H

NOTA DINAS TIM PENGUJI

Lamp. : -

Hal : Skripsi a.n. Sidar Saputri

Yth. Dekan Fakultas Syariah

Palopo

Assalamu 'alaikum Warahmatullahi Wabarakatuh.

Setelah menelaah naskah perbaikan berdasarkan seminar hasil penelitian terdahulu, baik dari segi isi, bahasa maupun teknik penulisan terhadap naskah skripsi mahasiswa di bawah ini:

Nama : Sidar Saputri

NIM : 2003020108

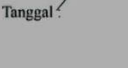
Program Studi : Syariah

Judul Skripsi : Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace.

Maka naskah skripsi tersebut dinyatakan sudah memenuhi syarat-syarat akademik dan layak diajukan untuk diujikan pada ujian *munaqasyah*.

Demikian disampaikan untuk proses selanjutnya.

Wassalamu 'alaikum Warahmatullahi Wabarakatuh.

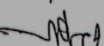
1. Ilham, S.Ag., M.A (Penguji I)	() Tanggal :
2. Firmansyah, S.Pd., S.H., M.H. (Penguji II)	() Tanggal:
3. Dr. H. Firman Muhammad Arif, Lc., M.HI (Pembimbing 1)	() Tanggal :
4. Fitriani Jamaluddin, S.H., M.H (Pembimbing 2)	() Tanggal :

Lampiran 5 Halaman Persetujuan Tim Penguji

HALAMAN PERSETUJUAN TIM PENGUJI

Skripsi yang berjudul "Kepastian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace" yang ditulis oleh Sidar Saputri, NIM 2003020108, mahasiswa Program Studi Hukum Tata Negara Fakultas Syariah Universitas Islam Negeri Palopo, yang telah diujikan dalam seminar hasil penelitian pada hari kamis 28 Agustus 2025 bertepatan dengan 4 Rabi'ul Awal 1447 telah diperbaiki sesuai cacatan dan permintaan Tim Penguji, dan dinyatakan layak untuk diajukan pada sidang Ujian *Munaqasyah*.

Tim Penguji

- | | |
|--|---|
| 1. Dr. Muhammad Tahmid Nur, M.Ag.
Ketua Sidang/Penguji | ()
Tanggal : |
| 2. Dr. Fasiha, S.E.L., M.E.L.
Sekretaris Sidang/Penguji | ()
Tanggal : |
| 3. Ilham, S.Ag., M.A.
Penguji I | ()
Tanggal : |
| 4. Firmansyah, S.Pd., S.H., M.H.
Penguji II | ()
Tanggal : |
| 5. Dr. H. Firman Muhammad Arif, Lc., M.HI
Pembimbing I | ()
Tanggal : |
| 6. Fitriani Jamaluddin, S.H., M.H
Pembimbing 2 | ()
Tanggal : |

Lampiran 6 Tim Verifikasi

TIM VERIFIKASI NASKAH SKRIPSI
FAKULTAS SYARIAH

NOTA DINAS

Lamp. :
Hal : Skripsi an. Sidar Saputri
Yth. Dekan Fakultas Syariah
Di-
Palopo

Assalamu 'alaikumWarahmatullahi Wabarakatuh.

Tim Verifikasi Naskah Skripsi Fakultas Syariah IAIN Palopo setelah menelaah naskah skripsi sebagai berikut:

Nama : Sidar Saputri
NIM : 2003020108
Program Studi : Hukum Tata Negara (Siyasah)
Judul Skripsi : Kepasatian Hukum Pidana Terhadap Kebocoran Data Pribadi Pada Marketplace

Menyatakan bahwa penulisan naskah skripsi tersebut

1. Telah memenuhi ketentuan sebagaimana dalam Buku Pedoman Penulisan Skripsi, Tesis dan Artikel Ilmiah yang berlaku pada Fakultas Syariah IAIN Palopo.
2. Telah sesuai dengan kaidah tata bahasa sebagaimana diatur dalam Pedoman Umum Ejaan Bahasa Indonesia.

Demikian disampaikan untuk proses selanjutnya.

Wassalamu 'alaikumWarahmatullahi Wabarakatuh

Tim Verifikasi

1. Nirwana Halide, S.HI., M.H. Tanggal :	()
2. Firmansyah, S Pd., S.H., M.H. Tanggal :	()

Lampiran 7 Plagiasi

sidar			
ORIGINALITY REPORT			
12%	14%	3%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	repository.iainpalopo.ac.id Internet Source	5%	
2	Submitted to State Islamic University of Alauddin Makassar Student Paper	1%	
3	j-innovative.org Internet Source	1%	
4	ifrelresearch.org Internet Source	1%	
5	repositori.uin-alauddin.ac.id Internet Source	1%	
6	pta-samarinda.go.id Internet Source	1%	
7	review-unes.com Internet Source	1%	
8	123dok.com Internet Source	1%	

DAFTAR RIWAYAT HIDUP



Sidar Saputri, lahir di Belopa pada tanggal 25 oktober 2001. Penulis merupakan anak pertama dari 2 bersaudara dari pasangan seorang ayah yang bernama Ridwan dan ibu Sinar. Saat ini penulis tinggal di Jalan Pahlawan, Kecamatan Belopa, Kabupaten Luwu. Pendidikan dasar penulis diselesaikan pada tahun 2013 di SD Negeri 24 Kampung Tangnga. Kemudian di tahun yang saa menempuh pendidikan di MTS Negeri 1 Belopa hingga tahun 2016. Pada tahun 2016 melanjutkan pendidikan di SMK Negeri 2 Luwu, penulis mengambil jurusan Otomatisasi Tata Kelola Perkantoran. Setelah lulus SMK di tahun 2019 penulis melanjutkan pendidikan SI pada tahun 2020 di Universitas Islam Negeri (UIN) Palopo dengan Program Studi Hukum Tata Negara Fakultas Syariah.