TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL

Oleh :

NURSYAHRANI SABILA ELAKE

04020220147

SKRIPSI

Diajukan sebagai Tugas Ujian Akhir dalam rangka penyelesaian Studi
Pada Program Studi Ilmu Hukum

FAKULTAS HUKUM

UNIVERSITAS MUSLIM INDONESIA

MAKASSAR

2026

HALAMAN JUDUL

TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL

SKRIPSI

Skripsi ini diajukan untuk salah satu persyaratan guna memperoleh gelar Sarjana Hukum pada Fakultas Hukum program studi Ilmu Hukum di Universitas Muslim Indonesia

Oleh:

Nursyahrani Sabila Elake

040 2022 0147

FAKULTAS HUKUM

UNIVERSITAS MUSLIM INDONESIA

MAKASSAR

2026

PERSETUJUAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa:

Nama Mahasiswa	: Nursyahrani Sabila Elake
Stambuk	04020220147
Program Studi	: Ilmu Hukum
Bagian	: Hukum Pidana
Judul	:TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL
No.SK Penetapan	: Nomor: 0110/H.05/FH-UMI/IX/2025

Telah diperiksa dan disetujui untuk diajukan dalam Ujian Skripsi

Makassar, Maret 2026

Pembimbing I

Prof. Dr. Hj. Muiyati Pawennei., SH., M. Hum.
NIPS. 196112011987032003

Pembimbing II

Dr. H. Salle,SE.,SH.,MH.
NIPS.104140474

Mengetahui
Ketua Bagian Hukum Pidana

Dr. H. Azwad Rachmat Hambali, SH.,MH.
NIPS. 104101114

PERSETUJUAN UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: Nursyahrani Sabila Elake
NIM	04020220147
Bagian	: Hukum Pidana
Judul Skripsi	: Tinjauan Yuridis Tindak Pidana Pelanggaran Privasi Data Pribadi Dalam Era Digital
No.SK Penetapan	: Nomor: 0110/H.05/FH-UMI/IX/2025

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, Maret 2026

A.n. Dekan

Wakil Dekan I

Dr. Andika Prawira Buana, S.H., M.H.

NIPs.104151319

PENGESAHAN SKRIPSI

TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PROBADI DALAM ERA DGITAL

Disusun dan diajukan oleh:

NURSYARANI SABILA ELAKE
04020220147

Telah dipertahankan dihadapan Panitia Ujian Skripsi pada Program Studi Sarjana Ilmu Hukum Fakultas Hukum Universitas Muslim Indonesia
Pada 2 April 2026
dan dinyatakan diterima

Panitia Ujian

Ketua	Anggota
Prof. Dr. Hj. Mulyati Pawennei, S.H., M. Hum	**Dr. H. Salle, S.E., S.H., M.H**
NIPs. 196112011987032003	NIPs. 104140474

Dekan Fakultas Hukum
Universitas Muslim Indonesia

Prof. Dr. Muhammad Rinaldy Bima, S.H., M.H.
NIPs.104101110

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini:

Nama	: Nursyahrani Sabila Elake
NIM	: 040 2022 0147
Program Studi	: Ilmu Hukum

Menyatakan dengan sebenarnya bahwa skripsi saya ini benar merupakan hasil karya sendiri, bukan merupakan hasil plagiasi terhadap karya ilmiah orang lain. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan dari skripsi ini merupakan hasil plagiasi, maka saya bersedia menerima sanksi karena perbuatan tersebut.

Makassar, 2 April 2026

Yang menyatakan,



Nursyahrani Sabila Elake

PENGESAHAN PENGUJI

Diterangkan bahwa skripsi mahasiswa:

Nama	: Nursyahrani Sabila Elake
NIM	: 04020220147
Bagian	: Hukum Pidana
Judul Skripsi	:Tinjauan Yuridis Tindak Pidana Pelanggaran Privasi Data Pribadi Dalam Era Digital
No. SK Penetapan	: Nomor. 0110/H.05/FH-UMI/IX/2025

Telah dipertahankan di hadapan Majelis Ujian Skripsi dan dinyatakan Lulus oleh:

1. Prof. Dr. Hj. Mulyati Pawennei, S.H., M. Hum. (.....)
   (Pembimbing I)
2. Dr. H. Salle, S.E., S.H., M.H (.....)
   (Pembimbing II)
3. Dr. Sutiawati, S.H., M.H (.....)
   (Penguji I)
4. Dr. Syarifuddin, S.H., M.H (.....)
   (Penguji II)

KATA PENGANTAR



Puji syukur kita panjakan kehadirat Allah Swt. Yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul **"TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL"** sebagai salah satu syarat untuk memperoleh gelar sarjana hukum di program studi Ilmu Hukum, Fakultas Hukum, Universitas Muslim Indonesia.

Penyusunan skripsi ini tentunya tidak terlepas dari dukungan berbagai pihak yang tak ternilai harganya, tak henti-hentinya mendoakan, memberi semangat, menemani, membantu penulis secara langsung maupun tidak langsung. Maka dari itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih diiringi do'a kepada Allah SWT, kepada kedua orang tua tercinta, Ayahanda Bahrun Elake S.Pd dan Ibunda Nurisyah Manggis S.Pd yang dengan penuh kasih sayang membersarkan, mendidik, dan untuk setiap doa-doa yang tidak pernah lepas untuk penulis serta kesabaran dan pengorbanan yang begitu besar sampai saat ini.

Melalui kesempatan ini, penulis juga menyampaikan rasa hormat dan banyak terima kasih kepada:

1. Bapak Prof. Dr. H. Hambali Thalib, SH., M.H selaku Rektor Universitas Muslim Indonesia.
2. Bapak Prof. Dr. Muhammad Rinaldy Bima, SH., M.H., selaku

   Dekan Fakultas Hukum Universitas Muslim Indonesia.
3. Bapak Dr. H. Azwad Rachmat Hambali, SH.,MH. Selaku Ketua Hukum Pidana.

4. Ibu Prof. Dr. Hj. Mulyati Pawennei., SH., M. Hum. Selaku Pembimbing I, dan Bapak Dr. H. Salle,SE.,SH.,MH. Selaku pembimbing II yang selalu meluangkan waktu untuk memberikan bimbingan, arahan serta saran kepada penulis dari penyusunan proposal sampai skripsi ini selesai. Semoga semua hal yang telah diberikan dari pembimbing bisa menjadi berkah untuk penulis kedepanya.
5. Ibu Dr. Sutiawati, SH., MH. dan Bapak Dr. Syarifuddin, SH., MH. selaku tim penguji yang telah memberikan masukan dan saran pada ujian seminar proposal sampai skripsi.
6. Seluruh dosen Fakultas Hukum Universitas Muslim Indonesia yang telah memberikan ilmu yang sangat bermanfaat kepada penulis.
7. Kepada adik penulis, Fazar Ashar Elake yang menjadi penyemangat untuk penulis menyelesaikan skripsi ini dan semoga menjadi motivasi untuk meraih mimpi-mimpi di masa depan.
8. Kepada Naya, Salsa, Fara dan Pinkan yang sudah seperti saudara untuk penulis terima kasih selalu mendukung walaupun terpisah jarak dan waktu, selalu menghibur dengan cerita yang tiada habisnya dan selalu setia menemani dan mendengarkan setiap keluh kesah penulis.
9. Kepada Suci, Kikay, Utami dan Tys teman seperjuangan yang selalu menguatkan dalam proses skripsi ini, berbagi tawa, menjadi teman diskusi, teman senasip sepenanggungan dan untuk semangat yang selalu ada.
10. Kepada NCT, EXO, BTS, BLACKPINK, SVT, RED VELVET, TWS, BND, DAY6, XDINARYHEROES, CORTIS, STRAY KIDS, TWICE, H2H yang melalui karya-karya telah menjadi teman setia di setiap malam panjang pengerjaan skripsi ini. Musik dan lirik-lirik tidak hanya menjadi penghibur, tetapi juga penyemangat untuk penulis. Dan terkhusus untuk NA JAEMIN yang menjadi penyemangat, mood booster, dan segala kata-kata penyemangatnya ”jangan

penuh menyerah pada impianmu. Kerja keras dan kesabaran akan membawamu ke sana". Yang membuat penulis semangat untuk menyelesaikan skripsi ini.

11. Kepada banyak pihak yang tak mampu penuis sebutkan satu per satu, namun setiap kebaikan dan doa tulus yang hadir di sepanjang proses ini adalah bagian penting yang tak tergantikan.
12. Dan terakhir penulis ingin mengucapkan kepada seseorang yang selama ini diam-diam berjuang tanpa henti, melawan dirinya yang *introvet*, pemalu, dan selalu *insecure* atau merasa kurang pada dirnya sendiri, seorang perempuan sederhana dengan impian tinggi. Terima kasih kepada diri sendiri, Nursyahrani Sabila Elake. Terima kasih telah bertahan sejauh ini, dan terus berjalan melewati segala tantangan. Terima kasih karena tetap berani menjadi diri sendiri, walaupun sering meragukannya. Terima kasih karena tetap jujur pada rasa takut, namun tidak membiarkan rasa takut itu membatasi langkah, karena keberanian bukanlah ketiadaan rasa takut, melainkan keinginan untuk tetap bergerak meski takut masih melekat erat, dan paling penting terima kasih karena sudah berani memilih, memilih untuk mencoba, memilih untuk belajar, dan memilih untuk menyelesaikan apa yang telah kamu mulai.

Akhirnya penulis mengharap semoga dengan hadirnya skripsi ini dapat memberikan manfaat bagi pengembangan ilmu dalam bidang ilmu hukum umum dan hukum ilmu pidana khusunya.

Wassalamu Alaikum Warahmatullahi Wabarakatuh.

Makassar, 2026



Nursyahrani Sabila Elake

ABSTRAK

Nursyahrani sabila elake. 04020220147: dengan judul **”TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL”.** Dibawah bimbingan **Mulyati Pawennei** selaku Ketua Pembimbing dan **Salle** sebagai Anggota Pembimbing.

Penelitian ini bertujuan untuk mengetahui pengaturan hukum tindak pidana pelanggaran privasi data pribadi dalam era digital, serta mengetahui pertanggungjawaban pidana terhadap pelaku tindak pidana pelanggaran privasi data pribadi.

Penelitian ini menggunakan metode penelitian hukum normatif. Pendekatan penelitian dengan melakukan pendekatan perundang-undangan pendekatan konseptual dan pendekatan kasus. Jenis dan sumber data yang digunakan berupa bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Teknik pengumpulan bahan hukum yaitu Studi kepustakaan. Hasil analisis tersebut akan penulis hubungkan dengan permasalahan dalam penelitian ini untuk menghasilkan suatu penelitian obyektif untuk menjawab permasalahan dalam penelitian.

Hasil penelitian ini menunjukan bahwa: 1. Pengaturan hukum tindak pidana pelanggaran privasi data pribadi dalam era digital di Indonesia diatur melalui peraturan mengenai perlindungan data pribadi dan sistem elektronik, yang menjadi dasar hukum dalam melindungi data pribadi serta menindak penggunaan, akses, dan penyalahgunaan data tanpa izin. 2. Pertanggungjawaban pidana terhadap pelaku pelanggaran privasi data pribadi dikenakan kepada setiap orang yang dengan sengaja dan melawan hukum memperoleh, menggunakan, mengungkapkan, atau memalsukan data pribadi orang lain, yang dapat dijatuhi pidana berupa penjara dan/atau denda sebagai bentuk penegakan hukum dan perlindungan hak privasi.

Penelitian ini merekomendasikan, Pemerintah perlu memperkuat pelaksanaan perlindungan data pribadi melalui penyempurnaan dan perpaduan pengaturan antara Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik agar tidak terjadi tumpang tindih dalam penegakan hukum, memperepat pembentukan lembaga pengawas yang independen, peningkatan kapasitas aparat penegak hukum di bidang keamanan siber, serta peningkatan edukasi kepada masyarakat guna mencegah penyalahgunaan data pribadi di era digital.

Kata Kunci: Tindak Pidana, Pelanggaran, Data Pribadi, Era Digital

DAFTAR ISI

HASIL PENELITIAN ..... **i**

HALAMAN JUDUL ..... **ii**

PERSETUJUAN SKRIPSI ..... **iii**

PERSETUJUAN UJIAN SKRIPSI ..... **iv**

PENGESAHAN SKRIPSI ..... **v**

PERNYATAAN KEASLIAN SKRIPSI ..... **vi**

PENGESAHAN PENGUJI ..... **vii**

KATA PENGANTAR ..... **viii**

ABSTRAK ..... **xi**

DAFTAR ISI ..... **xii**

BAB I PENDAHULUAN **1**

A. Latar Belakang Masalah 1

B. Rumusan Masalah 7

C. Tujuan Penelitian 7

D. Manfaat Penelitian 8

BAB II TINJAUAN PUSTAKA **9**

A. Tinjauan umum Tindak Pidana 9

1. Pengertian tindak pidana 9

2. Unsur-unsur tindak pidana 11

3. Pembagian Tindak Pidana 13

B. Tinjauan Umum Tentang Pelanggaran Privasi 15

1. Pengertian pelanggaran privasi 15

2. Dampak pelanggaran privasi 16

C. Tinjauan Umum Tentang Data Pribadi di Era Digital 18
1. Pengertian data pribadi..... 18
2. Ruang lingkup data pribadi 21
3. Tantangan pengelolaan data pribadi akibat kemajuan teknologi 28
BAB III METODE PENELITIAN..... 36
A. Tipe Penelitian..... 36
B. Pendekatan Metode Penelitian 36
C. Jenis dan Sumber Bahan Hukum..... 37
D. Teknik Pengumpul Bahan Hukum 37
E. Analisis Bahan Hukum 38
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 39
A. Pengaturan Hukum tindak pidana pelanggaran privasi data pribadi dalam era digital..... 39
B. Sanksi hukum terhadap pelaku tindak pidana pelanggaran privasi data pribadi dalam era digital 94
BAB V PENUTUP..... 65
A. Kesimpulan 65
B. Saran..... 66
DAFTAR PUSTAKA 67

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dalam era digital, perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan manusia. Dalam prosesnya, data pribadi menjadi semakin penting dan sensitif karena banyak aktivitas yang dilakukan secara online. Data pribadi mencakup informasi seperti nama, alamat, nomor identitas, informasi finansial, riwayat kesehatan, dan informasi sensitif lainnya yang berkaitan dengan individu.

Di tengah era digital yang pesat, data pribadi individu semakin rentan terhadap potensi penyalahgunaan dan pelanggaran privasi. Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati. Indonesia, sebagai negara berkembang dengan adopsi teknologi yang pesat, memiliki tanggung jawab untuk melindungi data pribadi sebagai hak privasi. Dalam konteks ini, hak privasi menjadi isu yang mendesak untuk diatasi. Hak privasi adalah hak asasi setiap individu untuk menjaga kerahasiaan dan keamanan data pribadi mereka. Dengan meningkatnya kasus pelanggaran privasi dan penyalahgunaan data pribadi, penting bagi setiap negara untuk memiliki peraturan perundang-undangan yang efektif untuk melindungi hak privasi warganya.

Di Indonesia, kesadaran akan perlunya perlindungan data pribadi telah semakin meningkat, terutama seiring dengan pertumbuhan penggunaan internet dan aplikasi berbasis teknologi. Hak membela diri merupakan salah satu hak hukum yang digariskan dalam UUD 1945. Menurut Pasal 28G Ayat (1), warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta miliknya. Namun demikian, dengan kemajuan teknologi informasi dan komunikasi, hak pribadi seharusnya tidak hanya dipahami sebagai hak milik sebagaimana diatur dalam pasal tersebut. Hak privasi harus menjadi salah satu yang mendasar. Karena berurusan dengan informasi pribadi atau identitas seseorang, hak privasi lebih sensitif dan dapat dilihat sebagai hak pribadi.[1]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan hukum yang lebih kuat bagi individu terkait pengumpulan, penggunaan, dan penyebaran data pribadi mereka. Undang-undang ini juga mengatur mekanisme pengawasan dan penegakan hukum melalui pembentukan lembaga pengawas independen. Dalam konteks hukum pidana, undang-undang ini mengatur sanksi terhadap pelanggaran data pribadi, seperti pencurian dan penyalahgunaan data. Perlindungan data pribadi menjadi semakin relevan dengan meningkatnya transaksi *ecommerce* dan perkembangan teknologi informasi. Namun, risiko kebocoran data

[1] Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia." *Jurnal Analisis Hukum* 6.1 (2023): hlm. 133-134.

pribadi juga meningkat, seperti kasus kebocoran data Tokopedia dan Facebook. Oleh karena itu, perlindungan hukum yang efektif dan regulasi yang kuat diperlukan untuk melindungi data pribadi dan hak privasi individu. Undang-Undang Nomor 27 Tahun 2022 menjadi landasan penting untuk mengatur perlindungan data pribadi di Indonesia, memastikan bahwa data pribadi dihormati dan dilindungi sesuai dengan kemajuan teknologi dan kebutuhan masyarakat.[2]

Namun demikian, dengan kemanjuan teknologi informasi dan komunikasi, hak pribadi seharusnya tidak hanya dipahami sebagai hak milik sebagaimana yang diatur dalam pasal tersebut. Hak Privasi 1 harus menjadi salah satu yang mendasar. Karena berurusan dengan informasi pribadi atau identitas seseorang, hak privasi lebih sensitif dan dapat dilihat sebagai hak pribadi. Indonesia mengakui bahwa perlindungan data pribadi sebagai bagian dari privasi adalah hak asasi manusia. Pengakuan ini tercermin dalam konstitusi dan juga beragam peraturan pada tingkat hukum yang sama. Namun, peraturan khusus tentang perlindungan data pribadi pada tingkat hukum belum dimiliki. Untuk mengisi kekosongan hukum, pengaturan rinci mengenai perlindungan data pribadi diakomodasi dalam peraturan pada tingkat menteri dan juga peraturan sektoral teknis. Dengan demikian, dapat disimpulkan bahwa pengaturan perlindungan data pribadi di Indonesia masih bersifat sektoral. Perlu pengaturan perlindungan data pribadi

[2] Mamonto, Dewi Fortuna. "Analisis Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *LEX PRIVATUM* 13.4 (2024). Hlm.1

pada tingkat hukum karena perlindungan data pribadi sebagai bagian dari privasi adalah hak asasi manusia.[3]

Tetapi contoh kebocoran data pribadi baru-baru ini menjadi masalah yang parah. Kebocoran data pribadi adalah masalah yang serius yang dapat menyebabkan kerugian finansial. Pada era sekarang hampir seluruh perangkat terhubung dan memiliki koneksi internet, semuanya dapat dikelola dari mana saja. Teknologi berbasi komputer untuk informasi dan komunikasi berkembang pesat di masa sekarang dalam kehidupan masyarakat. Kemajuan ini sangat membantu masyarakat. Meskipuin tersebar berbagai undang-undang, perlindungan-perlindungan data pribadi di Indonesia. RUU Perlindungan Data Pribadi (RUU PDT) yang dimiliki Indonesia saat ini perlu dikasi regulasinya masih perlu penyempurnaan. Supaya RUU PDT dapat disandingkan dengan undang-undang perlindungan data yang dimiliki oleh negara luar seperti Malaysia, Singapura, dan Korea Selatan. Perlindungan hukum atas data pribadi sudah dijamin oleh undang-undang khusus di beberapa negara tersebut. RUU PDT memiliki tujuan dan manfaat yang penting dalam konteks perlindunga privasi dan penggunaan data pribadi di Indonesia, dan bertujuan menciptakan lingkungan digital yang aman, terpercaya sambil tetap memungkinkan pertumbuhan ekonomi dan inovasi di era digital.

[3] Muhammad Rifqi Adil Nur, Muhammad Fachri Said, Mursyid Mursyid. (2025). Analisis Hukum tentang Tanggung Jawab Pidana Pelaku Pornografi Balas Dendam dalam Perlindungan Data Pribadi Korban. Horizon Public Legal Studies. Vol. 1 No. 2

Indonesia mengalami peningkatan signifikan kasus pelanggaran privasi data pribadi dari 2020 hingga 2025.

1. **2020 (Tokopedia & KPU):** Kebocoran 91 juta data pengguna Tokopedia (Mei 2020) dan 2,3 juta data pemilih Komisi Pemilihan Umum (KPU).
2. **2021 (BPJS Kesehatan):** Dugaan kebocoran 279 juta data penduduk Indonesia, dengan 100.002 data terkonfirmasi bocor dan dijual di forum online.
3. **2022-2023 (Bjorka & Dukcapil):** Serangkaian kebocoran data yang diklaim oleh peretas "Bjorka", termasuk data surat-menyurat negara. Terjadi juga dugaan kebocoran data 34 juta data paspor dan data Dukcapil.
4. **2023 (KPU):** Dugaan kebocoran 204 juta data Daftar Pemilih Tetap (DPT) KPU.
5. **2024 (Pusat Data Nasional/PDN):** Serangan *ransomware* pada PDN Sementara (PDNS 2) di Surabaya pada Juni 2024 yang melumpuhkan 282 layanan publik.
6. **2025 (Nasional & Daerah):** Pada awal 2025, dilaporkan 210 instansi mengalami kebocoran data. Selain itu, terdapat kasus peretasan 4,5 juta data warga Jawa Barat oleh *Digital Ghost*.

Al-Qur’an menjelaskan betapa pentingnya untuk menjaga privasi orang lain, sebagaimana yang telah dijelaskan dalam Surah Surah Al-Hujurat (49:12):

يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجْتَنِبُواْ كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُواْ وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَٱتَّقُواْ ٱللَّهَ ۚ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ ١٢

Terjemahan:

"Hai orang-orang yang beriman, hindarilah sebagian besar prasangka, karena sebagian prasangka itu dosa. Dan janganlah mencari-cari kesalahan orang lain dan janganlah menggunjing satu sama lain."

Ayat ini menekankan larangan untuk menjaga privasi orang lain, seperti tidak mencari-cari kesalahan (tajassus) atau mengganggu urusan pribadi. yang merupakan bentuk pelanggaran privasi. ini bisa dihubungkan dengan pelanggaran privasi data, di mana pencurian atau penyalahgunaan data pribadi mirip dengan bentuk tajassus modern. Prinsip ini mendukung perlindungan hukum pidana sebagai bentuk menjaga keadilan dan hak asasi, sesuai dengan era digital di Indonesia.

Dengan adanya variasi sistem hukum tersebut, maka asas universalitas dapat digunakan, khususnya untuk kepentingan kepentingan global yang didasarkan pada anggapan bahwa setiap bangsa di dunia wajib ikut serta dalam melaksanakan sistem hukum

global tersebut. Berdasarkan Fenomena dan penyalahgunaan data privasi diatas, maka peneliti tertarik untuk mengkaji mengenai Bagaimana Prinsip Hak Privasi Terhadap Data Pribadi dan apakah Tanggung Jawab Indonesia Terhadap Data Pribadi sebagai Hak Privasi Melalui Peraturan Undang-Undangan. [4]

Berdasarkan uraian tersebut, maka penulis tertarik untuk mengangkat judul proposal tentang "**TINJAUAN YURIDIS TINDAK PIDANA PELANGGARAN PRIVASI DATA PRIBADI DALAM ERA DIGITAL"**

B. Rumusan Masalah

Berdasarkan latar belakang di atas dapat dirumuskan masalah sebagai berikut:

1. Bagaimanakah pengaturan hukum tindak pidana pelanggaran privasi data pribadi dalam era digital?
2. Bagaimanakah pertanggungjawaban pidana terhadap pelaku tindak pidana pelanggaran privasi data pribadi?

C. Tujuan Penelitian

1. Untuk mengetahui bagaimana pengaruh hukum tindak pidana pelanggaran privasi data pribadi dalam era digital.
2. Untuk mengetahui bagaimana sanksi hukum terhadap pelaku tindak pidana pelanggaran privasi data pribadi dalam era digital.

[4] Op. Cit., hlm.133-134

D. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat baik secara teoritis maupun praktis:

1. Secara teoritis

   Dengan adanya penelitian ini dapat Memberikan kontribusi terhadap pengembangan ilmu hukum, khususnya dalam bidang hukum pidana dan hukum perlindungan data pribadi di era digital.

2. Secara praktis

   Dengan adanya penelitian ini diharapkan bisa Memberikan informasi dan pemahaman kepada masyarakat umum mengenai pentingnya perlindungan data pribadi dan risiko hukum yang muncul akibat pelanggaran tersebut.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan umum Tindak Pidana

1. Pengertian tindak pidana

Pengertian tindak pidana yang di muat di dalam Kitab Undang-Undang Hukum Pidana (KUHP) oleh pembentuk undang-undang sering disebut dengan *strafbaarfeit* maksud dan tujuan mengenai *strafbaarfeit* tersebut sering dipergunakan oleh pakar hukum pidana dengan istilah tindak pidana, perbuatan pidana, peristiwa pidana, serta delik. Di antara istilah-istilah itu, yang paling tepat dan baik digunakan adalah istilah tindak pidana dengan pertimbangan selain mengandung pengertian yang tepat dan jelas dengan istilah hukum juga sangat praktis untuk diucapkan. Di samping itu di dalam peraturan perundang-undangan Negara Indonesia pada umumnya menggunakan istilah tindak pidana. [5]

Kitab Undang-undang Hukum Pidana (KUHP) menggunakan istilah umum yang dipakai adalah tindak pidana karena bersifat netral, dan pengertian tersebut meliputi perbuatan pasif dan aktif Jadi dapat dikatakan bahwa pengertian tindak pidana mempunyai arti perbuatan melawan hukum atau melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana.

[5] Putri, Rianda Prima. "Pengertian Dan Fungsi Pemahaman Tindak Pidana Dalam Penegakan Hukum Di Indonesia." *Ensiklopedia Social Review* 1.2 (2019). Hlm.131

Berdasarkan pendapat-pendapat di atas jelaslah bahwa dalam perbuatan tindak pidana tersebut didapatkan unsur-unsur adanya suatu kejadian tertentu, serta adanya orang-orang yang berbuat guna menimbulkan suatu akibat karena melanggarperaturan perundang-undangan yang disertai ancaman/sanksi yang berupa pidana tertentu Dengan demikian, dalam perbuatan pidana harus mengandung unsur-unsur penyebab dan orang-orang yang terlibat didalam perbuatan tersebut.

Tindak pidana merupakan perbuatan yang dilakukan oleh seseorang dengan melakukan suatu kejahatan atau pelanggaran pidana yang merugikan kepentingan orang lain atau merugikan kepentingan umum. Beberapa sarjana hukum pidana di Indonesia menggunakan istilah yang berbeda-beda dalam menyebut kata pidana ada beberapa sarjana menyebutkan tindak pidana, perbuatan pidana atau delik. [6]

Hukum pidana didasarkan pada dasar atau aturan yang diadopsi oleh suatu negara. Jadi pada kenyataannya hukum pidana terbagi menjadi dua, yaitu hukum pidana formal dan hukum pidana material. Berbicara tentang hukum material. Hukum pidana yang termasuk dalam hukum material adalah aturan yang berkaitan dengan peristiwa yang dilarang, di mana dalam hal ini keberadaan aturan mengenai penerapan hukum pidana dan

[6] Moeljatno. (1993). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta. Hlm.54-56

prosedur pidana bagi pelaku atau terpidana merupakan ketentuan hukum yang dapat digunakan sebagai acuan untuk proses penegakan hukum. Sementara penegakan hukum dapat disimpulkan sebagai upaya hukum sebagaimana mestinya. Yaitu, dapat memantau suatu peristiwa sehingga tidak terjadi pelanggaran dan jika terjadi pelanggaran, harus segera dipulihkan, itulah yang dapat kita simpulkan dengan proses penegakan hukum.[7]

2. Unsur-unsur tindak pidana

Unsur-unsur tindak pidana menurut RUU KUHP, berikut ini dikutipkan Pasal 12 RUU KUHP 2016 yang terdiri dari 3 (tiga) ayat:

a. Tindak pidana adalah perbuatan melakukan atau tidak melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana.
b. Untuk dapat dipidananya perbuatan yang dilarang dan diancam pidana oleh peraturan perundang-undangan, perbuatan tersebut harus juga bersifat melawan hukum atau bertentangan dengan kesadaran hukum masyarakat.
c. Setiap tindak pidana selalu dipandang bersifat melawan hukum, kecuali ada alasan pembenar.

[7] Andien Mutiara Zahra, Mulyati Pawennai, Muhammad Faisal. (2025) Konsekuensi Hukum bagi Pelaku Kejahatan Penipuan Online di Media Sosial Elektronik. Horizontal Public Lagal Studies Vol. 1 No. 2

Berdasarkan Pasal 12 RUU KUHP, dapat disimpulkan bahwa unsur-unsur tindak pidana meliputi:

1) perbuatan (perbuatan aktif, berupa melakukan sesuatu perbuatan yang dilarang; dan perbuatan pasif, berupa tidak melakukan atau melalaikan suatu perbuatan yang diperintahkan atau diwajibkan);
2) ancaman pidana;
3) sifat melawan hukum (tidak ada alasan pembenar. Unsur pertama tindak pidana berupa perbuatan aktif dan perbuatan pasif, mengisyaratkan adanya dua macam kaidah atau norma hukum pidana, yakni norma larangan dan norma perintah atau kewajiban. Pelanggaran terhadap norma larangan berbentuk dilakukannya perbuatan yang dilarang dan diancam pidana, sedangkan pelanggaran terhadap norma perintah atau kewajiban berbentuk tidak dilakukannya atau diabaikannya perbuatan yang diperintahkan atau diwajibkan. Contoh tindak pidana pelanggaran larangan adalah: pembunuhan, penganiayaan, pencurian, penggelapan, penipuan, perusakan barang, penadahan, dan lain sebagainya. Sementara itu, contoh untuk tindak pidana pelanggaran perintah adalah: tidak hadir di pengadilan memenuhi panggilan sebagai saksi, tidak menolong

orang yang berada dalam keadaan bahaya.[8]

3. Pembagian Tindak Pidana

Perbuatan pidana juga dibedakan atas perbuatan pidana kesengajaan *(delik dolus)* dan kealpaan *(delik culpa). Delik dolus* adalah delik yang memuat unsur kesengajaan. Misalnya perbuatan pidana pembunuhan dalam Pasal 338 KUHP. Sedangkan delik culpa adalah delik-delik yang memuat unsur kealpaan. Misalnya Pasal 359 KUHP tentang kealpaan seseorang yang mengakibatkan matinya seseorang.

KUHP mengadakan pembagian ke dalam (2) jenis tindak pidana yaitu sebagai berikut:

a. Kejahatan *(misdrijven);*

   adalah perbuatan-perbuatan optimum yang dianggap telah mengandung sifat ketidakadilan dan berdasarkan sifat itu supaya perbuatan yang demikian itu sudah patut dilarang dan diancam hukuman. Sungguh pun perbuatan itu belum dilarang dan diancam dengan hukum oleh UU, toh perbuatan itu sudah patut dihukum. Contoh: Pembunuhan, pencurian, penipuan, dll.

b. Pelanggaran *(overtredingen);*

   Pelanggaran *(overtredingen)* adalah perbuatan-perbuatan yang hanya dapat dihukum oleh karena dilarang oleh UU *(die hen strafwaardigheid ontle nen aan de wet).* Contoh: dilarang buang

[8] Sudaryono, Natangsa. "Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP." (2024).hlm.97

sampah sembarangan, dll.

Dalam KUHP kita sebelum tahun 1918 dikenal 3 jenis tindak pidana, yaitu:

1) Kejahatan-kejahatan (misdaden)
2) Perbuatan-perbuatan buruk (wanbedrijven)
3) Pelanggaran-pelanggaran (overtredingen).

Pembagian 3 jenis ini sesuai dengan KUHP di Negeri Belanda yang waktu itu berlaku Code Penal Perancis sebagai negara penjajah yang memberlakukan KUHPnya dengan 3 pembagian yaitu:

1) *Misdaden: crimes*
2) *Wanbedrijven: delits*
3) *Overtredingen: contraventions*

Hal-hal ini menunjukkan bahwa pembagian tindak pidana itu tidak selamanya harus terdiri dari dua jenis saja seperti dalam KUHP kita sekarang. KUHP sendiri tidak merumuskan atau menjelaskan dasar dari pembagian tersebut. Pembagian tersebut hanya didasarkan atas penempatan saja, yaitu: semua perbuatan yang dilarang dan diancam dengan pidana yang ditempatkan dalam Buku kedua merupakan “kejahatan”, sedangkan yang

ditempatkan dalam Buku Ketiga merupakan “pelanggaran”. Hal ini ternyata dari bab-bab dari KUHP itu sendiri.[9]

B. Tinjauan Umum Tentang Pelanggaran Privasi

1. Pengertian pelanggaran privasi

Pelanggaran Privasi merupakan bentuk penyalahgunaan akses data pribadi orang lain yang melawan hukum yang mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seizin yang bersangkutan.

Dalam Hukuman dan Pidana tentang privasi pada Pasal 29: Pelanggaran Hak Privasi yang berbunyi:” barang siapa dengan sengaja dan melawan hukum memanfaatkan Teknologi Informasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seijin yang bersangkutan, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh).

Kasus pelanggaran privasi banyak terjadi di dunia maya maupun di dunia nyata. Salah satu contoh adalah maraknya pelanggaran privasi di dunia maya khususnya pada aplikasi media sosial seperti facebook. Pada media sosial facebook pengguna bebas mengunggah, membagikan dan menyukai ataupun memberikan komentar pada foto maupun video milik orang lain. Dengan adanya facebook seseorang bisa menjalin pertemanan

[9] Tofik, Dr Tofik Yanuar Chandra, and MH SH. "Buku Referensi Hukum Pidana."hlm.47-48

dengan jaringan yang luas. Namun dari jalinan pertemanan tersebut menimbulkan banyak kekhawatiran, seperti situs pertemanan dimanfaatkan sebagai media untuk menebar kebencian, penghinaan, penghasutan, penipuan dan lain-lain.[10]

2. Dampak pelanggaran privasi

Penyalahgunaan pelanggaran privasi dapat berisiko menimbulkan dampak yang sangat merugikan, seperti penipuan, pencurian identitas, dan pelanggaran privasi. Oleh karena itu, dibutuhkan regulasi yang tegas untuk melindungi hak individu atas data pribadi mereka. Untuk menjawab kebutuhan ini, Undang-Undang Perlindungan Data Pribadi (UU PDP) disusun untuk memberikan perlindungan hukum bagi data pribadi masyarakat di era digital. Undang-undang ini mencakup berbagai aturan mengenai pengumpulan, pengelolaan, dan penggunaan data pribadi oleh pihak ketiga, serta menetapkan sanksi yang tegas bagi pihak yang melanggar hak privasi data pribadi konsumen. Semuel Abrijani Pangerapan, Dirjen Aplikasi dan informatika (Aptika), menjelaskan bahwa data pribadi merupakan bagian dari hak asasi manusia danprivasi yang diakui dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia 1948. UU Perlindungan Data Pribadibertujuan untuk mengurangi pelanggaran terhadap privasi

[10] Islamy, Imam Teguh, et al. "Pentingnya memahami penerapan privasi di era teknologi informasi." *Jurnal Teknologi Informasi dan Pendidikan* 11.2 (2018): hlm.24

serta meningkatkan kesadaran masyarakat dalam menjaga keamanan data pribadi mereka.

Data pribadi yang tersimpan dalam sistem elektronik membentuk jejak digital yang sulit dihapus, sehingga penting untuk memberikan perlindungan guna mencegah kebocoran dan penyalahgunaan data tersebut. Meskipun demikian, dalam praktiknya sering kali terjadi kesalahan yang tidak disengaja akibat sistem keamanan yang kurang memadai, sehingga membuka celah bagi pihak yang tidak bertanggung jawab untuk mencuri, memperjual belikan, atau memanfaatkan data pribadi untuk tujuan yang tidak sah. Beberapa insiden kebocoran data yang mencuat di Indonesia selama era digital antara lain kebocoran data Tokopedia pada 2020, kebocoran data Kredit Pluspada 2020, peretasan terhadap situs BPJS Kesehatan pada 2021, kebocoran data kartu SIM prabayar pada 2022, serta kebocoran data nasabah Bank Syariah Indonesia pada 2023.

Pasal 1 ayat (2) Undang-Undang tersebut menyatakan bahwa "Perlindungan data pribadi adalah upaya menyeluruh untuk melindungi data pribadi dalam proses pengolahan data guna menjamin hak konstitusional subjek data pribadi." Hal ini menegaskan bahwa data pribadi dilindungi oleh hukum sebagai bagian dari hak dasar warga negara.BerdasarkanPasal 2 ayat (1), Undang-Undang Perlindungan Data Pribadi berlaku untuk semua

pihak, termasuk individu, badan publik, dan organisasi internasional. Hal ini mencakup pengaturan baik di dalam maupun luar wilayah Indonesia, dengan dampak hukum yang berlaku di Indonesia. Asas ini mencerminkan prinsip extra territorialdalam hukum Indonesia, yang mengatur perlindungan data pribadi di tingkat global. Sejalan dengan itu, Undang-Undang ini mengadopsi prinsip yurisdiksi perlindungan yang mengikat seluruh pihak yang memproses data pribadi,baik di dalam maupun luar negeri, selama memiliki dampak hukum di Indonesia.[11]

C. Tinjauan Umum Tentang Data Pribadi di Era Digital

1. Pengertian data pribadi

Data pribadi adalah data perseorangan yang disimpan, dirawat dan dijaga kebenarannya serta dilindungi kerahasiaannya. Oleh karena itu, petugas penyelenggara dan Insatansi pelaksana pengumpul data pribadi penduduk mempunyai kewajiban untuk menjaga kerahasiaan dan informasi data tersebut, pengaturannya lebih rinci diatur dalam Peraturan Presiden No 67 Tahun 2011 Tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.[12] Pelindung data pribadi ini agar melindungi hak individu pada masyarakat berhubungan dengan proses data pribadi baik yang dilaksanakan secara elektronik dan

[11] Alfitri, N. A., R. Rahmawati, and F. Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." (2022).hlm.97

[12] Nirwana, Muhammad Alfaruq. "Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual." *AL WASATH Jurnal Ilmu Hukum* 3.2 (2022): hlm.97

nonelektronik yang memakai perangkat oleh data. Dalam UU PDP sudah diresmikan dan diundangkan di NRI serta berlangsung mulai sejak tanggal pengundangannya pada tanggal 17 Oktober 2022. Dalam UU ini terdiri oleh 26 bab dan 76 Pasal yang dimana ditetapkan bermacam hal yang berhubungan pada upaya perlindungan data pribadi, yaitu "hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali dan prosesor data pribadi, larangan hingga sanksi yang berbentuk administratif maupun pidana, bagi setiap pihak yang melakukan pelanggaran terhadap upaya perlindungan data pribadi."[13]

Adapun pengaturan mengenai data pribadi yang ada di Indonesia sampai saat ini, menurut Permenkominfo No.20 Tahun 2016 tentang Perlindungan Data Pribadi diberikan pengertian bahwa "data pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya." Sedangkan yang dimaksud dengan "Data Perseorangan Tertentu ialah setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang undangan." Selanjutnya dalam RUU PDP, memberikan gagasan pengertian "data pribadi adalah setiap data tentang seseorang baik

[13] Putri, Ni Made Dwi Gayatri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Preferensi Hukum* 5.2 (2024): hlm. 242

yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik."[14]

Secara spesifik data pribadi dibagi menjadi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keterangan pribadi, dan data lainnya sesuai dengan ketentuan peraturan perundang-undangan." Selain itu data pribadi yang secara publik yakni seperti nama lengkap, jenis kelamin, agama, status perkawinan, dan data pribadi yang digabungkan agar mengidentifikasi seseorang.Pengendali data pribadi dan prosesor, data pribadi merupakan suatu identifikasi terhadap pihak yang terlibat dalam pemrosesan data pribadi. Pengendali data pribadi seperti setiap orang, institusi, dan organisasi yang melakukan pemrosesan data pribadi atas nama pemrosesan data pribadi. Sedangkan pengendali data pribadi seperti setiap orang, badan publik, dan organisasi yang melaksanakan pemrosesan data pribadi yang meliputi pemerolehan dan pengumpulan, penyimpanan, perbaikan dan

[14] Purnama, Thiara Dewi, and Abdurrakhman Alhakim. "Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *Jurnal Komunitas Yustisia* 4.3 (2021): hlm.1061

pembaruan, penyebarluasan, serta penghapusan atau pemusnahan data pribadi.[15]

2. Ruang lingkup data pribadi

Nilai data pribadi sebagai hak pribadi (*Privacy Rights*) terdiri dari sejumlah arti penting yaitu:

a. hak pribadi adalah hak menikmati kehidupan personal dan kebebasan terlepas dari segala distraksi;
b. hak pribadi adalah hak bersosialisasi dengan individu lain tanpa adanya tindakan pengamatan secara diam;
c. hak pribadi adalah hak melakukan pengawasan terhadap akses informasi terkait kehidupan personal dan informasi individu.

Di sisi lain, cakupan hak pribadi juga termuat secara implisit dalam Pasal 29 ayat (1), Pasal 30, Pasal 31, Pasal 32 Undang-Undang HAM. Secara garis besar, keempat pasal ini mengungkapkan bahwa cakupan hak pribadi di Indonesia meliputi keseluruhan informasi personal, keluarga, kehormatan, dan barang pribadi; berbuat ataupun tidak berbuat sesuatu; kediaman pribadi; serta komunikasi pribadi. Selain itu, Pasal 26 ayat (1) UU ITE menyatakanbahwa pemakaian platform digital yang menyangkut data pribadi individu lain harus melalui izin kepada

[15] Putri, Ni Made Dwi Gayatri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Preferensi Hukum* 5.2 (2024): hlm. 242-243

yang bersangkutan dan tidak diperbolehkan untuk bertindak semena-mena atau melawan hukum.

Menjawab keresahan terkait perlindungan data pribadi di tingkat nasional, DPR RI mengesahkan UU PDP di tanggal 20 September 2022. Hal ini dipicu dari kewaspadaan dunia internasional terhadap pengaturan perlindungan data pribadi, sehingga saat ini ada132 negara yang memiliki produk hukum khusus seperti UU PDP. Di tingkat ASEAN, Indonesia menduduki urutan negara ke-5 yang telah mengesahkan hukum perlindungan data pribadi mengikuti Malaysia, Singapura, Filipina, dan Thailand. Apabila ditinjau berdasarkan substansinya, UU PDP mengatur hal-hal krusial seperti kategorisasi data yang tercantum dalam Pasal 4, berbunyi “Data Pribadi terdiri atas:

a. Data Pribadi yang bersifat spesifik; dan
b. Data pribadi yang bersifat umum. Lebih lanjut, hak-hak subjek data juga ditegaskan dalam Pasal 5 hingga Pasal 15. Kumpulan pasal ini membahas apa saja hak orang secara perseorangan yang melekat kepada data pribadi dirinya. Selain daripada hak, ada juga kewajiban pengendali data yang terdiri dari setiap orang, badan publik, dan organisasi internasional yang kemudian bertindak sendiri atau secara bersama mencapai tujuan serta kendali terhadap pemrosesan data pribadi. Segala hal mengenai kewajiban dari

pengendali data dirinci lebih lanjut dalam Pasal 20 hingga Pasal 50. Tidak hanya itu, UU PDP juga menegaskanbahwa pembentukan lembaga perlindungan data pribadi akan bertanggungjawab langsung kepada Presiden. Ketentuan ini termuat dalam Pasal 58 hingga Pasal 60.

Keterkaitan literatur tentang data pribadi sejalan dengan konsepprivasi yang dikembangkan oleh Warren dan Brandheis sebagai pelopor utama dalam sebuah tulisan yang berjudul "*The Right to Privacy*"atau hak untuk tidak diganggu. Lebih lanjut, tulisan ini juga menyatakan bahwa perkembangan teknologi memberikan kesadaran kepada masyarakat bahwa mereka memiliki hak menikmati hidup. Warren dan Brandeis pernah menyatakan, bahwa *"Privacy is the rught to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition".* Secara sederhana, definisi dari kata privasi merujuk kepada the right to be let alone. Selain itu, William L. Prosser (1960) berusaha untuk melanjutkan konsep tersebut dengan penjelasan detail apa saja cakupan ruang lingkup dari privasi, bahwasannya ada 4 jenis gangguan terhadap privasi individu, antara lain:

a. gangguan yang merujuk perbuatan individu yang menyendiri atau mengasingkan diri, serta gangguan terhadap jalinan pribadi;

b. penyebaran fakta memalukan individu ke ranah publik;

c. penempatan informasi yang keliru di hadapan publik;

d. Otorisasi tanpa izin atas persamaan seseorang hanya demi keuntungan dari pihak lain.

Pengertian lain dari privasi juga disampaikan oleh Julie Innes (1992) bahwa ini meliputi bagaimana individu memiliki kontrol terhadap ranah keputusan privatnya, yang terdiri dari akses, informasi, dan tindakan. Hal ini beriringan dengan penjelasan Solovr (2008) bahwa konteks privasi mencakup keluarga, tubuh fisik, jenis kelamin, rumah, serta informasi personal lainnya. Polarisasi tersebut pada intinya menyimpulkan bahwa privasi adalah wujud klaim hak individu untuk membatasi atau self-controlterhadap apa saja informasi pribadi, kerahasiaan identitas, dan pihak lain yang mempunyai akses indrawi yang dapat disampaikan kepada orang lain.

Perlindungan privasi dan data privasi tidak terlepas dari keberadaan hukum sebagai alat untuk melindungi hak konstitusional individu.20Selain itu, ruang lingkup hukum dari perlindungan data pribadi sangat luas mulai dari jenis, prinsip, hak dan kewajiban subjek, kewajiban data control lerdan juga data processor, transmisidata melewati jalurperbatasan negara lain, kedaulatan, data protection officer, data protection authority, serta bagaimana penyelesaian sengketa dan sanksinya bagi

pelanggar hukum. Adapun penjelasan terkait jenis data pribadi diatur dalam GDPR bahwa *"The following personal data is considered 'sensitive' and is subject to specific processing conditions:*

a. *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;*
b. *trade-union membership;*
c. *genetic data, biometric data processed solely to identify a human being;*
d. *health-related data;*
e. *data concerning a person's sex life or sexual orientation".*

Sedangkan, kategori data pribadi terdiri dari data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. "Uraian dari data pribadi yang bersifat umum meliputi:

a. nama lengkap;
b. jenis kelamin;
c. kewarganegaraan;
d. agama;
e. kombinasi data pribadi guna dalam pengindentifikasian individu.

Selain itu, data pribadi yang bersifat spesifik yakni:

a. informasi kesehatan;
b. data biometrik;

c. data genetika;
d. kehidupan/orientasi seksual;
e. pemikiran politik;
f. riwayat kejahatan;
g. data anak;
h. data keuangan;
i. data lain sesuai dengan ketentuan yang ada". Semua ini tertera jelas dalam RUU PDP.

Setiap silkus data pribadi mulai dari pengumpulan hingga aturan pemusnahannya wajib memperhatikan prinsip perlindungan data pribadi yang dianut oleh masing-masing negara. Adapun sebagai gambaran umum, GDPR (2016) menganut tujuh prinsip dalam upaya perlindungan data pribadinya. Pertama, *lawfulness, fairness, and transparency* artinya bahwa pemrosesan data harus dilakukan secara legal, adil, dan transparan dengan persetujuan subjek data. Kedua, *purpose limitation* mengungkapkan bahwa pengolahan data harus sesuai dengan tujuan awal perusahaan. Ketiga, data *minimization* bahwa pemrosesan data harus memadai, relevan, dan terbatas pada tujuannya. Keempat, accuracyartinya dalam pemrosesan data harus dilakukan secara akurat dan diperbarui jika diperlukan. Kelima, *strorage limitation* menegaskan bahwa penyimpanan data harus memiliki jangka waktu retensi.

Keenam,*integrity and confidentiality* adalah prinsip yang menyatakan bahwa perusahaan harus memiliki langkah-langkah untuk memberikan keamanan dalam melindungi data pribadi yang disimpan. Ketujuh, *accountability* merupakan prinsip bahwa perusahan harus bertanggung jawab sehubungan dengan setiap tindakan yang diambil terhadap data pribadi pengguna dan bagaimana perusahaan mematuhi prinsip-prinsip lainnya. Apabila dalam implementasinya mengacu kepada prinsip tersebut, maka pemproseskan data pribadi akan ditindak lanjuti setelah alasan hukumnya terpenenuhi seperti persetujuan dari pemilik data; memastikan keperluan pemrosesan mengenai kontrak yang terjalin dengan pemilik data; kepatuhan hukum terhadap kewajibannya; melindungi kepentingan hakiki dari pemilik data; pelaksanaan tugas demi kepentingan umum yang diberikan kepada pengendali data; atau pelaksanaan tujuan kepentingan sah (*legitimate interest*) oleh pengendali data atau pihak ketiga.

Syarat vital dalam perlindungan data pribadi tidak hanya mengutamakan implementasi prinsip, tetapi juga pemenuhan hak subjek data dan kewajiban pengendali data. Faktanya, seorang pemilik data memiliki hak-hak yang terdiri dari: “hak untuk mendapatkan informasi; hak atas akses; hak untuk menyangkal; hak untuk memperbaiki, memblokir, dan menghapus; hak atas portabilitas data; hak pemrofilan dan pengambilan keputusan

secara otomatis; hak pemulihan yang efektif, serta hak atas kompensasi dan pertanggungjawaban". Sedangkan, kewajiban pengendali data harus memberikan langkah-langkah organisasional dan teknis guna menunjukkan bahwa pengolahan data telah dilakukan sesuai dengan kaidah hukum yang berlaku. Adapun penjelasan secara spesifik kewajibannya meliputi: menyediakan audit data terbaru; ketentuan dan prosedur yang komprehensif 1terkait perlindungan data pribadi; *privasiby design& by default*; Data *Protection Officer;* tata cara yang jelas bagi subjek data; penilaian terhadap dampak perlindungan data (data protection assessment); peningkatan kapasitas SDM; teknis keamanan data yang kuat; prosedur tentang pelanggaran; serta prosedur evaluasi terhadap langkah yang telah dilaksanakan.Dengan demikian, ruang lingkup hukum perlindungan privasi dan data pribadi cukup kompleks dan hukum melindungi kepentingan individu dengan cara mengalokasikan kekuasaannya guna dapat bertindak sebagaimana mestinya, yang mana kekuasaan inilah disebut sebagai hak. [16]

3. Tantangan pengelolaan data pribadi akibat kemajuan teknologi

Perlindungan data pribadi di Indonesia telah menjadi isu

[16] Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia." *Ganesha Law Review* 5.1 (2023): hlm. 46-49

yang semakin penting seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. UndangUndang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) diharapkan dapat memberikan kerangka hukum yang jelas untuk melindungi hak-hak individu terkait data pribadi mereka. Namun, dalam implementasinya, terdapat berbagai tantangan yang harus dihadapi. Dalam bagian ini, akan dibahas secara mendalam tantangan-tantangan tersebut, dilengkapi dengan data dan fakta yang relevan serta pendapat ahli di bidang perlindungan data pribadi.

a. Kurangnya Kesadaran Masyarakat

Salah satu tantangan utama dalam penegakan hukum perlindungan data pribadi adalah kurangnya kesadaran masyarakat mengenai hak-hak mereka. Menurut survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022, sekitar 60% pengguna internet di Indonesia tidak mengetahui hak-hak mereka terkait perlindungan data pribadi. Hal ini menunjukkan adanya kesenjangan informasi yang signifikan antara regulasi yang ada dan pemahaman masyarakat.

Kurangnya kesadaran ini berpotensi mengakibatkan masyarakat tidak melaporkan pelanggaran data yang mereka alami. Sebagai contoh, dalam Pasal 26 UU PDP, diatur mengenai hak subjek data untuk mendapatkan informasi tentang

pengolahan data pribadi mereka. Namun, tanpa pemahaman yang memadai, individu tidak akan menyadari hak ini dan tidak akan mengambil langkah untuk melindungi data pribadi mereka.

Ahli perlindungan data, Dr. Rudi Hartono, menyatakan bahwa "Pendidikan dan sosialisasi mengenai perlindungan data pribadi harus menjadi prioritas. Tanpa pemahaman yang baik, masyarakat tidak akan mampu melindungi diri mereka dari pelanggaran data." Oleh karena itu, upaya untuk meningkatkan kesadaran masyarakat melalui kampanye edukasi dan sosialisasi sangat penting.

b. Keterbatasan Sumber Daya Penegak Hukum

Tantangan lain yang signifikan adalah keterbatasan sumber daya yang dimiliki oleh lembaga penegak hukum. Banyak lembaga yang belum memiliki kapasitas yang memadai untuk menangani kasus-kasus pelanggaran data pribadi secara efektif. Menurut laporan dari Kementerian Komunikasi dan Informatika (Kominfo), pada tahun 2022 terdapat lebih dari 1.000 kasus pelanggaran data yang dilaporkan, namun hanya sebagian kecil yang berhasil ditangani secara tuntas.

Keterbatasan ini mencakup kurangnya jumlah personel yang terlatih dalam bidang perlindungan data pribadi, serta minimnya anggaran yang dialokasikan untuk penegakan hukum. Dalam Pasal 45 UU PDP, diatur mengenai sanksi administratif bagi pelanggar, namun tanpa adanya sumber

daya yang cukup, penegakan sanksi tersebut menjadi sulit dilakukan.

Dr. Siti Nurjanah, seorang pakar hukum siber, menambahkan bahwa "Penegakan hukum yang efektif memerlukan dukungan sumber daya yang memadai, baik dari segi personel maupun anggaran. Tanpa itu, regulasi yang ada hanya akan menjadi teks tanpa makna." Oleh karena itu, penting bagi pemerintah untuk meningkatkan alokasi anggaran dan pelatihan bagi penegak hukum agar dapat menangani kasus pelanggaran data dengan lebih baik.

c. Kompleksitas Regulasi

Kompleksitas regulasi yang ada juga menjadi hambatan dalam penegakan hukum perlindungan data pribadi. Beberapa ketentuan dalam UU PDP masih memerlukan klarifikasi lebih lanjut agar dapat diterapkan secara efektif. Misalnya, dalam Pasal 14 UU PDP, diatur mengenai persetujuan subjek data untuk pengolahan data pribadi. Namun, definisi dan mekanisme persetujuan yang jelas masih perlu diperjelas agar tidak menimbulkan kebingungan di lapangan.

Selain itu, terdapat juga tumpang tindih regulasi antara UU PDP dengan undangundang lain, seperti UU ITE (Informasi dan Transaksi Elektronik) dan UU Perlindungan Konsumen. Hal ini dapat menyebabkan kebingungan dalam penegakan

hukum, di mana pelanggaran data pribadi dapat diinterpretasikan dengan cara yang berbeda oleh berbagai lembaga.

Ahli hukum, Prof. Ahmad Zainuri, berpendapat bahwa "Harmonisasi regulasi sangat penting untuk menciptakan kepastian hukum. Tanpa adanya kejelasan, penegakan hukum akan terhambat dan pelanggaran data pribadi akan terus terjadi." Oleh karena itu, diperlukan upaya untuk menyusun regulasi yang lebih sederhana dan harmonis agar penegakan hukum dapat dilakukan dengan lebih efektif.

d. Tindak Lanjut yang tidak memadai

Tindak lanjut terhadap pelanggaran data pribadi yang dilaporkan juga menjadi masalah yang signifikan. Meskipun UU PDP memberikan kerangka hukum yang jelas, implementasi di lapangan sering kali tidak sejalan dengan harapan. Banyak laporan pelanggaran data yang tidak ditindaklanjuti dengan serius oleh lembaga penegak hukum, yang menyebabkan ketidak puasan di kalangan Masyarakat.

Data dari Kominfo menunjukkan bahwa dari lebih dari 1.000 laporan pelanggaran data, hanya sekitar 20% yang mendapatkan tindak lanjut yang memadai. Hal ini menunjukkan adanya kesenjangan antara harapan masyarakat dan realitas penegakan hukum. Dalam Pasal 46

UU PDP, diatur mengenai kewajiban lembaga untuk melakukan investigasi terhadap laporan pelanggaran, namun tanpa adanya mekanisme yang jelas dan dukungan sumber daya, banyak laporan yang terabaikan.

Dr. Budi Santoso, seorang praktisi hukum, menekankan bahwa "Tindak lanjut yang tidak memadai terhadap pelanggaran data akan menciptakan rasa ketidakadilan di masyarakat. Jika masyarakat merasa bahwa laporan mereka tidak ditanggapi, maka kepercayaan terhadap sistem hukum akan menurun." Oleh karena itu, penting bagi lembaga penegak hukum untuk meningkatkan responsivitas dan transparansi dalam menangani laporan pelanggaran data.

e. Peran Sektor Swasta

Sektor swasta juga memiliki peran penting dalam penegakan hukum perlindungan data pribadi. Banyak perusahaan yang mengumpulkan dan mengolah data pribadi, namun tidak semua dari mereka mematuhi ketentuan yang ada dalam UU PDP. Dalam Pasal 15 UU PDP, diatur mengenai kewajiban pengendali data untuk melindungi data pribadi yang mereka olah. Namun, masih banyak perusahaan yang belum menerapkan praktik terbaik dalam perlindungan data.

Menurut survei yang dilakukan oleh lembaga riset, sekitar 40% perusahaan di Indonesia belum memiliki kebijakan perlindungan data yang jelas. Hal ini menunjukkan bahwa kesadaran perusahaan terhadap pentingnya perlindungan data pribadi masih rendah. Dr. Rina Wulandari, seorang ahli manajemen risiko, menyatakan bahwa "Perusahaan harus menyadari bahwa perlindungan data bukan hanya kewajiban hukum, tetapi juga merupakan bagian dari tanggung jawab sosial mereka." Oleh karena itu, diperlukan upaya untuk mendorong perusahaan agar lebih proaktif dalam menerapkan kebijakan perlindungan data yang sesuai dengan UU PDP.

f. Ketidakpastian Hukum

Ketidakpastian hukum juga menjadi tantangan dalam penegakan hukum perlindungan data pribadi. Banyak pihak yang merasa bingung mengenai batasan dan konsekuensi dari pelanggaran data pribadi. Hal ini diperparah dengan kurangnya preseden hukum yang jelas terkait pelanggaran data pribadi di Indonesia. Dalam Pasal 47 UU PDP, diatur mengenai pidana bagi pelanggar, namun implementasi sanksi tersebut masih belum konsisten.

Ahli hukum, Dr. Andi Prasetyo, berpendapat bahwa "Ketidakpastian hukum dapat menghambat penegakan hukum. Jika pelanggar tidak merasa ada konsekuensi yang jelas,

mereka akan cenderung mengabaikan regulasi yang ada." Oleh karena itu, penting untuk menciptakan preseden hukum yang jelas dan konsisten agar dapat memberikan efek jera bagi pelanggar.

g. Perkembangan Teknologi yang Cepat

Perkembangan teknologi yang sangat cepat juga menjadi tantangan dalam penegakan hukum perlindungan data pribadi. Dengan munculnya teknologi baru seperti *blockchain, big data, dan internet of things*, cara pengolahan dan penyimpanan data pribadi semakin kompleks. Hal ini membuat regulasi yang ada menjadi sulit untuk diadaptasi dengan cepat.

Dalam Pasal 5 UU PDP, diatur mengenai prinsip-prinsip pengolahan data pribadi, namun prinsip-prinsip tersebut perlu diperbarui agar sesuai dengan perkembangan teknologi terkini. Dr. Siti Aisyah, seorang pakar teknologi informasi, menyatakan bahwa "Regulasi harus mampu mengikuti perkembangan teknologi agar dapat memberikan perlindungan yang efektif bagi data pribadi." Oleh karena itu, diperlukan upaya untuk melakukan revisi regulasi secara berkala agar tetap relevan dengan perkembangan teknologi.[17]

[17] Randy Artawijaya, Sidi Ahyar Wiraguna, "Tantangan Penegak Hukum Dalam Pelindungan Data Pribadi Perspektif Undang-Undang No. 27 Tahun 2022", Jurnal Ilmiah Kajian Multidisipliner (2025): hlm. 233-236

BAB III

METODE PENELITIAN

A. Tipe Penelitian

Penelitian ini merupakan penelitian hukum normatif. Penelitian hukum normatif adalah penelitian yang berfokus pada kajian terhadap norma-norma hukum positif, baik yang tertulis dalam peraturan perundang-undangan maupun yang terdapat dalam putusan pengadilan, doktrin, dan asas-asas hukum.

Dalam konteks penelitian ini, pendekatan normatif digunakan untuk menganalisis pengaturan hukum pidana yang berkaitan dengan perlindungan terhadap pelanggaran privasi data pribadi di Indonesia, khususnya dalam menghadapi perkembangan era digital yang menimbulkan berbagai bentuk kejahatan siber (cybercrime).

B. Pendekatan Metode Penelitian

Dalam penelitian ini, penulis akan menggunakan pendekatan perundang-undangan pendekatan konseptual dan pendekatan kasus. Pendekatan perundang-undangan dilakukan dengan menelaah semua peraturan perundang-undangan yang berkaitan dengan isu hukum yang sedang ditangani. Pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum dari para ahli hukum atau teori-teori hukum yang berkembang maupun asas hukum yang relevan dengan

permasalahan. Pendekatan kasus dilakukan dengan menelaah kasus-kasus yang berkaitan dengan isu hukum yang sedang ditangani.

C. Jenis dan Sumber Bahan Hukum

Penelitian ini menggunakan jenis data sekunder. Sumber data yang diperoleh berupa bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Adapun penjelasan dari ketiga bahan hukum tersebut adalah sebagai berikut :

1. Bahan hukum primer yaitu bahan-bahan hukum yang mengikat mulai dari Undang-Undang Dasar dan peraturan terkait lainnya.
2. Bahan hukum sekunder yaitu bahan-bahan hukum yang memberikan penjelasan atas bahan hukum primer.
3. Bahan hukum tersier yaitu bahan-bahan hukum yang memberikan petunjuk atas bahan hukum primer dan sekunder antara lain Kamus Besar Bahasa Indonesia, Kamus Hukum, dan Laporan dari media massa (Jurnal Hukum, Artikel Hukum dan sebagainya).

D. Teknik Pengumpul Bahan Hukum

Pengumpulan bahan hukum dilakukan dengan kegiatan menghimpun bahan hukum primer dan sekunder secara sistematis sesuai permasalahan penelitian. Oleh karena itu, Teknik pengumpulan bahan hukum yang digunakan adalah dengan studi kepustakaan. Studi kepustakaan dilakukan dengan cara membaca, menelaah, mencatat, membuat ulasan bahan-bahan Pustaka (buku, jurnal, tulisan para ahli,

dan peraturan perundang-undangan) dan membuat ulasan dari internet.

E. Analisis Bahan Hukum

Seluruh bahan hukum yang diperoleh, baik bahan hukum primer maupun bahan hukum sekunder dianalisis dengan metode penalaran hukum, argumentum hukum, serta interpretasi hukum sebagaimana lazimnya penelitian hukum normatif. Hasil analisis tersebut akan penulis hubungkan dengan permasalahan dalam penelitian ini untuk menghasilkan suatu penelitian obyektif untuk menjawab permasalahan dalam penelitian.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Hukum tindak pidana pelanggaran privasi data pribadi dalam era digital

Di Indonesia saat ini telah disahkan peraturan yang mengatur tentang perlindungan data pribadi warga negara Indonesia yang tertuang dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dimana tercantum: Pasal 1 ayat (1) Data Pribadi, didefinisikan sebagai “Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik” sedangkan pada Pasal 2 menjelaskan bahwa “Perlindungan Data Pribadi adalah keseluruhan Upaya untuk melindungi data pibadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi”. Di dalam kedua pasal tersebut telah menegaskan bahwa data pribadi dilindungi oleh hukum sebagai jaminan hak dasar warga negara.[18]

Selama bertahun-tahun, perlindungan data pribadi di Indonesia tidak memiliki landasan hukum yang kuat dan khusus. Sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang

[18] Dade, L. L., Waha, C. J., & Nachrawy, N. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. *Lex Privatum*, *13*(3).

Perlindungan Data Pribadi (UU PDP), berbagai ketentuan mengenai perlindungan data terfragmentasi dalam sejumlah peraturan. Beberapa di antaranya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta peraturan sektoral lainnya. Kondisi fragmentasi regulasi ini berujung pada inkonsistensi dalam penerapan hukum, ketidakjelasan mengenai kewenangan, dan lemahnya mekanisme penegakan hukum terhadap pelanggaran data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), muncul sebagai langkah signifikan dalam sistem hukum Indonesia, bertujuan untuk menyediakan kerangka hukum yang lebih menyeluruh dan terpusat dalam mengatur hak-hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi terhadap pelanggaran data pribadi. Undang-undang ini mengadopsi berbagai prinsip dari General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa, termasuk prinsip keabsahan pemrosesan data, hak untuk mengakses dan menghapus data, serta kewajiban untuk melaporkan kebocoran data. Namun, pelaksanaan UU PDP masih dihadapkan pada beberapa tantangan, seperti rendahnya kesadaran masyarakat mengenai hak-hak mereka, kurangnya

kesiapan dari institusi pengendali data, serta keterbatasan infrastruktur dan sumber daya manusia dalam bidang keamanan siber.[19]

Dalam konteks hukum, perlindungan data pribadi mencakup dua aspek penting: perlindungan terhadap privasi sebagai hak asasi manusia dan perlindungan terhadap data yang merupakan aset rentan terhadap penyalahgunaan. Hak atas privasi telah diakui secara konstitusional melalui Pasal 28G ayat (1) UUD 1945, yang menegaskan bahwa setiap individu berhak mendapatkan perlindungan terkait diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada di bawah penguasaan mereka. Oleh karena itu, negara memiliki tanggung jawab untuk memastikan bahwa proses pengumpulan, penyimpanan, pengolahan, dan distribusi data pribadi dilakukan dengan cara yang sah, adil, dan transparan.[20]

Undang-undang Informasi dan Transaksi Elektronik selanjutnya disebut ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Namun secara implisit undang-undang ini memunculkan pemahaman baru mengenai perlindungan terhadap keberadaan suatu data atau informasi elektronik baik yang bersifat umum maupun pribadi. Perlindungan data pribadi dalam sebuah sistem elektronik meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan

[19] Alexander Kennedy.(2024). Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. Hukum Dinamika Ekselensia, 6(2): 82–98

[20] Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2), 145-157.

dari akses dan interfensi illegal.[21] Terkait dengan perlindungan data pribadi dari penggunaan tanpa izin, pasal 26 undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus mendapat persetujuan dari pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan. Bunyi pasal 26 undang-undang ITE sebagai berikut:[22] "Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan" sedangkan pada ayat (2) menjelaskan bahwa: "Setiap orang yang dilanggar haknya sebagaimana dimaksut pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini". Pasal 26 ayat (1) menyatakan kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Ayat (2) kemudian menyatakan setiap orang yang dilanggar haknya sebagaimana dimaksut pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini. Penjelasan pasal 26 ayat (1) menerangkan bahwa

[21] Erlina Maria Christin Sinaga dan Mery Christian Putri, 2020, Formulasi Perlindungan Data Pribadi dalam Revolusi Industri, Jurnal Hukum Media Pembinaan Hukum Nasional, Volume 9 No. 9, agustus 2020, hal. 65
[22] Ibid

dalam pemanfaatan teknologi informasi, perlindungan data pibadi merupakan salah satu bagian dari hak pribadi (*privasi right*). Hak pribadi mengandung pengertian sebagai berikut: [23]

1. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;
2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai;
3. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Penjelasan pasal 26 undang-undang ITE menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang, sedangkan definisi data pribadi dapat dilihat dalam pasal 1 Peraturan Pemerintah tentang Penyelenggaraan Sistem Transaksi Elektronik yaitu data perorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Undang-undang Informasi dan Transaksi Elektronik sebenarnya secara komprehensif telah memuat ketentuan yang mengatur bagaimana perlindungan data diberikan kepada individu, badan hukum, dan pemerintah. Secara tegas undang-undang ITE melarang adanya akses secara melawan hukum kepada data milik orang lain melalui sistem elektronik untuk memperoleh informasi dengan cara menerobos sistem pengaman.

[23] Pelindungan Privacy dan Personal Data, Diakses dari https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20210422 090703-5599.pdf pada 3 Desember 2025

Secara tegas undang-undang ITE menyatakan bahwa penyadapan (*interceptio*n) adalah termasuk perbuatan yang dilarang kecuali dilakukan oleh pihak yang memiliki kewenangan untuk itu dalam rangka upaya hukum. Berdasarkan undang-undang ITE ini juga, setiap orang dilarang dengan cara apapun untuk membuka informasi milik orang lain dengan tujuan apapun bahkan jika data yang sifatnya rahasia sampai dapat terbuka kepada public.[24]

Perlindungan hukum merupakan langkah yang bertujuan untuk menjamin hak-hak subjek hukum melalui penerapan peraturan perundang-undangan yang berlaku, serta disertai dengan sanksi untuk memastikan kepatuhan terhadap ketentuan hukum tersebut. Subjek hukum yang dimaksud mencakup baik individu maupun badan hukum.[25] Dalam praktiknya, perlindungan hukum terbagi menjadi dua bentuk, yaitu preventif dan represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya pelanggaran hukum. Bentuk ini umumnya dilakukan melalui penyusunan regulasi oleh pemerintah yang memberi pedoman dan rambu-rambu dalam menjalankan hak dan kewajiban hukum.

Sementara itu, perlindungan hukum represif diberikan setelah terjadinya pelanggaran atau sengketa, sebagai bentuk penegakan hukum yang dapat berupa pemberian sanksi administratif,

[24] Judhari Sawan, Pengantar Hukum Telekomunikasi, PT. Raja Grafindo Persada, Jakarta, 2009, hal. 13

[25] Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. Journal Social Society, 4(2), 92-111

denda, pidana, atau sanksi tambahan lainnya. Dalam konteks data pribadi, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi hadir sebagai dasar hukum yang memberikan jaminan perlindungan terhadap individu sebagai pemilik data. Undang-undang ini tidak hanya mengatur hak dan kewajiban para pihak dalam pengelolaan data pribadi, tetapi juga menetapkan mekanisme preventif untuk mencegah kebocoran dan penyalahgunaan data, serta menyediakan jalur represif melalui sanksi hukum terhadap pelanggaran yang terjadi.[26]

1. Perlindungan Preventif

   Perlindungan hukum preventif dalam pengelolaan data pribadi mencakup serangkaian tindakan strategis untuk mencegah terjadinya penyalahgunaan data. Salah satu langkah utama yang harus dilakukan oleh pihak pengendali data adalah memperoleh persetujuan yang sah, eksplisit, dan berdasarkan kesadaran dari pemilik data sebelum data pribadi tersebut diproses. Persetujuan ini berfungsi sebagai bentuk perlindungan awal agar data tidak digunakan secara tidak sah atau tanpa sepengetahuan subjek data.[27] Ketentuan ini sejalan dengan prinsip-prinsip fundamental yang tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menekankan pentingnya

[26] Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Lex Renaissance, 7(3), 445-461

[27] Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. Sang Sewagati Journal, 1(2), 66-90

transparansi serta memberikan kendali penuh kepada individu atas data pribadi yang mereka miliki.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan sejumlah hak penting kepada subjek data, termasuk hak untuk mengakses, memperbarui, menghapus, serta menarik persetujuan atas pemrosesan data pribadi mereka. Pemberian hak-hak ini dimaksudkan untuk menjaga privasi individu dan memastikan bahwa data yang dikelola tetap akurat, sesuai kebutuhan, dan tidak berlebihan. Hal ini menunjukkan bahwa adanya hak tersebut memungkinkan setiap individu untuk tetap memiliki kendali atas informasi pribadinya, terutama di tengah perkembangan teknologi digital yang semakin kompleks dan terbuka.[28]

Pemberian edukasi dan penyuluhan kepada masyarakat mengenai pentingnya perlindungan data pribadi serta langkah-langkah untuk menjaga keamanannya merupakan hal yang sangat krusial. Upaya edukatif ini dapat dilakukan melalui berbagai media, seperti media massa, kegiatan seminar, maupun melalui integrasi materi perlindungan data pribadi dalam kurikulum pendidikan di sekolah. Penyuluhan yang terarah dan efektif dapat berperan besar dalam meningkatkan kesadaran publik dan mengurangi potensi penyalahgunaan data. Masyarakat yang memiliki pemahaman yang

[28] Kusuma, S. C. B. (2023). Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

baik cenderung lebih berhati-hati dalam menggunakan layanan digital, memahami potensi risiko, serta mampu menjaga data pribadinya secara lebih aktif dan bertanggung jawab.

2. Perlindungan Represif

Perlindungan hukum secara represif dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mencakup penerapan sanksi administratif, pidana, dan perdata terhadap pihak-pihak yang terbukti melanggar ketentuan dalam undang undang tersebut.[29] Sanksi administratif ditujukan kepada pengendali maupun prosesor data pribadi yang tidak mematuhi aturan, dengan bentuk sanksi yang bervariasi, seperti teguran tertulis, penghentian sementara aktivitas pemrosesan data, kewajiban untuk menghapus atau memusnahkan data pribadi, hingga denda administratif yang nilainya bisa mencapai dua persen dari total pendapatan atau penerimaan tahunan, tergantung pada jenis pelanggaran yang dilakukan.[30]

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga menetapkan ketentuan pidana terhadap perorangan maupun badan hukum yang melakukan pelanggaran

[29] Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 2(2), 145-157

[30] Saddam, M. S. A. S. A. & AliarahmanMoch, A. S. “Perlindungan hukum terhadap pengguna layanan penyelenggara sistem elektronik akibat penyalahgunaan data pribadi (Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta). Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. VERITAS, 10(1), 121-135.

terhadap isi undang-undang tersebut. Jenis pidana yang dapat dikenakan mencakup hukuman penjara, denda, serta pidana tambahan seperti penyitaan keuntungan atau aset yang diperoleh dari tindak pidana, dan kewajiban membayar ganti rugi kepada pihak yang dirugikan.[31] Dalam Pasal 67, dijelaskan bahwa setiap individu yang dengan sengaja mengakses, menyebarluaskan, atau menggunakan data pribadi milik orang lain secara melanggar hukum, dapat dijatuhi hukuman penjara hingga lima tahun atau dikenakan denda maksimal sebesar lima miliar rupiah.[32] Sementara itu, bagi pelaku yang membocorkan data pribadi milik orang lain tanpa hak, ancaman pidana yang dikenakan dapat berupa penjara paling lama empat tahun atau denda hingga empat miliar rupiah. Penerapan pidana secara tegas mampu memberikan efek jera yang signifikan bagi para pelanggar dan berkontribusi dalam memperkuat sistem perlindungan data pribadi di Indonesia.

Terkait penerapan pidana terhadap korporasi, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menetapkan bahwa hukuman yang dikenakan terbatas pada pidana denda.[33] Nilai denda yang dapat dijatuhkan kepada korporasi bisa mencapai hingga sepuluh kali dari batas maksimum

[31] Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. VERITAS, 10(1), 121-135.
[32] Sianturi, C. G. P., Nababan, R., & Siregar, R. J. (2024). Peran Hukum Dalam Melindungi Data Pribadi. Innovative: Journal Of Social Science Research, 4(5), 2607-2624
[33] Satria, M., & Handoyo, S. (2022). Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. Journal de Facto, 8(2), 108-121.

denda yang diatur dalam undang-undang tersebut. Selain pidana denda, korporasi juga dapat dikenakan sanksi tambahan, seperti penyitaan keuntungan atau aset yang diperoleh dari tindak pidana, pembekuan sebagian atau seluruh kegiatan usaha, pelarangan permanen terhadap aktivitas tertentu, penutupan tempat usaha secara sebagian atau menyeluruh, kewajiban untuk memenuhi tanggung jawab yang sebelumnya diabaikan, pembayaran kompensasi kepada pihak yang dirugikan, pencabutan izin operasional, hingga pembubaran perusahaan.[34]

B. Pertanggungjawaban pidana terhadap pelaku tindak pidana pelanggaran privasi data pribadi

Pertanggungjawaban pidana berarti bahwa setiap individu yang melakukan kejahatan atau pelanggaran yang dijelaskan dalam hukum harus menanggung konsekuensi dari tindakan tersebut sesuai dengan kesalahannya. Dengan kata lain. individu yang terlibat dalam kriminalitas harus dihadapkan pada sanksi jika terbukti bersalah. Seseorang dinyatakan bersalah jika saat melakukan tindakan, menurut pandangan masyarakat. mencerminkan pandangan norma tentang kesalahan yang diperbuat oleh individu tersebut. pada Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. setiap individu yang dengan sengaja dan ilegal memperoleh atau

[34] Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2), 172-191.

mengumpulkan data pribadi milik orang lain dapat dikenakan hukuman penjara hingga lima tahun dan/atau denda maksimum sebesar Rp 5 miliar. Sementara itu, individu yang dengan sengaja dan tanpa izin mengungkapkan data pribadi yang bukan miliknya dapat menghadapi hukuman penjara hingga empat tahun dan/atau denda maksimal Rp 4 miliar.

Bagi individu yang dengan sengaja dan melanggar hukum menggunakan data pribadi milik orang lain, hukuman penjara yang diterapkan dapat mencapai lima tahun dan/atau denda maksimum Rp 5 miliar. Selain itu, sanksi juga berlaku bagi mereka yang dengan sengaja memalsukan data pribadi demi keuntungan pribadi atau orang lain yang dapat mendatangkan kerugian bagi pihak lain. Pelanggar yang melakukan tindakan tersebut dapat dipenjara hingga enam tahun dan/atau denda paling tinggi Rp 6 miliar. Selain mendapat pidana ini, pelaku juga mungkin akan dikenakan hukuman tambahan yang berupa pengambilan keuntungan dan/atau aset yang diperoleh dari tindakan ilegal serta pembayaran kompensasi. Apabila tindakan ini dilakukan oleh suatu perusahaan, maka sanksi dapat dikenakan kepada manajer, pemegang kontrol, pihak yang memberi instruksi. pemilik manfaat, dan/atau perusahaan tersebut. Sanksi yang bisa diterima oleh perusahaan hanya berupa denda, yang jumlahnya tidak boleh lebih dari sepuluh kali lipat dari denda maksimum yang terancam.

Ada empat kesalahan yang bisa mendapat pidana menurut

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi:

1. Mengungkapkan informasi pribadi milik orang lain atau doxing. Tindakannya dapat berujung pada hukuman penjara dengan maksimal empat tahun dan denda hingga Rp4 miliar.
2. Mengumpulkan informasi pribadi dengan cara yang tidak sah. Pelanggar dapat dijatuhi hukuman penjara maksimum lima tahun dan denda maksimal Rp5 miliar.
3. Memanfaatkan informasi pribadi orang lain. Salah satu contoh tindakan ini adalah mendaftar kartu SIM dengan menggunakan identitas orang lain. Pelakunya menghadapi ancaman penjara maksimal lima tahun dan denda hingga Rp5 miliar.
4. Membuat informasi pribadi yang tidak valid atau memalsukan data pribadi. Pelakunya akan dihukum penjara dengan maksimal enam tahun dan denda sebesar Rp6 miliar.[35]

Berdasarkan sanksi diatas bisa dilihat contoh kasus Bjorka yang merupakan seorang peretas yang telah menjadi sorotan publik sejak pertengahan 2022, dikenal karena serangkaian aksi peretasan dan kebocoran data pribadi yang melibatkan jutaan warga negara Indonesia, termasuk data dari berbagai instansi pemerintah dan lembaga strategis. Kasus ini tidak hanya menimbulkan keresahan publik yang luar biasa, tetapi juga

[35] Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2), 145-157.

mengekspos kerentanan sistem keamanan siber nasional yang mendesak untuk diperbaiki. Pengenaan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dengan ancaman pidana maksimal 12 tahun penjara dan denda hingga Rp12 miliar menunjukkan keseriusan negara dalam menangani kejahatan siber yang mengancam kedaulatan data dan privasi warga negara.

Tindak pidana pertama yang dilakukan Bjorka adalah akses ilegal ke sistem elektronik, yang merupakan inti dari seluruh rangkaian kejahatannya. Bjorka diduga melakukan penetrasi tidak sah ke berbagai basis data pemerintah dan swasta, termasuk sistem Direktorat Jenderal Imigrasi, Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, dan berbagai instansi lainnya. Modus operandi yang digunakan kemungkinan melibatkan teknik hacking canggih seperti SQL injection, phishing, atau eksploitasi kerentanan keamanan (vulnerability exploitation) pada sistem yang ditargetkan. Tindakan tersebut telah secara tegas ditentukan dalam Pasal 46 ayat (1) UU ITE, yang menyatakan bahwa setiap orang yang dengan sengaja serta tanpa hak atau secara melanggar hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 30 ayat (1) yaitu melakukan akses terhadap komputer dan/atau sistem elektronik milik orang lain

dengan metode apa pun dapat dijatuhi pidana. Kritik yang muncul adalah bahwa meskipun undang-undang ini telah ada, implementasi sistem keamanan siber di Indonesia masih sangat lemah, sehingga memudahkan peretas seperti Bjorka untuk melancarkan aksinya tanpa hambatan berarti selama bertahun-tahun.

Setelah berhasil mengakses sistem elektronik, Bjorka kemudian melakukan pencurian data dalam skala masif yang mencakup informasi pribadi jutaan warga negara Indonesia. Data yang dicuri meliputi Nomor Induk Kependudukan (NIK), informasi paspor, data kesehatan dari BPJS, hingga data registrasi kartu SIM yang sangat sensitif. Perbuatan pencurian data ini dikategorikan sebagai tindak pidana berdasarkan Pasal 32 ayat (1) UU ITE melarang setiap orang untuk dengan sengaja dan tanpa hak atau secara melawan hukum melakukan tindakan apa pun yang berupa mengubah, menambah, mengurangi, mentransmisikan, merusak, menghapus, memindahkan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik pihak lain maupun milik publik. Pencurian data dalam konteks ini bukansekadar perbuatan kriminal biasa, melainkan adalah salah satu bentuk pelanggaran terhadap hak asasi manusia terkait hak atas privasi sebagaimana dijamin dalam UUD 1945 Pasal 28G ayat (1), sehingga dampaknya melampaui kerugian material dan menciptakan ancaman jangka panjang terhadap keamanan personal

korban.

Tindakan Bjorka tidak berhenti pada pencurian data, tetapi berlanjut dengan penyebarluasan data pribadi tersebut melalui berbagai platform internet, termasuk forum-forum dark web dan media sosial. Bjorka secara terbuka membagikan sampel data curian sebagai bentuk "pembuktian" atas keberhasilannya meretas sistem-sistem Indonesia, bahkan menawarkan data tersebut untuk dijual kepada pihak-pihak yang berkepentingan. Perbuatan ini secara eksplisit melanggar Pasal 26 UU ITE tentang perlindungan data pribadi, yang kemudian diperkuat dengan ketentuan dalam UU PDP. Penyebarluasan data ini menimbulkan efek domino yang sangat berbahaya: korban menjadi rentan terhadap berbagai bentuk kejahatan lanjutan seperti pencurian identitas (identity theft), penipuan (fraud), pemerasan, hingga ancaman keamanan fisik. Dari perspektif kritis, kasus ini mengungkapkan kegagalan sistemik dalam penegakan hukum perlindungan data di Indonesia, di mana sanksi yang ada belum memberikan efek jera yang memadai, dan mekanisme perlindungan preventif masih sangat terbatas.

Dimensi lain dari kejahatan Bjorka adalah upaya pemerasan dan intimidasi yang dilakukannya terhadap pemerintah Indonesia. Bjorka tidak hanya membocorkan data, tetapi juga melakukan tindakan yang dapat dikategorikan sebagai cyber extortion dengan mengancam akan terus membocorkan data lebih banyak

jika tuntutannya tidak dipenuhi, serta melontarkan berbagai pernyataan provokatif yang merendahkan kapabilitas keamanan siber Indonesia. Tindakan ini dapat dijerat dengan Pasal 29 UU ITE mengatur mengenai ancaman kekerasan atau tindakan menakut-nakuti yang ditujukan kepada seseorang, meskipun dalam kasus ini sasaran utamanya adalah lembaga negara. Lebih jauh lagi, perbuatan Bjorka juga mengandung unsur cyber terrorism karena menimbulkan rasa takut massal dan mengancam stabilitas keamanan nasional. Argumentasi yang perlu dikemukakan adalah bahwa kejahatan siber seperti ini tidak dapat lagi dipandang sebagai kejahatan individu biasa, melainkan sebagai ancaman keamanan nasional yang memerlukan respons terintegrasi dari berbagai lembaga negara, termasuk penguatan kapasitas cyber defense dan intelligence Indonesia.

Aksi Bjorka juga menimbulkan gangguan signifikan terhadap operasional sistem elektronik berbagai instansi yang diretas, meskipun tidak ada laporan tentang kerusakan permanen pada sistem tersebut. Gangguan ini mencakup keharusan melakukan investigasi forensik digital, pemulihan sistem, peningkatan protokol keamanan darurat, dan upaya mitigasi dampak kebocoran data yang memerlukan sumber daya besar dan mengganggu pelayanan publik. Tindakan tersebut dapat digolongkan sebagai bentuk pelanggaran terhadap Pasal 33 UU ITE mengatur mengenai

perbuatan yang dilakukan dengan sengaja dan tanpa hak atau secara melawan hukum yang menyebabkan terganggunya sistem elektronik dan/atau membuat sistem tersebut tidak berfungsi sebagaimana mestinya. Kritik yang perlu diajukan adalah bahwa pemerintah dan lembaga-lembaga yang menjadi korban seharusnya juga memikul tanggung jawab atas kelalaian dalam mengamankan data publik yang dipercayakan kepada mereka, sehingga penanganan kasus ini tidak boleh hanya fokus pada penghukuman pelaku tetapi juga pada reformasi tata kelola keamanan siber nasional.

Kasus Bjorka merepresentasikan kompleksitas kejahatan siber modern yang melibatkan multiple layers of criminality, mulai dari akses ilegal, pencurian data, penyebarluasan informasi pribadi, pemerasan, hingga gangguan terhadap kepentingan umum. Pengenaan UU ITE dengan ancaman pidana maksimal 12 tahun penjara dan denda Rp12 miliar menunjukkan bahwa hukum Indonesia telah mengantisipasi keseriusan kejahatan siber, namun efektivitas penegakan hukum ini sangat bergantung pada kemampuan aparat dalam melakukan investigasi digitaldan menghadirkan bukti-bukti forensik yang kuat di pengadilan. Secara kritis, kasus ini seharusnya menjadi momentum bagi Indonesia untuk melakukan reformasi menyeluruh dalam sistem keamanan siber nasional, termasuk peningkatan investasi pada infrastruktur keamanan, capacity building

bagi aparat penegak hukum, harmonisasi regulasi perlindungan data, dan pembangunan kesadaran literasi digital masyarakat. Tanpa langkah-langkah komprehensif tersebut, penangkapan Bjorka hanya akan menjadi kemenangan simbolis tanpa dampak preventif terhadap ancaman kejahatan siber di masa depan.

Penanganan kasus Bjorka menghadirkan kompleksitas yuridis yang unik karena melibatkan penerapan dua instrumen hukum utama secara bersamaan, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE lebih menekankan pada aspek teknis kejahatan siber seperti akses ilegal, interferensi sistem, dan penyalahgunaan teknologi informasi, sementara UU PDP secara spesifik mengatur tentang perlindungan hak privasi individu atas data pribadinya. Dalam konteks kasus Bjorka, penerapan kedua undang-undang ini secara kumulatif memberikan landasan hukum yang komprehensif untuk menjerat pelaku dengan berbagai pasal yang relevan, mulai dari tindakan peretasan sistem hingga pencurian dan penyebarluasan data pribadi jutaan warga negara. Namun, penerapan kerangka hukum ganda ini juga menimbulkan pertanyaan kritis mengenai potensi tumpang tindih pengaturan dan bagaimana aparat penegak hukum harus mengonstruksi dakwaan

yang tepat untuk menghindari gugurnya dakwaan karena obscuur libel atau dakwaan yang tidak jelas.

Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan terbaru dari UU ITE memberikan instrumen hukum yang kuat untuk menjerat Bjorka atas tindakan peretasan dan akses ilegal yang dilakukannya. Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE secara tegas melarang akses ke komputer dan/atau sistem elektronik milik orang lain tanpa hak, dengan ancaman pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp600 juta. Dalam kasus Bjorka yang melibatkan penetrasi ke multiple systems seperti basis data Direktorat Jenderal Imigrasi, BPJS Kesehatan, dan sistem registrasi SIM, penerapan pasal ini dapat dilakukan secara berlapis karena setiap akses ilegal ke sistem yang berbeda merupakan tindak pidana tersendiri. Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE yang mengatur tentang pemindahan atau pentransferan informasi elektronik dengan ancaman pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar, juga sangat relevan mengingat Bjorka tidak hanya mengakses tetapi juga mengekstraksi data dalam jumlah masif. Kritik yang perlu dikedepankan adalah ancaman pidana yang ada masih belumsebanding dengan dampak masif yang ditimbulkan, sehingga perlu ada diskursus mengenai pemberatan hukuman khususnya untuk kejahatan siber yang

berdampak pada keamanan nasional.

UU PDP memberikan dimensi jaminan hukum yang lebih spesifik terhadap aspek pencurian dan penyalahgunaan data pribadi yang menjadi inti pelanggaran dalam kasus Bjorka. Pasal 65 ayat (1) UU PDP menegaskan bahwa setiap orang yang dengan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri, dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp5 miliar. Pasal 67 ayat (1) UU PDP mengatur tentang tindak pidana pengungkapan data pribadi secara melawan hukum, dengan ancaman pidana penjara paling lama 4 tahun dan/atau pidana denda paling banyak Rp4 miliar, yang sangat relevan dengan perbuatan Bjorka yang menyebarluaskan data curian melalui dark web dan media sosial. Tetapi, penerapan UU PDP undang-undang ini baru disahkan pada tahun 2022 dan banyak ketentuan pelaksanaannya belum terbentuk, termasuk belum terbentuknya Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas, sehingga efektivitas penerapan UU PDP masih menghadapi berbagai hambatan implementatifmeskipun secara substansi memberikan perlindungan yang sangat dibutuhkan.

Penerapan UU ITE dan UU PDP dalam kasus Sanksi terhadap Bjorka tidak hanya mencakup hukuman pokok berupa

pidana penjara dan denda, tetapi juga membuka peluang penjatuhan pidana tambahan yang memberikan efek jera lebih besar dan keadilan restoratif bagi korban. Pasal 69 Undang-Undang Perlindungan Data Pribadi menetapkan adanya pidana tambahan berupa: penyitaan keuntungan dan/atau kekayaan yang diperoleh dari tindak pidana; penyitaan aset yang digunakan untuk melakukan tindak pidana; serta kewajiban membayar ganti rugi kepada korban. UU ITE juga memuat ketentuan mengenai pidana tambahan berupa pengumuman putusan pengadilan sebagaimana tercantum dalam Pasal 52, yang bertujuan memberikan efek pencegahan umum (general deterrence). Hakim juga dapat memerintahkan pemusnahan data curian yang masih dikuasai terpidana atau pihak ketiga, serta pemblokiran akses terhadap konten atau platform yang digunakan untuk menyebarkan data curian. Kritik yang muncul adalah implementasi pidana tambahan di lapangan masih menghadapi kendala, terutama mekanisme eksekusi ganti kerugian kepada korban yang jumlahnya masif dan tersebar, serta kompleksitas melacak dan merampas aset hasil kejahatan yang telah dikonversi ke berbagai bentuk termasuk cryptocurrency.[36]

Menurut penulis, Masih terdapat berbagai kelemahan mendasar dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi

[36] Inggria, D., Bella, W. G. O., & Hosnah, A. U. (2025). Penegakan hukum terhadap tindak pidana cybercrime dalam kasus peretasan dan pelanggaran data pribadi oleh hacker Bjorka. *Jurnal Review Pendidikan dan Pengajaran*, 8(4), 8284–8292.

Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024, sehingga penegakan hukum terhadap pelanggaran privasi data pribadi di era digital belum berjalan secara efektif. Permasalahan tersebut tidak hanya disebabkan oleh ketidaksesuaian antar ketentuan, norma hukum yang belum dirumuskan secara jelas, serta lambatnya pembentukan lembaga pendukung, tetapi juga karena kedua undang-undang tersebut belum sepenuhnya mampu menghadapi kejahatan siber lintas negara, sebagaimana terlihat dalam kasus kebocoran data yang dikenal sebagai kasus Bjorka.

Sebagai contoh, Sebagai ilustrasi, Pasal 67 UU PDP mengatur ancaman pidana penjara paling lama lima tahun atau denda paling banyak Rp5 miliar bagi setiap orang yang mengakses data pribadi secara tidak sah. Meskipun ketentuan ini tampak tegas, penggunaan frasa “melawan hukum” masih membuka peluang arti yang berbeda-beda. Selain itu, ketentuan tersebut belum mengatur perbedaan sanksi berdasarkan tingkat kerugian yang ditimbulkan. Dalam kasus kebocoran data dalam skala besar, seperti kebocoran jutaan Nomor Induk Kependudukan dan data peserta BPJS, ancaman pidana yang diterapkan sama dengan pelanggaran yang berdampak kecil. Akibatnya, sanksi yang dijatuhkan sering kali tidak sebanding dengan kerugian yang dialami korban, yang jumlahnya banyak dan sulit memperoleh ganti kerugian. Oleh karena itu, diperlukan perbaikan

pengaturan pidana yang lebih berorientasi pada kepentingan korban, antara lain melalui pengaturan yang lebih tegas mengenai gugatan kelompok serta penguatan sanksi tambahan berupa kewajiban pembayaran ganti rugi secara bersama-sama.

Selain itu, terdapat tumpang tindih pengaturan antara UU PDP dan UU ITE. Misalnya, Pasal 30 jo. Pasal 46 UU ITE mengatur tindak pidana akses ilegal terhadap sistem elektronik dengan ancaman pidana penjara antara enam hingga dua belas tahun, sedangkan Pasal 65 UU PDP mengatur pengumpulan data pribadi secara ilegal. Tumpang tindih ini berpotensi menimbulkan dakwaan ganda atau dakwaan yang tidak jelas, sehingga berisiko melanggar asas *ne bis in idem* (larangan menghukum seseorang dua kali atas perbuatan yang sama). Kondisi tersebut terlihat dalam kasus Bjorka, di mana aparat penegak hukum mengalami kesulitan menentukan undang-undang yang paling tepat untuk diterapkan. Oleh sebab itu, diperlukan penyesuaian pengaturan melalui ketentuan penghubung yang menegaskan bahwa UU PDP digunakan sebagai dasar utama untuk pelanggaran yang secara langsung menyangkut data pribadi, sedangkan UU ITE diterapkan untuk perbuatan yang berkaitan dengan gangguan teknis terhadap sistem elektronik. Selain itu, perlu dipertimbangkan pengaturan mengenai kejahatan siber gabungan dengan ancaman pidana yang lebih berat untuk kasus pelanggaran yang bersifat kompleks dan berlapis.

Permasalahan paling serius terletak pada keterlambatan pembentukan Dewan Perlindungan Data Pribadi (DPDP) sebagaimana diatur dalam pasal 49 UU PDP Hingga awal tahun 2026, lembaga ini belum terbentuk secara efektif akibat kendala politik dan anggaran. Akibatnya, tidak terdapat lembaga independen yang berwenang melakukan pengawasan preventif, seperti pemeriksaan kepatuhan Penyelenggara Sistem Elektronik serta penjatuhan sanksi administratif. Tanpa kehadiran DPDP, fungsi pengawasan masih dibebankan kepada kementerian atau aparat penegak hukum yang tidak memiliki spesialisasi di bidang perlindungan data pribadi. Oleh karena itu, diperlukan percepatan pembentukan peraturan pelaksana yang memperkuat kedudukan DPDP sebagai lembaga independen dengan kewenangan penyelidikan dan pendanaan yang memadai.

UU PDP dan UU ITE juga dinilai belum mampu mengikuti perkembangan teknologi terbaru, seperti penggunaan kecerdasan buatan dalam peretasan, penyalahgunaan data melalui teknologi deepfake, serta pemanfaatan blockchain untuk menyamarkan identitas pelaku. Definisi data pribadi dalam Pasal 1 UU PDP masih bersifat umum dan belum membedakan antara data pribadi biasa dan data pribadi sensitif, seperti data biometrik dan pola perilaku digital, yang seharusnya mendapatkan perlindungan lebih ketat. Sementara itu, Pasal 32 UU ITE masih terbatas pada pengaturan pemindahan atau perubahan data, tanpa menyesuaikan bentuk serangan siber modern

seperti eksploitasi celah keamanan dan serangan ransomware. Oleh karena itu, diperlukan perubahan untuk memperluas definisi data pribadi, mewajibkan standar keamanan sistem yang lebih ketat, serta mewajibkan pelaporan kebocoran data dalam jangka waktu tertentu. Selain itu, kerja sama internasional perlu diperkuat melalui partisipasi aktif dalam konvensi internasional tentang kejahatan siber.

pengaturan sanksi terhadap korporasi dalam Pasal 68 UU PDP masih belum sebanding dengan potensi kerugian negara dan masyarakat akibat kebocoran data berskala besar. Denda maksimal yang diatur belum memberikan efek jera yang memadai, terutama bagi korporasi besar. Selain itu, belum terdapat pengaturan mengenai pertanggungjawaban pidana korporasi dalam kasus pelanggaran data yang menimbulkan dampak serius terhadap keselamatan atau kehidupan manusia. Oleh karena itu, diperlukan revisi regulasi dengan pendekatan berbasis risiko, yang mengatur tingkat sanksi berdasarkan berat ringannya pelanggaran, sekaligus mendorong kepatuhan melalui insentif bagi penyelenggara sistem elektronik yang telah memenuhi standar keamanan tinggi. Dengan demikian, sistem perlindungan data pribadi di Indonesia dapat bertransformasi dari pendekatan yang bersifat reaktif menjadi sistem yang lebih preventif dan adaptif terhadap ancaman kejahatan siber di era digital.

BAB V

PENUTUP

A. Kesimpulan

1. Pengaturan tindak pidana pelanggaran privasi data pribadi di indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU PDP mengatur bentuk pelanggaran serta sanksinya, dan UU ITE mengatur tentang pengamanan data di sistem elektronik, penggunaan tanpa izin, akses tanpa hak, dan penyadapan. Kedua peraturan tersebut menjadi dasar hukum untuk memberikan perlindungan dan penegakan hukum terhadap pelanggaran data pribadi di Indonesia.
2. Pertanggungjawaban pidana atas pelanggaran data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik menegaskan bahwa setiap orang yang secara sengaja dan melawan hukum memperoleh, menggunakan, mengungkapkan, atau memalsukan data pribadi orang lain dapat dikenai pidana berupa penjara dan/atau denda sebagai bentuk penegakan hukum dan perlindungan hak privasi.

B. Saran

1. Saran penulis untuk pemerintah perlu memperkuat pelaksanaa Undang-Undang Perlindungan Data Pribadi melalui penyusunan peraturan pelaksana yang lebih jelas dan komprehensif. Selain itu, diperlukan peningkatan kapasitas aparat penegak hukum dalam bidang keamanan siber serta penguatan pengawasan terhadap pengelolaan data oleh penyelenggara sistem elektronik. Pemerintah juga perlu meningkatkan edukasi dan sosialisasi kepada masyarakat mengenai pentingnya perlindungan data pribadi agar kesadaran dan partisipasi publik dalam menjaga keamanan data dapat meningkat.
2. Saran penulis untuk pemerintah perlu menyempurnakan pengaturan perlindungan data pribadi melalui perpaduan antara Undang-Undang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik agar tidak terjadi tumpang tindih pengaturan dalam penegakan hukum. percepatan pembentukan lembaga pengawas perlindungan data pribadi yang independen, penguatan sanksi terhadap pelanggaran data dalam skala besar, serta peningkatan kapasitas aparat penegak hukum di bidang keamanan siber. Upaya edukasi dan sosialisasi kepada masyarakat mengenai pentingnya perlindungan data pribadi juga perlu terus ditingkatkan agar mencegah terjadinya penyalahgunaan data pribadi di era digital.

DAFTAR PUSTAKA

Al-Qur'an dan terjemahannya.

Literatur

Satjipto Raharjo, (2000), Ilmu Hukum, Bandung: PT. Citra Aditya Bakti.

Phillipus M. Hadjon, (1987), Perlindungan Hukum Bagi Rakyat Indonesia, Surabaya: PT. Bina Ilmu.

Muhammad Rifqi Adil Nur, Muhammad Fachri Said, Mursyid Mursyid. (2025). Analisis Hukum tentang Tanggung Jawab Pidana Pelaku Pornografi Balas Dendam dalam Perlindungan Data Pribadi Korban. Horizon Public Legal Studies. Vol. 1 No. 2.

Kamus Besar Bahasa Indonesia (KBBI), Edisi Kedua, Cet. 1, Jakarta: Balai Pustaka.

Qodariah Barkah, M.H.I, Andriyani, M.Sy, et al. (2024). Perlindungan Hukum. Palembang: CV. Doki Course and Training.

Sudaryono, N. (2024). Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP. Surakarta: Muhammadiyah University Press.

Andien Mutiara Zahra, Mulyati Pawennai, Muhammad Faisal. (2025) Konsekuensi Hukum bagi Pelaku Kejahatan Penipuan Online di Media Sosial Elektronik. Horizontal Public Lagal Studies Vol. 1 No. 2.

Tofik Yanuar Chandra (2022) Hukum Pidana. PT. Sangir Multi Usaha.

John Kenedi (2020). Perlindungan Saksi Dan Korban. Pustaka Pelajar.

C.S.T. Kansil, 1989, Pengantar Ilmu Hukum dan Tata Hukum Indonesia, Balai Pustaka, Jakarta.

Philipus M. Hadjon, (2011), Pengantar Hukum Administrasi Indonesia, Gajah Mada University Press, Yogyakarta.

Lilik Mulyadi. (2018). “Perlindungan Hukum terhadap Korban Tindak Pidana dalam Sistem Peradilan Pidana di Indonesia.” *Jurnal Hukum dan Peradilan*, Vol. 7 No. 3.

Putri, Rianda Prima. "Pengertian Dan Fungsi Pemahaman Tindak Pidana Dalam Penegakan Hukum Di Indonesia." *Ensiklopedia Social Review* 1.2 (2019).

Moeljatno. (1993). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.

Islamy, Imam Teguh, et al. "Pentingnya memahami penerapan privasi di era teknologi informasi." *Jurnal Teknologi Informasi dan Pendidikan* 11.2 (2018).

Alfitri, N. A., R. Rahmawati, and F. Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." (2022).

Nirwana, Muhammad Alfaruq. "Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual." *Al Wasath Jurnal Ilmu Hukum* 3.2 (2022).

Putri, Ni Made Dwi Gayatri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Preferensi Hukum* 5.2 (2024).

Purnama, Thiara Dewi, and Abdurrakhman Alhakim. "Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *Jurnal Komunitas Yustisia* 4.3 (2021).

Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia." *Ganesha Law Review* 5.1 (2023)

Randy Artawijaya, Sidi Ahyar Wiraguna, “Tantangan Penegakan Hukum Dalam Perlindungan Data Pribadi Perspektif Undang-Undang

No. 27 Tahun 2022", Jurnal Ilmiah Kajian Multidisipliner (2025).

Bawole, B. Y. (2021). Perlindungan Hukum Bagi Korban Dalam Sistem Peradilan Pidana. *Lex Et Societatis*, *9*(3).

Dade, L. L., Waha, C. J., & Nachrawy, N. (2024). Kajian yuridis tentang tindak pidana penyebaran data pribadi melalui internet (doxing) di Indonesia. *Lex Privatum*, *13*(3).

Pelindungan Privacy dan Personal Data, Diakses dari https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20210422090703-5599.pdf pada 3 Desember 2025.

Alexander Kennedy.(2024). Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. Hukum Dinamika Ekselensia, 6(2)

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2)

Erlina Maria Christin Sinaga dan Mery Christian Putri, 2020, Formulasi Perlindungan Data Pribadi dalam Revolusi Industri, Jurnal Hukum Media Pembinaan Hukum Nasional, Volume 9 No. 9, agustus 2020.

Judhari Sawan, Pengantar Hukum Telekomunikasi, PT. Raja Grafindo Persada, Jakarta, 2009.

Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. Journal Social Society, 4(2)

Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Lex Renaissance, 7(3)

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. Sang Sewagati Journal, 1(2)

Kusuma, S. C. B. (2023). Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 2(2)

Saddam, M. S. A. S. A. & AliarahmanMoch, A. S. “Perlindungan Hukum Terhadap Penguna Layanan Penyelenggaraan Sistem Elektronik Akibat Penyalagunaan Data Pribadi (Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta).

Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. Veritas, 10(1)

Sianturi, C. G. P., Nababan, R., & Siregar, R. J. (2024). Peran Hukum Dalam Melindungi Data Pribadi. Innovative: Journal Of Social Science Research, 4(5)

Satria, M., & Handoyo, S. (2022). Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. Journal de Facto, 8(2)

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2)

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(2)

Inggria, D., Bella, W. G. O., & Hosnah, A. U. (2025). Penegakan hukum terhadap tindak pidana cybercrime dalam kasus peretasan dan pelanggaran data pribadi oleh hacker Bjorka. *Jurnal Review Pendidikan dan Pengajaran*, 8(4)

PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

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