REKONSTRUKSI HUKUM PERLINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK DI ERA DIGITAL UNTUK MEWUJUDKAN KEADILAN BERDASARKAN PANCASILA

Oleh:
Raihan Imam Cahya Akbar
NPM. 2330010012

DISERTASI
Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Doktor Hukum Pada
Program Studi Hukum Program Doktor
Universitas Muhammadiyah Sumatera Utara



PROGRAM STUDI HUKUM PROGRAM DOKTOR
SEKOLAH PASCASARJANA
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026

PENGESAHAN DISERTASI

Nama : Raihan Imam Cahya Akbar

NIM : 2330010012

Program Studi : Hukum Program Doktor

Judul : Rekonstruksi Hukum Perlindungan Data Pribadi yang Bersifat Spesifik Di Era Digital Untuk Mewujudkan Keadilan Berdasarkan Pancasila

Pengesahan Disertasi:

Medan, 21 Juli 2026

Promotor	Ko-Promotor
Assoc. Prof. Dr. Ramlan, S.H., M.Hum., C.CLE.	**Assoc. Prof. Dr. Ida Nadirah, S.H., M.H.**

Diketahui

Direktur	Ketua Program Studi
Prof. Dr. Triono Eddy, S.H., M.Hum.	**Prof. Dr. Muhammad Arifin, S.H., M.Hum.**

PENGESAHAN DISERTASI

REKONSTRUKSI HUKUM PERLINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK DI ERA DIGITAL UNTUK MEWUJUDKAN KEADILAN BERDASARKAN PANCASILA

RAIHAN IMAM CAHYA AKBAR
NPM: 2330010012

Disertasi ini Telah Dipertahankan Dihadapan penguji
pada sidang Ujian Promosi Doktor
Dinyatakan telah memenuhi syarat dan Berhak Menyandang Gelar
Doktor (Dr.) di Bidang Hukum
pada tanggal 21 Juli 2026

1. **Prof. Dr. Akrim, M.Pd.** 1. .....
   Ketua Penguji

2. **Prof. Dr. Tarmizi, S.H., M.Hum.** 2. .....
   Penguji I

3. **Prof. Dr. Ida Hanifah, S.H., M.H.** 3. .....
   Penguji II

4. **Assoc. Prof. Dr. Farid Wajdi, S.H., M.Hum.** 4. .....
   Penguji III

UMSU Unggul | Cerdas | Terpercaya

ABSTRAK

Perkembangan teknologi informasi di era digital telah mengubah cara pengelolaan data pribadi, khususnya data pribadi yang bersifat spesifik. Kemudahan pengumpulan, pengolahan, dan distribusi data memberi manfaat, tetapi juga menimbulkan risiko kebocoran, penyalahgunaan, serta pelanggaran privasi tanpa persetujuan pemilik data. Penelitian ini bertujuan mengkaji urgensi rekonstruksi hukum perlindungan data pribadi spesifik di Indonesia agar lebih adil, responsif, dan selaras dengan nilai keadilan sosial berdasarkan Pancasila. Selain itu, penelitian ini berupaya menawarkan solusi terhadap berbagai tantangan perlindungan data pribadi di era digital, baik dari aspek regulasi, penegakan hukum, maupun pemenuhan hak subjek data secara efektif, transparan, akuntabel, dan berorientasi pada kepentingan masyarakat.

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*), pendekatan perbandingan (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Penelitian ini bersifat eksplanatoris untuk menjelaskan permasalahan hukum yang berkaitan dengan perlindungan data pribadi yang bersifat spesifik serta menganalisis pengaturannya dalam sistem hukum Indonesia. Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan. Seluruh bahan hukum dianalisis secara kualitatif untuk memperoleh pemahaman yang komprehensif mengenai perlindungan data pribadi yang bersifat spesifik serta merumuskan rekonstruksi hukum yang sesuai dengan perkembangan teknologi digital dan nilai-nilai keadilan Pancasila.

Hasil penelitian ini menunjukkan bahwa meskipun Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (*UU PDP*), namun pelaksanaannya masih menemui berbagai kendala. Banyaknya kasus kebocoran data pribadi yang terjadi, serta kelemahan dalam pengawasan dan penegakan hukum, menjadi tantangan utama dalam perlindungan data pribadi yang bersifat spesifik di Indonesia. Selain itu, masih terdapat kesenjangan antara regulasi yang ada dengan nilai-nilai keadilan yang terkandung dalam Pancasila, seperti dalam hal transparansi pengolahan data pribadi dan pemberian hak akses yang setara kepada semua individu. Oleh karena itu, diperlukan rekonstruksi hukum yang tidak hanya memperbaharui regulasi yang ada, tetapi juga mengintegrasikan prinsip-prinsip keadilan sosial yang bersumber dari Pancasila.

Kesimpulan dari penelitian ini adalah bahwa rekonstruksi hukum perlindungan data pribadi yang bersifat spesifikdi Indonesia sangat diperlukan untuk menghadapi tantangan di era digital. Penguatan regulasi, peningkatan kesadaran hukum masyarakat, serta pembentukan lembaga pengawas yang independen menjadi solusi yang diusulkan. Pemerintah juga diharapkan untuk memperbaharui regulasi yang ada agar lebih responsif terhadap perkembangan teknologi dan lebih sesuai dengan nilai-nilai keadilan sosial dalam Pancasila.

Kata Kunci: Perlindungan Data Pribadi, Rekonstruksi Hukum, Pancasila, Keadilan Sosial, Era Digital.

ABSTRACT

The rapid advancement of information technology in the digital era has transformed the management of personal data, particularly specific personal data. While the ease of collecting, processing, and disseminating personal data offers significant benefits, it also creates substantial risks, including data breaches, misuse of personal information, and violations of privacy rights without the consent of the data subject. This research aims to examine the urgency of reconstructing the legal framework governing the protection of specific personal data in Indonesia in order to establish a system that is more equitable, responsive, and aligned with the principles of social justice embodied in Pancasila. Furthermore, this study seeks to propose solutions to the challenges of personal data protection in the digital era from the perspectives of regulatory reform, law enforcement, and the effective, transparent, accountable, and public-oriented fulfillment of data subjects' rights.

This study employs normative legal research utilizing a statute approach, a comparative approach, and a conceptual approach. The research is explanatory in nature, aiming to examine legal issues related to the protection of specific personal data and to analyze their regulation within the Indonesian legal system. The legal materials consist of primary, secondary, and tertiary legal sources obtained through library research. All legal materials were analyzed qualitatively to develop a comprehensive understanding of the protection of specific personal data and to formulate a legal reconstruction that is responsive to technological developments and consistent with the values of justice embodied in Pancasila.

The findings indicate that although Indonesia has enacted Law Number 27 of 2022 on Personal Data Protection, its implementation continues to face significant challenges. The increasing number of personal data breach incidents, coupled with weaknesses in supervision and law enforcement mechanisms, constitutes a major obstacle to the protection of specific personal data in Indonesia. The study also reveals a gap between the existing regulatory framework and the principles of justice embodied in Pancasila, particularly concerning transparency in personal data processing and the equal protection of individuals' rights. Accordingly, legal reconstruction is required not only to improve the existing regulatory framework but also to integrate the principles of social justice derived from Pancasila into the governance of personal data protection.

This study concludes that the reconstruction of the legal framework governing the protection of specific personal data in Indonesia is essential to address the challenges posed by the digital era. Strengthening legal regulations, enhancing public legal awareness, and establishing an independent supervisory authority are among the proposed solutions. The government is also expected to reform existing regulations to ensure greater responsiveness to technological developments and closer alignment with the principles of social justice embodied in Pancasila.

Keywords: Personal Data Protection, Legal Reconstruction, Pancasila, Social Justice, Digital Era.

KATA PENGANTAR



Segala puji dipanjatkan kepada Allah SWT berkat ridho-Nya disertasi dengan judul "Rekonstruksi Hukum Perlindungan Data Pribadi Yang Bersifat Spesifik Di Era Digital Untuk Mewujudkan Keadilan Berdasarkan Pancasila" dapat diselesaikan. Sholawat beriring salam dihaturkan kepada Nabi Besar Muhammad SAW semoga kita mendapat syafa'at Beliau di *Yaumul Mahsyar* nanti, Aamiin.

Terima kasih dan penghormatan setinggi-tingginya kepada yang terhormat dan terpelajar Bapak Assoc. Prof. Dr. Ramlan, S.H., M.Hum., C.CLE. selaku Promotor dan Ibu Assoc. Prof. Dr. Ida Nadirah, S.H., M.H. selaku Ko-Promotor yang dengan penuh kesabaran telah membimbing, mengoreksi, mengkritisi, serta memberikan motivasi dalam proses penyelesaian disertasi ini. Semoga ilmu dan bimbingan yang diberikan menjadi amal jariyah yang terus mengalir.

Ucapan terima kasih dan penghormatan yang setinggi-tingginya juga disampaikan kepada:

1. Prof. Dr. Akrim, M.Pd., selaku Rektor Universitas Muhammadiyah Sumatera Utara (UMSU) yang memimpin dan menyediakan wadah pendidikan Strata-3 Program Studi Hukum Program Doktor UMSU.
2. Prof. Dr. Triono Eddy, S.H., M. Hum., selaku Direktur Sekolah Pascasarjana UMSU yang telah banyak membantu mulai awal proses studi hingga penyelesaian Strata-3 pada Program Studi Hukum Program Doktor UMSU.

3. Prof. Dr. Muhammad Arifin Gultom, S.H., M.Hum., selaku Wakil Rektor I UMSU sekaligus Ketua Program Studi Hukum Program Doktor UMSU dan Prof. Ida Hanifah, S.H., M.H., selaku Sekretaris Program Studi Hukum Program Doktor UMSU yang telah memberikan pelayanan akademik dengan sangat baik dan memuaskan pada saat mengikuti pendidikan Program Studi Hukum Program Doktor UMSU di Kampus UMSU tercinta.
4. Kepada seluruh penguji, Prof. Dr. Tarmizi, S.H., M. Hum., Prof. Ida Hanifah, S.H., M.H., dan Assoc. Prof. Farid Wajdi, S.H., M.Hum., terima kasih telah memberikan catatan, komentar, saran dan penilaian terhadap disertasi ini.
5. Seluruh Staf Pengajar Program Studi Hukum Program Doktor Program Pascasarjana UMSU yang telah mendidik dan memberikan ilmunya selama proses studi, dan seluruh tenaga pendidik pada Biro Tata Usaha Pascasarjana yang senantiasa membantu dalam proses administrasi akademik selama menempuh studi di Program Studi Hukum Program Doktor Program Pascasarjana UMSU.
6. Istri tercinta, Isnaini Fitri, yang bukan hanya menjadi pendamping hidup, tetapi juga sahabat, tempat berbagi keluh kesah, dan sumber kekuatan terbesar. Terima kasih atas cinta, kesabaran, dan pengorbanan selama ini. Setiap kata penyemangat, setiap senyuman, dan setiap dukungan yang diberikan menjadi cahaya yang menerangi jalan ini. Kehadirannya adalah anugerah terindah yang Allah titipkan dalam hidup saya.
7. Ibunda tercinta, Dr. Ir. Eliya Nova Lubis, S.H., M.Kn., M.Si., sosok luar biasa yang dengan penuh kasih sayang telah membimbing, mendidik, dan mendoakan

saya sejak lahir hingga saat ini. Setiap pengorbanan, perjuangan, dan doa yang dipanjatkan tanpa henti telah menjadi cahaya dalam perjalanan hidup saya. Tiada kata yang mampu menggambarkan betapa besar cinta dan hormat saya kepada ibunda. Setiap pencapaian yang saya raih adalah bukti dari keikhlasan dan ketulusan yang beliau curahkan sepanjang hidupnya. Semoga Allah Subhanahu wa Ta'ala senantiasa melimpahkan keberkahan, kesehatan, serta kebahagiaan bagi ibunda, dan menjadikannya penghuni surga yang tertinggi. Aamiin Ya Rabbal 'Alamin.

8. Papa tercinta, dr. Pahala, Sp.P. terima kasih atas kasih sayang, perhatian, pengorbanan, serta dukungan yang telah Papa berikan sepanjang perjalanan hidup saya. Meskipun jalan kehidupan membawa kita melalui berbagai dinamika, kasih seorang ayah tetap menjadi bagian yang tidak pernah hilang dari langkah-langkah saya. Setiap nasihat, perhatian, dan semangat dari Papa telah menjadi kekuatan yang mengiringi saya dalam menghadapi berbagai tantangan hingga mampu menyelesaikan disertasi ini. Pencapaian ini juga merupakan bagian dari buah kasih, didikan, dan dukungan yang Papa berikan. Semoga Papa senantiasa dikaruniai kesehatan yang baik, umur yang panjang, hati yang penuh sukacita, serta kehidupan yang damai dan penuh kebahagiaan. Terima kasih, Papa, untuk semua cinta yang telah Papa berikan. Semoga kasih sayang dan kebanggaan ini akan selalu menjadi ikatan yang abadi di antara kita. Semoga Allah Subhanahu wa Ta'ala membalas segala kebaikan dan ketulusan hati Ayah dengan limpahan rahmat, kesehatan, dan kebahagiaan yang tiada putus. Aamiin Ya Rabbal 'Alamin.

9. Mertua tersayang, Bapak Saufi Abdullah dan Ibunda Mai Salmah, yang telah menerima saya dengan penuh cinta dan kasih sayang, serta tak pernah lelah mendoakan dan mendukung di setiap langkah perjalanan ini. Doa-doa tulus dari beliau berdua adalah energi yang menguatkan. Semoga Allah membalas setiap kebaikan dan memberikan kesehatan serta kebahagiaan yang tiada tara.
10. Putri tersayang, Ziya Faiza Afsheen, bidadari kecil yang selalu menjadi alasan untuk terus berjuang. Senyumnya adalah kebahagiaan, tawanya adalah obat dari segala lelah, dan pelukannya adalah pelipur lara dari setiap perjuangan. Semoga ia tumbuh menjadi anak yang shalihah, penuh kasih sayang, dan selalu dalam lindungan Allah SWT. Saya akan selalu berjuang demi masa depannya.
11. "Jabuhela Family", keluarga besar di lingkungan Fakultas Kedokteran Universitas Prima Indonesia yang berisi adik-adik sejawat sekaligus rekan seperjuangan dalam menempuh pendidikan kedokteran. Terima kasih atas kebersamaan, dukungan, semangat, dan rasa kekeluargaan yang selalu hadir di tengah perjalanan akademik ini. Kehadiran kalian bukan hanya menjadi teman berdiskusi dan berbagi ilmu, tetapi juga menjadi tempat saling menguatkan dalam menghadapi berbagai tantangan selama proses perkuliahan. Semoga tali silaturahmi, kekompakan, dan persaudaraan ini senantiasa terjaga dengan baik.
12. Seluruh rekan-rekan mahasiswa Program Studi Hukum Program Doktor Program Pascasarjana UMSU Angkatan V Tahun 2023, terima kasih atas semangat dan dukungan yang kalian berikan: "menyegerakan yang wajib segera ditunaikan adalah salah satu wujud komitmen kita terhadap kehidupan dan penghidupan".

13. Kepada keluarga besar yang tidak dapat disebutkan semua namanya, terima kasih atas dukungan semangat yang diberikan dalam penuntasan disertasi ini.
14. Sahabat semua yang tidak dapat dituliskan namanya satu/satu, semoga Allah SWT membalas segala budi baik dari semua pihak yang telah membantu proses penyelesaian disertasi ini.

Akhir kata, dengan penuh kesadaran bahwa penulisan disertasi ini masih jauh dari tingkat sempurna. Oleh karenanya, saran dan masukan dalam rangka perbaikan adalah suatu hal yang sangat diharapkan.

Medan, 21 Juli 2026

Penulis,

Raihan Imam Cahya Akbar
NPM. 2330010012

DAFTAR SINGKATAN/AKRONIM

ACCS	: *ASEAN Cybersecurity Cooperation Strategy*
AI	: *Artificial Intelligence* (Kecerdasan Buatan)
APJII	: Asosiasi Penyelenggara Jasa Internet Indonesia
ASEAN	: *Association of Southeast Asian Nations* (Perhimpunan Bangsa-Bangsa Asia Tenggara)
BSSN	: Badan Siber dan Sandi Negara
COPPA	: *Children's Online Privacy Protection Act*
DPIA	: *Data Protection Impact Assessment*
DPMR	: *Development Policy and Management Review*
DPO	: *Data Protection Officer*
EDPB	: *European Data Protection Board*
EU	: *European Union* (Uni Eropa)
FTC	: *Federal Trade Commission*
GINA	: *Genetic Information Nondiscrimination Act*
GPA	: *Global Privacy Assembly*
HAM	: Hak Asasi Manusia
ICO	: *Information Commissioner's Office*
IKD	: Identitas Kependudukan Digital
IOT	: *Internet of Things*
ISMS	: *Information Security Management System*
ITE	: Informasi dan Transaksi Elektronik (dalam s
KPDP	: Komisi Pelindungan Data Pribadi
KUHP	: Kitab Undang-Undang Hukum Pidana
LSM	: Lembaga Swadaya Masyarakat
MAFINDO	: Masyarakat Anti Fitnah Indonesia
MFA	: *Multi-Factor Authentication*
MHI	: Media Hukum Indonesia
NCOLS	: *National Conference on Law Studies*
NDA	: *Non-Disclosure Agreement*
NGO	: *Non-Governmental Organization*
NIK	: Nomor Induk Kependudukan
OECD	: *Organisation for Economic Co-operation and Development*

OJK	: Otoritas Jasa Keuangan
PDP	: Pelindungan Data Pribadi (*Personal Data Protection*)
PDPA	: *Personal Data Protection Act*
PDPC	: *Personal Data Protection Commission*
PP	: Peraturan Pemerintah
PSE	: Penyelenggara Sistem Elektronik
RPJMN	: Rencana Pembangunan Jangka Menengah Nasional
SCC	: *Standard Contractual Clauses*
SNS	: *Social Networking Sites*
SPBE	: Sistem Pemerintahan Berbasis Elektronik
TAXPEDIA	: Jurnal *Taxpedia Accounting*
UKM	: Usaha Kecil dan Menengah
UU	: Undang-Undang
UU HAM	: Undang-Undang Hak Asasi Manusia
UU ITE	: Undang-Undang Informasi dan Transaksi Elektronik
UU PDP	: Undang-Undang Pelindungan Data Pribadi
UUD 1945	: Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
UUHAM	: Undang-Undang Hak Asasi Manusia

SURAT PERNYATAAN BEBAS PLAGIAT

Yang bertanda tangan di bawah ini:

Nama	:	Raihan Imam Cahya Akbar
NPM	:	2330010012
Program Studi	:	Program Doktor Hukum
Judul Disertasi	:	Rekonstruksi Hukum Perlindungan Data Pribadi Yang Bersifat Spesifik Di Era Digital Untuk Mewujudkan Keadilan Berdasarkan Pancasila

Dengan ini saya menyatakan bahwa karya ilmiah Disertasi ini bebas Plagiat. Apabila dikemudian hari terbukti Plagiat dalam karya ilmiah ini, maka saya bersedia menerima sanksi sebagaimana diatur dalam Peraturan Perundang-undangan yang berlaku.

Medan,

Yang menyatakan,

Materai 10.000.-

Raihan Imam Cahya Akbar

DAFTAR ISI

Halaman

PERSETUJUAN TIM PROMOTOR i

PENGESAHAN TIM PROMOTOR ii

LEMBAR PENGESAHAN iii

ABSTRAK iv

ABSTRACT v

KATA PENGANTAR vi

DAFTAR SINGKATAN/AKRONIM xi

SURAT PERNYATAAN BEBAS PLAGIAT xiii

DAFTAR ISI xiv

BAB I : PENDAHULUAN 1

A. Latar Belakang 1

B. Rumusan Masalah 27

C. Tujuan Penelitian 27

D. Manfaat Penelitian 28

1. Manfaat Teoritis 28

2. Manfaat Praktis 28

E. Keaslian Penelitian 29

F. Kerangka Teori 31

1. Teori Keadilan Pancasila 31

2. Teori Perlindungan Hukum 38

3. Teori Hukum Pembangunan 43

G. Metode Penelitian 48

1. Jenis Penelitian 49

2. Pendekatan Penelitian 50

3. Sifat Penelitian 51

4. Bentuk Penelitian 52

5. Sumber Data 53

6. Alat Pengumpul Data 56

7. Analisis Hasil Penelitian 57

BAB II : INEFEKTIVITAS PERLINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK AKIBAT PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL 59

A. Perlindungan Data Pribadi Yang Bersifat Spesifik di Era Digital Dalam Perspektif Hukum Positif di Indonesia 59

B. Implikasi Hukum Perlindungan Data Pribadi Yang Bersifat Spesifik di Era Digital 118

C. Inefektivitas Perlindungan Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi Di Era Digital 137

BAB III : KEBIJAKAN PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI YANG BERSIFAT SPESIFIK AKIBAT PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL 159

A. Perlindungan Hukum Terhadap Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi di Era Digital 159

1. Perlindungan Pemerintah terhadap Warga Negara dalam Pengelolaan Data Pribadi yang Bersifat Spesifik 167

2. Perlindungan Hak-Hak Warga Negara sebagai Subjek Data 173

3. Sanksi Tegas terhadap Pelanggaran Data Pribadi 177

B. Jaminan Kepastian Hukum Terhadap Data Pribadi yang Bersifat Spesifik di Era Digital…. 180

1. Konsep Kepastian Hukum dalam Perlindungan Data Pribadi 182

2. Eksistensi Dan Peran Undang-Undang Pelindungan Data Pribadi..... 188

3. Kepastian Hukum dalam Regulasi Data Pribadi di Indonesia..... 194

4. Kepastian Hukum Berbasis Nilai-Nilai Pancasila..... 206

C. Kebijakan Perlindungan Hukum Terhadap Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi Di Era Digital..... 212

BAB IV : REKONSTRUKSI HUKUM PERLINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK TERHADAP PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL YANG SESUAI DENGAN NILAI-NILAI KEADILAN BERDASARKAN PANCASILA..... 219

A. Dasar Kebutuhan Rekonstruksi Hukum Perlindungan Data Pribadi yang Bersifat Spesifik di Era Digital untuk Mewujudkan Keadilan Berdasarkan Pancasila..... 219

B. Unsur-Unsur Rekonstruksi Sistem Hukum Perlindungan Data Pribadi yang Bersifat Spesifik Berbasis Nilai Keadilan Pancasila..... 254

1. Rekonstruksi Substansi Hukum (*Legal Substance*) 260

2. Rekonstruksi Struktur Hukum (*Legal Structure*)..... 262

3. Rekonstruksi Kemanfaatan dan Keadilan... 264

4. Rekonstruksi Budaya Hukum (*Legal Culture*) 266

C. Rekonstruksi Hukum Perlindungan Data Pribadi Yang Bersifat Spesifik Terhadap Perkembangan Teknologi Di Era Digital Yang Sesuai Dengan Nilai-Nilai Keadilan Berdasarkan Pancasila..... 272

BAB V : KESIMPULAN DAN SARAN..... 308

A. Kesimpulan 308

B. Saran 310

DAFTAR PUSTAKA 312

LAMPIRAN

BAB I
PENDAHULUAN

A. Latar Belakang

Di era digitalisasi yang masif, data pribadi telah bertransformasi menjadi aset bernilai tinggi yang rentan terhadap penyalahgunaan. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) secara tegas telah membedakan klasifikasi data pribadi ke dalam data umum dan data yang bersifat spesifik. Data pribadi yang bersifat spesifik seperti data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, dan data keuangan pribadi membutuhkan tingkat perlindungan yang jauh lebih ketat. Hal ini dikarenakan kebocoran jenis data tersebut tidak hanya berpotensi melanggar privasi, tetapi dapat beresiko langsung pada kerugian finansial yang masif, pencurian identitas (*identity theft*), hingga ancaman terhadap keselamatan fisik dan psikologis subjek data. Risiko privasi di era digital tidak hanya terbatas pada potensi penyalahgunaan data oleh pihak ketiga yang tidak berwenang, tetapi juga termasuk ancaman dari kebocoran data, serangan siber,[1] dan penggunaan data tanpa persetujuan yang sah.[2]

[1] Serangan siber adalah upaya individu atau kelompok untuk mengakses, merusak, atau mengganggu sistem komputer dan jaringan melalui berbagai teknik seperti phishing, ransomware, DDoS, Man-in-the-Middle attack, SQL Injection, dan malware. Serangan ini dapat menyebabkan kerugian finansial, kehilangan data rahasia, dan gangguan operasional. Oleh karena itu, diperlukan kebijakan keamanan yang kuat, penggunaan antivirus, serta pembaruan sistem secara berkala untuk melindungi data dan infrastruktur digital. (W Duo, M Zhou, dan A Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances dan Challenges," *IEEE/CAA Journal of Automatica Sinica* 9, no. 5 (2022). hlm. 784–800).

[2] Dinda Aprilita Herera dan Muhamad Hasan Sebyar, "Pelindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru," *Jurnal Hukum dan Kewarganegaraan* 1, no. 5 (2023), hlm. 1–16.

Pelaksanaan perlindungan data pribadi di Indonesia belum sepenuhnya sejalan dengan cita-cita hukum tersebut. Berbagai insiden keamanan siber menunjukkan bahwa sistem perlindungan data, baik di sektor publik maupun privat, masih menghadapi kerentanan serius dalam melindungi data pribadi yang bersifat spesifik. Ancaman nyata terlihat, antara lain, dalam kasus serangan ransomware terhadap Bank Syariah Indonesia pada tahun 2023 yang mengompromikan data keuangan pribadi dan riwayat transaksi nasabah. Praktik pinjaman online ilegal juga memperlihatkan pola penyalahgunaan data biometrik, seperti foto wajah, serta data keuangan pribadi debitur untuk kepentingan intimidasi dan penagihan yang melanggar hukum. Fakta tersebut menunjukkan bahwa kewajiban hukum pengendali data pribadi, termasuk penerapan inventarisasi data dalam pemrosesan data, belum sepenuhnya dijalankan secara akuntabel.[3]

Kesenjangan antara pengaturan normatif dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan pelaksanaannya di lapangan memperlihatkan bahwa perlindungan data pribadi yang bersifat spesifik belum berjalan secara efektif. Persoalan yang muncul tidak hanya berkaitan dengan keberadaan norma hukum, tetapi juga menyangkut efektivitas pengawasan, kepatuhan pengendali data, penerapan sanksi, dan mekanisme pemulihan hak korban. Penyalahgunaan data pribadi yang bersifat spesifik dapat menghilangkan kendali seseorang atas identitas dirinya, menimbulkan kerugian ekonomi, merusak reputasi, menciptakan diskriminasi, serta mengganggu rasa aman warga negara

[3] Ferry Andika Harmen, "Website DJKN," last modified 2023, (April 1, 2026), https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html.

dalam ruang digital. Oleh karena itu, perlindungan data pribadi yang bersifat spesifik perlu ditempatkan sebagai bagian dari perlindungan hak asasi manusia dan penghormatan terhadap martabat pribadi warga negara, bukan semata-mata sebagai kewajiban administratif dalam pengelolaan sistem elektronik.

Perkembangan teknologi digital juga menciptakan relasi yang tidak seimbang antara subjek data dan pihak yang menguasai serta mengolah data. Subjek data sering berada pada posisi yang lebih lemah karena tidak memiliki pengetahuan, akses, dan kemampuan teknis yang memadai untuk mengontrol penggunaan data pribadinya. Sebaliknya, pengendali data memiliki kemampuan yang lebih besar dalam mengumpulkan, menyimpan, menganalisis, dan mendistribusikan data. Ketimpangan tersebut menuntut pembaruan hukum yang tidak hanya memperbaiki rumusan norma, tetapi juga memperkuat struktur kelembagaan, mekanisme pengawasan, penegakan hukum, jaminan ganti rugi, dan budaya hukum digital yang berorientasi pada nilai keadilan Pancasila.

Penggunaan istilah rekonstruksi dalam kajian ini mencerminkan kebutuhan untuk membangun kembali arah pengaturan hukum perlindungan data pribadi yang bersifat spesifik secara lebih mendasar, sistemik, dan menyeluruh. Istilah reformulasi cenderung terbatas pada perumusan ulang norma hukum, sedangkan harmonisasi lebih menitikberatkan pada penyelarasan antarperaturan perundang-undangan. Kedua istilah tersebut belum sepenuhnya mewakili kebutuhan pembaruan hukum dalam perlindungan data pribadi yang bersifat spesifik, karena persoalan yang dihadapi tidak hanya terletak pada teks peraturan, tetapi juga pada struktur kelembagaan, mekanisme pengawasan, efektivitas sanksi, akses pemulihan

bagi subjek data, dan budaya hukum digital. Rekonstruksi hukum lebih tepat digunakan karena memuat gagasan pembenahan hukum secara utuh, mulai dari substansi hukum, struktur hukum, hingga budaya hukum.

Arah rekonstruksi hukum tersebut ditujukan untuk memperkuat perlindungan data pribadi yang bersifat spesifik agar lebih responsif terhadap perkembangan teknologi digital dan selaras dengan nilai keadilan Pancasila. Pembaruan yang diperlukan mencakup penguatan substansi UU PDP, pembentukan lembaga pengawas yang independen, peningkatan efektivitas sanksi administratif dan mekanisme ganti rugi, serta pembentukan kesadaran hukum digital yang menempatkan martabat manusia, hak privasi, kepastian hukum, kemanfaatan, dan keadilan sosial sebagai orientasi utama perlindungan hukum

Perlindungan hukum terhadap data pribadi yang bersifat spesifik tidak hanya memiliki dasar dalam hukum positif, tetapi juga memperoleh penguatan dari nilai-nilai kewahyuan dalam ajaran Islam. Data pribadi yang bersifat spesifik merupakan bagian dari identitas, kehormatan, dan ruang privat seseorang, sehingga pengumpulan, penggunaan, penyebaran, dan pemanfaatannya harus dilakukan secara sah, etis, dan bertanggung jawab. Dalam perspektif Islam, penghormatan terhadap ruang privat manusia tidak semata-mata dipahami sebagai norma sosial, tetapi juga sebagai bagian dari kewajiban moral untuk menjaga kehormatan dan martabat sesama manusia.

Landasan kewahyuan yang paling relevan dengan perlindungan privasi dapat dilihat dalam Surah Al-Hujurat ayat 12 yang melarang perbuatan tajassus atau mencari-cari kesalahan dan informasi pribadi orang lain tanpa alasan yang sah.

Larangan tajassus dalam ayat tersebut memiliki relevansi langsung dengan perlindungan data pribadi di era digital, karena praktik pengintaian, pengumpulan data tanpa izin, peretasan akun, doxing, dan penyebaran informasi pribadi pada hakikatnya merupakan bentuk pelanggaran terhadap ruang privat individu. Kajian kontemporer terhadap Tafsir Al-Azhar menunjukkan bahwa larangan tajassus tidak hanya berkaitan dengan perilaku sosial dalam ruang fisik, tetapi juga dapat dikembangkan sebagai dasar etika digital untuk mencegah pelanggaran privasi, penyebaran aib, dan eksploitasi data pribadi di ruang siber.[4] Allah SWT berfirman dalam Surah Al-Hujurat ayat 12: [5]

يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوا ٱجْتَنِبُوا كَثِيرًا مِّنَ ٱلظَّنِّ إِنَّ بَعْضَ ٱلظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَٱتَّقُوا ٱللَّهَ ۚ إِنَّ ٱللَّهَ تَوَّابٌ رَّحِيمٌ

> *"Wahai orang-orang yang beriman! Jauhilah banyak dari prasangka, sesungguhnya sebagian prasangka itu dosa, dan janganlah kamu mencari-cari kesalahan orang lain, serta janganlah ada di antara kamu yang menggunjing sebagian yang lain. Adakah seorang di antara kamu yang suka memakan daging saudaranya yang sudah mati? Tentu kamu merasa jijik kepadanya. Bertakwalah kepada Allah, sesungguhnya Allah Maha Penerima tobat, Maha Penyayang."*[6]

Analisis terhadap Surah Al-Hujurat ayat 12 menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik berkaitan erat dengan perlindungan kehormatan manusia. Data kesehatan, data biometrik, data genetika, data anak, data keuangan pribadi, dan catatan kejahatan bukan sekadar informasi teknis, melainkan bagian dari identitas pribadi yang apabila disalahgunakan dapat menimbulkan

[4] Diana Durrotul Lum'ah, Suqiyah Musafa'ah, dan Muhammad Ihsan Mahbub, "The Paradigm of Digital Privacy in Indonesian Tafsir: A Study of Tafsir Al-Azhar on QS. Al-Hujurāt (49): 12 in the Age of Information," *MUSHAF: Jurnal Tafsir Berwawasan Keindonesiaan* 5, no. 2 (2025): hlm. 240–244.

[5] Al-Qur'an*,* 49:12.

[6] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 49:12

kerugian sosial, ekonomi, psikologis, bahkan diskriminatif. Oleh karena itu, larangan tajassus dapat dijadikan dasar etis bahwa setiap pihak, baik negara, korporasi, maupun individu, tidak boleh memperoleh, mengakses, atau menyebarkan data pribadi seseorang tanpa dasar hukum dan persetujuan yang sah. Dalam konteks ini, nilai kewahyuan berfungsi sebagai dasar moral bagi penguatan prinsip legalitas, kerahasiaan, pembatasan tujuan, dan akuntabilitas dalam perlindungan data pribadi.

Prinsip persetujuan dalam perlindungan data pribadi juga memiliki landasan kewahyuan dalam Surah An-Nur ayat 27 yang menegaskan larangan memasuki rumah orang lain sebelum meminta izin dan memberi salam kepada penghuninya. Secara tekstual, ayat ini mengatur etika memasuki ruang fisik berupa rumah. Secara substantif, ayat tersebut mengandung prinsip penghormatan terhadap ruang privat dan hak seseorang untuk menentukan siapa yang boleh memasuki wilayah pribadinya. Dalam masyarakat digital, ruang privat tidak lagi hanya berbentuk rumah secara fisik, tetapi juga mencakup akun digital, perangkat elektronik, data pribadi, rekam medis, identitas biometrik, riwayat transaksi, serta informasi lain yang berada dalam penguasaan subjek data.[7] Allah SWT berfirman dalam Surah An-Nur ayat 27: [8]

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

[7] Khairul Fikri dan Umi Wasilatul Firdausiyah, "Privasi dalam Dunia Digital: Analisis QS. An-Nur (24): 27 Menggunakan Pendekatan Ma'na-Cum-Maghza," *Islamika Inside: Jurnal Keislaman dan Humaniora* 7, no. 2 (2021): hlm. 211–218.

[8] Al-Qur'an*,* 24:27

> *"Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu agar kamu selalu ingat."*[9]

Kajian Khairul Fikri dan Umi Wasilatul Firdausiyah terhadap Surah An-Nur ayat 27 dengan pendekatan ma'na-cum-maghza menegaskan bahwa ayat tersebut tidak hanya melarang seseorang memasuki rumah tanpa izin, tetapi juga dapat dipahami sebagai larangan untuk mengusik data pribadi orang lain di dunia digital. Data pribadi dalam ruang digital dapat dianalogikan sebagai rumah dalam kehidupan nyata, karena keduanya sama-sama memuat sisi privat yang tidak boleh dimasuki tanpa izin.[10] Dengan demikian, prinsip isti'dzan atau permintaan izin dalam ayat tersebut dapat dikontekstualisasikan sebagai prinsip consent dalam perlindungan data pribadi. Pengendali data wajib memperoleh persetujuan yang sah, jelas, sadar, dan tidak manipulatif sebelum memproses data pribadi yang bersifat spesifik.

Surah Al-Baqarah ayat 188 juga relevan sebagai dasar etis dalam mencegah penyalahgunaan data pribadi untuk memperoleh keuntungan secara tidak sah. Ayat tersebut melarang tindakan memakan atau mengambil harta orang lain dengan cara batil. Dalam konteks perlindungan data pribadi, larangan ini dapat dikaitkan dengan praktik jual beli data, pemanfaatan data untuk penipuan, pemerasan berbasis data, manipulasi identitas, pinjaman online ilegal, serta eksploitasi data pribadi untuk keuntungan ekonomi tanpa persetujuan subjek data. Tafsir terhadap ayat ini menekankan bahwa mengambil hak orang lain dengan cara yang batil tidak hanya

---

[9] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 24:27
[10] Khairul Fikri dan Umi Wasilatul Firdausiyah, *loc.cit.*

terbatas pada penguasaan harta secara fisik, tetapi juga mencakup berbagai bentuk penguasaan manfaat ekonomi secara tidak sah.[11] Allah SWT berfirman dalam Surah Al-Baqarah ayat 188:[12]

وَلَا تَأْكُلُوٓا۟ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُوا۟ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُوا۟ فَرِيقًا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ

"Janganlah kamu makan harta di antara kamu dengan jalan yang batil dan (janganlah) kamu membawa (urusan) harta itu kepada para hakim dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui."[13]

Keterkaitan ketiga ayat tersebut menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik dalam perspektif Islam bertumpu pada tiga prinsip utama. Pertama, larangan tajassus sebagai dasar perlindungan terhadap privasi dan kehormatan individu. Kedua, prinsip isti'dzan sebagai dasar keharusan adanya persetujuan sebelum memasuki atau mengakses ruang privat seseorang. Ketiga, larangan mengambil manfaat secara batil sebagai dasar pencegahan eksploitasi ekonomi atas data pribadi. Ketiga prinsip tersebut memperkuat argumentasi bahwa perlindungan data pribadi yang bersifat spesifik bukan hanya kewajiban administratif dalam hukum negara, tetapi juga kewajiban moral dan etis yang berakar pada penghormatan terhadap martabat manusia.

Perspektif kewahyuan tersebut juga dapat dipahami melalui kerangka maqāṣid al-syarī'ah, khususnya prinsip ḥifẓ al-'irḍ atau perlindungan kehormatan dan ḥifẓ al-māl atau perlindungan harta. Data pribadi yang bersifat spesifik memiliki hubungan langsung dengan kehormatan dan keamanan seseorang,

---

[11] M. Quraish Shihab, *Tafsir al-Mishbah: Pesan, Kesan, dan Keserasian Al-Qur'an*, Jilid I, Cet. V (Jakarta: Lentera Hati, 2005), hlm. 413–415.

[12] Al-Qur'an, 2:188.

[13] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 2:188

sekaligus memiliki nilai ekonomi yang dapat disalahgunakan oleh pihak lain. Penguatan perlindungan hukum terhadap data pribadi yang bersifat spesifik karena itu sejalan dengan tujuan syariat untuk mewujudkan kemaslahatan dan mencegah kemudaratan.[14] Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik memiliki dasar normatif yang kuat, baik dalam hukum positif, nilai keadilan Pancasila, maupun nilai kewahyuan Islam yang menempatkan kehormatan, persetujuan, dan perlindungan hak individu sebagai prinsip utama.

Ayat ini relevan dalam konteks modern, dimana penyebaran data pribadi tanpa persetujuan merupakan pelanggaran hukum dan nilai Islam. Regulasi data pribadi harus mampu mencegah penyalahgunaan dan menjamin keadilan sosial bagi individu yang datanya disalahgunakan. Terakhir, Surah An-Nur Ayat 27 menegaskan pentingnya meminta izin sebelum memasuki ranah privasi orang lain, yang dalam perlindungan data pribadi yang bersifat spesifik dapat diterjemahkan sebagai prinsip "*consent*" atau persetujuan dalam pemrosesan data:

Ayat ini menegaskan bahwa perlindungan data pribadi yang bersifat spesifik bukan sekadar kepatuhan hukum, tetapi juga mencerminkan nilai moral yang harus diterapkan dalam kehidupan masyarakat. Ayat ini melarang tindakan mencari-cari kesalahan atau mengungkapkan aib orang lain, yang dalam konteks modern dapat diartikan sebagai larangan untuk menyebarkan data pribadi tanpa izin. Oleh karena itu, perlindungan data pribadi yang bersifat spesifik juga harus dilihat sebagai

[14] Busyro, *Maqāṣid al-Syarī'ah: Pengetahuan Mendasar Memahami Maslahah* (Jakarta: Kencana, 2019), hlm. 1–8.

kewajiban moral dan etika, yang sejalan dengan prinsip-prinsip keadilan sosial yang diusung oleh Pancasila.

Pesatnya perkembangan teknologi informasi dan komunikasi di era reformasi membawa tantangan baru, menuntut adanya pengaturan yang lebih komprehensif dan adaptif untuk melindungi data pribadi di era digital. Pelindungan data pribadi yang bersifat spesifik di Indonesia saat ini tersebar dalam berbagai peraturan perundang-undangan di Indonesia, baik yang bersifat umum maupun khusus. UUD 1945 sebagai landasan konstitusional, mengamanatkan perlindungan hak atas privasi dalam Pasal 28G ayat 1 yang berbunyi:[15]

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Sejarah perlindungan data pribadi yang bersifat spesifik di Indonesia mengalami dinamika dari era pra-kemerdekaan hingga reformasi. Pada masa Orde Baru, perlindungan data pribadi yang bersifat spesifik masih lemah dan sering disalahgunakan untuk kepentingan politik. Reformasi 1998 membawa perubahan dengan Amandemen UUD 1945 Pasal 28G ayat 1 yang mengakui hak privasi, diperkuat dengan Undang-Undang Nomor 39 Tahun 1999 tentang HAM (UUHAM). Pelindungan data pribadi yang bersifat spesifik secara khusus telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

---

[15] Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," *Pasal 28G Ayat 1* (Pemerintah Republik Indonesia, 1945).

Pancasila sebagai dasar negara dan pandangan hidup berbangsa dan bernegara, memberikan kerangka filosofis yang komprehensif untuk memahami pentingnya perlindungan data pribadi yang bersifat spesifik yang sifatnya spesifik.[16] Nilai-nilai luhur yang terkandung dalam Pancasila, seperti Ketuhanan Yang Maha Esa, Kemanusiaan Yang Adil dan Beradab, Persatuan Indonesia, Kerakyatan yang dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan, dan Keadilan Sosial bagi seluruh rakyat Indonesia, memberikan landasan etika dan moral yang kuat dalam merumuskan kebijakan perlindungan data pribadi yang bersifat spesifik yang adil.[17]

Fenomena kebocoran data dalam skala besar *(massive data leak)* dan pelanggaran keamanan data *(data breach)* menjadi salah satu persoalan utama dalam tata kelola data pribadi di era digital. *Massive data leak* merujuk pada peristiwa terbukanya atau tersebarnya data pribadi dalam jumlah sangat besar akibat lemahnya sistem keamanan atau kelalaian pengelola data, sedangkan data breach merupakan peristiwa akses tidak sah terhadap sistem yang menyimpan data pribadi sehingga memungkinkan pihak tertentu memperoleh, mencuri, atau memanfaatkan data tersebut secara ilegal.[18] Kedua fenomena ini menunjukkan bahwa kerentanan tidak hanya terletak pada aspek teknologi, tetapi juga pada tata kelola hukum dan kelembagaan yang belum sepenuhnya mampu mengantisipasi

[16] Jonaedi Efendi, *Rekonstruksi Dasar Pertimbangan Hukum Hakim* (Prenada Media, 2018). hlm. 294.

[17] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan data pribadi yang bersifat spesifik (UU RI No. 27 Tahun 2022)* (Jakarta: Sinar Grafika, 2023). hlm. 11-43.

[18] Dominik Molitor et al., "Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study," *Journal of Information Security* Vol. 15, no. 02 (2024): hlm. 168-195.

kompleksitas pengolahan data digital.[19] Oleh karena itu, meningkatnya insiden *massive data leak* dan *data breach* menegaskan urgensi penguatan kerangka hukum perlindungan data pribadi yang bersifat spesifik yang lebih spesifik, adaptif, dan efektif dalam menjamin keamanan serta hak privasi masyarakat.

Fenomena *massive data leak* dan *data breach* menunjukkan bahwa data pribadi tidak lagi hanya menjadi isu teknis dalam keamanan sistem informasi, tetapi telah berkembang menjadi persoalan hukum, ekonomi, dan sosial yang kompleks. Kebocoran data dalam jumlah besar dapat mengakibatkan kerugian yang luas, baik bagi individu maupun negara. Bagi individu, kebocoran data dapat menyebabkan pencurian identitas, penipuan digital, pemerasan, hingga kerusakan reputasi.[20] Sementara bagi negara, kebocoran data berpotensi mengganggu stabilitas sistem administrasi publik, menurunkan tingkat kepercayaan masyarakat terhadap institusi negara, serta membuka peluang eksploitasi data oleh pihak asing.[21] Oleh karena itu, fenomena massive data leak tidak dapat dipandang semata sebagai kegagalan teknis dalam pengelolaan sistem elektronik, tetapi juga sebagai indikasi adanya kelemahan dalam kerangka regulasi dan tata kelola perlindungan data pribadi yang bersifat spesifik.

Pelindungan data pribadi yang bersifat spesifik sejalan dengan nilai-nilai Pancasila yang menekankan keadilan sosial, persatuan, dan penghormatan terhadap

---

[19] Richart Sahatatua et al., "Cyber Law Analysis of E-KTP Data Leakage: A Case Approach of 102 Million KTP Data Allegedly Leaked from the Ministry of Social Affairs to a Hacker Forum," *Journal of Multidisciplinary Academic and Practice Studies* Vol. 2, no. 3 (2024): hlm. 151-161.

[20] Cassandra Cross and Thomas J Holt, "Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims," *Journal of Crime and Justice* Vol. 1, no. 1 (2025): hlm. 1-24.

[21] Onome Edo et al., "Zero Trust Architecture: Trend and Impact on Information Security," *International Journal of Emerging Technology and Advanced Engineering* Vol. 12, no. 7 (2022): hlm. 140-147.

hak individu. Regulasi yang kuat akan mencegah eksploitasi data yang dapat menimbulkan ketimpangan sosial serta memastikan setiap warga negara mendapatkan perlakuan yang adil dan setara dalam ekosistem digital. Oleh karena itu, kebijakan perlindungan data harus disusun secara demokratis, transparan, dan melibatkan seluruh pemangku kepentingan guna menciptakan keadilan bagi masyarakat.

Keseriusan pemerintah, dalam memberikan perlindungan terhadap data pribadi warga negara mulai terjadi setelah munculnya banyak kasus-kasus penyalahgunaan data pribadi di Indonesia. Sebelumnya, pada Maret 2019 Peretas Gnosticplayes mengklaim menjual 13 juta data akun pengguna dari Bukalapak. Pihak Bukalapak menyatakan peretas gagal menembus sistem keamanan mereka.[22] Juni 2021 sebanyak 2 juta nasabah perusahaan Asuransi BRI Life diduga bocor dan diperjualbelikan di dunia Maya, tahun 2022 dan 2023, tercatat beberapa kasus kebocoran data pribadi warga negara Indonesia, berasal dari aplikasi milik pemerintah atau intitusi negara, yakni kasus pelanggan Indi Home, Data Pelanggan PLN, Jasa Internal Jasa Marga, Data SIM Card, Data Komisi Pemilihan Umum, Data My Pertamina, Data Peduli Lindungi.[23] Dengan berbagai kasus pembobolan, peretasan, dan/atau pencurian data pribadi warga negara yang sudah seharusnya dan

[22] BBC Indonesia, "Bukalapak Diserang Peretas, Pengguna Diimbau Ganti Password," https://www.bbc.com/indonesia, (10 April 2025).

[23] CNN Indonesia, "10 Kasus Kebocoran Data 2022, Bjorka Dominan, Ramai-Ramai Bantah," last modified 2022, (pada April 9, 2025, https://www.cnnindonesia.com/techno. Lihat juga Berita Satu, "Deretan Kasus Kebocoran Data yang Pernah Terjadi di Indonesia," https://www.beritasatu.com , (April 9, 2025).

menjadi tanggungjawab negara untuk melindunginya, maka pada tahun 2022, oleh pemerintah mengeluarkan satu produk perundang-undangan yakni UU PDP.

UU PDP dikeluarkan oleh Pemerintah dengan dasar pertimbangan bahwa perlindungan data pribadi yang bersifat spesifik masuk dalam perlindungan hak asasi manusia dengan demikian, pengaturan menyangkut data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak dasar manusia. Keberadaan suatu Undang-Undang tentang perlindungan data pribadi yang bersifat spesifik suatu keharusan yang tidak dapat ditunda lagi karena sangat mendesak bagi berbagai kepentingan nasional. Pergaulan intemasional Indonesia turut menuntut adanya perlindungan data pribadi yang bersifat spesifik. Pelindungan tersebut dapat memperlancar perdagangan, industri, dan investasi yang bersifat transnasional. Disamping itu, UU PDP ditujukan untuk untuk melindungi hak individu di dalam masyarakat sehubungan dengan pemrosesan data pribadi baik yang dilakukan secara elektronik dan non elektronik menggunakan perangkat olah data.

Pelindungan yang memadai atas data pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak pribadinya. Dengan demikian, pengaturan ini akan menciptakan keseimbangan antara hak individu dan masyarakat yang diwakili kepentingannya oleh negara.[24] Peningkatan kasus *data breach* menegaskan pentingnya penguatan rezim perlindungan data pribadi yang bersifat spesifik yang mampu memberikan

[24] Lihat, Konsideran, Menimbang huruf (b), dan Pejelasan Umum Paragraf kedua dan keempat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi yang bersifat spesifik.

kepastian hukum, akuntabilitas, dan mekanisme penegakan yang efektif. *Data breach* sering terjadi akibat lemahnya standar keamanan data, kurangnya pengawasan terhadap pengendali dan prosesor data, serta belum optimalnya penerapan prinsip kehati-hatian dalam pengolahan data pribadi. Kondisi tersebut menunjukkan bahwa pengaturan yang bersifat umum belum cukup untuk memberikan perlindungan yang memadai, terutama terhadap data pribadi yang bersifat spesifik atau sensitif seperti data kesehatan, biometrik, keuangan, dan identitas kependudukan. Oleh karena itu, diperlukan penguatan dan rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik yang lebih spesifik, komprehensif, dan adaptif terhadap perkembangan teknologi digital guna mencegah terjadinya massive data leak dan data breach di masa mendatang.[25]

Pasal yang berkaitan dengan perlindungan data pribadi yang bersifat spesifik di era digital antara lain Pasal 4 UU PDP yang mengatur jenis data pribadi yang mencakup data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik atau sensitif. Pasal 9 UU PDP menegaskan hak subjek data pribadi untuk mendapatkan informasi mengenai pengolahan data pribadinya. Pasal 15 UU PDP menentukan kewajiban pengendali data untuk melindungi data pribadi dari akses tidak sah dan penyalahgunaan. Pasal 16 UU PDP mengatur kewajiban pengendali data dalam menjaga keamanan data pribadi. Pasal 20 UU PDP menyatakan bahwa pemrosesan data pribadi harus berdasarkan persetujuan eksplisit dari subjek data. Pasal 22 menetapkan bahwa penghapusan data pribadi harus dilakukan jika tujuan

[25] Daniela Wawra, "Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison," in *De Gruyter EBooks* (Berlin, 2023), hlm. 169-194.

pemrosesan telah selesai atau atas permintaan subjek data. Pasal 39 UU PDP mengatur sanksi administratif bagi pelanggaran pengolahan data pribadi. Sementara itu, Pasal 67 hingga 73 UU PDP menetapkan sanksi pidana bagi pihak yang menyalahgunakan atau memperjualbelikan data pribadi tanpa izin.

Regulasi di Indonesia mengatur perlindungan data pribadi yang bersifat spesifik juga pada UU HAM yang menegaskan hak setiap orang untuk bebas dari perlakuan sewenang-wenang terhadap privasi dan nama baik. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) melarang akses dan penyebaran data pribadi tanpa izin (Pasal 30 & 32)[26]. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik menjamin hak atas informasi publik. Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan melindungi data kependudukan sebagai bagian dari data pribadi. Peraturan Menkominfo Nomor 20 Tahun 2016 secara khusus mengatur perlindungan data pribadi yang bersifat spesifik dalam sistem elektronik.

Pelindungan konsumen daring oleh undang-undang sangat penting mengingat pesatnya perkembangan teknologi digital yang menciptakan berbagai platform transaksi dan komunikasi baru. Konsumen sering kali tidak menyadari bagaimana data pribadi mereka digunakan dan diproses, sehingga rentan terhadap penyalahgunaan. Dalam beberapa kasus, data pribadi konsumen digunakan untuk

[26] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada Pasal 30 dan Pasal 32 mengatur larangan terhadap akses dan penyebaran data pribadi tanpa izin. Pasal 30 melarang setiap orang untuk mengakses informasi elektronik milik orang lain tanpa hak, sedangkan Pasal 32 melarang penyebaran informasi yang dapat merugikan pihak lain, termasuk data pribadi, tanpa izin. Kedua pasal ini bertujuan untuk melindungi privasi individu dan mencegah penyalahgunaan data pribadi, serta memberikan sanksi bagi pelaku yang melanggar ketentuan tersebut.

tujuan pemasaran tanpa persetujuan eksplisit, atau bahkan dijual kepada pihak ketiga. Oleh karena itu, regulasi yang ketat dan jelas diperlukan untuk memastikan bahwa hak-hak konsumen terlindungi dan mereka memiliki kontrol penuh atas data pribadi mereka.[27]

Pemerintah perlu menetapkan kebijakan yang mendukung inovasi sekaligus melindungi hak-hak konsumen[28]. Masalah kepastian hukum dalam layanan berbasis digital tidak hanya terbatas pada perlindungan data pribadi yang bersifat spesifik, tetapi juga mencakup layanan lainnya, seperti layanan registrasi tanah secara daring yang menghadapi tantangan terkait implementasi teknologi dan kepastian hukum[29]. Data-data ini, terutama data pribadi yang bersifat spesifik, menyimpan potensi luar biasa, baik untuk kemajuan maupun ancaman. Di satu sisi, data dapat dimanfaatkan untuk mendorong inovasi, meningkatkan efisiensi, dan menciptakan layanan yang lebih personal. Namun di sisi lain, data juga rentan disalahgunakan, mengancam privasi, dan melanggengkan ketidakadilan.[30]

Persetujuan adalah elemen kunci dalam perlindungan data pribadi yang bersifat spesifik, terutama dalam konteks digital dimana data dapat dengan mudah dikumpulkan dan diproses. Persetujuan dalam konteks daring juga harus mempertimbangkan aspek edukasi dan literasi digital masyarakat. Banyak pengguna yang masih belum memahami pentingnya perlindungan data pribadi yang

---

[27] *Ibid*.

[28] Taufiq A Gani, *Kedaulatan Data Digital Untuk Integritas Bangsa* (Syiah Kuala: Syiah Kuala University Press, 2023). hlm. 87-89.

[29] Abdul Halim Barkatullah, "Pelindungan Hukum Bagi Konsltmen Dalam Transaksi E-Commerce Lintas Negara Di Indonesia," *Universitas Islam Indonesia* (Universitas Islam Indonesia, 2006).

[30] Yohanes Ngamal dan Maximus Ali Perajaka, "Penerapan Model Manajemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia," *Jurnal Manajemen Risiko* 2, no. 2 (2021), hlm. 59–74.

bersifat spesifik dan bagaimana persetujuan yang mereka berikan dapat mempengaruhi privasi mereka.[31] Implementasi Pasal 15 UU PDP, yang mewajibkan persetujuan yang jelas dan tegas, pada praktiknya menghadapi tantangan struktural yang berakar pada belum maksimalnya kesadaran keamanan digital di masyarakat. Secara empiris, kegagalan dalam mewujudkan persetujuan yang bermakna (*meaningful consent*) ini sejalan dengan hasil laporan *Status Literasi Digital di Indonesia 2023* oleh Kementerian Kominfo, di mana pilar Keamanan Digital (*Digital Safety*) baru memperoleh skor 3,29 atau berada pada kategori sedang. Lemahnya pemahaman dalam menganalisis dan menimbang perlindungan data pribadi ini dibuktikan dengan fakta bahwa hanya sedikit masyarakat yang telah melakukan upaya pencegahan terhadap bocornya data pribadi mereka. Laporan tersebut mencatat bahwa 48,3% hingga 53,0% responden secara sadar masih mencantumkan informasi spesifik seperti tanggal lahir dan nomor *handphone* secara terbuka di internet.[32]

Masyarakat Indonesia sebanyak 36,1% masih dengan mudah memberikan data dan informasi pribadi kepada pihak yang baru dikenal melalui dunia maya. Kerentanan literasi digital ini memperburuk situasi ketika pengguna dihadapkan pada kebijakan privasi platform yang panjang dan kompleks. Sebagai dampaknya, ketika disajikan tombol persetujuan elektronik (*clickwrap agreement*), pengguna terpaksa atau cenderung menyetujui penyerahan data spesifik mereka semata-mata

[31] Tiolina Evi, *Transformasi Transaksi Tunai Ke Digital Di Indonesia* (CV. AA. Rizky, 2023). hlm. 154-156.

[32] Kementerian Komunikasi dan Informatika Republik Indonesia and Katadata Insight Center, "Status Literasi Digital di Indonesia 2023" (Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia, 2023).

agar dapat mengakses layanan, tanpa dilandasi oleh pemahaman dan kesadaran utuh mengenai implikasi atas klausul baku yang mereka setujui.[33] Regulasi ini memberikan kerangka kerja yang komprehensif untuk melindungi data pribadi konsumen dan menetapkan standar tinggi untuk persetujuan, transparansi, dan hak-hak individu.[34]

Pelindungan data pribadi yang bersifat spesifik tidak hanya menjadi isu nasional tetapi juga internasional seiring dengan meningkatnya globalisasi dan digitalisasi karena pada era digital data pribadi sering berpindah antar negara melalui transaksi dan pertukaran informasi maka penggunaan sertifikat *Apostille*[35] dalam pengesahan dokumen resmi semakin menjadi penting diadakan bagi setiap negara salah satunya Indonesia. Dalam konteks hukum internasional, banyak dokumen yang terkait dengan data pribadi memerlukan pengakuan legal di berbagai yurisdiksi, terutama ketika data tersebut terlibat dalam transaksi lintas negara., sehingga penting bagi Indonesia untuk mengadopsi mekanisme *Apostille* guna menyederhanakan pengakuan legal dokumen lintas negara tanpa proses legalisasi berlapis-lapis. *Apostille* juga krusial dalam melindungi hak-hak data pribadi warga

---

[33] Erna Priliasari, "Pelindungan data pribadi yang bersifat spesifik Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia)," *Jurnal Rechts Vinding* 12, no. 2 (2023), hlm. 261–279.

[34] Ahmad Fachri Yamin et al., "Pelindungan data pribadi yang bersifat spesifik Dalam Era Digital: Tantangan Dan Solusi," *Meraja Journal* 5, no. 3 (2022), hlm. 115–137.

[35] *Apostille* adalah sertifikat yang dilekatkan pada dokumen resmi untuk mengesahkan keaslian tanda tangan, segel, atau cap jabatan pada dokumen tersebut, sehingga dokumen tersebut diakui secara sah di negara-negara lain yang menjadi anggota Konvensi Apostille Den Haag 1961. Konvensi ini menyederhanakan proses legalisasi dokumen di negara-negara anggota, yang mencakup lebih dari 120 negara di seluruh dunia. *Ibid.*

Indonesia yang datanya diolah oleh entitas asing, memperkuat posisi hukum Indonesia di ranah internasional. [36]

Kasus kebocoran data di Indonesia menunjukkan lemahnya sistem perlindungan data pribadi yang bersifat spesifik, baik di sektor publik maupun swasta. Meskipun sudah terdapat UU PDP, masih terjadi juga beberapa kasus yang fatal seperti insiden 34,9 juta data bocor dari Ditjen Imigrasi pada tahun 2023 [37] menyoroti tingginya risiko keamanan siber. Selain itu, kebocoran data pada MyPertamina, Bank Syariah Indonesia (BSI), dan MyIndihome membuktikan bahwa sistem keamanan perusahaan masih rentan terhadap serangan siber.Selain kebocoran data, penyalahgunaan data pribadi juga marak dalam praktik pinjaman *online* (pinjol) ilegal.

Kasus PT. Barracuda Fintech Indonesia dan PT. Vega Data Indonesia, terdakwa terbukti menggunakan data pribadi nasabah secara ilegal untuk melakukan intimidasi dalam penagihan utang. Ancaman dan penyebaran informasi pribadi korban tanpa izin menjadi bukti lemahnya perlindungan hukum terhadap konsumen pinjol.[38]Kejadian tersebut diperburuk oleh lemahnya pengawasan dan sanksi hukum yang belum memberikan efek jera. Banyak perusahaan dan lembaga belum menerapkan standar keamanan yang memadai, sementara kebijakan perlindungan data masih menghadapi tantangan dalam implementasi. Oleh karena

---

[36] Melly Aida et al., "Kepentingan Indonesia Mengaksesi Konvensi Apostille Dan Relevansinya Di Bidang Kenotariatan," *Jurnal Ilmiah Hukum Kenotariatan* 12, no. 1 (2023), hlm .85–98.

[37] Kominfo, "Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia," last modified 2023, accessed August 27, 2024, https://www.kominfo.go.id/content/detail/50017/siaran-pers-no-132hmkominfo072023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia/0/siaran_pers.

[38] Mahkamah Agung Republik Indonesia, "Putusan Nomor 438/Pid.Sus/2020/PN Jkt.Utr," 2020.

itu, penguatan regulasi, peningkatan keamanan siber, serta pengawasan ketat terhadap penyalahgunaan data menjadi langkah mendesak untuk mencegah pelanggaran serupa di masa depan. Undang-undang perlindungan data pribadi yang bersifat spesifik di Indonesia mengalami masalah seperti fragmentasi regulasi dan penegakan hukum yang lemah. Perkembangan teknologi juga menambah kerumitan pengumpulan data pribadi, yang sering menjadi sasaran kejahatan siber. Oleh karena itu, rekonstruksi hukum untuk perlindungan data pribadi yang bersifat spesifik sangat penting.[39]

Indonesia dapat menjamin privasi data pribadi dengan menerapkan regulasi global yang optimal. Ini meningkatkan kepemimpinan digital Indonesia dan melindungi warga negara dari pencurian data asing. Untuk merumuskan regulasi teknologi yang fleksibel dan memperkuat identitas nasional, legislasi harus menggabungkan prinsip-prinsip Pancasila, termasuk nilai-nilai sosial dan individu.[40] Penelitian ini menafsirkan kembali hukum privasi sebagai pelindung terhadap risiko digital dan instrumen untuk meningkatkan keamanan masyarakat. Ketidakjelasan definisi persetujuan ini membuka peluang interpretasi berbeda oleh pengguna, penyedia layanan, dan penegak hukum, serta memungkinkan perusahaan menghindari tanggung jawab atas penyalahgunaan data pribadi. Selain itu, sanksi

[39] Hariyanto et al., "Meningkatkan Literasi Teknologi Di Masyarakat Pedesaan Melalui Pelatihan Digital," *Jurnal Abdimas Peradaban* 4, no. 2 (2023), hlm. 12–21.

[40] Irsan Rahman et al., "Hukum Pelindungan Konsumen Di Era E-Commerce: Menavigasi Tantangan Pelindungan Konsumen Dalam Lingkungan Perdagangan Digital," *Jurnal Hukum dan HAM Wara Sains* 2, no. 08 (2023), hlm. 704–712.

dalam Pasal 36 UU PDP dianggap tidak cukup memberikan efek jera, terutama bagi perusahaan besar yang memandang denda sebagai biaya operasional.[41]

Rekonstruksi hukum dalam perlindungan data pribadi yang bersifat spesifik harus mencakup perumusan definisi persetujuan yang lebih jelas, standar verifikasi yang lebih ketat, serta peningkatan sanksi guna mencegah terjadinya pelanggaran dan mendorong keseriusan perusahaan dalam melindungi data pribadi masyarakat. Dalam era digital, dimana data pribadi memiliki nilai yang sangat tinggi dan rentan terhadap pencurian maupun penyalahgunaan, kelemahan dalam pengaturan hukum dapat menimbulkan kerugian sosial yang signifikan. Oleh karena itu, rekonstruksi hukum diperlukan untuk memastikan bahwa setiap individu memiliki kendali atas data pribadinya, termasuk hak untuk memberikan persetujuan, menarik kembali persetujuan, serta mengetahui bagaimana data tersebut dikumpulkan, diproses, dan digunakan. Selain itu, rekonstruksi juga harus mengatur secara tegas kewajiban penyedia layanan digital dalam menjaga keamanan data pribadi guna menciptakan ekosistem digital yang aman.[42]

Rekonstruksi hukum harus mencerminkan prinsip keadilan, transparansi, dan akuntabilitas, memastikan bahwa data pribadi dihormati dan dilindungi, sambil tetap memberi ruang bagi inovasi dan pertumbuhan ekonomi. [43] Dengan menggantikan aturan yang kaku dengan pendekatan hukum progresif, rekonstruksi

---

[41] Indonesia, "UU Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik," *Undang-Undang Republik Indonesia* (Pemerintah Republik Indonesia, 2022).

[42] Riduan Siagian, Leonard Siahaan, and Ichwan Hamzah, "Human Rights in The Digital Era: Online Privacy, Freedom Of Speech, and Personal Data Protection," *Journal Of Digital Learning And Distance Education* Vol. 2, no. 4 (September 28, 2023): hlm. 513-523.

[43] Yuyut Prayuti, "Dinamika Pelindungan Hukum Konsumen Di Era Digital : Analisis Hukum Terhadap Praktik E-Commerce Dan Pelindungan Data Konsumen Di Indonesia" 5, no. 1 (2024), hlm. 903–913.

hukum berupaya menciptakan suatu sistem yang responsif terhadap dinamika sosial dan mampu menjadi instrumen yang efektif untuk melindungi hak-hak masyarakat secara adil dan merata.[44] Rekonstruksi hukum ini bertujuan memperbarui regulasi agar lebih sesuai dengan kebutuhan masyarakat dan perkembangan teknologi, sambil tetap menegakkan prinsip keadilan dan melindungi hak-hak individu. [45]

UU PDP sebenarnya telah mengatur mengenai klasifikasi data pribadi dalam Pasal 4 dan Pasal 4 ayat (2), yang membedakan antara data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Pasal 28 hingga Pasal 32 UU PDP mengatur mengenai hak-hak subjek data, seperti hak untuk mengakses, mengoreksi, dan menghapus data pribadi. Namun, dalam praktiknya, masih banyak kasus dimana hak-hak ini sulit diimplementasikan karena kurangnya mekanisme pengawasan yang efektif. Pasal 58 hingga Pasal 64 mengatur tentang sanksi administratif, tetapi masih belum menunjukkan efektivitas yang optimal dalam memberikan efek jera kepada pelanggar. [46]

Data pribadi yang bersifat spesifik mencakup informasi yang memiliki tingkat sensitivitas tinggi, seperti data kesehatan, data biometrik, data genetika, data keuangan, serta data lain yang berkaitan langsung dengan kondisi pribadi seseorang. Karakteristik data tersebut menjadikannya memiliki tingkat kerentanan yang lebih tinggi terhadap penyalahgunaan apabila tidak dikelola dan dilindungi secara memadai. Meskipun demikian, pengaturan yang ada masih bersifat umum

---

[44] Efendi, *op.cit*. hlm. 260.

[45] Muhammad Alkirom Wildan et al., *Menuju Masa Depan Digital: Peran Manajemen Sumber Daya Manusia Dalam Mendorong Kreativitas Dan Inovasi Industri Pariwisata Halal Madura Pada Era Industri 4.0* (Indramayu: Penerbit Adab, 2024). hlm. 11-19.

[46] Rosadi, *Pembahasan UU Pelindungan data pribadi yang bersifat spesifik (UU RI No. 27 Tahun 2022)*. hlm. 25-40.

dan belum secara komprehensif memberikan standar perlindungan yang lebih ketat terhadap data pribadi yang bersifat spesifik, terutama dalam konteks pemrosesan data di ekosistem digital yang ditandai oleh tingginya intensitas pengumpulan, penyimpanan, dan pertukaran data.

Kondisi tersebut menunjukkan bahwa kerangka hukum perlindungan data pribadi yang bersifat spesifik yang berlaku saat ini masih memerlukan penguatan, khususnya dalam menjamin keamanan dan kerahasiaan data pribadi yang bersifat spesifik. Dalam praktiknya, berbagai kasus kebocoran dan penyalahgunaan data menunjukkan bahwa data yang bersifat sensitif seringkali tidak memperoleh perlakuan perlindungan yang berbeda dengan data pribadi yang bersifat umum. Hal ini mengindikasikan bahwa mekanisme pengaturan, pengawasan, dan penegakan hukum terhadap pengelolaan data pribadi yang bersifat spesifik belum berjalan secara optimal. Padahal, karakteristik data yang bersifat sensitif menuntut adanya standar perlindungan yang lebih ketat guna mencegah terjadinya penyalahgunaan yang dapat merugikan pemilik data.

Penguatan pengaturan mengenai klasifikasi data pribadi yang bersifat spesifik sebagaimana diatur dalam Pasal 4 ayat (2) UU PDP harus diiringi dengan jaminan terhadap pemenuhan hak-hak subjek data. UU PDP melalui Pasal 28 hingga Pasal 32 telah mengatur berbagai hak subjek data, antara lain hak untuk mengakses, memperbaiki, serta menghapus data pribadi yang berada dalam penguasaan pengendali data. Pengaturan tersebut dimaksudkan untuk memberikan kendali kepada pemilik data atas informasi pribadi yang dimilikinya. Namun dalam praktiknya, implementasi hak-hak tersebut masih menghadapi berbagai kendala,

terutama berkaitan dengan keterbatasan mekanisme pengawasan serta rendahnya tingkat kepatuhan penyelenggara sistem elektronik dalam memenuhi kewajiban mereka terhadap pemilik data. Kondisi ini menunjukkan bahwa pengakuan normatif terhadap hak subjek data belum sepenuhnya diikuti oleh mekanisme perlindungan yang efektif, khususnya terhadap data pribadi yang bersifat spesifik yang memiliki tingkat sensitivitas dan risiko penyalahgunaan yang lebih tinggi.

Efektivitas perlindungan data pribadi yang bersifat spesifik juga sangat dipengaruhi oleh keberadaan mekanisme penegakan hukum yang mampu memberikan efek jera terhadap pelanggaran. UU PDP telah mengatur sanksi administratif dalam Pasal 58 hingga Pasal 64 bagi pihak yang melanggar ketentuan pengelolaan data pribadi. Meskipun demikian, penerapan sanksi tersebut dalam praktik masih menghadapi berbagai tantangan, baik dari aspek pengawasan maupun dari sisi efektivitas pemberian sanksi dalam mencegah terjadinya pelanggaran yang serupa di masa mendatang. Kondisi tersebut menunjukkan bahwa sistem penegakan hukum terhadap pelanggaran data pribadi masih memerlukan penguatan, terutama dalam memberikan perlindungan yang lebih optimal terhadap data pribadi yang bersifat spesifik yang memiliki tingkat kerentanan lebih tinggi dibandingkan dengan data pribadi yang bersifat umum.

Kebutuhan untuk memperkuat sistem perlindungan data pribadi yang bersifat spesifik tersebut menunjukkan pentingnya rekonstruksi hukum yang berfokus pada perlindungan data pribadi yang bersifat spesifik di era digital. Rekonstruksi hukum diarahkan pada penyempurnaan norma yang berkaitan dengan klasifikasi data pribadi sebagaimana diatur dalam Pasal 4 ayat (2) UU PDP, yang didukung oleh

penguatan jaminan hak-hak subjek data sebagaimana diatur dalam Pasal 28 hingga Pasal 32 serta efektivitas penerapan sanksi administratif sebagaimana diatur dalam Pasal 58 hingga Pasal 64.[47] Rekonstruksi hukum terhadap ketentuan-ketentuan tersebut sangat mendesak dilakukan karena regulasi yang ada saat ini masih memiliki celah normatif yang belum mampu memberikan perlindungan berkeadilan bagi subjek data di tengah disrupsi teknologi digital. Pertama, rekonstruksi Pasal 4 ayat (2) diperlukan karena klasifikasi data spesifik saat ini cenderung kaku (limitatif) dan belum proaktif mengantisipasi munculnya varian data sensitif baru akibat konvergensi teknologi terkini. Kedua, penyempurnaan Pasal 28 hingga Pasal 32 krusial untuk mengatasi ketimpangan relasi kuasa antara masyarakat dan Pengendali Data, di mana eksekusi hak-hak subjek data praktiknya sering dihalangi oleh prosedur teknis yang manipulatif (*illusion of consent*). Terakhir, rekonstruksi sanksi administratif pada Pasal 58 hingga Pasal 64 dibutuhkan untuk mengubah orientasi penegakan hukum dari sekadar sanksi retributif yang menyetorkan denda ke kas negara, menjadi pendekatan keadilan restoratif berdasarkan nilai-nilai Pancasila yang secara nyata menjamin mekanisme ganti rugi dan pemulihan langsung bagi korban kebocoran data.

[47] Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Pasal 4 ayat (2) mengklasifikasikan data pribadi yang bersifat spesifik meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai ketentuan peraturan perundang-undangan. Selanjutnya, jaminan hak-hak subjek data diatur secara komprehensif dalam Pasal 28 hingga Pasal 32, yang mencakup hak untuk mendapatkan informasi yang jelas, hak melengkapi dan memperbarui, hak mengakses, hak menghapus atau memusnahkan data, serta hak untuk menarik kembali persetujuan pemrosesan data yang telah diberikan. Adapun Pasal 58 hingga Pasal 64 memuat regulasi mengenai pengenaan sanksi administratif atas pelanggaran pemrosesan data, dengan tingkatan sanksi yang membentang dari peringatan tertulis, penghentian sementara kegiatan pemrosesan, penghapusan atau pemusnahan data, hingga sanksi berupa denda administratif.

Rekonstruksi tersebut perlu diselaraskan dengan nilai-nilai keadilan berdasarkan Pancasila, sehingga perlindungan data pribadi yang bersifat spesifik tidak hanya dipahami sebagai persoalan teknis dalam tata kelola data digital, tetapi juga sebagai bentuk penghormatan terhadap martabat manusia dan hak privasi setiap warga negara. Dengan demikian, penelitian ini berangkat dari adanya kesenjangan antara pengaturan normatif mengenai perlindungan data pribadi yang bersifat spesifik dengan realitas implementasinya dalam praktik, sehingga diperlukan rekonstruksi hukum yang lebih komprehensif, adaptif, dan berkeadilan berdasarkan Pancasila.

B. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana inefektivitas perlindungan data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital?
2. Bagaimana kebijakan perlindungan hukum terhadap data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital?
3. Bagaimana rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik terhadap perkembangan teknologi di era digital yang sesuai dengan nilai-nilai keadilan berdasarkan Pancasila?

C. Tujuan Penelitian

Tujuan dari penelitian ini yaitu:

1. Untuk mengkaji inefektivitas perlindungan data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital.

2. Untuk mengkaji kebijakan perlindungan hukum terhadap data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital.
3. Untuk mengkaji rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik terhadap perkembangan teknologi di era digital yang sesuai dengan nilai-nilai keadilan berdasarkan Pancasila.

D. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini akan memberikan pemahaman tentang interaksi antara teknologi dan hukum, khususnya dalam mengatasi tantangan perlindungan data pribadi yang bersifat spesifik dan privasi konsumen di era digital. Ini akan memperkaya literatur hukum dengan analisis kerangka regulasi yang ada dan reformasi yang diperlukan, serta meningkatkan pemahaman tentang faktor-faktor yang mempengaruhi efektivitas implementasi undang-undang perlindungan data, seperti Undang-Undang Pelindungan data pribadi yang bersifat spesifik Indonesia, memperkuat dasar teoritis untuk pengembangan hukum yang lebih responsif dan adaptif terhadap inovasi teknologi.

2. Manfaat Praktis

Penelitian ini diperuntukan kepada regulator dalam merumuskan kebijakan perlindungan data pribadi yang bersifat spesifik yang responsif serta menjadi referensi bagi sektor publik dan swasta. Selain itu, hasil penelitian dapat mendukung pengembangan kurikulum hukum siber, meningkatkan literasi hukum digital, dan memberikan rekomendasi berbasis

bukti bagi pembuat kebijakan. Penelitian ini juga bertujuan membantu regulator, akademisi, dan praktisi hukum dalam menyusun strategi penegakan hukum yang lebih komprehensif untuk melindungi hak privasi warga negara.

E. Keaslian Penelitian

Berdasarkan hasil pencarian melalui media internet (*searching*) mengenai tema penilitian yang akan peneliti angkat dalam penulisan disertasi ini yaitu tentang "Rekonstruksi Hukum Pelindungan data pribadi yang bersifat spesifik di Era Digital untuk Mewujudkan Keadilan Berdasarkan Pancasila" peneliti tidak menemukan judul yang sama dengan yang akan peneliti tulis. Namun, peneliti menemukan beberapa penelitian terdahulu yang terkait dengan perlindungan data pribadi yang bersifat spesifik dan regulasi di era digital. Beberapa di antaranya adalah:

1. Disertasi Mohammad Wira Utama. Rekonstruksi Regulasi Pelindungan data pribadi yang bersifat spesifik bagi Nasabah Perbankan yang Berbasis Nilai Keadilan. Program Doktor Ilmu Hukum, Universitas Islam Sultan Agung (UNISSULA), Semarang, 2024.

   Bahwa adapun rumusan masalah yang diangkat adalah :

   1. Mengapa regulasi perlindungan data pribadi yang bersifat spesifik bagi nasabah perbankan belum berbasis nilai keadilan?
   2. Bagaimana kelemahan-kelemahan regulasi perlindungan data pribadi yang bersifat spesifik bagi nasabah perbankan pada saat ini?
   3. Bagaimana rekonstruksi regulasi perlindungan data pribadi yang bersifat spesifik bagi nasabah perbankan yang berbasis nilai keadilan?

2. Disertasi Andi Widiatno Hummerson. Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Pengendali Dan Prosesor Terhadap Kebocoran Data Pribadi Di Indonesia. Program Studi Doktor Hukum Universitas Tarumanagara, 2023.

   Bahwa adapun rumusan masalah yang diangkat adalah :

   a. Bagaimana klasifikasi subjek-subjek hukum dalam peraturan mengenai data pribadi di peraturan perundang-undangan Indonesia?
   b. Apa bentuk tanggung jawab hukum Penyelenggara Sistem Elektronik, Pengendali, dan Prosesor berkaitan dengan kebocoran data pribadi menurut peraturan perundang-undangan di Indonesia?
   c. Bagaimana model tanggung jawab hukum bagi Penyelenggara Sistem Elektronik, Pengendali, dan Prosesor data pribadi terhadap kebocoran data pribadi di Indonesia?

3. Disertasi Abdul Halim Barkatullah. Pelindungan Hukum Bagi Konsumen dalam Transaksi E-Commerce Lintas Negara di Indonesia. Program Doktor Ilmu Hukum, Universitas Islam Indonesia, Yogyakarta, 2006.

   Bahwa adapun rumusan masalah yang diangkat adalah :

   a. Mengapa konsumen dalam transaksi *e-commerce* lintas negara secara hukum berada dalam posisi tawar yang lemah?
   b. Apakah peraturan perlindungan hukum bagi konsumen dalam hukum nasional dan internasional telah memberikan jaminan bagi konsumen dalam transaksi *e-commerce* lintas negara?

c. Bentuk perlindungan hukum apa yang dapat ditawarkan bagi konsumen dalam transaksi *e-commerce* lintas negara di Indonesia?

F. Kerangka Teori

Kerangka teori dalam penelitian ini berfungsi sebagai landasan konseptual dalam menganalisis dan mengembangkan rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik di Indonesia. Dalam kajian hukum, pendekatan teoritis yang digunakan menjadi fondasi dalam memahami persoalan serta merumuskan solusi yang tepat terhadap tantangan hukum yang ada. Oleh karena itu, penelitian ini menggunakan tiga pendekatan teori yang relevan, yaitu *Grand Theory* (Teori Keadilan Pancasila), *Middle Range Theory* (Teori Perlindungan Hukum), dan *Applied Theory* (Teori Hukum Pembangunan).

1. Teori Keadilan Pancasila

Teori keadilan yang digunakan dalam penelitian ini adalah Teori Keadilan Pancasila. Pemilihan teori ini didasarkan pada karakter penelitian yang tidak hanya membahas perlindungan data pribadi sebagai persoalan normatif dalam hukum positif, tetapi juga menempatkannya sebagai bagian dari penghormatan terhadap martabat manusia, hak asasi warga negara, tanggung jawab negara, dan keadilan sosial dalam kehidupan berbangsa. Keadilan Pancasila dipandang sebagai teori yang paling relevan karena lahir dari nilai dasar bangsa Indonesia dan memuat keseimbangan antara hak individu, kepentingan masyarakat, kewajiban negara, serta tanggung jawab sosial dalam penyelenggaraan kehidupan hukum.[48]

[48] Yudi Latif, *Negara Paripurna: Historisitas, Rasionalitas, dan Aktualitas Pancasila* (Jakarta: Gramedia Pustaka Utama, 2011), hlm. 41–46.

Keadilan Pancasila tidak dapat dipahami secara terpisah dari lima sila yang membentuk satu kesatuan nilai. Sila Ketuhanan Yang Maha Esa memberikan landasan moral bahwa pengelolaan data pribadi harus dijalankan secara jujur, bertanggung jawab, dan tidak merugikan martabat manusia. Sila Kemanusiaan yang Adil dan Beradab menegaskan bahwa setiap orang memiliki hak untuk dihormati kehormatan, privasi, dan integritas dirinya. Sila Persatuan Indonesia menempatkan perlindungan data pribadi sebagai bagian dari ketahanan sosial dan keamanan nasional di era digital. Sila Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan menghendaki adanya tata kelola data yang transparan, akuntabel, dan melibatkan kepentingan subjek data. Sila Keadilan Sosial bagi Seluruh Rakyat Indonesia menegaskan bahwa perlindungan data pribadi harus memberikan manfaat yang setara, termasuk bagi kelompok masyarakat yang rentan secara sosial, ekonomi, dan teknologi.[49]

Soekarno memandang Pancasila sebagai dasar filosofis negara yang digali dari kepribadian dan pengalaman hidup bangsa Indonesia. Gagasan Soekarno mengenai gotong royong menunjukkan bahwa Pancasila tidak hanya berisi nilai individual, tetapi juga nilai sosial yang menuntut tanggung jawab bersama dalam membangun kehidupan bangsa.[50] Dalam konteks perlindungan data pribadi, semangat gotong royong dapat dimaknai sebagai kewajiban kolektif antara negara, pengendali data, prosesor data, pelaku usaha digital, dan masyarakat untuk menciptakan ekosistem digital yang aman. Perlindungan data pribadi tidak dapat

[49] Notonagoro, *Pancasila Secara Ilmiah Populer* (Jakarta: Pantjuran Tujuh, 1980), hlm. 39–44.

[50] Soekarno, *Lahirnya Pancasila* (Jakarta: Departemen Penerangan Republik Indonesia, 1947), hlm. 19–22.

hanya dibebankan kepada subjek data, sebab posisi subjek data sering kali lebih lemah dibandingkan penyelenggara sistem elektronik yang menguasai teknologi, infrastruktur, dan informasi.

Pemikiran Mohammad Hatta memperdalam dimensi keadilan Pancasila melalui gagasan demokrasi yang tidak berhenti pada demokrasi politik, tetapi juga mencakup demokrasi ekonomi dan demokrasi sosial. Hatta menegaskan bahwa demokrasi Indonesia harus menjamin kedaulatan rakyat, penghormatan hak, dan keadilan sosial dalam kehidupan nyata.[51] Sri Soeprapto menjelaskan bahwa dalam pemikiran Hatta, Pancasila merupakan norma etis yang menuntut negara untuk menjamin hak kemanusiaan, penghidupan yang layak, persatuan dalam keberagaman, permusyawaratan, serta keadilan politik dan ekonomi.[52] Pemikiran ini relevan untuk membaca persoalan perlindungan data pribadi, karena relasi antara subjek data dengan pengendali data sering kali bersifat tidak seimbang. Subjek data membutuhkan perlindungan agar tidak menjadi objek eksploitasi ekonomi dalam industri digital.

Soepomo memberikan kontribusi penting melalui pemikiran negara integralistik yang menekankan persatuan, kekeluargaan, dan keterikatan antara negara dengan rakyat. Pemikiran ini perlu dibaca secara kritis dalam kerangka negara hukum modern agar tidak meniadakan hak individu, tetapi tetap menegaskan tanggung jawab negara untuk menjaga kepentingan seluruh rakyat.[53] Dalam

[51] Mohammad Hatta, *Demokrasi Kita* (Djakarta: Pustaka Antara, 1966), hlm. 8–11.

[52] Sri Soeprapto, "Konsep Muhammad Hatta tentang Implementasi Pancasila dalam Perspektif Etika Pancasila," *Jurnal Filsafat* 23, no. 2 (2013): hlm. 99–116.

[53] Agus Sutono, Fuad Noorzeha, dan Supriyono Purwosaputro, "Konsep Negara Integral Soepomo dan Relevansinya pada Penerapan Konstitusi di Indonesia Tahun 2024," *PACIVIC: Jurnal Pendidikan Pancasila dan Kewarganegaraan* 5, no. 1 (2025): hlm. 39–42.

perlindungan data pribadi, negara tidak boleh hanya menjadi pembentuk norma, tetapi juga harus hadir sebagai pengawas, pelindung, dan pemulih hak korban. Negara yang berlandaskan Pancasila harus memastikan bahwa kepentingan pembangunan teknologi tidak mengorbankan hak privasi warga negara.

Yudi Latif menempatkan Pancasila sebagai dasar negara, pandangan hidup, dan ideologi yang memiliki kemampuan untuk menyatukan nilai religiusitas, kebangsaan, kemanusiaan, demokrasi, dan keadilan sosial. Pancasila tidak hanya dipahami sebagai doktrin normatif, tetapi juga sebagai bintang penuntun dalam penyelenggaraan kehidupan publik.[54] Dalam masyarakat digital, Pancasila harus diaktualisasikan dalam kebijakan yang mampu menjawab perkembangan teknologi, termasuk dalam pengaturan data pribadi yang bersifat spesifik. Data kesehatan, biometrik, genetika, keuangan, data anak, dan catatan kejahatan merupakan informasi yang melekat langsung pada martabat pribadi seseorang. Penyalahgunaan terhadap jenis data tersebut dapat menimbulkan kerugian yang tidak hanya bersifat materiil, tetapi juga psikologis, sosial, dan moral.

Franz Magnis-Suseno menekankan bahwa keadilan dalam kehidupan bernegara selalu berkaitan dengan legitimasi moral kekuasaan, penghormatan hak asasi manusia, dan tanggung jawab sosial negara.[55] Kekuasaan negara memperoleh dasar etis apabila digunakan untuk melindungi manusia dari tindakan sewenang-wenang, termasuk tindakan penyalahgunaan data pribadi oleh pihak yang memiliki kekuatan ekonomi dan teknologi. Pemikiran ini memperkuat posisi Keadilan

---

[54] Yudi Latif, "Identitas Keindonesiaan dan Aktualisasi Pancasila bagi Generasi Milenial di Era Digital," *Jurnal Lemhannas RI* 6, no. 1 (2018): hlm. 5–19.

[55] Franz Magnis-Suseno, *Etika Politik: Prinsip-Prinsip Moral Dasar Kenegaraan Modern* (Jakarta: Gramedia Pustaka Utama, 2016), hlm. 143–180 dan 407–423.

Pancasila sebagai teori yang tidak semata-mata melihat hukum sebagai teks peraturan, tetapi juga sebagai sarana etis untuk menjaga martabat manusia.

Keadilan Pancasila dalam penelitian ini digunakan sebagai pisau analisis untuk menilai apakah hukum perlindungan data pribadi yang bersifat spesifik telah memenuhi tiga ukuran utama. Pertama, perlindungan hukum harus menghormati martabat manusia sebagai subjek data. Ukuran ini berkaitan dengan pengakuan bahwa data pribadi bukan sekadar komoditas ekonomi, melainkan bagian dari identitas dan kehormatan individu. Kedua, perlindungan hukum harus menjamin keseimbangan antara inovasi digital dan hak warga negara. Ukuran ini penting karena pembangunan ekonomi digital tidak boleh mengabaikan keamanan, privasi, dan kendali subjek data atas informasi pribadinya. Ketiga, perlindungan hukum harus menyediakan mekanisme pemulihan yang adil bagi korban pelanggaran data pribadi. Keadilan tidak cukup diwujudkan melalui sanksi administratif atau pidana, tetapi juga melalui pemulihan hak korban secara nyata.

Teori Keadilan Pancasila juga digunakan untuk menganalisis urgensi perlindungan data pribadi yang bersifat spesifik akibat perkembangan teknologi digital. Perkembangan teknologi telah meningkatkan kapasitas pengumpulan, penyimpanan, pengolahan, dan penyebaran data pribadi dalam skala besar. Keadaan ini menimbulkan risiko baru berupa kebocoran data, pencurian identitas, pemprofilan digital, diskriminasi algoritmik, intimidasi berbasis data, serta eksploitasi ekonomi terhadap subjek data. Dalam perspektif Keadilan Pancasila, risiko tersebut menunjukkan adanya ancaman terhadap sila kemanusiaan dan sila

keadilan sosial, karena subjek data dapat kehilangan kendali atas dirinya sendiri di hadapan sistem digital yang tidak transparan.

Kebijakan hukum yang adil menurut Pancasila harus menempatkan subjek data sebagai pusat perlindungan, bukan sekadar objek pengolahan data. Oleh karena itu, setiap pengaturan mengenai persetujuan, hak akses, hak koreksi, hak penghapusan, kewajiban pengendali data, penilaian dampak perlindungan data, keamanan sistem, dan pemberitahuan kegagalan perlindungan data harus diarahkan pada perlindungan hak warga negara. Kebijakan hukum yang hanya menekankan kepatuhan administratif tanpa menjamin pemulihan korban belum sepenuhnya mencerminkan Keadilan Pancasila.

Rekonstruksi hukum tidak hanya diarahkan pada perubahan norma dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, tetapi juga pada pembaruan struktur kelembagaan dan budaya hukum. Substansi hukum perlu diperkuat dengan pengaturan yang lebih jelas mengenai standar perlindungan data spesifik, mekanisme persetujuan eksplisit, larangan penyalahgunaan data, kewajiban penilaian risiko, dan hak pemulihan bagi korban. Struktur hukum perlu diperkuat melalui pembentukan lembaga pengawas independen yang memiliki kewenangan efektif. Budaya hukum perlu dibangun melalui peningkatan literasi digital, kesadaran masyarakat, dan kepatuhan pelaku usaha dalam memperlakukan data pribadi sebagai hak asasi manusia.

Keadilan Pancasila menuntut agar sanksi dalam pelanggaran data pribadi tidak hanya berorientasi pada penghukuman, tetapi juga pemulihan. Sanksi administratif, denda, penghentian pemrosesan, penghapusan data, dan sanksi

pidana harus ditempatkan dalam kerangka perlindungan korban. Korban kebocoran atau penyalahgunaan data pribadi perlu memperoleh akses terhadap informasi, pengaduan, pembuktian, kompensasi, dan pemulihan nama baik. Dengan demikian, keadilan yang diwujudkan bukan hanya keadilan formal, tetapi juga keadilan substantif yang dirasakan langsung oleh subjek data.

Keadilan Pancasila juga menghendaki perlindungan khusus bagi kelompok rentan. Anak, penyandang disabilitas, pasien, konsumen jasa keuangan, pengguna layanan digital dengan literasi rendah, dan masyarakat yang bergantung pada layanan publik elektronik berada dalam posisi yang lebih mudah dirugikan apabila data pribadinya disalahgunakan. Perlindungan terhadap kelompok tersebut merupakan perwujudan sila Kemanusiaan yang Adil dan Beradab serta sila Keadilan Sosial bagi Seluruh Rakyat Indonesia. Regulasi yang adil harus mampu memberikan perlakuan proporsional sesuai tingkat risiko, bukan hanya perlakuan yang sama secara formal.

Teori Keadilan Pancasila dalam penelitian ini berfungsi sebagai dasar filosofis, kerangka evaluatif, dan pisau analisis untuk menilai serta merekonstruksi hukum perlindungan data pribadi yang bersifat spesifik. Teori ini digunakan untuk menguji apakah pengaturan hukum yang berlaku telah menghormati martabat manusia, memberikan kepastian hukum, menjamin kemanfaatan, melindungi kelompok rentan, menguatkan tanggung jawab negara, serta menyediakan pemulihan yang adil bagi korban. Melalui teori ini, rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik diarahkan untuk membangun sistem hukum yang tidak hanya adaptif terhadap perkembangan teknologi, tetapi

juga berakar pada nilai Ketuhanan, kemanusiaan, persatuan, permusyawaratan, dan keadilan sosial.

2. Teori Perlindungan Hukum

Teori perlindungan hukum lahir dari kebutuhan untuk memberikan pengakuan dan jaminan terhadap hak-hak dasar warga negara. Konsep ini bertumpu pada prinsip keadilan, kepastian hukum, dan kemanfaatan. Raharjo menjelaskan bahwa perlindungan hukum bertujuan untuk mengayomi masyarakat agar dapat menikmati hak-hak mereka secara adil sesuai dengan ketentuan hukum yang berlaku.[56] Perlindungan hukum didasarkan pada aliran hukum alam yang dipelopori oleh Plato, dan Aristoteles dimana aliran ini menekankan bahwa hukum bersumber dari Tuhan dan bersifat universal, sehingga hukum dan moral tidak dapat dipisahkan.[57] Dalam pandangan ini, perlindungan hukum menjadi manifestasi dari aturan moral yang mengatur hubungan antarindividu dan antara individu dengan negara. Pandangan ini masih relevan dalam pengaturan perlindungan hukum modern yang mengedepankan keadilan substantif.

Teori perlindungan hukum berakar pada kebutuhan untuk menjamin pengakuan dan perlindungan atas hak-hak dasar warga negara. Hadjon menjelaskan bahwa perlindungan hukum memiliki dua bentuk utama, yaitu perlindungan preventif yang bertujuan mencegah tindakan sewenang-wenang sebelum pelanggaran terjadi, dan perlindungan represif yang memberikan pemulihan setelah

[56] Syaharie Jaang, "Analisis Pelindungan Hukum Terhadap Konsumen Berdasarkan Prinsip Keadilan," *Jurnal Hukum Dan HAM Wara Sains* 2, no. 05 (2023), hlm. 349–357.

[57] Wahyu Simon Tampubolon, "Upaya Pelindungan Hukum Bagi Konsumen Ditinjau Dari Undang Undang Pelindungan Konsumen," *Jurnal Ilmiah Advokasi* 4, no. 1 (2016), hlm. 53–61.

pelanggaran terjadi.[58] Rahardjo menambahkan bahwa perlindungan hukum harus berpihak pada kelompok masyarakat lemah dengan mengedepankan prinsip keadilan sosial dan memberikan rasa aman.[59] Menurut Kusumaatmadja, hukum sebagai alat pembaharuan masyarakat harus memastikan ketertiban serta mendorong pembangunan dengan tetap menjunjung tinggi keadilan dan kepastian hukum[60].

Perlindungan hukum di Indonesia memiliki dasar konstitusional yang kuat. Pasal 1 ayat (3) UUD 1945 menegaskan bahwa Indonesia adalah negara hukum, sehingga setiap kebijakan dan tindakan pemerintah harus berdasarkan prinsip hukum yang melindungi hak-hak warga negara. Indrati menggarisbawahi bahwa perundang-undangan adalah instrumen utama untuk mewujudkan perlindungan hukum[61], sementara Asshiddiqie menekankan pentingnya supremasi konstitusi dalam menjamin hak asasi manusia dan keadilan sosial[62]. Dalam konteks yang lebih luas, Achmad Ali menyatakan bahwa perlindungan hukum harus mengintegrasikan nilai moral dan budaya lokal untuk menciptakan sistem hukum yang inklusif dan responsif terhadap kebutuhan masyarakat.[63]

---

[58] Philipus M Hadjon, *Pelindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara* (Bina Ilmu, 1987). hlm. 110.

[59] Satjipto Rahardjo, *Biarkan Hukum Mengalir: Catatan Kritis Tentang Pergulatan Manusia Dan Hukum* (Penerbit Buku Kompas, 2007). hlm. 20.

[60] Mochtar Kusumaatmadja, *Konsep-Konsep Hukum Dalam Pembangunan* (Bandung: PT. Alumni Penerbit Akademik, 2002). hlm. 45.

[61] Maria Farida Indrati Soeprapto, *Ilmu Perundang-Undangan 2: Proses Dan Teknik Penyusunan* (Yogyakarta: PT Kanisius, 2018). hlm. 8.

[62] Jimly Asshiddiqie, *Konstitusi Dan Konstitusionalisme Indonesia* (Bengkulu: Sinar Grafika, 2021). hlm. 131.

[63] Achmad Ali, *Menguak Teori Hukum Dan Teori Peradilan.* (Jakarta: Kencana, 2012). hlm. 75.

Indonesia sebagai negara hukum meletakkan perlindungan hukum sebagai elemen esensial dalam konstitusinya. Pasal 1 Ayat (3) UUD 1945 menyatakan bahwa Indonesia adalah negara hukum, yang berarti setiap kebijakan dan tindakan pemerintah harus berdasarkan hukum.[64] Perlindungan hukum menjadi bagian dari upaya negara untuk menjamin hak-hak dasar warganya, termasuk perlindungan dari tindakan diskriminatif atau eksploitatif yang dapat merugikan individu atau kelompok tertentu. Dalam konteks negara hukum, perlindungan ini mencerminkan pengakuan terhadap harkat dan martabat manusia sebagai individu. Dalam hubungannya dengan hukum positif, perlindungan ini menjadi kewajiban negara untuk memberikan rasa aman dan keadilan bagi setiap warganya.

Teori perlindungan hukum yang dikembangkan oleh Philipus M. Hadjon menekankan pentingnya keberadaan hukum yang memberikan perlindungan kepada individu dari tindakan pemerintah yang sewenang-wenang. Menurut Hadjon, perlindungan hukum dapat dibagi menjadi dua bentuk: perlindungan preventif dan perlindungan represif. Perlindungan preventif bertujuan untuk mencegah terjadinya pelanggaran hak-hak individu, sedangkan perlindungan represif bertujuan untuk memberikan solusi atau pemulihan setelah terjadi pelanggaran hak.[65]

Perlindungan hukum sebagian besar terdiri dari membuat undang-undang yang melindungi orang, termasuk klien dari kejadian yang tidak terduga. Paradigma ini menekankan, mencakup kebijakan pencegahan dan penindasan, ide-

---

[64] Ismail Koto et al., "Pelindungan Hukum Atas Kekayaan Intelektual Perspektif Hukum Islam," *Jurnal Yuridis* Vol. 10 No. 2 (2023), hlm. 66–73.

[65] M Hadjon Philipus, *Pelindungan Hukum Bagi Rakyat Indonesia*, (Surabaya*:* Bina Ilmu, 1987), hlm. 25.

ide hukum tentang keadilan, utilitas, dan kepastian. Sementara asuransi represif membayar setelah kejadian, asuransi preventif mengurangi kerugian klien dengan kontrol. Hukum melindungi konsumen dari praktik bisnis yang tidak adil dan menjamin tanggung jawab di antara pemilik perusahaan. Melalui perlindungan konsumen, keterbukaan, dan peningkatan kualitas produk dan layanan, hukum berusaha menyeimbangkan hak konsumen dengan kewajiban perusahaan. Konsep ini mendukung ketertiban sosial dengan menawarkan kerangka hukum yang fleksibel yang sesuai untuk kemajuan masyarakat dan kebutuhan komunitas.[66]

Regulasi perlindungan hukum harus mampu beradaptasi dengan kemajuan teknologi untuk menjamin kepastian hukum bagi masyarakat. Layanan digital seperti pendaftaran tanah dengan daring di Indonesia menghadapi berbagai tantangan hukum, terutama dalam memastikan keandalan informasi dan kepastian hukum dalam layanan berbasis digital.[67] Hal ini memperkuat argumen bahwa regulasi di era digital harus mengakomodasi perubahan teknologi dan memastikan perlindungan hak-hak individu, termasuk data pribadi. Pentingnya nilai keadilan dalam kerangka perlindungan hukum, khususnya terkait dengan kekayaan intelektual dalam perspektif hukum Islam.[68] Keamanan data adalah area lain dimana ide ini diterapkan karena hak pengguna harus dihormati dan dilindungi. Teori menengah bahwa regulasi data pribadi harus tidak hanya adaptif terhadap teknologi dan sesuai dengan universal.

---

[66] Farid Wajdi dan Diana Susanti, *Hukum Pelindungan Konsumen* (Malang: Setara Press, 2023). hlm. 27-28.

[67] Farid Wajdi dan Rahmat Ramadhani, "Legal Problems of Ldan Services Online," *International Journal Reglement & Society (IJRS)* Vol. 3 No. 1. (April, 2022), hlm. 19–29.

[68] Ismail Koto et al., *loc.cit*.

Perlindungan hukum konsumen menjadi salah satu aspek penting dalam teori perlindungan hukum. Hukum harus memberikan perlindungan preventif dan represif terhadap konsumen, terutama dalam menghadapi praktik bisnis yang tidak adil.[69] Perlindungan preventif berfokus pada pengawasan regulasi, sementara perlindungan represif mencakup penanganan sengketa melalui pengadilan atau mekanisme non-litigasi seperti mediasi. Perlindungan hukum atas juga menjadi aspek penting dala hak kekayaan intelektual. Perlindungan hukum dalam hak kekayaan intelektual bertujuan untuk melindungi hak eksklusif pencipta dan hak kekayaan intelektual memberikan kontribusi signifikan terhadap pertumbuhan ekonomi dan mendorong kreativitas.[70] Penerapan hukum HKI memerlukan pendekatan yang lebih inklusif dengan menginternalisasi nilai-nilai lokal seperti Pancasila.

Islam menawarkan perlindungan hukum normatif melalui *hifz al-mal* (perlindungan harta) dan *'adl* (keadilan). Di bawah hukum positif, ide ini berhubungan dengan perlindungan hak kekayaan intelektual. Dirancang untuk mencapai keseimbangan antara hak pribadi dan komunitas, perlindungan ini mencakup hak cipta, paten, dan Dagang. Perlindungan hukum preventif berfokus pada bagaimana aturan dan pengawasan membantu menghindari kekhawatiran konsumen. Tampubolon menjelaskan bahwa pendekatan ini bertujuan untuk memastikan kepatuhan terhadap hukum sebelum timbulnya sengketa.[71]

---

[69] Wahyu Simon Tampubolon, *loc.cit*.
[70] Ismail Koto et al., *loc.cit.*
[71] Yamin et al., *loc.cit*.

Pendekatan ini memerlukan koordinasi antara pemerintah, masyarakat, dan sektor swasta untuk menciptakan ekosistem yang aman dan transparan. Pendekatan represif dilakukan setelah terjadinya pelanggaran dengan tujuan memberikan sanksi yang setimpal. Penelitian Hidayat menunjukkan bahwa mekanisme litigasi dan non-litigasi dapat digunakan untuk menyelesaikan sengketa secara adil.[72] Dalam konteks konsumen, pendekatan ini memastikan bahwa hak-hak konsumen terlindungi dan pelanggar mendapatkan hukuman sesuai peraturan yang berlaku.

Nilai-nilai Pancasila memberikan kerangka filosofis yang unik dalam perlindungan hukum di Indonesia. Pentingnya menginternalisasi nilai-nilai Pancasila dalam regulasi hukum agar lebih inklusif dan adil. Hal ini mencakup pengakuan terhadap keragaman budaya dan kearifan lokal yang menjadi karakteristik masyarakat Indonesia.[73] Ekonomi digital membawa tantangan baru dalam perlindungan hukum, terutama dalam aspek perlindungan data pribadi. Penelitian Justisia menekankan pentingnya regulasi yang melindungi data individu dari eksploitasi komersial.[74] Perlindungan ini menjadi penting untuk menciptakan kepercayaan dalam transaksi digital.

3. Teori Hukum Pembangunan

Teori Hukum Pembangunan yang dikemukakan oleh Mochtar Kusumaatmaja sampai ini adalah teori hukum eksis, yang dihasilkan oleh orang Indonesia berdasarkan dimensi dan budaya mereka. Inilah sebabnya teori hukum pembangunan telah terletak, tumbuh, dan berkembang sesuai dengan kondisi

[72] Wahyu Hidayat dan Agus Sarono, "Pelindungan Hukum Terhadap Konsumen Jasa Umroh/Haji Dalam Perbuatan Melawan Hukum," *Notarius* 15, no. 1 (2022), hlm. 283–295.
[73] Arkansyah, Nadirah, dan Arbas, *loc.cit*.
[74] Yamin et al., *loc.cit*.

Indonesia; jadi, jika diterapkan, teori ini akan sejalan dengan masyarakat Indonesia yang pluralistik. *The Pancasila principles serve as a reference framework for the way of life of the Indonesian society and nation based on the Pancasila principles that are familial in nature, and those norms, principles, institutions, and rules*.[75] Ketiga, pada dasarnya Teori Hukum Pembangunan memberikan dasar fungsi hukum sebagai "sarana pembaharuan masyarakat" [76] *(law as a tool social engeneering)* dan hukum sebagai suatu sistem sangat diperlukan bagi bangsa Indonesia sebagai negara yang sedang berkembang.[77]

Teori hukum pembangunan yang dikemukakan oleh para pakar hukum di Indonesia menempatkan hukum sebagai sarana pembaruan masyarakat (*law as a tool of social engineering*). Hukum berfungsi sebagai alat transformasi sosial yang mampu menciptakan ketertiban dan mendukung pembangunan nasional. [78]

---

[75] Lawrence W. Friedman, *American Law: An invaluable guide to the many faces of the law, dan how it affects our daily our daily lives,* W.W. Norton & Company, New York, 1984, hlm. 1-8. dan pada *Legal Culture dan Social Development,* Stanford Law Review, New York, hlm. 1002 - 1010 serta dalam *Law in America: a Short History,* Modern Library Chronicles Book, New York, 2002, hlm. 4 -7 menentukan pengertian struktur adalah, *"The structure of a system is its skeleton framework; it is the permanent shape, the institutional body of the system, the though rigid nones that keep the process flowing within bounds.",* kemudian substansi dirumuskan sebagai, *"The substance is composed of substantive rules dan rules about how institutions should behave,"* dan budaya hukum dirumuskan sebagai, *"The legal culture, system their beliefs, values, ideas dan expectation. Legal culture refers, then, to those ports of gener al culture customs, opinions ways of doing dan thinking that bend social forces toward from the law dan in particular ways."*

[76] Pada dasarnya, fungsi hukum sebagai "sarana pembaharuan masyarakat" *(law as a tool of social engeneering)* relative masih sesuai dengan pembangunan hukum nasional saat ini, namun perlu juga dilengkapi dengan pemberdayaan birokrasi (*beureucratic engineering*) yang mengedepankan konsep panutan atau kepemimpinan, sehingga fungsi hukum sebagai sarana pembaharuan dapat menciptakan harmonisasi antara elemen birokrasi dan masyarakat dalam satu wadah yang disebut " *beureucratic dan social engineering"* (BSE). Lihat Romli Atmasasmita , *Menata Kembali Masa Depan Pembangunan Hukum Nasional ,* Makalah disampaikan dalam "Seminar Pembangunan Hukum Nasional VIII" di Denpasar, 14 -18 Juli 2003, hlm. 7.

[77] Terhadap eksistensi Hukum sebagai suatu system dapat diteliti lebih detail dan terperinci pada: Lili Rasjidi dan Ida Bagus Wiyasa Putra, *Hukum Sebagai Suatu Sistem,* Penerbit: CV. Mandar Maju, Bandung, 2003, hlm. 5

[78] John Kenedi, *Buku Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia* (Pustaka Pelajar, 2017). hlm. 75.

Soedikno Mertokusumo mengemukakan bahwa hukum sebagai kaidah tidak hanya mengatur perilaku masyarakat, tetapi juga mendorong inovasi untuk menciptakan keteraturan hukum dalam pembangunan.[79] Peran hukum dalam mendorong perubahan sosial yang adaptif terhadap globalisasi, yang merupakan tantangan bagi pembangunan hukum di Indonesia.[80] Bernard Arief Sidharta menekankan pentingnya mengintegrasikan nilai-nilai lokal dengan norma global untuk memastikan regulasi yang relevan dan berkelanjutan.[81]

Hukum pembangunan juga berfungsi sebagai katalisator bagi pertumbuhan ekonomi. Erman Rajagukguk menjelaskan bahwa regulasi yang progresif dapat mempercepat pembangunan ekonomi dengan tetap menjaga keadilan sosial.[82] Hukum pembangunan harus fleksibel dan mendukung inovasi sosial serta ekonomi, dengan tetap berlandaskan pada keadilan substantif untuk menciptakan keteraturan dan mendorong transformasi sosial.[83] Hukum progresif tidak hanya bertumpu pada teks hukum, tetapi juga pada konteks sosial, menjadikannya alat yang dinamis untuk merespons tantangan zaman.[84] Hukum harus adaptif terhadap perubahan sosial dan teknologi untuk mendukung keberlanjutan pembangunan.[85]

---

[79] Mertokusumo Sudikno, "Mengenal Hukum Suatu Pengantar," *Yogyakarta: Liberty* (2005). hlm. 101.

[80] Lawrence M Friedman, *Sistem Hukum: Perspektif Ilmu Sosial* (Bandung: Nusamedia, 2019). hlm. 362.

[81] Bernard Arief Sidharta, "Refleksi Tentang Struktur Ilmu Hukum," *II Bandung: Mandar Maju* (2000). hlm. 89.

[82] Erman Rajagukguk, "Peranan Hukum Dalam Pembangunan Ekonomi," *Penerbit Universitas Indonesia Fakultas Hukum-Pascasarjana, Jakarta Pusat* (2017). hlm. 34.

[83] Asep Dedi Suwasta dan Ujuh Juhana, *Pengantar Ilmu Hukum* (Tohar Media, 2024). hlm. 69.

[84] D R Abu Yasid, *Logika Hukum: Dari Mazhab Rasionalisme Hukum Islam Hingga Positivisme Hukum Barat* (Saufa, 2016). hlm. 91.

[85] Rusdin Tahir et al., *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik* (Jambi: PT. Sonpedia Publishing Indonesia, 2023). hlm. 71.

Hukum pembangunan harus mencerminkan nilai-nilai lokal dan formal untuk menciptakan keseimbangan antara inovasi teknologi dan hak masyarakat.[86]

Teori hukum pembangunan juga memprioritaskan integrasi antara moralitas dan regulasi. Dimensi moralitas tidak boleh diabaikan dalam hukum pembangunan untuk memastikan keadilan substantif.[87] Pembaruan hukum harus berbasis pada kebutuhan masyarakat kontemporer untuk menghadapi tantangan teknologi modern. [88] Hukum pembangunan nasional harus mencerminkan pluralitas masyarakat Indonesia, menciptakan alat pemersatu dalam keberagaman.[89] Hukum pembangunan harus melindungi hak asasi manusia di tengah perubahan sosial yang cepat.[90] Pentingnya sifat antisipatif dalam hukum pembangunan, mengintegrasikan hukum tertulis dan tidak tertulis untuk menciptakan sistem hukum yang responsif terhadap kebutuhan masyarakat yang terus berkembang.[91]

Hukum dan masyarakat memberi tahu kita bahwa tujuan hukum adalah untuk mencapai tujuan tertentu. Kemudian, kepastian hukum harus ada dalam kehidupan masyarakat jika kita ingin mencapai ketertiban karena tanpa itu individu tidak dapat berkembang dalam keterampilan dan kemampuannya.

---

[86] Pandapotan Damanik, Satriya Nugraha, dan Fuad Nur, "Hukum Administrasi Negara: Teori, Prinsip, Dan Praktik Tata Kelola Pemerintahan" (PT. Media Penerbit Indonesia, 2024). hlm. 33.

[87] Andri Yanto, *Mazhab-Mazhab Hukum: Suatu Pengantar Memahami Dimensi Pemikiran Hukum* (Penerbit Segap Pustaka, 2021). hlm. 70.

[88] Widyastuti Andriyani et al., *Technology, Law And Society* (Makassar: CV. Tohar Media, 2023). hlm. 10.

[89] Fara Amalia Lutfi Pratama et al., *Implementasi Nilai Pancasila Dalam Bhinneka Tunggal Ika Sebagai Alat Pemersatu Bangsa Di Era Generasi Milenial* (Unisri Press, 2023). hlm. 96.

[90] Hani Sholihah et al., *Hak Asasi Manusia: Asal Usul, Penyusunan, Dan Implementasi* (Jambi: PT. Sonpedia Publishing Indonesia, 2024). hlm. 70

[91] Siti Malikhatun Badriyah, *Sistem Penemuan Hukum Dalam Masyarakat Prismatik* (Sinar Grafika, 2022). hlm. 19.

Hukum dalam masyarakat Indonesia yang berkembang tidak cukup untuk menjaga perdamaian dan ketertiban. Dengan rekomendasi ini, Mochtar Kusumaatmadja berharap hukum harus beroperasi sebagai "sarana pembaharuan masyarakat," atau "hukum sebagai alat rekayasa sosial," atau "sarana pembangunan.": [92]

Mengatakan hukum merupakan "sarana pembaharuan masyarakat" didasarkan kepada anggapan bahwa adanya keteraturan atau ketertiban dalam usaha pembangunan dan pembaharuan itu merupakan suatu yang diin ginkan atau dipandang (mutlak) perlu. Anggapan lain yang terkandung dalam konsepsi hukum sebagai sarana pembaharuan adalah bahwa hukum dalam arti kaidah atau peraturan hukum memang bisa berfungsi sebagai alat (pengatur) atau sarana pembangunan dalam arti penyalur arah kegiatan manusia ke arah yang dikehendaki oleh pembangunan dan pembaharuan.

Tolak ukur konteks di atas menunjukkan ada 2 (dua) dimensi sebagai inti Teori Hukum Pembangunan yang diciptakan oleh Mochtar Kusumaatmadja, yaitu:

a) Ketertiban atau keteraturan dalam rangka pembaharuan atau pembangunan merupakan sesuatu yang diinginkan, bahkan dipandang mutlak adanya;
b) Hukum dalam arti kaidah atau peraturan hukum memang dapat berfungsi sebagai alat pengatur atau sarana pembangunan dalam arti penyalur arah kegiatan manusia yang dikehendaki ke arah pembaharuan.

"Hukum yang memadai harus tidak hanya memandang hukum itu sebagai perangkat kaidah dan asas-asas yang menusia dalam masyarakat, tetapi harus pula menusia (*institution*) dan proses (*processes*)," jelas Mochtar Kusumaatmadja. Pengertian hukum di atas menunjukkan bagaimana pemahaman hukum secara

[92] Mochtar Kusumaatmadja , *Hukum, Masyarakat, dan Pembinaan Hukum Nasional,* Penerbit Binacipta, Bandung, 1995, hlm. 13.

holistik mencakup hukum, organisasi, dan prosedur. Ditulis sesuai dengan pedoman perundang-undangan, elemen-elemen komponennya bekerja sama untuk mencapai keadilan dalam reformasi hukum yang pertama. Secara analog, keempat komponen hukum yang diperlukan untuk mewujudkan hukum dalam kenyataan adalah pembinaan hukum setelah pembaharuan hukum tertulis, utamanya melalui mekanisme yurisprudensi.

Teori Hukum Pembangunan menekankan pentingnya adaptasi hukum terhadap perubahan sosial, ekonomi, dan teknologi dalam kerangka pembangunan berkelanjutan. Dalam konteks perlindungan data, regulasi harus mendukung pertumbuhan industri digital sambil tetap menjaga kebebasan pribadi. Hukum berperan sebagai instrumen pasif dan aktif dalam pertumbuhan masyarakat, sehingga pembaruan hukum harus mencakup penguatan lembaga pengawasan.

G. Metode Penelitian

Penelitian yang dilakukan berfungsi sebagai alat untuk mengetahui sesuatu masalah yang akan diteliti, baik ilmu-ilmu sosial, ilmu hukum, maupun ilmu lainnya.[93] Suatu penelitian pada dasarnya merupakan rangkaian kegiatan dalam rangka menemukan jawaban atas rasa ingin tahu terhadap suatu permasalahan yang akan diteliti, sehingga dibutuhkan metode ilmiah untuk menjawab permasalahan-permasalahan dalam penelitian yang dimaksud.[94] Penelitian adalah sebagai alat untuk mengetahui suatu masalah yang akan diteliti baik ilmu-ilmu sosial, ilmu

[93] Mahlil Adriaman, *Pengantar Metode Penelitian Ilmu Hukum* (Agam: Yayasan Tri Edukasi Ilmiah, 2024). hlm. 82.

[94] *Ibid*.

hukum, maupun ilmu lainnya.[95] Hukum merupakan salah satu objek di bidang penelitian, merupakan seperangkat peraturan perundang-undangan yang menjadi aturan hidup bagi masyarakat untuk ditaati agar tercipta keteraturan dan ketertiban, jika dilanggar maka akan dikenakan sanksi. [96] Selanjutnya untuk menemukan suatu jawaban atas permasalahan-permasalahan pada penelitian pada penelitian ini, maka peneliti menggunakan metode sebagai berikut:

1. Jenis Penelitian

Penelitian ini merupakan penelitian hukum normatif. Penelitian hukum normatif adalah penelitian yang berfokus pada studi terhadap norma-norma hukum yang tertulis dalam peraturan perundang-undangan,[97] doktrin hukum, dan prinsip-prinsip hukum yang berlaku.

Penelitian ini dilakukan dengan cara menganalisis peraturan perundang-undangan yang terkait dengan perlindungan data pribadi yang bersifat spesifik, baik di tingkat nasional seperti UU PDP. Pendekatan normatif dalam penelitian ini digunakan untuk mengkaji sinkronisasi, kelemahan, dan kekuatan regulasi yang ada guna memberikan rekomendasi perbaikan dalam kerangka hukum perlindungan data pribadi yang bersifat spesifik di Indonesia.

---

[95] *Idem*. hlm. 82.

[96] Ramlan, *et. al.,* . *Metode Penelitian Hukum dalam Pembuatan Karya Ilmiah*, (Medan: Umsu Press, 2023), hlm. 65.

[97] Iman Jalaludin Rifa'i, *Ruang Lingkup Metode Penelitian Hukum*, *Metodologi Penelitian Hukum* (Banten: Sada Kurnia Pustaka, 2023). hlm. 127.

2. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan perbandingan (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan perbandingan digunakan dengan membandingkan pengaturan perlindungan data pribadi di Indonesia dengan Singapura dan Thailand guna mengidentifikasi praktik terbaik yang dapat menjadi bahan penguatan regulasi nasional.

Pendekatan konseptual dilakukan melalui kajian terhadap teori, doktrin, dan asas hukum yang berkaitan dengan perlindungan data pribadi, hak privasi, dan hak asasi manusia. Pendekatan ini digunakan untuk membangun kerangka berpikir dalam menganalisis permasalahan hukum yang diteliti serta merumuskan konsep rekonstruksi hukum yang sesuai dengan kebutuhan perlindungan data pribadi di era digital. Penggunaan ketiga pendekatan tersebut diharapkan menghasilkan analisis yang komprehensif dan berorientasi pada penguatan perlindungan data pribadi di Indonesia. Pendekatan-pendekatan tersebut saling melengkapi dalam mengkaji aspek normatif, teoritis, dan komparatif dari perlindungan data pribadi. Hasil kajian diharapkan dapat memberikan dasar yang kuat dalam merumuskan rekonstruksi hukum yang lebih efektif dan responsif terhadap perkembangan teknologi digital.

3. Sifat Penelitian

Penelitian ini bersifat eksploratoris *(exploratory legal study)*. Sifat eksploratoris digunakan untuk mengidentifikasi celah hukum, tantangan dalam implementasi regulasi, serta alternatif solusi hukum yang dapat diterapkan dalam rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik.[98] Penelitian eksploratoris digunakan untuk menggali secara mendalam suatu fenomena yang belum banyak diteliti, dengan tujuan menemukan pola, hipotesis, atau pemahaman baru. Pendekatan ini dimanfaatkan untuk mengidentifikasi celah hukum, tantangan dalam implementasi regulasi, serta alternatif solusi yang dapat diterapkan.[99]

Penelitian dengan sifat eksploratoris diterapkan ketika pengetahuan mengenai topik yang dikaji masih terbatas atau belum jelas. Pemahaman yang lebih mendalam diperoleh melalui metode kualitatif seperti wawancara mendalam, observasi partisipatif, dan studi kasus. Dalam pendekatan ini, berbagai perspektif dikaji agar rekomendasi yang lebih komprehensif dapat dihasilkan.[100]

Dalam studi hukum, penelitian eksploratoris digunakan untuk memahami konteks serta latar belakang suatu masalah sehingga pertanyaan penelitian yang lebih spesifik dapat dirumuskan. Kompleksitas isu yang ada dianalisis untuk mengidentifikasi kekurangan dalam regulasi yang berlaku, serta untuk merancang rekomendasi kebijakan yang lebih efektif. Dengan demikian, penelitian

---

[98] Dadang Sumarna dan Ayyub Kadriah, "Penelitian Kualitatif Terhadap Hukum Empiris," *Jurnal Penelitian Serambi Hukum* Vol. 16, no. 02 (2023), hlm. 101-113.

[99] Ervina Waty et al., *Metodologi Penelitian Bisnis: Teori & Panduan Praktis Dalam Penelitian Bisnis* (Jambi: PT. Sonpedia Publishing Indonesia, 2023). hlm. 36.

[100] Fatma Sarie et al., *Metodelogi Penelitian* (Batam: Cendikia Mulia Mandiri, 2023). hlm. 7.

eksploratoris berperan penting dalam memberikan landasan awal bagi rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik.[101]

4. Bentuk Penelitian

Penelitian ini berbentuk evaluatif, yang bertujuan untuk mendapatkan saran mengenai apa yang harus dilakukan untuk mengatasi masalah perlidungan data pribadi yang ada di Indonesia, khususnya dalam menghadapi tantangan di era digital. Penelitian ini berbentuk evaluatif, yang bertujuan untuk menilai efektivitas kebijakan dan regulasi terkait perlindungan data pribadi yang bersifat spesifik di Indonesia, khususnya dalam menghadapi tantangan di era digital. Penelitian evaluatif berfokus pada analisis implementasi kebijakan yang ada, mengidentifikasi kekuatan dan kelemahan dalam penerapannya, serta mengevaluasi dampaknya terhadap perlindungan hak individu dan kepentingan publik.

Dalam penelitian ini, akan dilakukan penilaian terhadap pelaksanaan UU PDP, termasuk sejauh mana regulasi tersebut mampu memberikan perlindungan yang efektif terhadap data pribadi, hambatan yang muncul dalam implementasinya, serta apakah sanksi yang diterapkan sudah sesuai dengan prinsip keadilan dan proporsionalitas. Selain itu, penelitian ini juga akan mengkaji sejauh mana regulasi ini selaras dengan perkembangan teknologi dan ekonomi digital di Indonesia.

Sebagai bagian dari pendekatan evaluatif, penelitian ini akan mengukur keberhasilan sistem perlindungan data pribadi yang bersifat spesifikdi Indonesia dengan membandingkannya dengan standar internasional yang lebih mapan, seperti

[101] Kristiawanto, *Pengantar Mudah Memahami Metode Penelitian Hukum* (Klaten: Nas Media Pustaka, 2024). hlm. 34.

PDPA Singapura. Perbandingan ini bertujuan untuk menilai kesesuaian kebijakan Indonesia dengan praktik terbaik global serta memberikan masukan untuk perbaikan regulasi yang lebih adaptif terhadap dinamika digital yang terus berkembang.

5. Sumber Data

Sumber data adalah tempat ditemukannya data tersebut diperoleh.[102] Sumber data yang digunakan dalam penelitian ini adalah data kewahyuan (bersumber dari Tuhan) dan data sekunder, yang diurakan sebagai berikut ini:

a. Data kewahyuan: Dalam konteks perlindungan data pribadi yang bersifat spesifik, penting untuk mempertimbangkan perspektif agama yang melarang penyebaran aib atau data pribadi seseorang tanpa izin. Hal ini juga diatur dalam ajaran agama Islam, yang melarang perbuatan tersebut sebagai bentuk penghormatan terhadap privasi dan kehormatan individu. Salah satu ayat Al-Qur'an yang relevan dengan isu ini adalah Surah Al-Hujurat ayat 12:[103]

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَ لَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ ١٢

"Wahai orang-orang yang beriman, jauhilah banyak dari prasangka, sesungguhnya sebagian dari prasangka itu adalah dosa. Dan janganlah kamu mencari-cari kesalahan orang lain, dan janganlah sebagian kamu menggunjing sebagian yang lain. Sukakah salah seorang di antara kamu memakan daging saudaranya yang sudah mati? Maka tentulah kamu merasa jijik kepadanya. Dan bertakwalah kepada Allah. Sesungguhnya Allah Maha Penerima Taubat lagi Maha Penyayang." (QS. Al-Hujurat: 12). [104]

---

[102] Suteki dan Galang Taufani, *Metode Penelitian Hukum: Filsafat, Teori dan Praktik* (Depok: Rajawali Pers, 2020)*.,* hlm. 214.

[103] Al-Qur'an, 47:12.

[104] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 47:12.

Ayat ini mengandung larangan prasangka buruk, *tajassus* (mencari-cari kesalahan orang lain), dan *ghibah* (menggunjing), yang dapat merusak hubungan sosial dan moral. Imam Al-Ghazali menekankan pentingnya menghormati hak privasi individu, yang dalam konteks modern dapat dikaitkan dengan perlindungan data pribadi yang bersifat spesifik. Perspektif agama ini menunjukkan bahwa menjaga privasi dan kehormatan individu merupakan nilai fundamental dalam hukum dan etika sosial.[105]

b. Data sekunder dalam penelitian ini merujuk pada informasi yang telah tersedia dan dapat diperoleh dari berbagai sumber yang sudah ada, seperti buku, artikel ilmiah, peraturan perundang-undangan, jurnal, dan laporan yang relevan.[106]

    1) Bahan hukum primer, yaitu bahan hukum yang mempunyai otoritas meliputi peraturan Perundang-Undangan; catatan resmi/risalah dalam pembuatan sutau peraturan Perundang-Undangan; putusan hakim.[107] Adapun bahan hukum primer dalam penelitian ini adalah:

        a) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi yang bersifat spesifik.

        b) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelindungan data pribadi yang bersifat spesifik.[108]

---

[105] Na'im Fadhilah dan Deswalantri, "Nilai-Nilai Pendidikan Karakter dalam Al-Qur'an Surat Al-Hujurat Ayat 11-13: Kajian Tafsir Al-Azhar Karya Hamka," Jurnal Pendidikan Tambusai Vol. 6, no. 3 (2022), hlm. 13525-13534, doi: 10.31004/jptam.v6i3.4468.

[106] Sugiyono, P. D., *Metode Penelitian Bisnis: Pendekatan Kuantitatif, Kualitatif, Kombinasi, Dan R&D* (Bandung: Penerbit CV. Alfabeta, 2017), hlm. 193.

[107] Zainuddin Ali, *op.cit.,* hlm. 47

[108] Indra Safitri, *Hukum Siber dan Pelindungan data pribadi yang bersifat spesifik di Indonesia* (Jakarta: Kencana, 2021), hlm. 152.

2) Bahan Hukum Sekunder terdiri dari publikasi hukum non-resmi yang relevan, buku, manual, jurnal, komentar putusan hukum. [109] Bahan hukum sekunder yang diterapkan dalam penelitian ini terdiri dari:

   a) Buku dan Monograf Hukum: Untuk penelitian ini, buku-buku yang dapat dijadikan sebagai bahan hukum sekunder meliputi karya-karya yang mengkaji perlindungan data pribadi yang bersifat spesifik dalam konteks hukum Indonesia dan internasional.

   b) Jurnal: Jurnal ilmiah yang diterbitkan dalam jurnal hukum akan menjadi sumber penting dalam penelitian ini.

   c) Laporan Penelitian dan Studi Kasus: Laporan dari lembaga riset, badan pemerintah, atau organisasi internasional yang berfokus pada perlindungan data pribadi yang bersifat spesifik juga akan digunakan sebagai bahan hukum sekunder.[110]

   d) Komentar terhadap undang-undang dan Peraturan: Komentar-komentar dari para ahli hukum terkait dengan peraturan perundang-undangan yang ada,[111]

   e) Dokumen Internasional dan Perjanjian Internasional: Dalam rangka memperkaya perspektif penelitian, dokumen internasional yang terkait dengan perlindungan data pribadi yang bersifat

[109] Peter Mahmud Marzuki, *Penelitian Hukum .,* hlm. 95.
[110] Iman Jalaludin Rifa'i et al., *Metodologi Penelitian Hukum* (Banten: PT Sada Kurnia Pustaka, 2023), hlm. 57.
[111] Zainuddin Ali, *Metode Penelitian Hukum* (Jakarta: Sinar Grafika, 2021), hlm. 54.

spesifik, seperti rekomendasi, pedoman, dan perjanjian internasional.[112]

Memanfaatkan bahan hukum sekunder ini, penelitian ini bertujuan untuk memberikan analisis yang komprehensif mengenai perlindungan data pribadi yang bersifat spesifik, memperkuat pemahaman terhadap regulasi yang ada, serta membandingkan kebijakan Indonesia dengan pengalaman negara lain. Ini juga akan membantu menggali potensi perbaikan dan pengembangan sistem perlindungan data pribadi yang bersifat spesifik di Indonesia, dengan merujuk pada standar internasional dan praktik terbaik yang diterapkan di negara-negara lain.

6. Alat Pengumpul Data

Alat pengumpul data yang dilakukan dalam penelitian ini adalah dengan teknik mengumpulkan data yang dilakukan dengan cara studi kepustakaan *(library research)*, untuk memperoleh sumber data sekunder maka dilakukan dengan cara penelusuran, penghimpunan bahan-bahan hukum yang relevan dengan judul penelitian ini dengan cara sebagai Studi kepustakaan (*Library Research*).

Pasal 20 Undang-Undang Nomor 43 Tahun 2007 tentang Perpustakaan menyatakan bahwa setiap perguruan tinggi wajib menyelenggarakan perpustakaan yang memenuhi standar nasional perpustakaan sebagai sumber belajar untuk mendukung pendidikan, penelitian, dan pengabdian kepada masyarakat. [113] Maka, dalam penelitian ini, studi kepustakaan dilakukan dengan mengacu pada berbagai

[112] Rosadi, *Pembahasan UU Pelindungan data pribadi yang bersifat spesifik (UU RI No. 27 Tahun 2022)*. (Jakarta: Sinar Grafika, 2023), hlm. 18.

[113] Pemerintah Republik Indonesia, "Undang-Undang Nomor 43 Tahun 2007 Tentang Perpustakaan" (Indonesia: Pemerintah Republik Indonesia, 2007).

sumber literatur yang relevan guna mendapatkan pemahaman mendalam mengenai konsep, regulasi, serta praktik perlindungan data pribadi yang bersifat spesifik di era digital. Studi ini dilakukan melalui Perpustakaan Universitas Muhammadiyah Sumatera Utara (UMSU), dan Perpustakaan Universitas Asahan (UNA), yang merupakan beberapa perguruan tinggi dengan koleksi literatur hukum yang cukup lengkap di Provinsi Sumatera Utara.

7. Analisis Hasil Penelitian

Dalam penelitian ini, metode analisis yang digunakan adalah analisis kualitatif. Analisis kualitatif bertujuan untuk menggali makna dan memahami fenomena yang diteliti secara mendalam, dengan fokus pada pemahaman terhadap konteks serta dinamika yang terlibat.[114] Langkah awal dalam analisis adalah pemeriksaan dan evaluasi seluruh data yang dikumpulkan melalui wawancara, observasi, dan sumber lainnya, untuk memastikan validitas dan kredibilitas data tersebut. Selanjutnya, data yang relevan dikelompokkan berdasarkan kategori atau tema yang muncul, kemudian dianalisis dengan menggunakan teori-teori yang relevan untuk memberikan interpretasi serta pemahaman yang lebih komprehensif. Proses ini melibatkan identifikasi pola, hubungan, serta implikasi dari data yang ada. Hasil analisis kemudian disistematiskan dan disajikan dalam bentuk temuan-temuan yang dapat memberikan jawaban atas permasalahan penelitian, dengan tujuan memberikan pemahaman yang lebih jelas mengenai fenomena yang diteliti serta menyarankan solusi atau rekomendasi yang relevan.[115]

---

[114] Muhammad Ridwan Lubis, "Analisis Kualitatif Dampak Hukum Pidana Terhadap Masyarakat.," *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)* 4, no. 4 (2024).

[115] Endah Marendah Ratnaningtyas et al., *Metodologi Penelitian Kualitatif* (Aceh: Yayasan Penerbit Muhammad Zaini, 2023). hlm. 61.

Analisis dapat dirumuskan sebagai suatu proses penguraian secara sistematis dan konsisten terhadap gejala-gejala tertentu, dengan menjelaskan dan memaknakan data melalui alat bantu berupa teori.[116] Analisis data merupakan aspek krusial dalam penelitian untuk memberikan jawaban terhadap masalah yang dikaji. Sebelum analisis dilaksanakan, dilakukan pemeriksaan dan evaluasi terhadap seluruh data yang ada guna menilai validitasnya. Selanjutnya diadakan pengelompokkan terhadap data sejenis dengan pendekatan kualitatif.[117] Setelah data dianalisis, langkah berikutnya adalah memproses data tersebut sehingga disistematiskan dan menghasilkan klasifikasi yang selaras dengan masalah penelitian, sehingga diperoleh kesimpulan yang memberikan jawaban atas permasalahan yang ada.[118]

[116] Qadriani Arifuddin et al., *Metodologi Penelitian Hukum* (Jambi: PT. Sonpedia Publishing Indonesia, 2025). hlm. 38.

[117] Andri Wicaksono, *Metodologi Penelitian Pendidikan: Pengantar Ringkas* (Yogyakarta: Garudhawaca, 2022). hlm. 107.

[118] *Ibid*.

BAB II
INEFEKTIVITAS PERLINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK AKIBAT PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL

A. Pelindungan Data Pribadi Yang Bersifat Spesifik di Era Digital Dalam Perspektif Hukum Positif di Indonesia

Eksistensi perlindungan data pribadi pada hakikatnya merupakan cerminan dari postulat bahwa hak seseorang manusia secara alami bersifat *ipso facto* dan *ab initio*, oleh karena dalam kenyataannya sudah ada sejak awal manusia itu dilahirkan. Hak yang dibawah sejak lahir itulah yang disebut hak alami *(natural rights)*, hak dasar atau hak privasi *(privacy)*, melekat dan dimiliki seluruh umat manusia *(human rights are rights belong to all human being at all time and in all place by virtue of being born as human beings)*[119] yang diyakini sebagai pemberian dari Sang Pencipta Tuhan Yang Maha Esa.[120]

Hak pribadi atau privasi seseorang berkembang sangat kompleks secara konseptual, ditandai dengan adanya berbagai macam ide, gagasan, pola pikir dan teoriteori beriringan dengan keberadaan, kognisi atau pemahaman manusia atas privasi yang dimilikinya, sebagai sesuatu yang mendasar dalam menjaga kerahasiaan atas diri pribadi dalam kajian teoritis dimaknai dengan berbagai konsep yakni *"privacy is the rights to be alone"*, "*the rights to individual autonomy"*, *"the rights to a private life"*, *"the rights to intimacy"*, *"the rights to enjoy reserve" and*

[119] Todung Mulya Lubis, *In Search of Human Rights: Legal-Political Dilemmas of Indonesia New Order, 1966-1990*, dalam Bunyamin, F.X. Watkat, dkk., *Pengantar Ilmu Hukum* (Padang: Get Press Indonesia, 2023), hlm. 93.

[120] Jimly Asshiddiqie, *Gagasan Konstitusi Sosial: Negara Kesejahteraan dan Konstitusi Indonesia*, (Jakarta: Konstitusi Press, 2014), hlm. 56.

"the rights to secrecy", oleh Westin dalam tulisannya *"Privacy and Freedom"*, dimaknai sebagai *"claim of individual, groups or institution to determinate for themselves when, how, and to what extent information about them is communicated to other"*.[121] Unsur utama dari konsep tersebut adalah fokusnya pada kontrol dari informasi tersebut untuk alasan apapun. Sedangkan dalam tataran praktik hak pribadi atau privasi bertansformasi menjadi dua sisi mata pisau yang sama tajamnya, pada sisi yang satu, memberikan sisi humanis yang perlu dilindungi sedangkan pada sisi yang lain privasi menjadi momok yang menakutkan bagi pengambil kebijakan karena penuh dengan dominasi kebijakan.[122]

Aspek dari privasi terdiri dari yang dilindungi atau diatur oleh hukum, dan tidak diatur oleh hukum. Oleh karenanya adalah penting untuk memahami bagaimana pengaruhnya terhadap hak seseorang untuk menggunakan, mengontrol, peredaran atau menyebarluaskan penggunaan hak tersebut, yakni menyangut *aspek "privacy of a person's persona," "privacy of data about a person" dan "privacy of a person's communication." Privacy of persona person's* merupakan aspek yang lebih menekankan pada prinsip umum bahwa seseorang mempunyai hak untuk dibiarkan sendiri dan/atau menyendiri *(the rights to be alone)*, hak seseorang untuk bebas dari kekuasan/campur tangan publik terhadap hal-hal yang dianggap tidak perlu/penting *(the right of a person to be free from warranted interference by the public in matters with the public is not necessarily concerned)*.[123] Selanjutnya aspek

---

[121] Allan F. Westin, *Privacy dan Freedom*, dalam Edmon Makarim, *Kompasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003), hlm. 145.

[122] H. A. R. Tilaar, *Membenahi Pendidikan Nasional*, (Jakarta: Rineka Cipta, 2012), hlm. 78.

[123] Ridwan Khairandy, *Hak Asasi Manusia dalam Perspektif Hukum*, (Yogyakarta: FH UII Press, 2019), hlm. 112.

privacy of data about a person's yakni informasi mengenai seseorang yang dikumpulkan dan digunakan oleh orang lain, di Indonesia lebih dikenal dengan istilah Data Pribadi. Sedangkan, aspek *privacy of a person's communication* lebih ditekankan pada hak seseorang dalam berkomunikasi.[124] Ketiga aspek tersebut secara universal dan oleh kebanyakan negara-negara dunia merupakan aspek terpenting dalam hubungannya dengan konsep Pelindungan data pribadi yang bersifat spesifik dan telah diakui sebagai salah satu Hak Asasi Manusia.[125]

Peraturan tentang perlindungan data pribadi yang bersifat spesifik sebenarnya telah diatur secara parsial dan tersebar di Indonesia dalam beberapa produk perundang-undangan, yakni Undang-Undang Nomor 7 Tahun 1971 Tentang Ketentuan-Ketentuan Pokok Kearsipan (diubah dengan Undang-Undang Nomor 43 Tahun 2009), Undang-Undang Nomor 23 Tahun 1992 Tentang Kesehatan (diubah terakhir dengan Undang-Undang Nomor: 17 Tahun 2023), Undang-Undang Nomor 8 Tahun 1997 Tentang Dokumen Perusahaan, Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia, Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaski Elektonik sebagaimana telah diubah dan ditambah

---

[124] Yahya Harahap, *Hukum tentang Perlindungan Privasi dan Data Pribadi*, (Jakarta: Sinar Grafika, 2020), hlm. 95.

[125] *Data Protection Directive* (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data) mulai berlaku pada tahun 1985. DPD dirumuskan oleh Komite Menteri-Menteri dan Organisasi Kerja Sama dan Pembangunan Ekonomi (*Organization for Economic Cooperation dan Development*/OECD), yang kemudian menghasilkan suatu pedoman, yaitu *Guidelines on Protection of Privacy dan Transborder Flows of Personal Data*. Pedoman ini memberikan prinsip dasar tentang pelindungan data dan kebebasan arus informasi di negara-negara yang memiliki undang-undang yang sesuai dengan pelindungan data. Edmon Makarim, *Ibid.*, hlm. 151.

terakhir dengan Undang-Undang Nomor 1 Tahun 2023 tentang Perubahan Kedua Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Pemanfaatan teknologi informasi tersebut mengakibatkan data pribadi seseorang sangat mudah untuk dikumpulkan dan dipindahkan dari satu pihak ke pihak lain tanpa sepengetahuan pemilik hak atau subjek data pribadi, sehingga mengancam hak konstitusional subjek data pribadi, secara tegas hak ini telah diatur dalam Pasal 28G ayat (1) Amandemen ke-3, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Contoh tersebut tentunya tidak akan terjadi bilamana aspek penegakan hukum diterapkan secara tegas, salah satu diataranya adalah melalui penerapanhukum pidana, sebab bagaimanapun UU PDP secara tegas telah mengatur bahwa subjek data pribadi mempunyai hak dalam pemrosesan data pribadi yang dijalankan oleh pengelola/pengendali/prosesor data pribadi, meliputi:[126]

1. pemerolehan dan pengumpulan;
2. pengolahan dan penganalisisan;
3. penyimpanan;
4. perbaikan dan pembaruan;

[126] Lihat, Pasal 16 sampai dengan Pasal 54 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi yang bersifat spesifik

5. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau
6. penghapusan atau pemusnahan.

Bahkan secara tegas dalam ketentuan Pasal 65 UU PDP diatur bahwa:

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

Pelanggaran terhadap ketentuan Pasal 65 UU PDP, apabila dilakukan oleh orang perorangan diancam dengan pidana penjara paling lama 4 (empat) sampai dengan 6 (enam) tahun dan/atau pidana denda paling banyak Rp.4.000.000.000,00 (empat milyar) sampai dengan Rp.6.000.000.000,00 (enam milyar) rupiah, ditambah dengan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari hasil tindak pidana. Sedangkan bagi korporasi ancaman pidana denda adalah 10 kali dari maksimal pidana denda yang diancamkan.[127]

[127] Lihat, Pasal 67 sampai dengan Pasal 73 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi yang bersifat spesifik

Perlindungan hukum terhadap data pribadi yang bersifat spesifik dalam konteks hukum positif tidak dapat dilepaskan dari perspektif nilai-nilai keagamaan, khususnya dalam Islam yang memiliki prinsip dasar terkait privasi dan kehormatan individu.[128] Islam sangat mengecam bentuk pengambilan informasi atau segala sesuatu tanpa izin dari si pemilik yang dikategorikan sebagai tindakan pencurian.[129] Setiap prilaku pencurian sangat dilarang keras dalam ajaran Islam.[130] Seperti yang termuat dalam Surah Al-Maidah Ayat 38:[131]

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوْٓا اَيْدِيَهُمَا جَزَاۤءًۢ بِمَا كَسَبَا نَكَالًا مِّنَ اللّٰهِ ۗوَاللّٰهُ عَزِيْزٌ حَكِيْمٌ

> Laki laki maupun perempuan yang mencuri, potonglah tangan kedua nya sebagai balasan atas perbuatan yang mereka lakukan dan sebagai siksaan dari Allah. Allah Mahaperkasa lagi Maha bijak sana.[132]

Mengambil sesuatu tanpa sepengetahuan pemiliknya merupakan Tindakan yang sangat tercela. Bahkan tindakan mencari keuntungan atas informasi orang lain tidak lepas dari kategori pencurian yang dikecam oleh Allah SWT.[133] Sebagaimana dijelaskan dalam Surah Al-Baqarah Ayat 188:[134]

وَلَا تَأْكُلُوْٓا اَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوْا بِهَآ اِلَى الْحُكَّامِ لِتَأْكُلُوْا فَرِيْقًا مِّنْ اَمْوَالِ النَّاسِ بِالْاِثْمِ وَاَنْتُمْ تَعْلَمُوْنَ ع

> Janganlah kamu makan harta di antara kamu dengan jalan yang batil dan (janganlah) kamu membawa (urusan) harta itu kepada para hakim dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui[135]

---

[128] Muhammad Abu Zahrah, *Konsep Hak Asasi Manusia dalam Islam*, (Jakarta: Pustaka Al-Kautsar, 2009), hlm. 45.

[129] Yusuf Al-Qaradawi, *Halal dan Haram dalam Islam*, (Jakarta: Gema Insani, 2010), hlm. 130.

[130] Quraish Shihab, *Tafsir Al-Mishbah: Pesan, Kesan, dan Keserasian Al-Qur'an*, (Jakarta: Lentera Hati, 2006), hlm. 412.

[131] Al-Qur'an, 5:38.

[132] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 5:38

[133] Yusuf Al-Qaradawi, *loc.cit.*

[134] Al-Qur'an, 2:188.

[135] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS.2:188

Data pribadi yang bersifat spesifik mencakup aspek-aspek sensitif dari kehidupan seseorang, sehingga dalam pelaksanaannya harus mempertimbangkan kaidah moral dan etika yang telah ditetapkan dalam ajaran Islam.[136] Al-Qur'an sebagai sumber utama hukum Islam mengandung prinsip-prinsip fundamental yang mendukung perlindungan terhadap hak privasi individu, sebagaimana dapat dianalisis melalui beberapa ayat, seperti dalam Surah Al-Hujurat Ayat 12, Surah An-Nur Ayat 11, dan Surah An-Nur Ayat 27.

Surah Al-Hujurat ayat 12 berbunyi:[137]

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوا اجْتَنِبُوْا كَثِيْرًا مِّنَ الظَّنِّۖ اِنَّ بَعْضَ الظَّنِّ اِثْمٌ وَّلَا تَجَسَّسُوْا وَلَا يَغْتَبْ بَّعْضُكُمْ بَعْضًاۗ اَيُحِبُّ اَحَدُكُمْ اَنْ يَّأْكُلَ لَحْمَ اَخِيْهِ مَيْتًا فَكَرِهْتُمُوْهُۗ وَاتَّقُوا اللّٰهَۗ اِنَّ اللّٰهَ تَوَّابٌ رَّحِيْمٌ

> Wahai orang-orang yang beriman! Jauhilah banyak dari prasangka, sesungguhnya sebagian prasangka itu dosa, dan janganlah kamu mencari-cari kesalahan orang lain, serta janganlah ada di antara kamu yang menggunjing sebagian yang lain. Adakah seorang di antara kamu yang suka memakan daging saudaranya yang sudah mati? Tentu kamu merasa jijik kepadanya. Bertakwalah kepada Allah, sesungguhnya Allah Maha Penerima tobat, Maha Penyayang.[138]

Ayat ini secara eksplisit menekankan larangan untuk mencari-cari kesalahan orang lain serta menggunjing *(ghibah)*, yang dalam konteks modern dapat diartikan sebagai tindakan mengakses, menyebarkan, atau mengeksploitasi data pribadi seseorang tanpa izin.[139] Penyebarluasan data pribadi yang bersifat spesifik, seperti rekam medis, informasi keuangan, atau data biometrik seseorang, tanpa persetujuan individu yang bersangkutan dapat dikategorikan sebagai pelanggaran terhadap prinsip yang disebutkan dalam ayat ini. Perlindungan

---

[136] *Ibid.*

[137] Al-Qur'an, 49: 12.

[138] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 49:12.

[139] Ahmad Azhar Basyir, *Prinsip-Prinsip Hukum Islam tentang Hak Asasi Manusia*, (Yogyakarta: UII Press, 1999), hlm. 56.

terhadap data pribadi bukan hanya sebatas peraturan hukum positif, tetapi juga merupakan bagian dari tuntutan ketakwaan kepada Allah.[140] Dalam konteks keadilan sosial, ayat ini mengajarkan bahwa hak privasi individu harus dihormati oleh seluruh elemen masyarakat, sehingga tidak terjadi ketimpangan atau eksploitasi yang merugikan kelompok tertentu.[141] Surah An-Nur ayat 11 berbunyi:[142]

اِنَّ الَّذِيْنَ جَآءُوْ بِالْاِفْكِ عُصْبَةٌ مِّنْكُمْۗ لَا تَحْسَبُوْهُ شَرًّا لَّكُمْۗ بَلْ هُوَ خَيْرٌ لَّكُمْۗ لِكُلِّ امْرِئٍ مِّنْهُمْ مَّا اكْتَسَبَ مِنَ الْاِثْمِۚ وَالَّذِيْ تَوَلّٰى كِبْرَهٗ مِنْهُمْ لَهٗ عَذَابٌ عَظِيْمٌ

> Sesungguhnya orang-orang yang membawa berita bohong itu adalah dari golongan kamu juga. Janganlah kamu mengira bahwa berita bohong itu buruk bagi kamu, bahkan itu baik bagi kamu. Setiap orang dari mereka mendapat balasan dari dosa yang dikerjakannya. Dan siapa di antara mereka yang mengambil bagian terbesar dalam penyebaran berita bohong itu, baginya azab yang besar.[143]

Ayat ini berkaitan dengan bahaya penyebaran informasi yang tidak benar atau hoaks, yang dalam konteks perlindungan data pribadi yang bersifat spesifik dapat dikaitkan dengan penyalahgunaan atau manipulasi data seseorang untuk tujuan tertentu, seperti pencemaran nama baik, pemerasan, atau bahkan kejahatan siber.[144] Penyebarluasan informasi pribadi seseorang tanpa validasi dan dengan tujuan yang tidak baik tidak hanya melanggar hukum positif tetapi juga bertentangan dengan prinsip moral Islam.[145] Oleh karena itu, regulasi mengenai perlindungan data pribadi yang bersifat spesifik harus memiliki mekanisme yang ketat untuk

---

[140] Mohammad Daud Ali, *Hukum Islam: Pengantar Ilmu Hukum dan Tata Hukum Islam di Indonesia*, (Jakarta: Rajawali Pers, 2010), hlm. 214.

[141] Kaelan, *Pancasila sebagai Ideologi dan Dasar Negara*, (Yogyakarta: Paradigma, 2016), hlm. 198.

[142] Al-Qur'an, 24:11.

[143] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 24:11

[144] Agus Raharjo, *Perlindungan Hukum terhadap Privasi dan Data Pribadi di Indonesia*, (Jakarta: Sinar Grafika, 2021), hlm. 147.

[145] *Ibid.*

mencegah penyalahgunaan data dan menjamin bahwa informasi yang beredar tidak disalahgunakan untuk merugikan individu.[146] Dalam perspektif keadilan sosial, ayat ini menegaskan bahwa setiap individu memiliki hak untuk dilindungi dari fitnah dan eksploitasi informasi yang dapat mencemarkan nama baiknya di hadapan publik.[147] Surah An-Nur ayat 27 berbunyi:[148]

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

> Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu agar kamu selalu ingat.[149]

Ayat ini memberikan prinsip dasar mengenai pentingnya meminta izin sebelum memasuki ranah privasi orang lain.[150] Dalam konteks perlindungan data pribadi yang bersifat spesifik, prinsip ini dapat diinterpretasikan sebagai larangan untuk mengakses informasi seseorang tanpa izin yang sah.[151] Sama seperti seseorang tidak boleh masuk ke dalam rumah orang lain tanpa izin, demikian pula dengan data pribadi, dimana akses terhadapnya harus melalui persetujuan pemiliknya.[152] Ayat ini menjadi dasar penting dalam pengaturan hukum yang berkaitan dengan prinsip *"consent"* atau persetujuan dalam pemrosesan data pribadi, yang juga tercantum dalam berbagai regulasi perlindungan data pribadi

---

[146] Wahbah Az-Zuhaili, *Al-Fiqh Al-Islami wa Adillatuhu*, (Jakarta: Gema Insani, 2011), hlm. 723.

[147] Lilik Mulyadi, *Hak Asasi Manusia dalam Perspektif Hukum dan Konstitusi Indonesia*, (Bandung: Alumni, 2018), hlm. 105.

[148] Al-Qur'an, 24:27.

[149] Al-Qur'an Terjemahan Kemenetrian Agama Republik Indonesia QS. 24:27.

[150] Ahmad Azhar Basyir, *loc.cit.*

[151] Mohammad Daud Ali, *Hukum Islam: Pengantar Ilmu Hukum dan Tata Hukum Islam di Indonesia*, (Jakarta: Rajawali Pers, 2010), hlm. 214.

[152] Jimly Asshiddiqie, *Gagasan Konstitusi Sosial: Negara Kesejahteraan dan Konstitusi Indonesia*, (Jakarta: Konstitusi Press, 2014), hlm. 89.

yang bersifat spesifik di dunia, termasuk di Indonesia.[153] Dalam perspektif pembangunan hukum, ayat ini menegaskan bahwa perlindungan data pribadi yang bersifat spesifik bukan hanya sebatas kepatuhan terhadap aturan teknis, tetapi juga mencerminkan nilai moral yang harus diinternalisasi dalam kehidupan masyarakat.[154] ika dikaitkan dengan konsep hukum dalam konteks negara Indonesia, perlindungan data pribadi yang bersifat spesifik dapat dianalisis menggunakan pendekatan hukum sebagai perlindungan, keadilan sosial, dan pembangunan hukum.[155]

Pendekatan hukum sebagai perlindungan menekankan bahwa negara memiliki kewajiban untuk memberikan perlindungan hukum bagi setiap individu dari ancaman penyalahgunaan data pribadi, sebagaimana yang dikemukakan dalam teori perlindungan hukum. Kedua, pendekatan keadilan sosial menegaskan bahwa regulasi perlindungan data pribadi yang bersifat spesifik harus mencerminkan distribusi perlindungan yang adil bagi seluruh masyarakat tanpa diskriminasi. Ketiga, pendekatan hukum sebagai sarana pembangunan hukum menuntut adanya formulasi kebijakan yang adaptif terhadap perkembangan zaman, sehingga regulasi yang ada dapat memberikan perlindungan yang efektif dan menjamin kepastian hukum.

Pelindungan data pribadi yang bersifat spesifik juga mencerminkan nilai-nilai dasar yang terkandung dalam sila-sila Pancasila. Prinsip Ketuhanan Yang

---

[153] Ridwan Khairandy, *Hak Asasi Manusia dalam Perspektif Hukum*, (Yogyakarta: FH UII Press, 2019), hlm. 175.

[154] Soerjono Soekanto, Pokok-Pokok Sosiologi Hukum, (Jakarta: Rajawali Pers, 2010), hlm. 84.

[155] Kaelan, *Pancasila sebagai Ideologi dan Dasar Negara*, (Yogyakarta: Paradigma, 2016), hlm. 198.

Maha Esa mengajarkan bahwa setiap individu memiliki hak untuk dihormati privasinya sebagai bagian dari penghormatan terhadap martabat manusia.[156] Prinsip Kemanusiaan yang Adil dan Beradab menegaskan bahwa penggunaan data pribadi harus dilakukan dengan cara yang adil dan menghormati hak asasi manusia. Prinsip Persatuan Indonesia menuntut agar kebijakan perlindungan data pribadi yang bersifat spesifik diterapkan secara menyeluruh dan tidak hanya terbatas pada kelompok tertentu. Prinsip Kerakyatan mengedepankan keterlibatan publik dalam penyusunan regulasi yang berkaitan dengan perlindungan data pribadi yang bersifat spesifik. Sementara itu, prinsip Keadilan Sosial menegaskan bahwa perlindungan data pribadi yang bersifat spesifik harus dapat diakses oleh semua individu tanpa adanya kesenjangan dalam penerapannya.

Pendekatan perlindungan data pribadi yang bersifat spesifik harus mencerminkan keseimbangan antara aspek hukum positif, nilai-nilai moral dalam Islam, dan prinsip-prinsip Pancasila sebagai dasar negara. Hal ini menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik bukan hanya masalah hukum semata, tetapi juga merupakan bagian dari tanggung jawab sosial dan etika yang harus ditegakkan demi menjaga kehormatan, keadilan, dan hak asasi setiap individu dalam Masyarakat.

Data Pribadi yang Bersifat Spesifik merujuk pada informasi individu yang memiliki tingkat sensitivitas tinggi dan berpotensi menimbulkan risiko serius jika disalahgunakan.[157] Berbeda dengan data pribadi umum yang mencakup informasi

---

[156] Qoidul Khoir et al., *Pancasila & Kewarganegaraan* (Batam: Cendikia Mulia Mandiri, 2023). hlm. 132.

[157] Umi Khoirun Nisak, *Pengantar Rekam Medis Dan Manajemen Informasi Kesehatan* (Sidoarjo: umikhoirun, 2021). hlm. 106.

dasar seperti nama dan alamat, data spesifik mencakup aspek yang lebih mendalam mengenai kehidupan seseorang, termasuk data kesehatan dan rekam medis, data biometrik, data genetika, data keuangan pribadi, orientasi seksual, keyakinan agama, catatan kriminal, serta data anak di bawah umur. Karena sifatnya yang lebih sensitif, data ini memiliki karakteristik khusus yang memerlukan perlindungan lebih ketat, baik dalam pengumpulan, penyimpanan, pemrosesan, maupun penggunaannya.

Data kesehatan dan rekam medis adalah salah satu kategori penting dari data pribadi yang bersifat spesifik, yang mencakup informasi mengenai kondisi kesehatan fisik dan mental seseorang, riwayat penyakit, hasil pemeriksaan medis, serta informasi terkait pengobatan.[158] Data pribadi spesifik seperti data biometrik dan genetika, keuangan, orientasi seksual, agama, catatan kriminal, serta data anak dan data kesehatan sangat sensitif karena berisiko tinggi menimbulkan diskriminasi, kejahatan siber, dan dampak psikologis jika disalahgunakan atau bocor. Karena itu, banyak negara (termasuk Indonesia) mensyaratkan persetujuan eksplisit, pembatasan tujuan yang jelas, dan standar keamanan ketat dalam pemrosesannya, sebagaimana tercermin pada regulasi seperti HIPAA. Perlindungan yang efektif menuntut regulasi yang kuat, sistem keamanan yang andal, dan kesadaran individu untuk menjaga privasi serta hak asasi manusia di era digital.[159]

---

[158] *Ibid.*

[159] Hotmaria Hertawaty Sijabat dan Gunawan Widjaja, "Privasi Dan Keamanan Data Dalam Layanan Cloud: Perspektif Hukum Dan Regulasi," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4, no. 4 (2025), hlm. 279-288.

Data biometrik termasuk dalam kategori data pribadi yang bersifat spesifik. Data biometrik mencakup informasi biologis unik seseorang, seperti sidik jari, pemindaian wajah, retina atau iris mata, serta rekaman suara. Dalam beberapa tahun terakhir, penggunaan data biometrik semakin meluas, terutama dalam sistem keamanan dan identifikasi digital, seperti pemindai wajah pada perangkat *smartphone* dan akses berbasis sidik jari di berbagai institusi.[160] Data biometrik memiliki keunggulan keamanan namun sangat rentan disalahgunakan karena tidak dapat diubah seperti kata sandi; jika bocor, dapat memicu pencurian identitas, pengawasan massal tanpa izin, dan kontrol individu oleh pemerintah atau swasta tanpa transparansi, sehingga sejumlah negara menerapkan regulasi ketat atas pengelolaannya.

Data genetika mencakup lebih dalam dan kompleks, karena melalui profil DNA dapat mengungkap keturunan, predisposisi penyakit, dan karakteristik biologis yang dimanfaatkan untuk penelitian, diagnosis, dan terapi, tetapi berisiko tinggi menimbulkan diskriminasi, misalnya penolakan atau kenaikan premi asuransi dan diskriminasi dalam rekrutmen kerja berdasarkan kecenderungan penyakit di masa depan. Untuk mencegah penyalahgunaan tersebut, beberapa negara melarang penggunaan data genetika dalam keputusan asuransi dan ketenagakerjaan, seperti melalui *Genetic Information Nondiscrimination Act* (GINA) di Amerika Serikat.

[160] Miftahul Jannah et al., "Implementasi Autentikasi Biometrik Untuk Meningkatkan Keamanan Dan Privasi Pengguna Dompet Digital," *Journal of Scientech Research and Development* 6, no. 2 (2024), hlm. 531-539.

Data keuangan pribadi termasuk dalam kategori data spesifik yang memerlukan perlindungan ketat. Data ini mencakup informasi mengenai rekening bank, nomor kartu kredit, riwayat transaksi, serta kepemilikan aset seseorang.[161] Kebocoran data keuangan dapat menimbulkan kerugian materiil signifikan melalui pencurian identitas, akses tidak sah ke rekening, dan penyalahgunaan kartu kredit, terutama karena kejahatan siber seperti *phishing* dan *hacking* yang secara khusus menargetkan data ini, sementara perusahaan *fintech* dan perbankan memiliki akses luas sehingga regulasi harus memastikan data tidak disalahgunakan untuk kepentingan komersial tanpa persetujuan, misalnya melalui standar seperti PCI DSS. Di sisi lain, data orientasi seksual tergolong sangat sensitif karena kebocorannya berpotensi menimbulkan diskriminasi di dunia kerja, pendidikan, maupun kehidupan sosial, bahkan ancaman kekerasan di negara-negara yang masih memandang negatif orientasi tertentu, sehingga banyak regulasi perlindungan data memberikan perhatian khusus agar informasi tersebut tidak disebarkan atau digunakan tanpa izin.[162]

Data keyakinan dan kepercayaan agama serta catatan kriminal merupakan data pribadi yang sangat sensitif dan rentan disalahgunakan sehingga berpotensi menimbulkan diskriminasi atau persekusi, misalnya pembatasan hak atau ketidakadilan di dunia kerja, layanan publik, maupun kehidupan sosial. Penggunaan data agama dalam administrasi publik atau korporasi harus sangat hati-hati agar

[161] Reihana Pemuli et al., "Liability of Business Actors for Breaches in Electronic Banking Systems Tanggung Jawab Pelaku Usaha Yang Dibobol Dalam Sistem Elektronik Perbankan," *Jurnal Hukum Sehasen* 10, no. 2 (2024), hlm. 535-550.

[162] Teti Indrawati Purnamasari dan Rendra Khaldun, "Relevansi Al- Qur ' An , Hak Asasi Manusia , Dan Gender Dalam Melindungi Hak Kehormatan Pribadi Di Era Digital : Tinjauan Literatur," *MODELING: Jurnal Program Studi PGMI* 11 (2024), hlm. 154-172.

tidak menjadi alat diskriminasi, sementara catatan criminal yang memuat riwayat tindak pidana, hukuman, dan status rehabilitasi jika bocor dapat menghambat akses seseorang terhadap pekerjaan, layanan keuangan, dan pemulihan sosial. Karena itu, banyak negara membatasi penggunaan data agama untuk menjamin kebebasan beragama dan melindungi dari diskriminasi, serta memberlakukan ketentuan agar individu yang telah menjalani hukuman dapat memulihkan haknya tanpa terus dibayangi stigma, dengan akses terhadap catatan kriminal yang sangat terbatas dan hanya untuk lembaga berwenang dengan alasan sah.[163]

Data anak di bawah umur mendapat perlindungan sangat ketat karena mereka merupakan kelompok yang rentan terhadap eksploitasi dan penyalahgunaan data, baik melalui pemasaran digital, kejahatan siber, maupun perdagangan anak; karena itu, banyak negara menerapkan aturan khusus seperti *Children's Online Privacy Protection Act* (COPPA) di Amerika Serikat yang mengatur pengumpulan dan penggunaan data anak. Secara keseluruhan, data pribadi yang bersifat spesifik memerlukan perlindungan ekstra karena dampaknya yang luas terhadap individu, sehingga regulasi yang ketat, transparansi dalam pengelolaan data, dan kesadaran masyarakat atas hak privasi menjadi kunci untuk mencegah penyalahgunaan sekaligus menjaga hak asasi manusia di era digital.[164]

Penerapan perlindungan data pribadi yang bersifat spesifik di Indonesia masih menghadapi tantangan besar, terutama dalam penegakan hukum dan

---

[163] Abigail Natalia Bukit dan Rahmi Ayunda, "Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat," *Reformasi Hukum* 26, no. 1 (2022), hlm. 1-20.

[164] Fauzi Rifa dan Maslihati Nur Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia," *Binamulia Hukum* 13, no. 2 (2024), hlm. 461-481.

kepatuhan pengelola data, meskipun UU PDP telah mengatur hak subjek data serta kewajiban pengendali dan pemroses. Berbagai kasus kebocoran data kesehatan pasien, data biometrik di sektor perbankan dan kependudukan, serta meningkatnya kerentanan data keuangan akibat maraknya layanan fintech menunjukkan masih lemahnya transparansi dan keamanan, sehingga individu berisiko mengalami penipuan, pemalsuan identitas, dan eksploitasi ekonomi. Untuk itu, Otoritas Jasa Keuangan (OJK) dan BI telah menerapkan regulasi tambahan guna memperkuat keamanan data keuangan, sementara implementasi sistem identifikasi biometrik melalui e-KTP dan database Dukcapil, meski mempermudah akses layanan publik, tetap menuntut penguatan sistem keamanan mengingat adanya dugaan kebocoran data e-KTP yang beredar di *dark web*.[165]

Data anak di bawah umur menjadi perhatian khusus dalam era digital karena meningkatnya penggunaan internet yang memperbesar risiko eksploitasi data mereka, sementara banyak platform dan media sosial di Indonesia belum memiliki mekanisme kuat untuk melindungi data anak sehingga informasi pribadi mudah dimanfaatkan untuk pemasaran atau kejahatan siber, meskipun UU PDP mewajibkan persetujuan orang tua atau wali untuk pemrosesan data anak, implementasinya masih perlu diperkuat lewat pengawasan pemerintah. Di sisi lain, akses terhadap catatan kriminal yang dikelola POLRI pada prinsipnya sangat terbatas dan hanya boleh diakses pihak berwenang dengan alasan sah, namun di era digital muncul kekhawatiran kebocoran data ini dan penggunaannya secara tidak

[165] Leski Rizkinaswara, "Kominfo Investigasi Dugaan Kebocoran Data KTP – Ditjen Aptika," https://aptika.kominfo.go.id/2021/05/kominfo-investigasi-dugaan-kebocoran-data-ktp/, (May 9, 2025).

adil, misalnya dalam rekrutmen kerja atau proses hukum yang bias, sehingga perlindungannya harus diperketat agar tidak menjadi alat diskriminasi bagi individu yang telah menyelesaikan masa hukuman.[166]

Ancaman yang meningkat terhadap data pribadi yang bersifat spesifik menuntut pemerintah Indonesia untuk memperkuat penegakan hukum, kapasitas pengawasan, dan kesadaran masyarakat, dengan mendorong peran aktif Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta aparat penegak hukum agar pengelolaan data oleh sektor publik dan swasta benar-benar sesuai ketentuan. Ke depan, penguatan regulasi dan infrastruktur keamanan siber akan menjadi faktor kunci dalam menjaga hak privasi masyarakat di era digital yang kompleks. [167] Sejalan dengan itu, Philipus M. Hadjon membedakan perlindungan hukum menjadi dua, yaitu perlindungan hukum preventif dan represif; dalam konteks perlindungan data pribadi yang bersifat spesifik spesifik, aspek preventif tercermin dalam pengaturan UU PDP yang mewajibkan pengendali data memperoleh persetujuan subjek data sebelum memproses informasi sensitif seperti data kesehatan, biometrik, genetika, dan keuangan pribadi, sehingga individu memiliki kontrol yang lebih besar atas informasi dirinya.

Nancy Fraser mengembangkan teori keadilan sosial berdasarkan tiga pilar utama, yaitu redistribusi, rekognisi, dan representasi. Ketiga aspek ini sangat

---

[166] Totok Imam Santoso, "Media Sosial Dalam Konteks Data Kependudukan Di Era Prosumsi Digital," *Komunikologi : Jurnal Ilmiah Ilmu Komunikasi* 18, no. 2 (2021), hlm. 101-113.

[167] Danil Erlangga Mahameru, Aisyah Nurhalizah, Ahmad Wildan, et al., "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia," *Jurnal ESENSI HUKUM* 5, no. 20 (2023), hlm. 115-131.

relevan dalam konteks perlindungan data pribadi yang bersifat spesifik, terutama dalam memastikan bahwa hak-hak subjek data dihormati tanpa diskriminasi, dan akses terhadap perlindungan hukum tersedia bagi semua lapisan masyarakat.[168] Pelindungan data pribadi yang bersifat spesifik harus mempertimbangkan kesenjangan akses terhadap teknologi dan informasi, karena masyarakat dengan literasi digital rendah seperti kelompok pedesaan, disabilitas, dan lansia sering tidak memahami bagaimana data mereka dikumpulkan, digunakan, dan apa makna persetujuan dalam layanan digital, sehingga kebijakan perlindungan data wajib menjamin semua warga memiliki kesempatan yang sama untuk memahami hak dan memperoleh perlindungan yang memadai.[169]

Data pribadi bersifat spesifik karena berpotensi menimbulkan diskriminasi dan marginalisasi, misalnya orientasi seksual, catatan kejahatan, dan data kesehatan yang dapat digunakan untuk menghambat akses terhadap pekerjaan maupun layanan publik. Dalam konteks ini, teori Fraser menekankan pentingnya pengakuan yang setara dan partisipasi setara dalam pengambilan keputusan, sehingga perumusan kebijakan perlindungan data tidak hanya dilakukan oleh negara dan perusahaan teknologi, tetapi juga melibatkan masyarakat sipil, akademisi, dan organisasi non-pemerintah (NGO). Dengan demikian, perlindungan data pribadi yang bersifat spesifik spesifik tidak cukup berhenti pada aspek hukum formal, tetapi

[168] Agus Miswanto, "Rekognisi Dan Redistribusi Dalam Pencapaian Keadilan Sosial: Analisis Komparatif Terhadap Model Teoritis Nancy Fraser Dan Axel Honneth," *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 11, no. 2 (2022), hlm. 141-160.

[169] Ricardo Santos dan Ermania Widjajanti, "Penyelesaian Perkara Pidana Siber Kasus Kebocoran," *Quantum Juris: Jurnal Hukum Modern* 07, no. 1 (2025), hlm. 128-137.

juga harus memperhatikan keadilan distributif, keadilan rekognitif, dan keadilan representatif.[170]

Akses yang setara harus dimiliki setiap individu terhadap perlindungan hukum atas data pribadinya tanpa diskriminasi berbasis status sosial atau ekonomi, sehingga selain regulasi yang ketat diperlukan juga edukasi dan literasi digital agar masyarakat memahami haknya dan mampu melindungi data secara mandiri. Negara juga harus mengakui bahwa data pribadi, terutama yang bersifat spesifik, terkait langsung dengan hak asasi manusia dalam kerangka keadilan rekognitif, sehingga kebijakan perlindungan data wajib mencegah penyalahgunaan yang berujung pada diskriminasi di layanan kesehatan, pekerjaan, maupun akses keuangan, serta bebas dari bias struktural yang menguntungkan pihak tertentu.

Kelompok rentan seperti pekerja informal, pengguna layanan finansial digital, dan komunitas dengan akses teknologi terbatas harus dilibatkan dalam perumusan kebijakan agar hasilnya inklusif dan adil menurut keadilan reperesentatif. Sejalan dengan pemikiran Mochtar Kusumaatmadja dalam Teori Hukum Pembangunan, hukum tidak hanya menjadi alat kontrol sosial, tetapi juga sarana perubahan dan pembangunan; dalam konteks perlindungan data pribadi yang bersifat spesifik, regulasi berfungsi bukan hanya melindungi individu, tetapi juga membangun ekosistem digital yang aman, terpercaya, dan mendukung pertumbuhan ekonomi berbasis data.[171]

---

[170] Herol Hansen Samin, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif," *Jurnal Sains Student Research* 1, no. 2 (2023), hlm. 1-15.

[171] Abdul Manan, "Disrupsi Teknologi Hukum Terhadap Jasa Advokat Dalam Pandangan Hukum Pembangunan Mochtar Kusumaatmadja," *Reformasi Hukum* 27, no. 2 (2023), hlm. 270-276.

Data pribadi merupakan aset ekonomi penting dalam ekonomi berbasis teknologi sehingga regulasi harus menyeimbangkan perlindungan hak individu dan kepentingan ekonomi: jika perlindungan terlalu lemah, individu rentan dieksploitasi korporasi, tetapi jika terlalu ketat, inovasi dalam ekonomi digital dapat terhambat. Dalam perspektif hukum pembangunan, regulasi perlu fleksibel dan adaptif terhadap perkembangan teknologi agar perlindungan data pribadi yang bersifat spesifik terutama yang bersifat spesifik dapat berjalan seiring dengan dorongan inovasi dan kepentingan nasional. Hal ini tercermin dalam UU PDP yang memberi ruang bagi pengendali data untuk mengelola data pribadi dengan tetap mengutamakan hak subjek data. Karena regulasi yang terlalu longgar membuka celah eksploitasi, sementara yang terlalu kaku menghambat perkembangan, kebijakan perlindungan data harus dirancang secara adaptif dan progresif, didukung sinergi antara pemerintah, sektor swasta, dan masyarakat melalui regulasi yang jelas, penerapan teknologi keamanan data, dan peningkatan kesadaran hukum pengguna layanan digital, sehingga tercipta ekosistem perlindungan data yang berkelanjutan.[172]

Pancasila sebagai dasar negara memiliki peran fundamental dalam membentuk kebijakan perlindungan data pribadi yang bersifat spesifik yang berkeadilan. Prinsip Kemanusiaan yang Adil dan Beradab (sila kedua) menekankan bahwa hak privasi adalah bagian dari hak asasi manusia yang harus dijaga dan dihormati. Pelindungan data pribadi yang bersifat spesifik menjadi bagian dari penghormatan terhadap martabat individu dan hak-hak dasar manusia yang tidak

[172] Hansen Samin, *loc.cit*.

boleh dilanggar. Prinsip Keadilan Sosial bagi Seluruh Rakyat Indonesia (sila kelima) juga berhubungan erat dengan perlindungan data pribadi yang bersifat spesifik, terutama dalam memastikan bahwa setiap warga negara memiliki kesempatan yang sama untuk mendapatkan perlindungan hukum atas data pribadinya.[173]

Keadilan sosial merupakan nilai utama dalam Pancasila yang harus dijadikan pedoman dalam perumusan regulasi perlindungan data pribadi. Keadilan sosial menuntut agar setiap individu mendapatkan perlindungan yang setara terhadap data pribadi mereka, tanpa adanya diskriminasi atau perlakuan tidak adil. Setiap individu, tanpa memandang status sosial atau ekonomi, harus memiliki hak yang sama dalam menjaga kerahasiaan dan keamanan data pribadi mereka.[174] Oleh karena itu, prinsip keadilan sosial menjadi dasar untuk menciptakan regulasi yang mengutamakan perlindungan data pribadi dengan cara yang adil dan merata bagi seluruh lapisan masyarakat.

Prinsip hak asasi manusia yang tercermin dalam Pancasila mengharuskan negara untuk memberikan perlindungan maksimal terhadap hak privasi individu. Setiap individu berhak untuk mengendalikan data pribadi mereka dan memastikan bahwa data tersebut tidak disalahgunakan. Negara sebagai pihak yang bertanggung jawab atas perlindungan hak-hak dasar warganya harus memastikan bahwa semua regulasi yang ada mendukung perlindungan hak atas data pribadi dengan sebaik-baiknya. Dengan prinsip ini, regulasi perlindungan data pribadi tidak hanya fokus

---

[173] Irman Syahriar, Jamil Bazarah, dan Khairunnisah Khairunnisah, "Keadilan Sosial Di Dalam Negara Hukum Indonesia," *Journal of Knowledge dan Collaboration* 1, no. 2 (2024), hlm. 28-38.

[174] Nurtresna dan Mabsuti, *loc.cit*.

pada pengelolaan data, tetapi juga pada hak individu untuk memiliki kendali atas data yang dimiliki.

Regulasi yang ada harus mencegah eksploitasi data yang hanya menguntungkan pihak tertentu, terutama perusahaan teknologi dan lembaga keuangan, dengan mengorbankan kepentingan masyarakat luas. Nilai musyawarah untuk mufakat (sila keempat) menuntut agar kebijakan perlindungan data dibuat secara partisipatif dengan melibatkan berbagai pihak, termasuk masyarakat sipil. Kebijakan yang inklusif akan memastikan bahwa setiap individu memiliki perlindungan yang setara, tanpa adanya dominasi korporasi atau kepentingan politik tertentu dalam pengelolaan data pribadi. Pelindungan data pribadi yang bersifat spesifik seharusnya mencerminkan nilai-nilai kemanusiaan yang adil dan beradab serta keadilan sosial bagi seluruh rakyat indonesia, karena data pribadi merupakan bagian dari hak asasi manusia yang wajib dihormati dan dilindungi negara; penyalahgunaannya yang merugikan individu jelas bertentangan dengan prinsip kemanusiaan, keadilan, dan Persatuan Indonesia, sehingga perlindungan harus diterapkan secara adil tanpa diskriminasi, termasuk bagi kelompok rentan.

Kebijakan perlindungan data harus berlandaskan nilai-nilai Pancasila, tidak hanya melayani kepentingan bisnis dan ekonomi, tetapi juga menjamin penghormatan atas hak-hak fundamental setiap individu, dengan menyeimbangkan aspek hukum, keadilan sosial, pembangunan ekonomi, dan nilai-nilai kebangsaan. Berdasarkan perspektif Philipus M. Hadjon, Nancy Fraser, Mochtar Kusumaatmadja, serta nilai-nilai Pancasila, perlindungan data pribadi yang bersifat spesifik spesifik perlu diimplementasikan secara komprehensif, mencakup

penguatan penegakan hukum, peningkatan literasi masyarakat, dan pembangunan infrastruktur keamanan data yang lebih baik guna menciptakan ekosistem digital yang adil, aman, dan selaras dengan prinsip keadilan sosial.[175]

Pelindungan data pribadi yang bersifat spesifik merupakan aspek krusial dalam era digital yang menuntut pendekatan hukum yang komprehensif untuk memastikan keadilan dan kepastian hukum bagi setiap individu. Dalam konteks ini, perlindungan hukum terhadap data pribadi tidak hanya sebatas regulasi normatif, tetapi juga harus mencerminkan nilai-nilai keadilan sosial serta mendukung pembangunan hukum yang progresif dan responsif terhadap perubahan zaman.[176]

Perlindungan hukum terhadap data pribadi yang bersifat spesifik harus berorientasi pada kepastian hukum yang menjamin hak subjek data, baik dalam aspek preventif maupun represif. Negara bertanggung jawab memastikan setiap individu memiliki hak atas privasi dan perlindungan data dari penyalahgunaan, dengan menyediakan instrumen hukum yang tidak hanya berupa regulasi, tetapi juga mekanisme pengawasan, penegakan hukum, dan pemulihan bagi korban pelanggaran. Dengan demikian, perlindungan hukum terhadap data pribadi merupakan bagian dari kewajiban negara dalam menjaga dan memenuhi hak-hak konstitusional warga negaranya.[177]

---

[175] Shendy Rahmat Farhan dan Asep Suherman, "Perlindungan Hukum Terhadap Penyandang Disabilitas Dalam Perspektif Hak Asasi Manusia Di Indonesia," *Jurnal Inovasi Hukum Dan Kebijakan* 5, no. 4 (2024), hlm. 287-303.

[176] Syahriar, Bazarah, dan Khairunnisah, *loc.cit*.

[177] Achmad Rufaiddin Syifa dan Richard C. Adam, "Perlindungan Data Pribadi Nasabah Peminjam Dalam Layanan Pinjaman Meminjam Berbasis Teknologi Informasi Berdasarkan Hukum Perlindungan Data Pribadi," *UNES Law Review* 6, no. 2 (2024), hlm. 6739-6752.

Keadilan sosial merupakan prinsip fundamental dalam perlindungan data pribadi yang bersifat spesifik, yang mengharuskan regulasi tidak hanya berpihak pada korporasi tetapi juga melindungi masyarakat luas, termasuk kelompok rentan, melalui penerapan keadilan distributif dan rekognitif agar setiap individu tanpa memandang status sosial atau ekonomi mendapat perlindungan setara atas data yang menjadi bagian dari identitas dan martabatnya. Regulasi harus fleksibel mengikuti perkembangan teknologi tanpa mengorbankan hak individu, dengan pendekatan multidisipliner yang memadukan aspek hukum, teknologi, sosial, dan ekonomi, serta kolaborasi pemerintah, sektor swasta, dan masyarakat untuk membangun sistem perlindungan yang komprehensif, mulai dari infrastruktur keamanan digital hingga peningkatan literasi digital. Dalam kerangka ketatanegaraan, kebijakan ini harus berlandaskan nilai-nilai Pancasila penghormatan martabat manusia, keadilan, etika, kesetaraan, partisipasi publik, dan akses merata sehingga perlindungan hukum terhadap data pribadi yang bersifat spesifik tidak sekadar menjadi instrumen regulasi, tetapi juga mencerminkan keadilan sosial dan mendukung pembangunan hukum yang adaptif dan responsif terhadap dinamika era digital.[178]

Regulasi di berbagai negara memberikan kerangka hukum yang relevan dalam perlindungan data pribadi yang bersifat spesifik. Di Malaysia, *Personal Data Protection Act 2010 (PDPA)* mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh perusahaan, dengan memberikan hak kepada

[178] Anajeng Esri Edhi Mahanani, "Urgensi Kewenangan Mahkamah Konstitusi Dalam Pengujian Dan Pengaduan Konstitusional Atas Undang-Undang Non-Meaningful Participation," *Journal of Indonesian Law* 5, no. 2 (2024), hlm. 199-229.

individu untuk mengakses dan mengoreksi data pribadi mereka (*Seksyen* 5-8). Sementara itu, di Singapura, *Personal Data Protection Act (PDPA)* memberikan individu hak untuk mengakses, memperbaiki, dan meminta penghapusan data pribadi mereka, serta mengharuskan organisasi untuk melindungi data pribadi dan memenuhi kewajiban transparansi (Pasal 13, 24, 22). Regulasi-regulasi ini mencerminkan komitmen masing-masing negara untuk memastikan perlindungan data pribadi yang bersifat spesifik di tengah perkembangan teknologi digital yang pesat.

Perkembangan teknologi yang pesat di era digital membawa dampak positif besar, seperti kecepatan penyebaran informasi yang membuat peristiwa global (misalnya invasi Rusia ke Ukraina) segera diketahui publik melalui media sosial, namun sekaligus meningkatkan risiko kejahatan siber seperti kebocoran data. Ancaman ini tampak nyata pada Maret 2022 saat peneliti siber DarkTracer melaporkan kebocoran data kredensial dari lebih 49 ribu situs pemerintah dunia, termasuk situs Ditjen Pajak Indonesia dengan 17.585 data kredensial yang bocor, serta kasus serupa di situs ereg.pajak.go.id, yang menunjukkan perlunya penguatan sistem keamanan digital untuk melindungi informasi sensitif dan pribadi. Menanggapi hal tersebut, Direktur Penyuluhan, Pelayanan, dan Hubungan Masyarakat (P2Humas) DJP pada 20 September 2024 menjelaskan bahwa kebocoran tidak berasal dari sistem internal DJP, melainkan dari perangkat

pengguna yang terinfeksi malware dan kemudian digunakan untuk mengakses situs pemerintah.[179]

Pendekatan berbasis teknologi sangat penting dalam upaya menciptakan regulasi yang lebih spesifik,. Teknologi informasi berkembang sangat pesat, dan setiap regulasi yang diterapkan harus mampu beradaptasi dengan dinamika teknologi. Penggunaan sistem teknologi yang aman, seperti enkripsi dan sistem autentikasi berlapis, harus menjadi bagian dari regulasi untuk menjamin bahwa data pribadi yang dikumpulkan dapat terhindar dari kebocoran atau penyalahgunaan. Dengan demikian, regulasi yang ada harus memanfaatkan kemajuan teknologi untuk mengoptimalkan perlindungan data pribadi yang bersifat spesifik.[180]

Pada Januari 2022, DarkTracer juga melaporkan bahwa lebih dari 40.000 pengguna internet di Indonesia terinfeksi *malware* seperti Redline, Raccoon, dan Vidar. Selain itu, lebih dari 502 ribu data kredensial yang mengakses domain.id bocor dan tersebar melalui situs gelap. Kebocoran data ini tidak hanya mencakup situs pemerintahan seperti Kemdikbud, BKN, Ditjen Pajak, dan BPJS Ketenagakerjaan, tetapi juga menyasar aplikasi *e-commerce* seperti Shopee dan Lazada. [181] Berdasarkan laporan yang disusun oleh UpGuard, terdapat enam penyebab umum kebocoran data yang terjadi pada tahun 2021. Penyebab tersebut antara lain: kesalahan konfigurasi perangkat lunak, rekayasa sosial *(social*

---

[179] Mahmud Ashari, "Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga Adalah Data Pribadi," *Djkn.Kemenkeu.Go.Id*, last modified 2022, accessed April 23, 2025, https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.htmln.

[180] Fuad, Baskara, dan Urbaningrum, *loc.cit*.

[181] Oktarina Paramitha Sandy, "Lebih Dari 40.000 Pengguna Indonesia Terinfeksi Malware Pencuri," *Cyberthreat.Id*, last modified 2022, accessed May 6, 2025, https://cyberthreat.id/read/13359/Lebih-dari-40000-Pengguna-Indonesia-Terinfeksi-Malware-Pencuri.

engineering), penggunaan kata sandi yang berulang, pencurian perangkat yang mengandung data sensitif, kerentanan perangkat lunak, dan penggunaan kata sandi bawaan *(default password)*.[182]

Kebocoran data sangat erat kaitannya dengan pembobolan data. Ketika data terekspos ke internet atau situs yang tidak aman, seorang peretas dapat dengan mudah mengakses informasi pribadi yang sensitif dan melakukan pembobolan data. Berdasarkan penelitian literatur, faktor-faktor penyebab kebocoran data dapat dikelompokkan menjadi tiga kategori utama:[183]

1. Kesalahan Manusia *(Human Error)*: Manusia cenderung mencari solusi ekonomis seperti mengunduh perangkat lunak bajakan atau menggunakan aplikasi gratis yang menawarkan iming-iming bonus. Praktik ini sering kali menyebabkan data pribadi pengguna terekspos di situs atau aplikasi yang tidak aman.
2. Serangan *Malware*: Pengguna seringkali lalai dan tidak teliti saat membuka email atau tautan yang mencurigakan, yang berpotensi menjadi pintu masuk malware. *Malware*, seperti *spyware*, dirancang untuk menyusup ke perangkat dan mengumpulkan data pribadi tanpa persetujuan pengguna.
3. Social Engineering: Teknik manipulasi psikologis yang digunakan untuk mengelabui pengguna dan mengumpulkan data sensitif seperti

[182] Privy, "Kebocoran Data Di Indonesia Dan Pencegahannya," *Privy.Id*, last modified 2024, accessed May 6, 2025, https://privy.id/blog/kebocoran-data-di-indonesia-dan-pencegahannya/.

[183] Bonggal Noveno, "Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAIS-Q) Di Universitas Telkom Bandung," *e-Proceeding of Engineering* 12, no. 1 (2025), hlm. 2282-2293.

nama lengkap, *username*, dan kata sandi. Salah satu metode yang umum adalah *phishing*, dimana penyerang mengirimkan email yang menyamar sebagai pihak yang dapat dipercaya untuk membujuk korban mengklik tautan berbahaya.

Kebocoran data menimbulkan dampak serius bagi individu maupun perusahaan, antara lain kerugian finansial akibat pencurian identitas dan penipuan, hilangnya kepercayaan konsumen yang merusak reputasi perusahaan, penyalahgunaan data untuk kejahatan siber seperti peretasan akun, pemerasan, dan penipuan, serta pelanggaran privasi karena informasi rahasia jatuh ke tangan pihak yang tidak berwenang. Di era digital, kebocoran data umumnya disebabkan oleh kesalahan manusia, *malware*, dan *social engineering*, sehingga pengguna dan perusahaan perlu rutin mengganti password, memperkuat sistem keamanan, serta meningkatkan kesadaran akan pentingnya perlindungan data pribadi yang bersifat spesifik. Dengan demikian, perlindungan data pribadi yang bersifat spesifik harus menjadi prioritas utama demi terciptanya ekosistem digital yang aman, dengan dukungan regulasi yang memadai dan tanggung jawab bersama:[184] Beberapa penyebab kebocoran data yang terjadi di Indonesia dapat dibagi menjadi beberapa faktor utama, sebagai berikut:[185]

1. Kurangnya Kesadaran Keamanan Digital

   Banyak individu yang masih kurang menyadari pentingnya menjaga

[184] Mohamad Soleh dan Zubakhrum Tjenreng, "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital," *Jurnal Kajian Pemerintah (JKP) Journal of Government, Social dan Politics* 11, no. 1 (2024), hlm. 1-10.

[185] Imam Gunawan, "Upaya Preventif Dan Represif Dalam Penanggulangan Kebocoran Data Pada Penyelenggaraan Pinjaman Online," *Officium Notarium* 4, no. 1 (2024), hlm. 25-49.

keamanan digital mereka. Penggunaan kata sandi yang lemah, serta berbagi informasi pribadi secara sembarangan, seringkali menjadi celah bagi pihak yang tidak bertanggung jawab untuk mengeksploitasi data pribadi. Tanpa kesadaran yang memadai tentang keamanan data, masyarakat lebih rentan terhadap ancaman pencurian data.

2. Ketidakamanan Sistem

   Banyak perusahaan yang belum cukup fokus pada pengamanan sistem mereka, yang mengakibatkan adanya celah yang bisa dimanfaatkan oleh peretas untuk mencuri data. Sistem yang tidak diperkuat dengan proteksi yang memadai membuka peluang bagi pelaku kejahatan siber untuk mengakses dan menyalahgunakan informasi pribadi.

3. Kurangnya Regulasi dan Penegakan Hukum

   Indonesia belum memiliki regulasi yang cukup kuat untuk mengatur perlindungan data pribadi yang bersifat spesifik secara menyeluruh. Tanpa penegakan hukum yang ketat, pelaku kejahatan siber memiliki ruang gerak yang lebih luas untuk mengeksploitasi kebocoran data. Kurangnya kebijakan yang jelas juga menyulitkan masyarakat untuk mendapatkan perlindungan yang layak terkait data pribadi mereka.

Data pribadi telah menjadi bagian yang sangat sensitif dan penting dalam kehidupan digital saat ini. Informasi seperti nama, alamat, nomor identitas, informasi keuangan, dan riwayat kesehatan adalah beberapa contoh data yang sering menjadi sasaran bagi pelaku kejahatan siber. Dalam konteks ini, keamanan data pribadi bukan hanya masalah teknologi, tetapi juga hak asasi manusia yang

harus dijamin dan dihormati. Setiap individu berhak atas perlindungan data pribadi mereka, yang merupakan bagian dari hak privasi.[186]

Kesadaran terhadap pentingnya perlindungan data pribadi semakin meningkat di Indonesia, terutama dengan pertumbuhan pesat penggunaan internet dan aplikasi berbasis teknologi. Hal ini sesuai dengan Pasal 28G Ayat (1) Undang-Undang Dasar 1945, yang menjamin hak setiap warga negara untuk memperoleh perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta milik mereka. Oleh karena itu, perlindungan data pribadi harus menjadi prioritas dalam menjamin hak privasi warganya. Beberapa kasus kebocoran data yang terjadi di Indonesia menunjukkan betapa seriusnya masalah ini. Beberapa contoh kebocoran data yang baru-baru ini terjadi antara lain:

1. Kasus Tokopedia (2020)

   Pada awal 2020, platform *e-commerce* besar Tokopedia dilaporkan mengalami pelanggaran keamanan yang mengakibatkan kebocoran informasi pribadi jutaan penggunanya. Data yang terdampak meliputi nama, alamat, nomor telepon, alamat email, dan kata sandi yang terenkripsi.[187]

2. Kasus Bukalapak (2021)

   Pada tahun 2021, Bukalapak, platform *e-commerce* lainnya, juga mengalami pelanggaran data yang mengakibatkan lebih dari 13 juta

[186] Hari Sutra Disemadi et al., "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati Journal* 1, no. 2 (2023), hlm. 66-90.

[187] Eisya A. Eloksari, "Tokopedia Data Breach Exposes Vulnerability of Personal Data - Business - The Jakarta Post," *Thejakartapost.Com*, last modified May 5, 2020, accessed May 9, 2025, https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html.

akun pengguna terdampak. Data yang bocor termasuk nama pengguna, alamat *email*, nomor telepon, dan kata sandi.[188]

Kebocoran data pribadi merupakan ancaman serius yang dapat menyebabkan kerugian finansial, pencurian identitas, dan penyalahgunaan data lebih lanjut. Di tengah pesatnya perkembangan teknologi informasi yang mengubah cara berinteraksi dan beraktivitas secara daring, risiko terhadap keamanan dan privasi data juga meningkat. Seluruh perangkat yang terhubung ke internet membawa efisiensi, namun sekaligus membuka peluang terjadinya akses tidak sah terhadap data rahasia. Oleh karena itu, peningkatan kesadaran akan pentingnya keamanan data serta penerapan langkah-langkah pencegahan yang tepat menjadi sangat penting.

Laporan *Hootsuite* pada tahun 2020 menyatakan bahwa 64% penduduk Indonesia, atau lebih dari separuh populasi, terhubung ke internet. Mengingat jumlah pengguna internet yang besar, potensi kebocoran data di Indonesia semakin tinggi. Hal ini menimbulkan kekhawatiran yang mendalam di kalangan masyarakat, terutama mengingat potensi risiko pemanfaatan data pribadi oleh pihak yang tidak berwenang.[189] Pelindungan data pribadi sangat penting untuk mencegah kerugian finansial dan pelanggaran privasi, terutama di era digital yang rawan kebocoran data akibat kesalahan manusia, malware, dan *social engineering*. Oleh karena itu,

---

[188] Twingate Team, "What Happened in the Bukalapak Data Breach? | Twingate," *Twingate.Com*, last modified 2024, accessed May 9, 2025, https://www.twingate.com/blog/tips/bukalapak-data-breach.

[189] Hezkiel Bram Setiawan dan Fatma Ulfatun Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," *Jurnal Kewarganegaraan* 6, no. 1 (2022), hlm. 976-982.

diperlukan peningkatan kesadaran masyarakat tentang keamanan siber, penguatan literasi digital, serta penerapan regulasi yang lebih ketat.

Pengesahan Undang-Undang Pelindungan data pribadi (UU PDP) pada 2022 di Indonesia menjadi langkah penting dalam memperkuat perlindungan hukum bagi data pribadi dan meminimalkan risiko kebocoran di tengah pesatnya perkembangan teknologi.[190] Untuk mengatasi masalah ini, penting bagi pemerintah, perusahaan, dan individu untuk bekerja sama dalam meningkatkan kesadaran tentang keamanan data, memperkuat regulasi perlindungan data, serta memastikan Dalam era digital yang terus berkembang, data pribadi telah menjadi salah satu aset yang paling berharga, baik bagi individu maupun organisasi. Namun, dengan eksistensi data ini, muncul pula risiko yang signifikan, terutama ketika data tersebut jatuh ke tangan pihak yang tidak bertanggung jawab.

Fenomena yang dikenal sebagai *Massive Data Leak* telah menjadi isu serius dalam beberapa tahun terakhir. Istilah ini merujuk pada kebocoran data dalam skala besar yang melibatkan volume data sangat signifikan, yang bisa mencakup informasi pribadi, finansial, hingga rahasia perusahaan. *Massive Data Leak* terjadi ketika sejumlah besar data dicuri, bocor, atau terekspos tanpa izin. *Massive Data Leak* memiliki dampak luas yang signifikan, baik bagi individu, perusahaan, maupun masyarakat secara keseluruhan. Beberapa dampak utama dari kebocoran data besar-besaran ini antara lain:[191]

---

[190] Annisa Erikha dan Zainal Arifin Hoesein, "Jurnal Retentum Strategi Pencegahan Kebocoran Data Pribadi Melalui Peran Kominfo Dan Gerakan Siberkreasi Dalam Edukasi Digital," *Jurnal Retentum* 7, no. 1 (2025), hlm. 48-64.

[191] Althea Serafim Kriswandaru, Berliant Pratiwi, dan Suwardi, "Efektivitas Kebijakan Perlindungan Data Pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus," *Jurnal Ilmu Hukum dan Sosial* 2, no. 4 (2024), hlm. 740-755.

1. Ancaman Privasi Individu

   Kebocoran data dapat menyebabkan terungkapnya informasi pribadi seperti nama, alamat, nomor telepon, serta informasi finansial atau medis. Hal ini mengancam privasi individu dan meningkatkan risiko pencurian identitas, penipuan, atau pelecehan daring.

2. Potensi Penyalahgunaan Data

   Data yang bocor dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk tujuan yang tidak etis atau bahkan kriminal, seperti penjualan data ke pasar gelap, pemerasan, atau penggunaan data untuk penipuan.

3. Kerugian Finansial

   Perusahaan yang menjadi korban *Massive Data Leak* dapat mengalami kerugian finansial yang besar. Biaya perbaikan kerentanan keamanan, denda atau kompensasi kepada individu yang terdampak, serta dampak negatif pada reputasi merek dapat mengurangi penjualan dan menyebabkan kehilangan pelanggan.

4. Penurunan Kepercayaan Publik

   Insiden *Massive Data Leak* sering kali menyebabkan penurunan kepercayaan publik terhadap organisasi yang terlibat. Konsumen mungkin kehilangan kepercayaan terhadap perusahaan dan memilih untuk tidak berbisnis dengan mereka lagi, yang dapat merugikan reputasi dan profitabilitas jangka panjang perusahaan.

5. Dampak Hukum dan Regulasi

   Perusahaan yang melanggar peraturan perlindungan data dapat menghadapi konsekuensi hukum yang serius, termasuk sanksi denda signifikan dari badan pengatur dan gugatan hukum dari individu atau kelompok yang terdampak. Hal ini juga dapat merusak reputasi perusahaan di mata masyarakat dan pemerintah.

6. Gangguan Operasional

   Kebocoran data dapat menyebabkan gangguan operasional yang besar bagi organisasi. Waktu yang dihabiskan untuk menyelidiki insiden, memperbaiki kerentanan keamanan, memberi pemberitahuan kepada korban, dan menangani konsekuensi hukum dapat sangat mempengaruhi kelancaran operasional perusahaan.

7. Kerugian Ekonomi dan Kerugian Daya Saing

   Secara lebih luas, *Massive Data Leak* dapat memberikan dampak negatif terhadap ekonomi dan daya saing suatu negara. Insiden yang sering terjadi dapat merusak citra negara sebagai lokasi yang aman untuk berbisnis serta mengurangi kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi data pribadi.

Kebocoran data besar di Indonesia menjadi isu yang mendesak dan mencerminkan kerentanan yang ada dalam infrastruktur digital negara ini. Berikut

adalah beberapa contoh signifikan yang menggambarkan dampak dari peristiwa kebocoran data secara luas di Indonesia:[192]

1. Kebocoran Data Digital Pribadi Kementerian Kesehatan (2018)

   Pada 2018, terungkap bahwa data pribadi lebih dari satu juta pasien di Indonesia bocor secara daring. Informasi yang terungkap mencakup data sensitif seperti nama, nomor identitas, alamat, dan riwayat medis.

2. Kebocoran Data Akun Pengguna Gojek (2021)

   Pada 2021, dilaporkan bahwa data lebih dari 1,2 juta akun pengguna Gojek bocor ke internet. Data yang terungkap meliputi nomor telepon, alamat email, dan kata sandi.

3. Kebocoran Data PT. Asuransi Sosial Indonesia (Persero) (2020)

   Pada tahun yang sama, BPJS Kesehatan mengalami kebocoran data melibatkan informasi lebih dari 270 ribu peserta Jaminan Kesehatan Nasional (JKN). Data yang bocor mencakup nomor identitas, nama, tanggal lahir, dan informasi penting lainnya.

Kasus *massive data leak* menunjukkan betapa serius dampak kebocoran data pribadi, seperti skandal Facebook–Cambridge Analytica (2018) ketika data puluhan juta pengguna dimanfaatkan tanpa izin untuk memengaruhi opini publik dalam kampanye politik, serangan berulang ke Yahoo (2013–2016) yang membocorkan data ratusan juta akun, serta kebocoran besar di Equifax (2017) yang mengungkap informasi pribadi dan finansial sekitar 147 juta konsumen. Kasus lain adalah

[192] Muhammad Bachtiar Nur Fa'izi, "Mencegah Massive Data Leak Di Era Digital," *Cyberhub.Id*, last modified 2024, accessed May 9, 2025, https://cyberhub.id/pengetahuan-dasar/mencegah-massive-data-leak.

kebocoran di Marriott International (2018) yang memengaruhi sekitar 500 juta tamu dengan terekspos nya nama, email, nomor paspor, dan data pembayaran, serta kebocoran pada sistem identifikasi biometrik nasional India, Aadhaar (2018), yang mengancam privasi jutaan warga karena bocornya nomor Aadhaar dan data biometrik dari berbagai sumber.[193]

Fenomena kebocoran data tersebut menunjukkan bahwa insiden *data breach* tidak lagi bersifat sporadis, tetapi telah berkembang menjadi ancaman sistemik dalam tata kelola ekosistem digital global. Laporan *IBM Cost of a Data Breach Report* tahun 2023 menunjukkan bahwa rata-rata kerugian global akibat kebocoran data mencapai sekitar USD 4,45 juta per insiden, meningkat dibandingkan tahun-tahun sebelumnya. [194] Laporan yang sama juga menunjukkan bahwa sektor kesehatan, keuangan, dan teknologi informasi merupakan sektor yang paling rentan mengalami kebocoran data karena tingginya volume pengolahan data pribadi yang bersifat sensitif. Di tingkat global, *Cybersecurity Ventures* memperkirakan bahwa kerugian akibat kejahatan siber, termasuk pencurian dan kebocoran data, dapat mencapai USD 10,5 triliun per tahun pada 2025, menjadikannya salah satu bentuk kejahatan dengan dampak ekonomi terbesar di dunia.[195]

Kondisi tersebut juga tercermin dalam situasi di Indonesia yang mengalami peningkatan jumlah insiden kebocoran data dalam beberapa tahun terakhir. Data

---

[193] Kania Sutisnawinata, "Massive Data Leak: Arti, Penyebab, Contoh Kasus Terkenal," *Asdf.Id*, last modified 2024, accessed May 9, 2025, https://www.asdf.id/definisi-massive-data-leak/.

[194] I B M Security, *Cost of a Data Breach Report 2023* (IBM Corporation, 2023), https://www.ibm.com/reports/data-breach.

[195] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine* (Cybersecurity Ventures, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-5-trillion-annually-by-2025/.

dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa Indonesia mencatat lebih dari 976 juta anomali trafik siber pada tahun 2022, yang sebagian besar berkaitan dengan upaya serangan terhadap sistem informasi dan potensi pencurian data.[196] Laporan dari Surfshark Data Breach Statistics juga menunjukkan bahwa Indonesia termasuk salah satu negara dengan jumlah akun yang paling sering mengalami kebocoran data di kawasan Asia Tenggara, dengan puluhan juta akun pengguna internet dilaporkan terekspos dalam berbagai insiden kebocoran data sepanjang periode 2019–2023. [197] Fenomena tersebut memperlihatkan bahwa sistem perlindungan data pribadi yang bersifat spesifik di Indonesia masih menghadapi tantangan besar dalam aspek keamanan infrastruktur digital, tata kelola data, serta efektivitas pengawasan terhadap penyelenggara sistem elektronik.

Kasus *data breach* menjadi semakin marak di Indonesia juga memperlihatkan bahwa data yang paling sering menjadi sasaran kebocoran adalah data yang bersifat sensitif atau spesifik, seperti data kesehatan, data identitas kependudukan, data biometrik, serta data keuangan. Karakteristik data tersebut menjadikannya sangat bernilai dalam praktik kejahatan siber, termasuk pencurian identitas, penipuan finansial, dan perdagangan data di pasar gelap digital (*dark web*).[198] Kondisi ini menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik memerlukan standar pengamanan yang lebih tinggi dibandingkan dengan data pribadi yang

[196] Badan Siber dan Sandi Negara, *Lanskap Keamanan Siber Indonesia Tahun 2022* (Jakarta: Direktorat Operasi Keamanan Siber BSSN, 2023).

[197] Surfshark, "Global Data Breach Statistics: 2023 Recap" (Surfshark, 2024), https://surfshark.com/research/study/data-breach-recap-2023.

[198] Lenny Maria Aritonang, Zyetwill Zyetwill, and Rara Handayani, "Analisis Hukum Terhadap Kebocoran Data Pribadi Dan Penyalahgunaan Identitas Dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Ranah Research: Journal of Multidisciplinary Research and Development* Vol. 7, no. 5 (2025): hlm. 3146-3158.

bersifat umum. Tanpa adanya kerangka hukum yang kuat dan mekanisme pengawasan yang efektif, potensi kebocoran data akan terus meningkat seiring dengan semakin pesatnya perkembangan teknologi digital dan meningkatnya volume pertukaran data dalam masyarakat.

Fenomena *massive data leak* dan *data breach* pada akhirnya memperlihatkan adanya kesenjangan antara perkembangan teknologi digital dengan kesiapan sistem hukum dalam memberikan perlindungan terhadap data pribadi masyarakat.[199] Kondisi ini menegaskan urgensi rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik agar mampu memberikan perlindungan yang lebih komprehensif, adaptif terhadap perkembangan teknologi, serta selaras dengan prinsip keadilan sosial yang terkandung dalam Pancasila. Rekonstruksi hukum diharapkan mampu memperkuat tata kelola data pribadi, meningkatkan akuntabilitas penyelenggara sistem elektronik, serta menjamin perlindungan hak privasi masyarakat dalam ekosistem digital nasional.

Peningkatan penggunaan *e-commerce* dan media sosial dalam kehidupan digital telah memperkenalkan ancaman baru, seperti peretasan rekening bank, pencurian data pribadi, dan penggunaan akses yang tidak sah oleh pihak yang tidak dikenal. Hal ini menimbulkan keresahan di kalangan masyarakat.[200] Dalam konteks hukum pidana, tindak pidana pencurian data pribadi dapat ditemukan dalam Pasal 482 dan Pasal 483 Kitab Undang-Undang Hukum Pidana (KUHP) yang baru.

---

[199] Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia," *Dame Journal of Law* Vol. 1, no. 1 (2025): hlm. 111-133, https://doi.org/10.64344/djl.v1i1.6.

[200] Hartanto Hartanto, "Antisipasi Dan Perkembangan Kejahatan Dunia Maya," *Virtue Jurisprudence* Vol. 2, no. 2 (2024): hlm. 162-173.

Namun, aturan ini belum secara spesifik mengatur pencurian data pribadi secara online, sehingga perlindungan terhadap data pribadi konsumen *e-commerce* masih belum memadai. Peningkatan risiko tindak pidana pencurian data dan pelanggaran privasi pengguna *e-commerce* mencerminkan pergeseran fokus kejahatan ke ranah digital. Fenomena ini semakin kompleks karena semakin banyak informasi sensitif yang disimpan dan dipertukarkan dalam ekosistem transaksi online.[201]

Insiden kebocoran data ini mengarah pada pertanyaan mendasar tentang tanggung jawab perusahaan, mekanisme ganti rugi bagi konsumen, serta efektivitas regulasi yang ada. Secara global, upaya untuk meningkatkan perlindungan data pribadi telah dilakukan melalui berbagai kerangka hukum. Di Indonesia, pengesahan UU PDP mencerminkan kesadaran pemerintah akan urgensi perlindungan data pribadi yang bersifat spesifik dalam menghadapi ancaman dunia digital. Undang-undang ini merupakan langkah penting dalam menciptakan kerangka hukum yang komprehensif. Namun, implementasi dan pengawasan terhadap undang-undang tersebut masih menghadapi berbagai tantangan, termasuk keterbatasan kapasitas institusi dan kesenjangan antara regulasi dan perkembangan teknologi.[202]

Hak konsumen dalam konteks perlindungan data pribadi menjadi salah satu isu penting yang harus mendapatkan perhatian serius. Konsumen memiliki hak fundamental untuk mengetahui bagaimana data mereka digunakan, serta untuk meminta perbaikan atau penghapusan data yang dianggap tidak relevan atau

---

[201] I Wayan Cenik Ardika, "Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Era Digital : Kasus Kebocoran Data Pengguna Layanan," *Indonesian Journal of Law and Justice* 2, no. 3 (2025), hlm. 1-11.

[202] Ardika, *loc.cit*.

digunakan secara tidak sah.[203] Konsumen sering mengalami kesulitan dalam menuntut keadilan akibat keterbatasan akses terhadap mekanisme hukum dan minimnya tanggung jawab proaktif dari perusahaan. Hal ini menunjukkan pentingnya keberadaan kerangka hukum yang jelas dan tegas untuk menjamin hak konsumen atas ganti rugi serta memastikan akuntabilitas perusahaan. Di sisi lain, perkembangan teknologi yang pesat kerap melampaui kemampuan regulasi untuk beradaptasi, menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab. Oleh karena itu, dibutuhkan pendekatan holistik melalui penguatan regulasi, pengawasan ketat, dan peningkatan literasi digital masyarakat. Dalam konteks ini, pertumbuhan pesat *e-commerce* di Indonesia yang didorong oleh meningkatnya pengguna internet, adopsi teknologi, serta kemajuan logistikjuga menuntut perlindungan data pribadi yang lebih kuat agar konsumen tetap terlindungi dalam ekosistem digital yang terus berkembang.[204]

Perkembangan *e-commerce* di Indonesia mencerminkan respons terhadap perubahan kebutuhan pasar, yang mendorong peningkatan pengalaman konsumen dan inklusi digital. Perubahan ini turut memengaruhi hak dan kesejahteraan konsumen melalui meningkatnya kesadaran hukum dan penguatan regulasi perlindungan konsumen. Dua regulasi utama yang berperan penting adalah UU Perlindungan Konsumen (UU No. 8 Tahun 1999)[205] dan UU ITE (UU No. 19 Tahun

---

[203] Ilham et al., "Komparasi Hukum Indonesia Dan Hukum Islam Terhadap Perlindungan Data Pribadi Dalam Transaksi Ekonomi Syariah Digital," *Jurnal Media Akademik (JMA)* 3, no. 4 (2025), hlm. 1-21.

[204] Abdan Sifa, "Transformasi Digital E-Commerce Dalam Menguasai Kosentrasi Pasar Di Indonesia," *Jurnal Ilmiah Ekonomi Dan Manajemen* 2, no. 12 (2024), hlm. 405-413.

[205] Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen merupakan payung hukum nasional yang mengatur upaya perlindungan konsumen melalui pengaturan

2016)[206], yang melindungi konsumen dalam transaksi digital, khususnya terkait privasi dan keamanan data. Regulasi ini menjamin hak atas informasi yang jujur serta privasi data pribadi, dan mewajibkan penyedia layanan memberikan informasi yang jelas, termasuk kebijakan privasi dalam transaksi elektronik. [207]

UU ITE menetapkan aturan terkait perlindungan data pribadi, mencakup pengumpulan, pengolahan, dan penggunaan data pribadi konsumen oleh penyedia layanan elektronik. UU ITE menekankan pentingnya agar penyedia layanan melindungi data pribadi konsumen dan menjaga kerahasiaan informasi tersebut. Selain itu, UU ITE memberikan sanksi hukum bagi pelanggaran privasi, termasuk tindakan yang melibatkan penggunaan data pribadi tanpa izin atau untuk tujuan yang tidak sah.

1. Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999)

   Undang-Undang Perlindungan Konsumen di Indonesia berperan penting dalam melindungi konsumen dan mengatasi tantangan baru

kedudukan konsumen dan pelaku usaha, asas-asas perlindungan (manfaat, keadilan, keseimbangan, keamanan dan keselamatan, serta kepastian hukum), serta hak dan kewajiban para pihak. UU ini juga memuat pengaturan mengenai perbuatan yang dilarang (seperti peredaran barang cacat atau iklan menyesatkan), ketentuan klausula baku, mekanisme penyelesaian sengketa (melalui BPSK maupun pengadilan), serta sanksi administratif dan pidana bagi pelaku usaha yang melanggar ketentuan perlindungan konsumen. Indonesia, Republik. "Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." Jakarta, 1999.

[206] Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen merupakan payung hukum nasional yang mengatur upaya perlindungan konsumen melalui pengaturan kedudukan konsumen dan pelaku usaha, asas-asas perlindungan (manfaat, keadilan, keseimbangan, keamanan dan keselamatan, serta kepastian hukum), serta hak dan kewajiban para pihak. UU ini juga memuat pengaturan mengenai perbuatan yang dilarang (seperti peredaran barang cacat atau iklan menyesatkan), ketentuan klausula baku, mekanisme penyelesaian sengketa (melalui BPSK maupun pengadilan), serta sanksi administratif dan pidana bagi pelaku usaha yang melanggar ketentuan perlindungan konsumen. Indonesia, Republik. *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia, 2016.

[207] Unun Hestianingsih dan Nurmadiah, "Analisis Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Elektronik Di Indonesia," *Jurnal Pro Justice* 2, no. 8 (2024), hlm. 234-235.

dalam era digital, termasuk manipulasi pasar dalam transaksi digital. UU ini memastikan hak konsumen untuk mendapatkan informasi yang jujur dan benar tentang barang/jasa, termasuk dalam transaksi elektronik. Selain itu, UU ini juga mengakui hak privasi konsumen dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Perlindungan Konsumen dalam Transaksi Elektronik diwujudkan melalui pengakuan terhadap transaksi elektronik serta regulasi yang memastikan hak konsumen, termasuk hak untuk mendapatkan informasi yang jelas dan kebijakan privasi penyedia layanan.

2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi (UU PDP)

   Undang-Undang PDP memberikan dasar hukum yang jelas mengenai tanggung jawab perusahaan dalam menjaga data konsumen. Dengan penerapan UU PDP, pemerintah Indonesia berusaha meminimalkan insiden kebocoran data yang sering terjadi di berbagai perusahaan teknologi. UU ini mencakup berbagai aspek penting, termasuk cara data dikumpulkan, disimpan, diproses, dan dihapus, serta hak individu untuk meminta akses, koreksi, dan penghapusan data pribadi mereka jika diperlukan. Pasal 1 Pasal 2 UU PDP menyatakan bahwa perlindungan data pribadi yang bersifat spesifik merupakan upaya untuk melindungi data dalam rangka pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi, serta mengatur bagaimana data

tersebut akan diberikan dan digunakan oleh pihak lain. Pasal 4 UU PDP membagi data pribadi menjadi dua jenis:[208]

a. Data pribadi umum, seperti nama, alamat, status, agama, nomor telepon, yang dapat digunakan secara umum.
b. Data pribadi spesifik, seperti data kesehatan, biometrika, atau catatan kriminal, yang dianggap lebih sensitif dan memerlukan perlindungan lebih ketat.

UU PDP mengatur kewajiban pihak yang mengelola data pribadi, seperti perusahaan atau lembaga, untuk memastikan data yang disimpan tetap aman. Salah satu hal penting dalam UU PDP adalah hak pemilik data untuk mengetahui bagaimana data mereka digunakan, siapa yang menggunakannya, memperbaiki data atau menolak penggunaan data, serta meminta penghapusan data jika diperlukan. Konsep ini memberikan hak penuh kepada pemilik data untuk mengelola penggunaan informasi pribadi mereka. Pengelola data bertanggung jawab atas penggunaan data dan tidak boleh menyebarluaskannya tanpa izin pemilik.[209] Jika terjadi kebocoran data, pengelola data wajib memberi tahu informasi tersebut kepada pemilik data dan dapat dikenakan sanksi hukum, termasuk denda besar atau hukuman pidana.

---

[208] Chessyca Veranda dan Muhammad Alwan Zain Nusantara, "Analisis Perbandingan Pelindungan data pribadi yang bersifat spesifik Antara Indonesia Dan Arab Saudi," *PUSKAPSI Law Review* 4, no. 2 (2024), hlm. 236-256.

[209] Noval bin Usman dan Satria Unggul Wicaksana Prakasa, "Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP Legal," *DOKTRINA Journal of Law* 7, no. 27 (2024), hlm. 178-201.

3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

   a. Pasal 1 Ayat 4 dan 5

      Penyedia Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik untuk keperluan dirinya dan/atau pihak lain. Penyedia Sistem Elektronik Lingkup Publik adalah penyelenggaraan sistem elektronik oleh instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara.

   b. Pasal 14 Ayat 5

      Jika terjadi kegagalan dalam perlindungan terhadap data pribadi yang dikelola, penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut.

   c. Pasal 100 Ayat 2 tentang Sanksi

      Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa:

      1) Teguran tertulis.
      2) Denda administratif.
      3) Penghentian sementara.
      4) Pemutusan akses.
      5) Dikeluarkan dari daftar.

4. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan data pribadi dalam Sistem Elektronik

   a. Pasal 2 Ayat 1 dan 2

      Pelindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi.

      Dalam melaksanakan ketentuan ini, harus berlandaskan pada asas perlindungan data pribadi yang baik, yang meliputi:[210]

      1) Penghormatan Terhadap Data Pribadi Sebagai Privasi.
      2) Data Pribadi Bersifat Rahasia Sesuai Persetujuan Dan/Atau Ketentuan Perundang-Undangan.
      3) Relevansi Dengan Tujuan Pengolahan Data Pribadi.
      4) Kelayakan Sistem Elektronik Yang Digunakan.
      5) Iktikad Baik Untuk Memberitahukan Kegagalan Pelindungan data pribadi Kepada Pemiliknya.
      6) Ketersediaan Aturan Internal Untuk Pengelolaan Data Pribadi.
      7) Tanggung Jawab Atas Data Pribadi Yang Ada Dalam Penguasaan Pengguna.
      8) Kemudahan Akses Dan Koreksi Data Pribadi Oleh Pemiliknya.
      9) Keutuhan, akurasi, keabsahan, dan kemutakhiran data pribadi.

[210] Duta Agung Rohmansyah, Kevin Mandela Saputra, dan Badrus Sholih, "Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi Di Era Digitilasasi Berdasarkan Prinsip Negara Hukum," *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam* 5, no. 2 (2023), hlm. 1099-1110.

b. Pasal 36 Ayat 1

Setiap orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan ini dikenai sanksi administratif berupa:[211]

1) Peringatan Lisan.
2) Peringatan Tertulis.
3) Penghentian Sementara Kegiatan.
4) Pengumuman di situs internet.

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi besar dalam pola interaksi sosial manusia. Salah satu hasil nyata dari kemajuan ini adalah media sosial (*social networking sites*), yang kini menjadi bagian integral dari kehidupan masyarakat modern. Media sosial memberikan beragam manfaat di berbagai sektor, seperti pendidikan, birokrasi, komunikasi, dan ekonomi digital. Dengan keunggulan berupa kecepatan, akses yang luas, dan biaya rendah, media sosial menjadi sarana interaksi yang dominan di era digital.[212] Kehadiran media sosial mendorong keterhubungan tanpa batas, dimana pengguna dapat terus menerima pesan secara *real-time* dan menjalin komunikasi virtual lintas komunitas, bahkan dengan orang yang tidak dikenal sebelumnya.

---

[211] Muhammad Triadi, Sumiadi, dan Yusrizal, "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital," *REUSAM: Jurnal Ilmu Hukum* 11, no. 1 (2023), hlm. 45.

[212] Noviani Arum Sari Nur Hidayat, Ratih Novi Septian, dan Yusuf Tri Herlambang, "Sosial Media Dalam Masyarakat Sebagai Konsep Nyata Determinisme Teknologi," *UPGRADE: Jurnal Pendidikan Teknologi Informasi* 1, no. 2 (2024), hlm. 73-80.

Evolusi teknologi ini tidak hanya menciptakan konektivitas, tetapi juga membentuk industri global dengan nilai ekonomi yang sangat besar. Di balik manfaat tersebut, terdapat persoalan serius yang patut dicermati, yaitu ancaman terhadap perlindungan data pribadi khususnya yang bersifat spesifik. *Platform* digital pada umumnya mensyaratkan pengguna untuk mengungkapkan informasi pribadi seperti usia, alamat email, preferensi politik, hingga riwayat transaksi. Dalam konteks ini, data pribadi yang dibagikan secara sadar maupun tidak, sangat rentan dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab. Sekitar 42% pengguna media sosial adalah mahasiswa yang mengalami bentuk ancaman terhadap privasi mereka sepanjang hidup. Praktik digital ini menunjukkan bahwa media sosial, meskipun menguntungkan secara sosial dan ekonomi, juga menciptakan celah keamanan yang signifikan.[213]

Isu kebocoran data kini menjadi masalah yang sangat mendesak, sebagaimana diungkapkan oleh pakar IT dan CEO Equnix Business Solutions, Julyanto Sutandang. Dalam wawancara pada 23 Mei 2024, ia menyampaikan bahwa:

> "Fenomena kebocoran data semakin sering terjadi seiring meningkatnya penggunaan teknologi dan internet dalam berbagai aspek kehidupan. Muncul tantangan yang begitu kompleks dalam mengelola data."

Pernyataan tersebut menunjukkan bahwa intensifikasi penggunaan teknologi secara luas ternyata belum diimbangi dengan kesiapan sistem pengelolaan data yang memadai. Kebocoran data, menurutnya, bukan semata disebabkan oleh

[213] Vannyora Okditazeini dan Irwansyah Irwansyah, "Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS)," *Jurnal Studi Komunikasi dan Media* 22, no. 2 (2018), hlm. 109.

serangan eksternal, tetapi juga faktor internal yang kerap diabaikan. Ia menambahkan lima penyebab utama kebocoran data, yakni:

1. Penipuan Internal (*Internal Fraud*).
2. Rendahnya Kesadaran Keamanan TI.
3. Akses Ilegal.
4. *Malware* (Virus, Trojan, Ransomware).
5. Pelanggaran Perjanjian Kerahasiaan.

Lebih lanjut, Julyanto menekankan pentingnya pendekatan teknologi yang serius dalam menjaga keamanan data pribadi. Ia menyatakan:

> "Keamanan berlapis dan komprehensif adalah jurus ampuh menghadapi ancaman kebocoran data. Ini adalah langkah untuk memastikan kepatuhan sebuah korporasi terhadap UU PDP."

Pernyataan tersebut merefleksikan pemikiran bahwa perlindungan data seharusnya tidak lagi bersifat opsional. Justru, keamanan digital kini menjadi bagian integral dari tata kelola perusahaan, khususnya dalam memastikan kepatuhan terhadap regulasi seperti Undang-Undang Pelindungan data pribadi (UU PDP). Teknologi yang bisa digunakan, seperti protokol SSL dan sistem 11DB/Postgres yang dilengkapi enkripsi AES-256, serta pengelolaan kunci digital dengan HSM. Sistem ini memungkinkan perlindungan *in-transit* maupun *at-rest* tanpa mengganggu operasional aplikasi.[214]

Kepentingan akan transparansi dalam penggunaan data pribadi turut ditegaskan oleh Menteri Komunikasi dan Informatika, Budi Arie Setiadi. Ia

---

[214] Reska K. Nistanto, "Equnix Luncurkan Solusi Keamanan Data Pribadi ESE 11DB/Postgres," *Tekno.Kompas.Com*, last modified 2024, accessed May 9, 2025, https://tekno.kompas.com/read/2024/05/25/16150007/equnix-luncurkan-solusi-keamanan-data-pribadi-ese-11db-postgres.

menyatakan bahwa masyarakat saat ini menuntut kejelasan kebijakan dari penyedia layanan digital. Dalam keterangannya, Budi menjelaskan:

> "Pengesahan UU PDP yang dilakukan tahun 2022 memberikan Indonesia berbagai kesempatan, baik dalam melindungi hak fundamental masyarakat, maupun dalam mendorong inovasi digital secara bijaksana."

Dukungan masyarakat terhadap perlindungan data pribadi juga tercermin dari data *International Association of Privacy Professionals*, yang menyebutkan bahwa 68% konsumen global khawatir terhadap perlindungan data mereka, sementara 85% menginginkan transparansi kebijakan dari penyedia layanan digital.[215]

Senada dengan pandangan pemerintah, pakar hukum dan aktivis dari PDP Watch Indonesia, Agus Djunarjanto, menyatakan bahwa data pribadi adalah hak milik yang melekat pada individu. Dalam wawancaranya, ia menyebutkan:

> "Data pribadi itu ada pemiliknya. Karena itu harus dilindungi oleh undang-undang. Data security adalah bagian yang tak terpisahkan dari hak atas data pribadi."

Pernyataan dari perspektif tersebut, jelas bahwa aspek hukum tidak dapat dipisahkan dari keamanan data. Pelindungan data pribadi tidak hanya menyangkut sisi teknis, tetapi juga aspek normatif dan etis yang menyentuh hak konstitusional warga negara.

Situasi kebocoran data di Indonesia semakin mengkhawatirkan. APJII melaporkan bahwa hingga Juli 2023, telah terjadi beberapa kebocoran data besar, seperti:

1. Kebocoran 34 juta data paspor penduduk Indonesia.

---

[215] Dwitri Waluyo, “Era Baru Perlindungan Data Pribadi,” *Indonesia.Go.Id*, last modified 2024, accessed May 9, 2025, https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1.

2. Kebocoran 337 juta data penduduk dari Dukcapil yang diperjualbelikan di forum daring.

Fenomena ini menunjukkan lemahnya sistem manajemen data nasional serta mendesaknya penyusunan aturan turunan dari UU PDP. UU ini memang telah disahkan sejak 17 Oktober 2022, tetapi memberikan masa transisi dua tahun bagi lembaga dan perusahaan untuk menyesuaikan diri. Sesuai Pasal 74 UU PDP, batas waktu tersebut akan berakhir pada 2024. Dengan demikian, seluruh entitas pengelola data wajib memastikan kepatuhan terhadap UU PDP, baik dalam hal teknis pengolahan maupun prosedur pemberitahuan bila terjadi insiden kebocoran.[216]

Transformasi digital telah memberikan banyak kemudahan dalam kehidupan manusia, tetapi juga memunculkan ancaman baru, khususnya terhadap privasi dan keamanan data pribadi. Fenomena kebocoran data yang semakin sering terjadi menjadi peringatan akan pentingnya sinergi antara regulasi hukum, kesadaran masyarakat, dan penerapan teknologi keamanan yang tepat. Pernyataan para ahli dan pemangku kepentingan menunjukkan bahwa perlindungan data pribadi adalah tanggung jawab kolektif, yang harus ditanggapi secara serius oleh pemerintah, dunia usaha, dan masyarakat luas dalam rangka menciptakan ekosistem digital yang aman dan terpercaya.

Pelindungan data pribadi yang bersifat spesifik di Indonesia membutuhkan pendekatan hukum yang lebih spesifik agar dapat mengakomodasi kebutuhan

[216] Mochamad Januar Rizki, "Aturan Turunan UU PDP Molor, Pemerintah Didesak Beri Penjelasan Ke Publik," *Hukumonline.Com*, last modified 2024, accessed May 9, 2025, https://www.hukumonline.com/berita/a/aturan-turunan-uu-pdp-molor--pemerintah-didesak-beri-penjelasan-ke-publik-lt6756aba6d3b66/.

masyarakat yang semakin digital.[217] Dalam beberapa tahun terakhir, pelanggaran terhadap data pribadi semakin sering terjadi, baik yang melibatkan perusahaan besar maupun lembaga pemerintah. Mengingat pentingnya data pribadi dalam kehidupan sehari-hari, rekonstruksi hukum yang lebih kuat dan spesifik sangat diperlukan untuk memastikan perlindungan yang optimal. Oleh karena itu, Unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik harus dirancang dengan memperhatikan berbagai aspek yang relevan, mulai dari penguatan regulasi hingga pengawasan yang lebih ketat.

Unsur-unsur rekonstruksi hukum yang diusulkan harus memperhatikan keberagaman jenis data pribadi yang perlu dilindungi. Tidak semua data pribadi memiliki tingkat sensitivitas yang sama. Data yang terkait dengan kesehatan, keuangan, dan identitas pribadi misalnya, memerlukan perlindungan yang lebih ketat daripada data lainnya. Oleh karena itu, regulasi yang ada perlu disesuaikan untuk memberikan perlindungan yang lebih spesifik berdasarkan tingkat kerentanannya. Penyusunan aturan yang membedakan jenis data pribadi serta tingkat perlindungannya harus menjadi bagian dari unsur-unsur rekonstruksi hukum yang efektif.

Pembentukan lembaga pengawas yang lebih terfokus pada data pribadi juga sangat diperlukan dalam unsur-unsur rekonstruksi hukum ini. Lembaga pengawas yang ada saat ini, seperti Komisi Pelindungan data Pribadi, harus memiliki kewenangan yang lebih besar dalam mengawasi dan menindaklanjuti setiap pelanggaran data pribadi. Lembaga ini perlu dilengkapi dengan tenaga ahli yang

[217] Setiawan dan Khasanah, *loc.cit*.

memiliki pemahaman yang mendalam tentang teknologi informasi dan hukum perlindungan data pribadi. Dengan demikian, pengawasan terhadap pengelolaan data pribadi dapat dilakukan dengan lebih efektif.

Regulasi perlindungan data pribadi yang bersifat spesifikharus melibatkan peran aktif sektor swasta. Perusahaan-perusahaan yang mengelola data pribadi harus memiliki kewajiban untuk memastikan bahwa data yang mereka kelola aman.[218] Perusahaan perlu mengikuti standar regulasi yang ditetapkan pemerintah dan membangun sistem yang dapat melindungi data pribadi konsumen mereka. Oleh karena itu, sektor swasta harus dilibatkan dalam setiap tahapan penyusunan regulasi untuk memastikan bahwa regulasi yang diterapkan dapat dijalankan dengan baik.

Pendidikan dan pelatihan tentang perlindungan data pribadi juga merupakan aspek yang harus diperhatikan dalam unsur-unsur rekonstruksi hukum ini. Pelatihan tidak hanya diberikan kepada lembaga pemerintah dan sektor swasta, tetapi juga kepada masyarakat. Masyarakat perlu diberi pemahaman mengenai hak-hak mereka terkait dengan data pribadi, serta bagaimana cara melindungi data mereka dari penyalahgunaan. Dengan meningkatnya literasi digital, masyarakat dapat lebih aktif dalam menjaga dan melindungi data pribadi mereka.

Penguatan sanksi terhadap pelanggar harus menjadi bagian dari unsur-unsur rekonstruksi hukum ini. Sanksi yang diberikan harus cukup berat untuk memberikan efek jera bagi pelaku pelanggaran data pribadi. Tanpa adanya sanksi

[218] Sepyah Sepyah et al., "Implikasi Hukum Terhadap Perlindungan Data Pribadi Di Era Digital," *AL-BALAD: Jurnal Hukum Tata Negara dan Politik Islam* 2, no. 1 (2022), hlm. 26-36.

yang tegas, pelanggaran terhadap data pribadi akan terus meningkat, dan pelanggaran yang dilakukan oleh pihak-pihak besar mungkin tidak mendapatkan hukuman yang setimpal. Oleh karena itu, penegakan hukum yang konsisten dan tegas sangat penting dalam menjaga keberhasilan perlindungan data pribadi.[219]

Sistem audit yang transparan dan berkala harus diterapkan dalam pengelolaan data pribadi. Audit ini dapat dilakukan oleh lembaga pengawas yang independen untuk memastikan bahwa pengelolaan data pribadi sesuai dengan regulasi yang telah ditetapkan. Selain itu, audit ini juga dapat membantu dalam mendeteksi adanya kebocoran data atau potensi penyalahgunaan data pribadi, sehingga langkah perbaikan dapat segera dilakukan. Tanpa audit yang transparan, potensi pelanggaran data pribadi dapat semakin meningkat.

Unsur-unsur rekonstruksi hukum ini juga harus memperhatikan aspek internasional, mengingat banyaknya perusahaan global yang beroperasi di Indonesia dan mengelola data pribadi masyarakat Indonesia. Kerjasama internasional dalam perlindungan data pribadi sangat penting, terutama dalam menghadapi tantangan globalisasi dan teknologi. Negara Indonesia harus memastikan bahwa perusahaan-perusahaan multinasional yang beroperasi di Indonesia mengikuti standar yang sama dalam hal perlindungan data pribadi.[220] Kerjasama ini juga dapat memperkuat penegakan hukum terhadap pelanggaran data pribadi yang melibatkan entitas asing.

---

[219] Fitri Salsabila, "Implementasi Undangundang Nomor 19 Tahun 2016 Terhadap Pelaku Tindak Pidana Perundungan Dunia Maya" (Jakarta: Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2024).

[220] Erlina Puspitaloka Mahadewi, *Pemasaran Internasional* (Jambi: PT. Sonpedia Publishing Indonesia, 2025). hlm. 164.

Penerapan unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik yang lebih spesifik akan sangat bergantung pada partisipasi aktif semua pihak, baik itu pemerintah, sektor swasta, maupun masyarakat. Regulasi yang efektif hanya dapat terwujud jika ada kerjasama yang solid antara semua pihak yang terlibat dalam pengelolaan data pribadi. Negara harus menjadi fasilitator utama dalam menciptakan kerangka hukum yang dapat melindungi data pribadi secara adil dan merata.

Penerapan unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik yang lebih spesifik akan memberikan dampak positif bagi masyarakat Indonesia, dengan menjamin bahwa data pribadi setiap individu dilindungi dengan baik. Dengan adanya regulasi yang jelas, lembaga pengawas yang kuat, dan teknologi yang mendukung, pelanggaran terhadap data pribadi dapat diminimalkan. Hal ini akan menciptakan rasa aman dan kepercayaan masyarakat terhadap pengelolaan data pribadi, serta mendukung terciptanya keadilan sosial yang sejati.

Pelindungan data pribadi yang bersifat spesifik di Indonesia memerlukan pembaruan dalam bentuk rekonstruksi hukum yang lebih terintegrasi dengan nilai-nilai Pancasila. Prinsip-prinsip dasar yang terkandung dalam Pancasila dapat menjadi landasan utama dalam merancang regulasi perlindungan data pribadi yang tidak hanya menjamin keamanan data, tetapi juga keadilan sosial bagi seluruh rakyat Indonesia. Dalam hal ini, setiap langkah dalam rekonstruksi hukum harus memperhatikan nilai-nilai Pancasila, yang meliputi keadilan sosial, persatuan, dan penghormatan terhadap hak asasi manusia. Oleh karena itu, penting untuk

mengidentifikasi prinsip-prinsip dasar Pancasila yang relevan dengan pengelolaan data pribadi.

Prinsip persatuan yang terkandung dalam Pancasila juga sangat relevan dalam konteks perlindungan data pribadi yang bersifat spesifik. Dalam masyarakat yang plural, data pribadi harus dilindungi dengan memperhatikan kepentingan bersama, bukan hanya kepentingan individu atau kelompok tertentu. Persatuan mengajarkan pentingnya untuk menjaga keharmonisan dalam masyarakat, yang dapat tercermin dalam cara data pribadi dikelola oleh sektor publik maupun swasta. Pengelolaan data pribadi yang baik harus dapat menghindari pemecahbelahan di masyarakat, misalnya dengan tidak mempergunakan data pribadi untuk kepentingan yang dapat merugikan kelompok tertentu.

Menghormati hak asasi manusia menjadi nilai yang tidak dapat dilepaskan dalam konteks rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik. Setiap individu memiliki hak yang melekat pada dirinya, termasuk hak atas privasi dan perlindungan data pribadi.[221] Negara sebagai pihak yang bertanggung jawab dalam melindungi hak-hak individu harus memastikan bahwa regulasi yang ada tidak hanya mengatur penggunaan data pribadi, tetapi juga memberikan perlindungan terhadap potensi penyalahgunaan data yang dapat merugikan individu. Prinsip penghormatan terhadap hak asasi manusia harus menjadi pedoman dalam setiap kebijakan yang mengatur pengelolaan data pribadi.

[221] Herol Hansen Samin, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif," *Jurnal Ilmiah Research Student* 1, no. 3 (2024), hlm. 1-15.

Prinsip musyawarah untuk mufakat yang juga terkandung dalam Pancasila dapat diadaptasi dalam penyusunan regulasi perlindungan data pribadi. Pembuatan kebijakan yang melibatkan partisipasi berbagai pihak, seperti masyarakat, pemerintah, dan sektor swasta, akan menghasilkan regulasi yang lebih inklusif dan representatif. Musyawarah untuk mufakat menciptakan ruang bagi setiap pihak untuk menyampaikan pendapatnya, sehingga setiap regulasi yang dihasilkan akan mencerminkan kepentingan bersama, bukan hanya kepentingan kelompok tertentu. Proses ini juga akan meningkatkan akseptabilitas kebijakan oleh masyarakat.

Penegakan prinsip transparansi dalam merumuskan prinsip-prinsip dasar rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik adalah elemen penting. Setiap kebijakan yang diambil dalam pengelolaan data pribadi harus jelas dan dapat dipahami oleh masyarakat. Transparansi dalam pengelolaan data pribadi akan menciptakan kepercayaan antara pemerintah, sektor swasta, dan masyarakat. Selain itu, prinsip transparansi juga berfungsi untuk memastikan bahwa data pribadi digunakan sesuai dengan tujuan yang telah ditetapkan, dan tidak disalahgunakan untuk kepentingan yang merugikan pihak lain.[222]

Prinsip akuntabilitas juga perlu diterapkan dalam regulasi perlindungan data pribadi. Akuntabilitas berarti setiap pihak yang terlibat dalam pengelolaan data pribadi harus bertanggung jawab atas tindakan mereka. Dalam hal ini, pemerintah dan sektor swasta harus dapat memberikan penjelasan mengenai bagaimana data pribadi dikelola dan digunakan.[223] Selain itu, mereka juga harus dapat

[222] Elvina Putri Maheswari and Sidi Ahyar Wiraguna, "Urgensi Persetujuan Pemilik Data Dalam Pengelolaan Data Pribadi Oleh Platform Digital," *Jurnal Ilmu Komunikasi Dan Sosial Politik* 2, no. 4 (2025), hlm. 908-914.

[223] Satria dan Yusuf, *loc.cit*.

mempertanggungjawabkan segala tindakan yang berkaitan dengan penyalahgunaan data pribadi. Negara harus menciptakan mekanisme yang memungkinkan masyarakat untuk menuntut pertanggungjawaban apabila terjadi pelanggaran terhadap data pribadi.

Prinsip keadilan ekonomi juga harus tercermin dalam regulasi perlindungan data pribadi yang bersifat spesifik. Setiap pihak yang mengelola data pribadi, baik itu sektor publik maupun swasta, harus mengedepankan prinsip keadilan dalam memanfaatkan data tersebut.[224] Tidak boleh ada pihak yang lebih diuntungkan secara ekonomi dari penggunaan data pribadi tanpa memberikan manfaat yang setara kepada pemilik data. Regulasi yang ada harus memastikan bahwa penggunaan data pribadi tidak hanya menguntungkan perusahaan besar atau pihak-pihak tertentu, tetapi juga memberikan manfaat bagi masyarakat secara umum.

Penguatan sistem perlindungan data pribadi juga harus diimbangi dengan prinsip keadilan sosial dalam pengawasan. Pengawasan terhadap pengelolaan data pribadi harus dilakukan dengan prinsip keadilan, tanpa memandang latar belakang atau status ekonomi individu. Pemerintah harus memastikan bahwa proses pengawasan tidak hanya menguntungkan pihak-pihak tertentu, tetapi juga mengutamakan kepentingan seluruh rakyat Indonesia. Pengawasan yang adil akan memastikan bahwa data pribadi dikelola dengan cara yang sesuai dengan prinsip-prinsip Pancasila.

---

[224] Elza Aulia, "Analisis Pasal 56 Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik Dari Perspektif Kepastian Hukum," *UNES Law Review* 7, no. 1 (2024), hlm. 220-227.

Keadilan sosial juga mengajarkan pentingnya pendidikan dan kesadaran masyarakat mengenai perlindungan data pribadi. Masyarakat harus diberdayakan dengan informasi yang cukup mengenai hak mereka atas data pribadi dan cara melindungi data mereka dari penyalahgunaan.[225] Negara harus mengembangkan program pendidikan yang mengedukasi masyarakat mengenai pentingnya perlindungan data pribadi dan bagaimana cara melindunginya. Pendidikan ini akan menciptakan masyarakat yang lebih paham dan lebih peduli terhadap hak mereka terkait data pribadi.

Pembangunan regulasi berbasis nilai Pancasila memerlukan komitmen dari berbagai pihak, terutama pemerintah, dalam mengimplementasikan prinsip-prinsip dasar tersebut dalam kebijakan publik. Negara harus berperan sebagai fasilitator utama dalam merumuskan dan menerapkan regulasi yang sesuai dengan prinsip keadilan sosial, penghormatan terhadap hak asasi manusia, serta keberagaman yang ada di masyarakat Indonesia. Pembangunan regulasi ini harus dilaksanakan dengan hati-hati, agar dapat mencapai tujuan yang telah ditetapkan tanpa mengabaikan kepentingan masyarakat yang lebih luas.

Regulasi perlindungan data pribadi yang bersifat spesifik yang berkeadilan menuntut penguatan komitmen negara pada prinsip-prinsip Pancasila dengan mengutamakan keadilan sosial, persatuan, dan penghormatan terhadap hak asasi manusia dalam setiap kebijakan. UU PDP yang sudah berlaku masih menghadapi berbagai tantangan implementasi, tercermin dari maraknya kebocoran data yang menunjukkan bahwa pengaturan yang ada belum cukup spesifik, adaptif terhadap

[225] Putri et al., *loc.cit*.

perkembangan teknologi, dan efektif melindungi data pribadi masyarakat. Penataan ulang regulasi diperlukan agar mampu melindungi seluruh jenis data pribadi, terutama data sensitif seperti data medis dan biometrik, dengan pembedaan tingkat perlindungan sesuai tingkat sensitivitas data. Pengelolaan data oleh sektor publik dan swasta wajib memenuhi standar keamanan tinggi melalui teknologi pengamanan canggih seperti enkripsi dan autentikasi berlapis, diawasi lembaga pengawas yang memiliki kewenangan memadai, serta didukung penegakan hukum dengan sanksi yang jelas, tegas, dan proporsional untuk menimbulkan efek jera dan memastikan perlindungan data pribadi yang optimal bagi seluruh masyarakat.[226]

Penyusunan regulasi perlindungan data pribadi yang bersifat spesifik yang lebih spesifik memerlukan pendekatan berbasis bukti melalui pengumpulan data yang akurat dan analisis menyeluruh terhadap pola kebocoran serta pelanggaran, sehingga regulasi yang dirumuskan benar-benar menjawab masalah yang ada. Unsur-unsur regulasi ideal harus menjamin transparansi pengelolaan data, mewajibkan pengelola data menjelaskan secara terbuka cara data dikumpulkan, disimpan, digunakan, serta siapa saja yang mengaksesnya, sekaligus meningkatkan kepercayaan masyarakat. Upaya ini perlu didukung oleh peningkatan kesadaran publik mengenai hak-hak atas data pribadi agar masyarakat mampu mengontrol dan melindungi data mereka sendiri. Regulasi juga harus responsif terhadap perkembangan teknologi dan mengatur secara tegas platform digital serta pihak-pihak yang mengumpulkan dan memproses data pribadi, termasuk penyedia *cloud* dan pihak *outsourcing*, dengan standar keamanan dan pengawasan yang ketat, serta

[226] Yamin et al., *loc.cit*.

diperkuat melalui kerja sama internasional untuk menghadapi perusahaan multinasional dan mendorong harmonisasi standar perlindungan data lintas negara.

Hak subjek data harus dijamin, meliputi hak untuk mengetahui jenis dan tujuan pemrosesan data, hak akses dan perbaikan, hak penghapusan, serta hak untuk memberikan dan menarik persetujuan secara sadar. Pengelola data berkewajiban menerapkan prinsip transparansi, keamanan, privasi, dan akuntabilitas melalui penggunaan teknologi pengamanan yang memadai, audit berkala, pembatasan akses yang sah, kewajiban pelaporan cepat atas kebocoran data beserta pemberitahuan kepada pemilik data, serta mekanisme penanganan pengaduan. Seluruh tata kelola ini perlu berlandaskan prinsip keadilan sosial dalam Pancasila, sehingga perlindungan data pribadi diberikan secara setara kepada seluruh warga tanpa diskriminasi, mengutamakan kepentingan masyarakat, dan ditegakkan melalui regulasi yang jelas, tegas, dan efektif untuk menjaga kepercayaan publik.

B. Implikasi Hukum Perlindungan Data Pribadi Yang Bersifat Spesifik di Era Digital

Pelindungan data pribadi yang bersifat spesifik merupakan elemen esensial dalam menjamin hak asasi manusia di era digital. Ketika perlindungan tersebut tidak memadai, individu menghadapi risiko serius berupa pencurian identitas, penyalahgunaan informasi, hingga manipulasi data untuk kepentingan ekonomi dan politik. Data pribadi yang bersifat spesifik, seperti informasi medis, biometrik, keuangan, serta rekam jejak digital, memiliki sensitivitas tinggi karena menyangkut aspek privat yang melekat pada identitas seseorang. Lemahnya sistem perlindungan data pribadi yang bersifat spesifik menjadikan data spesifik ini mudah diakses oleh

pihak tidak sah, yang berakibat pada pelanggaran privasi secara masif serta merugikan individu dan lembaga secara ekonomi dan hukum.[227]

Kerugian nyata dari lemahnya perlindungan data pribadi adalah pencurian identitas. Menurut Federal Trade Commission, lebih dari 1 juta laporan pencurian identitas terjadi setiap tahunnya di Amerika Serikat, dengan kerugian mencapai miliaran dolar. Pencurian ini biasanya melibatkan data spesifik seperti nomor jaminan sosial, identitas finansial, dan informasi pribadi lainnya.[228] Di Indonesia, belum ada angka resmi setara, namun laporan dari Masyarakat Anti Fitnah Indonesia (MAFINDO) menunjukkan bahwa laporan pencurian data meningkat drastis sejak pandemi COVID-19, seiring meluasnya penggunaan layanan digital yang tidak terlindungi oleh sistem keamanan siber yang kuat.

Data pribadi yang bersifat spesifik, terutama informasi medis, menjadi target empuk dalam serangan siber. Berdasarkan laporan dari IBM, sektor layanan kesehatan menjadi industri dengan biaya kebocoran data tertinggi, mencapai rata-rata USD 10,93 juta per insiden. Informasi medis mencakup diagnosis, riwayat penyakit, hingga hasil laboratorium, yang jika bocor tidak hanya memengaruhi reputasi pasien tetapi juga dapat dimanfaatkan untuk diskriminasi oleh asuransi atau pemberi kerja.[229] Di Indonesia, insiden kebocoran data medis pernah terjadi di

---

[227] Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* Vol. 6, no. 1 (April 25, 2023): hlm. 132-142.

[228] Tim Internet Sehat, "FTC : Orang Amerika Alami Kerugian 5,8 Miliar Dollar AS Karena Penipuan | Internetsehat.Id," *Internetsehat.Id*, last modified 2022, accessed May 9, 2025, https://internetsehat.id/2022/02/24/ftc-orang-amerika-alami-kerugian-58-miliar-dollar-as-karena-penipuan/.

[229] Restu Aji Siswanto, "Laporan IBM: Kebocoran Data Capai Rekor Tertinggi, Kerugian Terbesar Di Sektor Keuangan," *Pricebook.Co.Id*, last modified 2024, accessed May 9, 2025, https://www.pricebook.co.id/article/news/14155/laporan-ibm-kebocoran-data-capai-rekor-tertinggi-kerugian-terbesar-di-sektor-keuangan.

Kementerian Kesehatan pada tahun 2021, yang menunjukkan lemahnya pengamanan sistem informasi rumah sakit dan instansi kesehatan publik.[230]

Data biometrik seperti sidik jari, wajah, atau retina juga tergolong sebagai data pribadi spesifik. Kebocoran data biometrik berbahaya karena tidak dapat diubah seperti halnya kata sandi. Sekali bocor, data ini dapat digunakan secara permanen untuk akses ilegal ke berbagai sistem. Data biometrik memiliki "*non-repudiable identity value*" yang menjadikannya sangat rentan terhadap kejahatan siber jangka panjang. Di beberapa negara, data biometrik bahkan dijual di pasar gelap untuk membuka akses ke akun keuangan atau sistem pemerintahan.[231]

Dampak ekonomi akibat lemahnya perlindungan data pribadi spesifik sangat signifikan. Berdasarkan data dari Ponemon Institute**,** rata-rata kerugian finansial akibat kebocoran data mencapai USD 4,45 juta per organisasi di tahun 2022. Dalam konteks ini, data finansial seperti nomor rekening, kartu kredit, serta riwayat transaksi menjadi sasaran utama.[232] Di Indonesia, kebocoran data 91 juta pengguna Tokopedia pada tahun 2020 menjadi contoh nyata. Data pengguna yang bocor mencakup alamat email dan kata sandi yang dapat dikombinasikan dengan teknik rekayasa sosial untuk melakukan pembobolan akun bank dan dompet digital pengguna.

---

[230] Satu.xl.co.id, "Penting! Ini Penyebab Kebocoran Data Pribadi Di Era Digital," *Satu.Xl.Co.Id*, last modified 2025, accessed May 9, 2025, https://satu.xl.co.id/berita-dan-artikel/penyebab-kebocoran-data-pribadi/.

[231] Bimo Kresnomurti, "Jadi Data Biometrik, Pahami Bahaya Jual-Beli Informasi Iris Dan Retina Mata," *Caritahu.Kontan.Co.Id*, last modified 2025, accessed May 9, 2025, https://caritahu.kontan.co.id/news/jadi-data-biometrik-pahami-bahaya-jual-beli-informasi-iris-dan-retina-mata.

[232] Halock.com, "Summarizing the Ponemon Cost of a Data Breach Report 2022," *Halock.Com*, last modified 2022, accessed May 6, 2025, https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/.

Individu yang menjadi korban kebocoran data juga mengalami kerugian dari sisi psikologis mengalami stres, kecemasan, dan rasa takut akan penyalahgunaan informasi mereka. Korban pelanggaran privasi cenderung merasa kehilangan kendali atas kehidupan pribadi mereka dan mengalami trauma jangka panjang, terutama jika informasi yang bocor adalah data kesehatan mental, orientasi seksual, atau riwayat kriminal.[233] Kondisi ini diperburuk ketika tidak ada mekanisme pemulihan atau perlindungan hukum yang kuat untuk mengembalikan hak dan martabat korban.

Kelemahan dalam perlindungan data spesifik juga menimbulkan kerugian pada institusi. Reputasi perusahaan dapat hancur akibat kebocoran data, yang berujung pada penurunan kepercayaan pelanggan dan mitra bisnis. Kasus Equifax di Amerika Serikat, yang membocorkan data 147 juta konsumen pada tahun 2017, menyebabkan kerugian hingga USD 700 juta dalam bentuk denda dan gugatan hukum. Dalam konteks Indonesia, kepercayaan publik terhadap institusi seperti BPJS Kesehatan menurun setelah dugaan kebocoran data 279 juta penduduk pada tahun 2021, meskipun belum semua dikonfirmasi secara resmi.

Kebocoran data pribadi spesifik juga berimplikasi pada kerentanan terhadap manipulasi politik dan sosial. Contoh paling nyata adalah skandal Cambridge Analytica, dimana data spesifik tentang preferensi politik dan psikografi pengguna Facebook digunakan untuk memengaruhi pemilu di Amerika Serikat dan Inggris. Dalam konteks ini, data pribadi menjadi alat propaganda yang disalahgunakan

[233] Zul Khadir Kadir, "Dari Privasi Ke Eksploitasi : Memetakan Jejak Kriminalisasi Revenge Porn Dalam Era Media Sosial," *Dewantara: Jurnal Pendidikan Sosial Humaniora* 4, no. 1 (2025), hlm. 133-152.

untuk merusak tatanan demokrasi. Hal ini menimbulkan kekhawatiran bahwa tanpa perlindungan yang kuat, data masyarakat dapat dieksploitasi oleh aktor politik, baik domestik maupun asing.

Sistem perlindungan data pribadi yang bersifat spesifik yang kurang efisien juga menyebabkan pemborosan sumber daya negara. Pemerintah harus mengalokasikan dana besar untuk memulihkan sistem, membayar kompensasi, dan menangani dampak kebocoran data. Sebagai contoh, pemerintah Australia harus mengeluarkan lebih dari AUD 1,8 miliar untuk menangani insiden kebocoran data di lembaga-lembaga pelayanan publik antara tahun 2018–2022.[234] Tanpa sistem keamanan dan kebijakan data yang memadai, insiden serupa sangat mungkin terjadi berulang kali dengan dampak yang semakin luas.

Pelindungan data pribadi yang bersifat spesifik yang lemah membuat penegakan keadilan menjadi tumpul: banyak kasus kebocoran data tidak pernah sampai ke ranah hukum karena mekanisme pelaporan belum jelas dan korban tidak memahami hak-haknya. Di Indonesia, meskipun UU No. 27 Tahun 2022 tentang Pelindungan data pribadi telah disahkan, aturan turunan dan lembaga pengawasnya belum optimal, serta belum adanya lembaga independen semacam *Data Protection Authority* sehingga korban sering tidak memperoleh kompensasi dan pemulihan yang adil. Pelanggaran data pribadi juga menimbulkan konsekuensi hukum bagi institusi pengelola data, karena kebocoran data pelanggan dapat dianggap sebagai

[234] Australian Goverment, "Notifiable Data Breaches Report: July to December 2022 | OAIC," *Oaic.Gov.Au*, last modified 2022, accessed May 6, 2025, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022.

kelalaian atau wanprestasi yang membuka potensi gugatan perdata maupun sanksi pidana jika kelalaian bersifat sistemik.[235]

Kerugian akibat kebocoran data pribadi yang spesifik juga mencakup potensi eksploitasi terhadap kelompok rentan seperti anak-anak, penyandang disabilitas, dan lansia. Ketika data tentang status medis, keterbatasan fisik, atau kebutuhan khusus terekspos, kelompok ini dapat menjadi target diskriminasi atau penipuan yang lebih kompleks. Oleh karena itu, pendekatan berbasis HAM dalam perlindungan data menjadi sangat penting. Data dari UNICEF pada tahun 2022 menunjukkan bahwa anak-anak pengguna internet sering kali tidak memahami implikasi dari jejak digital mereka, menjadikan mereka sasaran empuk bagi pelaku kejahatan digital.[236]

Kebocoran data akademik atau psikologis siswa dapat menciptakan stigma dan tekanan sosial. Misalnya, hasil psikotes, nilai rapor, atau data kesehatan mental siswa jika bocor ke publik, dapat menyebabkan bullying atau pengucilan. Studi dari UNESCO menekankan bahwa sistem pendidikan yang tidak menerapkan prinsip keamanan digital yang kuat dapat memperburuk ketimpangan sosial dan emosional di kalangan pelajar. Institusi pendidikan wajib menyadari bahwa data siswa, terutama yang bersifat spesifik dan sensitif, harus dijaga ketat dan hanya diakses oleh pihak yang berwenang.[237]

---

[235] Teuku Riefky and Jahen F Rezki, "Isu Keamanan Siber Perbankan Dan Potensi Bank Run," *LPEM FEB UI: Institute for Economic and Social Reserach* 1, no. 1 (2023), hlm. 1-9.

[236] UNICEF, "UNICEF Annual Report 2022 | UNICEF," *Unicef.Org*, last modified 2022, accessed May 6, 2025, https://www.unicef.org/reports/unicef-annual-report-2022.

[237] UNESCO, "Bridging the Digital Divide and Ensuring Online Protection | UNESCO," *Unesco.Org*, last modified 2023, accessed May 6, 2025, https://www.unesco.org/en/right-education/digitalization.

Praktik penyimpanan data yang tidak aman menjadi salah satu penyebab utama terjadinya kebocoran data. Banyak institusi menyimpan data sensitif dalam server lokal tanpa enkripsi atau tanpa mekanisme autentikasi berlapis. Ketika server tersebut diretas, seluruh data rentan terekspos. Berdasarkan laporan Verizon tentang *Data Breach Investigations*, 45% kebocoran data terjadi akibat *misconfiguration* sistem dan lemahnya *access control*.[238]

Berdasarkan tinjauan literatur, penyebab kebocoran data pribadi dapat dikelompokkan menjadi tiga faktor utama:

1. Kesalahan Manusia (*Human Error*):

   Praktik seperti penggunaan perangkat lunak bajakan, pengunduhan dari sumber tidak resmi, serta pemakaian kata sandi yang mudah ditebak menjadi penyebab kebocoran data paling umum.

2. Serangan *Malware*:

   Malware seperti *spyware* dan *ransomware* menyusup melalui email palsu atau file yang tampak sah. Program ini dirancang untuk mencuri informasi secara diam-diam tanpa sepengetahuan pengguna.

3. Manipulasi Psikologis (*Social Engineering*):

   Teknik seperti *phishing*, *pretexting*, dan *baiting* digunakan untuk memancing korban memberikan data pribadi melalui komunikasi yang menipu.

[238] Verizon, "2025 Data Breach Investigations Report | Verizon," *Verizon.Com*, last modified 2025, accessed May 6, 2025, https://www.verizon.com/business/resources/reports/dbir/.

Kebocoran data pribadi spesifik juga menghambat akses ke layanan publik yang berbasis digital. Misalnya, jika data kependudukan atau kesehatan seseorang bocor dan disalahgunakan, hal tersebut dapat mengganggu proses administratif saat mengakses layanan rumah sakit, perbankan, atau pendidikan. Di Indonesia, kegagalan sistem *PeduliLindungi* yang sempat mengungkap data vaksinasi dan NIK pengguna menjadi bukti betapa pentingnya arsitektur keamanan siber dalam layanan publik. Tanpa sistem pelindung yang kuat, pelayanan berbasis digital justru menjadi ancaman bagi integritas data warga negara.[239]

Dampak reputasional terhadap korban kebocoran data tidak bisa diabaikan. Individu yang datanya bocor kerap menjadi sasaran penilaian negatif, apalagi bila informasi tersebut bersifat sensitif seperti status HIV, orientasi seksual, atau afiliasi politik. Di media sosial, fenomena *doxing*, yakni pembocoran data pribadi untuk mempermalukan atau mengintimidasi seseorang, kian marak terjadi. Amnesty International pada tahun 2023 melaporkan bahwa *doxing* telah digunakan secara luas untuk membungkam aktivis dan jurnalis di berbagai negara, termasuk Indonesia.[240]

Industri perbankan dan keuangan sangat rentan terhadap lemahnya perlindungan data karena kebocoran informasi rekening, transaksi, atau kartu kredit dapat menimbulkan kerugian besar dalam waktu singkat, Bank Indonesia mencatat

---

[239] Fitria Chusna Farisa dan Icha Rastika, "PeduliLindungi Dinilai Belum Sepenuhnya Lindungi Data Pribadi, Perlu Audit Dan Pembenahan Halaman All - Kompas.Com," *Nasional.Kompas.Com*, last modified September 5, 2021, accessed May 9, 2025, https://nasional.kompas.com/read/2021/09/05/14151171/pedulilindungi-dinilai-belum-sepenuhnya-lindungi-data-pribadi-perlu-audit?page=all.

[240] Amnesty International, "Amnesty International Report 2022/23: The State of the World's Human Rights - Amnesty International," *Amnesty.Org*, last modified 2023, accessed May 6, 2025, https://www.amnesty.org/en/documents/pol10/5670/2023/en/.

lebih dari 3.000 laporan kebocoran data nasabah melalui *phishing* dan *skimming* pada semester I 2023, dengan dampak kerugian yang ditanggung baik oleh individu maupun institusi keuangan melalui ganti rugi dan biaya pemulihan sistem. Di sektor pemerintahan, kebocoran data sensitif seperti biodata pejabat, dokumen intelijen, atau data administrasi kependudukan berpotensi mengancam keamanan nasional, misalnya melalui spionase atau tekanan diplomatik, sebagaimana dilaporkan CSIS (2022) bahwa negara seperti Tiongkok dan Rusia menggunakan *cyber espionage* untuk mencuri data strategis. Karena itu, keamanan data harus dipandang sebagai bagian integral dari strategi pertahanan negara, bukan sekadar urusan teknis.[241]

Perusahaan yang belum memiliki kebijakan internal khusus mengenai perlindungan data masih tergolong banyak. Padahal, menurut *ISO/IEC 27001***,** organisasi harus memiliki sistem manajemen keamanan informasi (ISMS) yang mencakup audit, pelatihan karyawan, dan pengendalian akses.[242] Tanpa SOP yang jelas, risiko kesalahan administrasi dan pelanggaran privasi menjadi tinggi. Studi oleh IBM pada tahun 2024 menunjukkan bahwa 82% insiden kebocoran data terjadi karena kelalaian internal yang bisa dicegah melalui pelatihan dasar keamanan digital.[243]

Aspek internasional perlindungan data pribadi tidak bisa diabaikan karena banyak perusahaan di Indonesia menyimpan data pengguna pada layanan *cloud* luar

---

[241] Goverment of Canada, "CSIS Public Report 2022 - Canada.Ca," *Canada.Ca*, last modified 2022, accessed May 6, 2025, https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2022.html.

[242] ISO, "ISO/IEC 27001:2022 - Information Security Management Systems," *Iso.Org*, last modified 2022, accessed May 6, 2025, https://www.iso.org/standard/27001.

[243] IBM, "Cost of a Data Breach 2024 | IBM," *Ibm.Com*, last modified 2024, accessed May 6, 2025, https://www.ibm.com/reports/data-breach.

negeri yang belum tentu mematuhi regulasi perlindungan data, sehingga menimbulkan celah hukum akibat data warga Indonesia berada di bawah yurisdiksi asing dan mendorong perlunya perjanjian bilateral atau penguatan regulasi nasional melalui kebijakan data sovereignty. Kerugian akibat lemahnya perlindungan data juga berdampak pada hubungan industrial, karena informasi sensitif karyawan (seperti status kesehatan, riwayat keluarga, dan catatan hukum) yang bocor dapat merusak kepercayaan internal, memicu tuntutan hukum, meningkatkan turn over rate, serta menurunkan motivasi kerja, dan membuat perusahaan dinilai tidak memiliki tata kelola SDM yang baik.[244]

Eksploitasi data untuk kejahatan lintas negara adalah salah satu bentuk kerugian yang paling mengkhawatirkan. Penjahat siber internasional dapat menggunakan data spesifik seperti nomor identitas dan biometrik untuk membuat paspor palsu, membuka rekening fiktif, atau melakukan penipuan lintas negara. Interpol mencatat bahwa data hasil kebocoran sering ditemukan dalam *dark web*, diperjualbelikan secara bebas. Dalam hal ini, pelanggaran terhadap data pribadi berpotensi memicu kejahatan global yang sulit dilacak dan diadili.

Lemahnya sistem perlindungan data juga memicu ketimpangan dalam akses layanan digital. Individu yang merasa tidak aman dalam menggunakan layanan online, terutama kelompok rentan, cenderung menghindari partisipasi dalam ekonomi digital. Ini menyebabkan eksklusi digital yang merugikan kelompok tersebut dalam jangka panjang. Berdasarkan riset oleh *World Bank* pada tahun

[244] Gartner, "Gartner Predicts Fines Related to Mismanagement of Data Subject Rights Will Exceed $1 Billion by 2026," *Gartner.Com*, last modified 2023, accessed May 6, 2025, https://www.gartner.com/en/newsroom/press-releases/2023-08-24-gartner-predicts-fines-related-to-mismanagement-of-data-subject-rights-will-exceed-1-billion-dollars-by-2026.

2022, ketidakpercayaan terhadap keamanan data adalah salah satu penghambat utama transformasi digital di negara berkembang, termasuk Indonesia.[245]

Korban dapat mengalami gangguan dalam pembukaan layanan keuangan ketika data pengguna bocor dan disalahgunakan, seperti gagal verifikasi saat membuka rekening bank atau mengakses pinjaman. Hal ini terjadi karena data pribadi mereka telah digunakan oleh pihak lain untuk keperluan ilegal. Terkait fenomena ini, OJK Indonesia telah menerima banyak laporan masyarakat terkait akun pinjaman online yang dibuka atas nama mereka tanpa persetujuan. Kerugian semacam ini tidak hanya bersifat material, tetapi juga mencederai reputasi dan hak sipil warga. Kerugian akibat lemahnya perlindungan data pribadi yang bersifat spesifik yang spesifik dapat dikelompokkan ke dalam beberapa kategori utama berikut:

1. Kerugian Finansial Langsung:

   Terjadi ketika pelaku menggunakan data korban untuk mengakses rekening, kartu kredit, atau sistem keuangan lainnya dan melakukan transaksi tanpa izin.

2. Kerugian Finansial Tidak Langsung:

   Berupa biaya pemulihan, penggantian identitas, biaya hukum, hingga hilangnya peluang ekonomi akibat rusaknya reputasi atau skor kredit korban.

[245] World Bank Group, "Digital Transformation Overview: Development News, Research, Data | World Bank," *Worldbank.Org*, last modified 2022, accessed May 6, 2025, https://www.worldbank.org/en/topic/digital/overview.

3. Kerugian Psikologis dan Sosial:

   Korban mengalami stres, rasa malu, kehilangan kepercayaan diri, bahkan trauma akibat kebocoran informasi sensitif.

4. Kerugian Hukum dan Administratif:

   Pelanggaran terhadap data spesifik dapat menyebabkan individu menghadapi kesulitan hukum karena data mereka dipakai untuk kejahatan yang tidak mereka lakukan.

5. Kerugian terhadap Hak Sipil:

   Terutama bila data digunakan untuk menghambat akses ke layanan dasar, seperti pendidikan, kesehatan, atau partisipasi politik.

Institusi pendidikan tinggi juga menghadapi risiko tinggi dalam hal keamanan data. Informasi mahasiswa seperti nilai akademik, beasiswa, bahkan catatan pelanggaran disiplin bersifat rahasia dan bisa disalahgunakan jika bocor. Berdasarkan temuan *EDUCAUSE* pada tahun 2024, lebih dari 60% universitas di dunia mengalami setidaknya satu insiden kebocoran data per tahun. Institusi yang tidak memiliki sistem perlindungan data yang baik berisiko kehilangan kepercayaan sivitas akademika serta menghadapi potensi gugatan hukum.[246] Agar kerugian akibat kebocoran data pribadi dapat dicegah, ada sejumlah langkah mitigasi yang dapat diterapkan baik oleh individu maupun institusi, di antaranya:

[246] SteelCloud, "Cybersecurity in Higher Education: Don't Let the Hackers Win | EDUCAUSE Review," *Educause.Edu*, last modified 2024, accessed May 6, 2025, https://er.educause.edu/articles/sponsored/2024/5/cybersecurity-in-higher-education-dont-let-the-hackers-win.

1. Enkripsi Data Secara *End-to-End*:

   Data penting harus dienkripsi sejak awal hingga akhir proses transmisi untuk mencegah intersepsi.

2. Autentikasi Ganda *(Two-Factor Authentication)*:

   Memberikan lapisan tambahan terhadap akses sistem agar tidak mudah dibobol.

3. Pengelolaan Hak Akses:

   Tidak semua pegawai atau pihak ketiga berhak mengakses seluruh data, maka pengaturan *user privileges* perlu diperketat.

4. Audit dan Pelatihan Berkala:

   Evaluasi keamanan serta pelatihan pegawai untuk mengenali potensi serangan sosial dan teknis.

5. Membangun Kesadaran Publik:

   Edukasi kepada masyarakat umum terkait pentingnya menjaga informasi pribadi di ruang digital.

Banyak usaha rintisan yang mengandalkan layanan *third-party* untuk menyimpan dan mengelola data pelanggan tanpa memahami risiko keamanan sibernya. Sebanyak 41% *startup* Asia Tenggara belum memiliki kebijakan keamanan data formal.[247] Ketika berbicara tentang data pribadi yang bersifat spesifik, kita juga harus memahami bahwa data ini memiliki nilai ekonomi tinggi. Menurut *World Economic Forum* pada tahun 2023**,** data pribadi disebut sebagai

[247] Akamai, "Keamanan Menjadi Prioritas Bisnis Generasi Era Digital Di Asia Untuk Mencapai Pertumbuhan Berkelanjutan 2024/25 Tech Insider," *Akamai.Com*, last modified 2024, accessed May 6, 2025, https://www.akamai.com/site/en/dl/2024/asia-digital-native-businesses-report.pdf.

"*the new oil*" karena menjadi bahan bakar utama ekonomi digital. Akibatnya, data sering diperdagangkan secara ilegal di pasar gelap.[248] Di Indonesia, data pribadi seperti NIK dan nomor KK dijual hanya dengan harga puluhan ribu rupiah per ribuan entri, memperlihatkan betapa rentannya sistem kita terhadap kebocoran yang terorganisir.

Kerugian akibat lemahnya perlindungan data pribadi yang bersifat spesifik bukanlah sekadar isu teknis, melainkan persoalan sistemik yang mencakup aspek hukum, sosial, ekonomi, dan hak asasi manusia. Tanpa regulasi yang kuat, teknologi pelindung yang memadai, dan literasi digital yang tinggi, data pribadi warga akan terus terekspos dan dieksploitasi. Oleh karena itu, perlindungan data harus dilihat sebagai bagian dari kebijakan strategis nasional, bukan hanya tugas lembaga TI, melainkan menjadi tanggung jawab kolektif lintas sektor.

1. Perbandingan Global: Unsur-unsur Pelindungan data Pribadi

Beberapa negara telah menunjukkan komitmen serius dalam perlindungan data pribadi yang bersifat spesifik dengan merancang kerangka hukum yang komprehensif dan mengikat. Di bawah ini adalah beberapa perundang-undangan internasional yang dapat dijadikan rujukan bagi Indonesia:

a. Singapura – *Personal Data Protection Act* (PDPA):

Singapura menetapkan PDPA sebagai kerangka hukum untuk memastikan bahwa entitas komersial mengelola data pribadi dengan

[248] World Economic Forum, "Fostering Effective Energy Transition 2023 Edition," *Weforum.Org*, last modified 2023, accessed May 6, 2025, https://www3.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2023.pdf.

etika dan akuntabilitas. Undang-undang ini juga menetapkan pembentukan *Data Protection Officers* di setiap organisasi.[249]

b. Thailand – *Personal Data Protection Act* (PDPA) Thailand:

PDPA Thailand telah menjadi acuan bagi banyak negara ASEAN lainnya.[250]

2. Arah Strategi Nasional untuk Indonesia

UU PDP merupakan titik awal yang penting. Namun agar regulasi ini tidak berhenti sebagai dokumen normatif, diperlukan strategi turunan yang konkret dan sistematis:

a. Pembentukan Otoritas Independen:

Perlu segera dibentuk lembaga pengawas data pribadi yang independen, memiliki kewenangan investigatif, serta diberi otoritas sanksi administratif dan pidana.

b. Regulasi Turunan Teknis:

Pemerintah perlu mempercepat penyusunan Peraturan Pemerintah (PP) dan Peraturan Menteri yang mengatur mekanisme pelaporan insiden, teknis pemrosesan data, dan kewajiban audit keamanan.

c. Kebijakan *Data Localization*:

Mendorong penyimpanan data strategis di dalam negeri untuk

---

[249] Singapore Statutes Online, "Personal Data Protection Act 2012 - Singapore Statutes Online," *Sso.Agc.Gov.Sg*, accessed May 9, 2025, https://sso.agc.gov.sg/Act/PDPA2012.

[250] Official Emblem of Royal Command, "Personal Data Protection Act B.E. 2562 (2019) (English Version) - Personal Data Protection Act B.E. 2562 (2019) (English Version) OD Mekong Datahub," *Data.Thailand.Opendevelopmentmekong.Net*, accessed May 9, 2025, https://data.thailand.opendevelopmentmekong.net/en/laws_record/2562/resource/ec616be5-9fbf-4071-b4b5-cb1f3e46e826.

menjamin kedaulatan digital, seperti yang diterapkan India dan Rusia melalui undang-undang *data sovereignty*.

d. Program Nasional Literasi Digital:

Pelindungan data tidak hanya soal teknologi dan hukum, tetapi juga budaya digital. Pemerintah harus memasukkan literasi data ke dalam kurikulum pendidikan dasar hingga tinggi.

e. Insentif Bagi Sektor Swasta:

Untuk mendorong adopsi keamanan data oleh pelaku usaha, perlu diberikan insentif berupa potongan pajak atau akses kredit bagi perusahaan yang mengimplementasikan standar perlindungan data yang tinggi, seperti ISO 27001.

3. Peran *Stakeholder*: Tanggung Jawab Kolektif

Pelindungan data pribadi yang bersifat spesifiktidak dapat dibebankan hanya pada satu entitas. Ada beberapa aktor utama yang memegang peranan strategis:[251]

a. Pemerintah: Menyediakan regulasi, pengawasan, dan edukasi publik.

b. Sektor Swasta: Mengembangkan sistem keamanan yang kuat dan transparan kepada pengguna.

c. Akademisi dan Peneliti: Memberikan masukan berbasis riset dan inovasi teknologi.

d. Media dan *Civil Society*: Meningkatkan kesadaran publik dan mengadvokasi hak-hak digital masyarakat.

---

[251] Leski Rizkinaswara, "Empat Pihak Yang Harus Melindungi Data Pribadi Di Ruang Digital – Ditjen Aptika," *Aptika.Kominfo.Go.Id*, accessed May 9, 2025, https://aptika.kominfo.go.id/2020/07/empat-pihak-yang-harus-melindungi-data-pribadi-di-ruang-digital/.

e. Masyarakat Umum: Menjaga informasi pribadi dengan bijak serta aktif melaporkan potensi pelanggaran data.

4. Tantangan Implementasi di Indonesia

Meski arah regulasi Indonesia sudah menuju ke pendekatan komprehensif, terdapat sejumlah tantangan besar yang harus segera diatasi, antara lain:[252]

a. Kesenjangan Infrastruktur Digital: Terutama di daerah luar Jawa yang belum memiliki sistem teknologi memadai.

b. Kurangnya SDM Keamanan Siber: Masih terbatasnya tenaga ahli keamanan informasi di sektor publik maupun swasta.

c. Birokrasi Regulasi yang Lambat: Pengesahan regulasi teknis sering memakan waktu terlalu lama, padahal perkembangan teknologi sangat cepat.

d. Rendahnya Kepatuhan Korporasi: Banyak perusahaan yang masih memandang perlindungan data sebagai beban biaya, bukan investasi jangka panjang.

5. Rekomendasi Kebijakan

Rekomendasi kebijakan untuk memastikan bahwa kerugian akibat lemahnya perlindungan data pribadi yang bersifat spesifik tidak terus berulang melalui penguatan regulasi, peningkatan pengawasan, serta penerapan sanksi yang efektif terhadap setiap bentuk pelanggaran data pribadi, maka beberapa rekomendasi berikut perlu diprioritaskan:[253]

---

[252] Claudia Wang et al., "Peran Teknologi Dalam Transformasi Pendidikan Di Indonesia," *Kemdikbud* 4, no. 2 (2023), hlm. 1-7.

[253] Achmad Solechan, *Audit Sistem Informasi Audit Sistem Informasi*, *Penerbit Yayasan Prima Agus Teknik* (Semarang: Yayasan Prima Agus Teknik, 2021). hlm. 1-138

a. Audit Wajib Tahunan Keamanan Data di seluruh lembaga dan perusahaan publik-swasta yang mengelola data pribadi.
b. Pelatihan dan Sertifikasi Keamanan Data untuk staf TI di institusi pendidikan, kesehatan, keuangan, dan pemerintahan.
c. Platform Aduan Digital Nasional dengan layanan 24/7 yang memungkinkan masyarakat melaporkan kebocoran data secara cepat dan transparan.
d. Sanksi Progresif terhadap pelaku pelanggaran, mulai dari denda, pencabutan izin, hingga proses hukum pidana.
e. Kolaborasi Internasional untuk pertukaran informasi, standar keamanan bersama, dan bantuan lintas negara dalam investigasi kejahatan data lintas batas.

Tabel 2. 1. Perbandingan UU PDP Indonesia, PDPA Singapura, dan PDPA Thailand

Aspek	Indonesia – UU PDP (UU No. 27/2022)	PDPA – Singapura	PDPA – Thailand
Ruang lingkup & cakupan	Payung hukum nasional perlindungan data pribadi, berlaku untuk *data controller* dan *processor* publik maupun privat, dengan cakupan ekstrateritorial ketika memproses data subjek di Indonesia.	Berlaku bagi organisasi sektor privat yang mengumpulkan, menggunakan, atau mengungkap data pribadi individu di Singapura	Berlaku untuk *data controller* dan *processor* yang memproses data subjek di Thailand, termasuk entitas asing yang menawarkan barang/jasa.
Prinsip & dasar pemrosesan	Mengadopsi prinsip legalitas, tujuan yang jelas, relevansi, akurasi, pembatasan penyimpanan, keamanan, dan akuntabilitas; dasar hukum meliputi	Mengatur 11 kewajiban utama *(consent, purpose limitation, notification, access & correction, accuracy, protection, retention*	(lawful basis, purpose limitation, data minimisation, security, akuntabilitas) serta mengatur khusus

	persetujuan, kewajiban hukum, kontrak, kepentingan vital, tugas publik, dan kepentingan sah tertentu.	*limitation, transfer limitation, breach notification, accountability, data portability).*	*sensitive personal data*.
Hak subjek data	Hak untuk informasi, akses, koreksi, penghapusan, keberatan/pembatasan pemrosesan, portabilitas tertentu, dan hak ganti rugi melalui mekanisme sengketa.	Hak akses dan koreksi, penarikan consent, keberatan dalam kondisi tertentu, serta hak untuk diberi tahu jika terjadi *data breach* yang menimbulkan *"significant harm"*.	Hak akses, koreksi, penghapusan, portabilitas tertentu, dan hak menarik consent/keberatan terhadap pemrosesan yang tidak sah atau berisiko tinggi.
Kewajiban utama pengendali/prosesor	Wajib menerapkan langkah teknis & organisasional yang memadai, menunjuk DPO dalam kondisi tertentu, membuat kebijakan internal, melakukan *data breach notification*, dan memastikan perjanjian dengan pemroses.	Wajib mematuhi 11 data protection obligations, termasuk perlindungan teknis, kebijakan internal, dan pelaporan *data breach* kepada PDPC dan individu terdampak.	Wajib menunjuk DPO untuk jenis pemrosesan tertentu, menerapkan langkah keamanan, mencatat pemrosesan, dan mematuhi pedoman PDPC Thailand, termasuk penanganan permintaan subjek data
Breach notification & transfer lintas negara	Mengatur kewajiban pemberitahuan kebocoran data kepada otoritas dan subjek data dalam waktu tertentu; transfer lintas negara mensyaratkan tingkat perlindungan yang sebanding atau dasar hukum yang sah.	Mewajibkan *data breach notification* kepada PDPC dan individu terdampak jika menimbulkan kerugian signifikan/berskala besar; transfer lintas negara mensyaratkan tingkat perlindungan yang sebanding.	Mengatur pelaporan kebocoran ke PDPC dan, bila relevan, ke subjek data; transfer lintas negara diperbolehkan jika perlindungan di negara tujuan atau mekanisme kontrak tidak lebih rendah dari PDPA Thailand.
Lembaga pengawas & sanksi	Diawasi oleh otoritas PDP (di bawah Presiden); mengenal sanksi administratif (peringatan, denda, penghentian sementara)	Diawasi oleh Personal Data Protection Commission (PDPC); sanksi berupa denda	Diawasi oleh Personal *Data Protection Committee* (PDPC Thailand); sanksi berupa denda

	serta sanksi pidana untuk pelanggaran berat dan penyalahgunaan data.	signifikan dan perintah perbaikan, dengan ancaman pidana terbatas untuk pelanggaran tertentu.	administratif dan pidana (termasuk penjara) untuk pelanggaran berat, terutama terkait *sensitive data* dan *data breach* serius.
Kelemahan / tantangan utama	Tahap implementasi dan penegakan masih berkembang: kebocoran data besar tetap terjadi, masa transisi lama, dan koordinasi dengan banyak regulasi sektoral menimbulkan risiko tumpang tindih dan ketidakpastian bagi pelaku usaha	Banyak pengecualian (mis. kepentingan bisnis yang wajar, public interest) sehingga kontrol individu terhadap data kadang dinilai sebagian aktivitas pemerintah berada di luar cakupan penuh PDPA.	Penegakan menghadapi keterbatasan kapasitas negara, tumpang tindih dengan regulasi sektoral, kurangnya sumber daya dan kesadaran pelaku usaha; banyak organisasi masih memandang kepatuhan sebagai "checklist minimal" sehingga implementasi substantif belum merata.

C. Inefektivitas Pelindungan Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi Di Era Digital

Kondisi 'darurat perlindungan' data pribadi spesifik saat ini menjadi momentum krusial bagi urgensi rekonstruksi hukum di Indonesia. Kebocoran data spesifik seperti rekam medis dan biometrik menimbulkan kerugian permanen (irreversible) karena karakter datanya melekat pada identitas biologis subjek seumur hidup, berbeda dengan data umum. Kelambanan pemerintah dalam membentuk aturan turunan dan otoritas pengawas independen pasca-pengesahan UU PDP di tengah masifnya insiden kebocoran justru menciptakan ruang hampa

hukum. Kekosongan perlindungan ini mendesak untuk segera direkonstruksi demi mencegah eksploitasi hak asasi masyarakat yang lebih masif.

Pengelolaan data pribadi spesifik yang berisiko tinggi pada kenyataannya belum diimbangi oleh penguatan keamanan informasi dan regulasi. Pemrosesan data spesifik menuntut penerapan prinsip keabsahan, transparansi, pembatasan tujuan, dan keamanan secara sangat ketat sesuai mandat UU PDP. Efektivitas pemberian hak subjek data masih terkendala oleh masa transisi dan keterbatasan institusional, sehingga berisiko menjadikan UU PDP sekadar regulasi simbolik. Survei Katadata Insight Center (2020) menggarisbawahi kesenjangan fatal ini dengan temuan 63% perusahaan digital belum memahami utuh isi dan konsekuensi UU PDP, padahal mereka adalah pemroses utama data rentan tersebut.[254]

Infrastruktur keamanan digital yang rapuh semakin memperparah kerentanan perlindungan data spesifik. Penyimpanan data pengguna tanpa enkripsi memadai atau sistem autentikasi ganda masih masif dipraktikkan oleh instansi publik maupun swasta. Laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023 membuktikan realitas mengerikan tersebut dengan catatan 54% serangan siber menargetkan sistem data instansi pemerintahan daerah akibat lemahnya pengamanan. [255] Ketiadaan sistem pemantauan keamanan secara *real-time* berakibat pada

[254] Katadata Insight Center, "Digitalisasi, Strategi UMKM Selamat Dari Krisis - Analisis Data Katadata | Berita Ekonomi Bisnis Terbaru Dan Terkini Hari Ini," *Katadata.Co.Id*, last modified 2020, accessed May 6, 2025, https://katadata.co.id/analisisdata/5f03cf11e0198/digitalisasi-strategi-umkm-selamat-dari-krisis.

[255] Annisa Rahayu, "Sektor Pemerintah Jadi Sasaran Empuk Serangan Siber - GoodStats," *Goodstats.Id*, last modified 2023, accessed May 6, 2025, https://goodstats.id/article/sektor-pemerintah-jadi-sasaran-empuk-serangan-siber-9EqE0.

keterlambatan deteksi, sehingga insiden persetasan sering kali baru disadari setelah kerugian terjadi.

Tingkat literasi digital warga negara yang rendah menjadi celah tambahan dalam rapuhnya ekosistem perlindungan data. Kesadaran masyarakat Indonesia terhadap hak privasi atas data pribadi masih berada pada level yang mengkhawatirkan. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 menunjukkan hanya 37% pengguna internet yang mengetahui hak mereka untuk menolak pemrosesan data oleh pihak ketiga.[256] Ketidaktahuan mendasar ini melumpuhkan instrumen kontrol masyarakat dan membuka lebar peluang eksploitasi data secara sepihak.

Ketiadaan lembaga pengawas independen menjadi puncak kelemahan arsitektur penegakan hukum perlindungan data di Indonesia. Persiapan pembentukan otoritas perlindungan data pribadi yang diamanatkan UU PDP hingga awal 2025 belum menghasilkan struktur dan anggaran definitif.[257] Penegakan hukum berjalan di tempat tanpa keberadaan lembaga yang kuat dan independen, dibuktikan dengan minimnya kasus persetasan data yang diproses secara tuntas hingga ke pengadilan. Fragmentasi kebijakan sektoral—antara perbankan, kesehatan, pendidikan, dan *e-commerce*—turut mengacaukan standar penanganan

[256] Hani Pebriyani, "Hasil Survei APJII : Pengguna Internet Di Indonesia Tembus 221 Juta, Mendominasi Gen Z | Komite," *Komite.Id*, last modified 2024, accessed May 6, 2025, https://www.komite.id/2024/02/06/hasil-survei-apjii-pengguna-internet-di-indonesia-tembus-221-juta-mendominasi-gen-z/.

[257] Novina Putri Bestari, "Misterius, Begini Nasib Lembaga Pengawasan Perlindungan Data Pribadi," *Cnbcindonesia.Com*, last modified 2024, accessed May 6, 2025, https://www.cnbcindonesia.com/tech/20241114193435-37-588354/misterius-begini-nasib-lembaga-pengawasan-perlindungan-data-pribadi.

data minimum.[258] Kondisi kritis inilah yang menuntut penundukan seluruh sektor layanan publik pada satu payung regulasi utama yang terintegrasi.

Untuk menilai efektivitas implementasi perlindungan data di lapangan, dapat digunakan beberapa indikator pengukuran kinerja perlindungan data pribadi yang bersifat spesifik berikut:

1. Jumlah insiden kebocoran data yang tercatat resmi.
2. Lama waktu yang dibutuhkan lembaga untuk merespons kebocoran.
3. Tingkat pemahaman pengguna atas hak-hak privasi mereka.
4. Proporsi perusahaan/institusi yang sudah mengimplementasikan prinsip *privacy by design*.
5. Jumlah kasus pelanggaran yang diproses secara hukum.

Efektivitas sistem perlindungan data di suatu negara dinilai dari indikator tersebut, semakin baik indikator-indikator tersebut semakin tinggi pula nilai efektivitasnya. Dalam konteks penyimpanan data, efektivitas perlindungan juga ditentukan oleh kebijakan lokalisasi data atau *data localization*. Pemerintah Indonesia telah mewajibkan penyimpanan data strategis di pusat data domestik.[259] Namun, implementasinya masih menghadapi tantangan seperti keterbatasan infrastruktur, biaya tinggi bagi pelaku usaha kecil-menengah, serta kurangnya *data center* bersertifikasi internasional. Tanpa insentif dan dukungan teknis dari

---

[258] R. Dwi Tjahja K. Wardhono, Wishnu Badrawani, Ayu Deviana, and Nadhia Shalehanti Melati Pramudyastuti, "Pelindungan data pribadi yang bersifat spesifik Di Bank Indonesia Dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan Dan Teknis Pengaturan," *Bi.Go.Id*, last modified 2024, accessed May 6, 2025, https://www.bi.go.id/id/publikasi/kajian/Pages/Pelindungan-Data-Pribadi-Di-Bank-Indonesia-Dan-Lembaga-Jasa-Keuangan.aspx.

[259] Intan Rakhmayanti, "Data Boleh Disimpan Di Luar Negeri, Ini Pembenaran Versi Kominfo," *Tekno.Sindonews.Com*, last modified 2019, accessed May 6, 2025, https://tekno.sindonews.com/berita/1455582/207/data-boleh-disimpan-di-luar-negeri-ini-pembenaran-versi-kominfo.

pemerintah, kebijakan ini belum memberikan dampak yang signifikan terhadap perlindungan data.

Penggunaan pihak ketiga dalam pemrosesan data, seperti *cloud service providers*, juga perlu mendapatkan perhatian khusus. Sering kali terjadi kebocoran bukan dari lembaga utama, tetapi dari vendor atau penyedia layanan digital yang menjadi mitra eksternal. Oleh karena itu, efektivitas perlindungan data harus mencakup pengawasan terhadap pihak ketiga, dengan cara:

1. Mewajibkan vendor menandatangani perjanjian kerahasiaan (NDA).
2. Menetapkan standar keamanan minimum bagi seluruh mitra sistem digital.
3. Melakukan audit berkala terhadap sistem penyimpanan dan pemrosesan data vendor.

Efektivitas dari segi respons cepat terhadap insiden kebocoran data juga hal yang penting untuk diperhatikan. Dalam praktik terbaik global, organisasi wajib melaporkan insiden kebocoran dalam jangka waktu tertentu. Di Indonesia, belum ada sistem notifikasi insiden yang terpusat dan wajib. Akibatnya, banyak insiden bocor tanpa penanganan atau laporan resmi, sehingga menurunkan kepercayaan masyarakat terhadap penyelenggara sistem elektronik. Selain lembaga pemerintah, peran industri dalam meningkatkan efektivitas perlindungan data sangat krusial. Banyak perusahaan yang telah menerapkan standar keamanan tinggi secara sukarela, antara lain:

1. Sertifikasi ISO/IEC 27001 (Manajemen Keamanan Informasi).
2. Enkripsi AES-256 untuk penyimpanan data *at-rest*.

3. Protokol TLS/SSL untuk pengiriman data *in-transit*.
4. Otentikasi multifaktor (MFA) untuk akses pengguna.

Masyarakat sebagai pengguna akhir sistem digital juga memiliki peran dalam memperkuat efektivitas perlindungan data pribadi yang bersifat spesifik. Pemerintah dapat mengembangkan program edukasi digital yang terstruktur melalui:[260]

1. Kampanye nasional literasi digital di media massa dan sekolah.
2. Modul pembelajaran khusus tentang data pribadi di jenjang pendidikan dasar dan menengah.
3. Pelatihan daring bersertifikat tentang keamanan siber bagi masyarakat umum.
4. Layanan konsultasi daring untuk laporan kebocoran data.

Edukasi publik menjadi fondasi agar masyarakat memahami hak dan kewajiban dalam ekosistem digital, sementara efektivitas perlindungan data pribadi yang bersifat spesifik di sektor publik sangat bergantung pada kesiapan kementerian dan lembaga menerapkan prinsip privasi padahal laporan BPK 2023 menunjukkan banyak instansi (pengelola data sensitif seperti Dukcapil, DJP, dan BPJS) belum memiliki kebijakan internal perlindungan data, sehingga tanpa penguatan sistem dan pelatihan SDM, tingkat perlindungannya tetap rendah.

Efektivitas juga ditentukan oleh seberapa tanggap sistem hukum dalam memberi pemulihan atau kompensasi, tetapi hingga kini belum ada mekanisme

[260] Ahmad Habib Al Faraby, "Perkembangan Teknologi Informasi Dan Transaksi Elektronika (ITE) Di Indonesia (Suatu Kajian Dari Peran Penyidik Kepolisian Dalam Menangani Penyalahgunaan Informasi Dan Transaksi Elektronika (Ite))," *Faraby Meraja Journal* 7, no. 1 (2024), hlm. 48-61.

sederhana yang memudahkan individu menuntut ganti rugi, membuat korban enggan melapor karena proses hukum panjang dan mahal; karena itu, sistem pengaduan yang cepat, sederhana, dan ramah korban sangat dibutuhkan. Untuk mengoptimalkan perlindungan data pribadi yang bersifat spesifik, banyak negara telah membentuk lembaga pelindung data independen yang berfungsi sebagai pengawas, penyuluh, dan mediator, dan Indonesia perlu segera merealisasikan lembaga serupa agar penegakan, edukasi, dan pemulihan hak korban dapat berjalan lebih efektif.[261] Untuk memastikan efektivitas penegakan dan edukasi tersebut, lembaga pelindung data independen ini idealnya harus dibekali dengan kewenangan strategis yang mencakup:

1. Menyusun pedoman teknis perlindungan data lintas sektor.
2. Melakukan audit dan inspeksi secara independen.
3. Menyediakan jalur penyelesaian sengketa non-litigasi.
4. Menjadi penghubung dengan otoritas perlindungan data negara lain.

Sektor kesehatan merupakan salah satu sektor dengan volume data spesifik tertinggi, dan menjadi indikator penting dalam menilai efektivitas perlindungan data. Sayangnya, sektor ini pula yang paling sering mengalami kebocoran data secara global. Di Indonesia, kasus kebocoran data BPJS Kesehatan pada tahun 2021, yang melibatkan lebih dari 270 juta data penduduk, menjadi sinyal lemahnya sistem informasi kesehatan. Data yang bocor meliputi nomor KTP, alamat, dan riwayat medis. Evaluasi yang dilakukan oleh Kementerian Kesehatan menyebutkan

[261] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024), hlm. 431-455.

bahwa sistem perlindungan data rumah sakit daerah masih belum terstandarisasi dan belum terintegrasi dengan sistem nasional yang aman.[262]

Kerentanan terhadap kebocoran data spesifik pada faktanya tidak eksklusif terjadi di sektor kesehatan saja. Risiko serupa juga membayangi sektor pelayanan publik strategis lainnya yang secara masif menghimpun rekam jejak individu, salah satunya adalah sektor pendidikan. Tantangan di lembaga pendidikan kini semakin nyata seiring dengan meluasnya penggunaan LMS, platform ujian daring, dan aplikasi pelaporan siswa, namun sering belum memiliki kebijakan internal terkait penyimpanan data akademik dan psikologis, termasuk hasil asesmen psikologi, data beasiswa berbasis status ekonomi, informasi kesehatan, dan riwayat pelanggaran kedisiplinan. Data spesifik ini berisiko menimbulkan diskriminasi atau stigma jika tersebar ke publik, sehingga efektivitas perlindungan tidak dapat dipisahkan dari komitmen manajemen tertinggi lembaga.

Pelindungan data pribadi yang bersifat spesifik spesifik berkaitan erat dengan sistem registrasi dan identitas digital nasional, seperti Identitas Kependudukan Digital (IKD) berbasis NIK, yang efektivitasnya sangat bergantung pada kualitas perlindungan data yang menyertainya. Beberapa risiko dalam sistem identitas digital yang belum diantisipasi dengan optimal antara lain:[263]

1. Akses tanpa otorisasi melalui perangkat hilang atau dicuri.

---

[262] Kementrian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, "Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi - Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas," *Menpan.Go.Id*, accessed May 9, 2025, https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas.

[263] Muhammad Alfi, Ni Putu Yundari, and Ahnaf Tsaqif, "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 2 (2023), hlm. 5.

2. Penggunaan identitas ganda melalui manipulasi biometrik.
3. Ketidaktahuan pengguna dalam mengatur hak akses aplikasi.
4. Lemahnya integrasi sistem antarinstansi yang menyebabkan celah keamanan.

Efektivitas perlindungan data spesifik juga dapat ditinjau dari komitmen perusahaan *platform digital*, terutama *e-commerce* dan fintech. Dua sektor ini menyimpan data transaksi finansial, data biometrik melalui verifikasi wajah, serta informasi identitas pengguna. Sayangnya, kebijakan privasi banyak platform masih menggunakan bahasa yang rumit, panjang, dan sulit dipahami. Survei Konsumen Digital Indonesia oleh Kominfo (2024) menunjukkan bahwa hanya 21% pengguna yang membaca kebijakan privasi sebelum menyetujui penggunaan aplikasi. Ini menjadi indikator penting bahwa keterbukaan informasi belum optimal diterapkan dalam sistem digital nasional.

Evaluasi efektivitas perlindungan data pribadi yang bersifat spesifik harus juga mempertimbangkan aspek kesiapan darurat dan pemulihan data (*disaster recovery plan*). Dalam sistem yang ideal, setiap institusi penyelenggara sistem elektronik wajib memiliki skenario tanggap darurat jika terjadi serangan siber atau bencana teknologi. Rencana ini harus mencakup:[264]

Pembuatan cadangan data secara berkala dan terenkripsi.

1. Uji coba pemulihan sistem (*disaster recovery drill*).
2. Penunjukan tim khusus keamanan informasi dan forensik digital.

[264] Setiawan Setiawan, Abdul Azis, and Eko Wahyudi, "Evaluasi Efektivitas Disaster Recovery Plan Dalam Pemulihan Layanan Teknologi Informasi Pasca Bencana Berbasis Iso 22301 (Studi Kasus PT. Jasa Raharja)," in *Prosiding Seminar SeNTIK*, vol. 8, 2024, hlm. 351-356.

3. Prosedur komunikasi publik saat terjadi kebocoran.

Lembaga yang belum memiliki protokol ini masih tergolong banyak, yang mana lembaga tersebut tidak memperbarui secara berkala sehingga menjadi tidak efektif. Komitmen negara terhadap perlindungan data pribadi yang bersifat spesifik juga dapat dinilai melalui keikutsertaan dalam forum internasional dan kerja sama multilateral. Indonesia sejauh ini belum menjadi anggota aktif dari *Global Privacy Assembly* (GPA), forum otoritas perlindungan data dari berbagai negara. Keikutsertaan dalam forum tersebut penting untuk memperkuat diplomasi digital, menyamakan standar regulasi dengan mitra dagang, dan mendapatkan bantuan saat terjadi insiden kebocoran yang melibatkan data lintas negara. Dalam dunia yang terhubung, efektivitas perlindungan data juga berarti kemampuan negara menjamin hak warganya di ruang siber internasional.

Dalam proses audit efektivitas sistem perlindungan data, pemerintah dapat mengembangkan indikator nasional dengan mengadopsi standar internasional, baik *NIST Privacy Framework* maupun ISO 27701. Secara komplementer, substansi dari standar-standar tersebut dapat diintegrasikan sebagai rujukan dalam menilai kesiapan institusi pada lima dimensi utama:[265]

1. Identifikasi aset dan risiko data pribadi.
2. Pengendalian akses dan pelatihan SDM.
3. Pengawasan aktivitas pemrosesan data.
4. Respons insiden dan pelaporan.

[265] Rexy, "Memahami ISO 27701: Sistem Manajemen Informasi Privasi Yang Efektif - ISOCENTER INDONESIA," *Isoindonesiacenter.Com*, accessed May 9, 2025, https://isoindonesiacenter.com/memahami-iso-27701-sistem-manajemen-informasi-privasi-yang-efektif/.

5. Dokumentasi, pelaporan, dan audit berkala.

Implementasi indikator ini harus diwajibkan terutama bagi lembaga yang menyimpan data berskala besar seperti fintech, kesehatan, dan pemerintah. Salah satu pendekatan untuk meningkatkan efektivitas perlindungan data adalah melalui insentif fiskal atau regulatif bagi pelaku usaha. Pemerintah dapat merancang skema yang memberikan manfaat bagi perusahaan yang telah memenuhi standar perlindungan data tinggi. Beberapa contoh insentif yang bisa diterapkan:

1. Potongan pajak bagi perusahaan yang tersertifikasi ISO 27001.
2. Kemudahan perizinan usaha berbasis risiko digital rendah.
3. Pengakuan publik melalui sistem rating keamanan data.
4. Prioritas dalam pengadaan pemerintah bagi penyedia jasa yang taat UU PDP.

Insentif seperti hal tersebut membuat perusahaan akan lebih terdorong untuk proaktif dalam membangun sistem perlindungan data. Meningkatkan efektivitas perlindungan data spesifik juga memerlukan pemutakhiran kurikulum pendidikan tinggi dan kejuruan, terutama di bidang teknologi informasi, hukum siber, dan kebijakan publik digital. Perguruan tinggi dan lembaga pelatihan profesional harus mengintegrasikan materi perlindungan data pribadi dalam bentuk mata kuliah wajib, studi kasus lokal, dan praktik audit data. Peningkatan kapasitas SDM ini akan melahirkan lebih banyak *data protection officer*, *cybersecurity auditor*, dan peneliti

hukum privasi yang diperlukan untuk membangun ekosistem perlindungan data nasional yang tangguh dan berkelanjutan.[266]

Keamanan data pribadi tidak dapat dipisahkan dari efektivitas regulasi terkait kewajiban teknis minimum yang harus dipenuhi oleh pengendali dan pemroses data. Dalam konteks Indonesia, efektivitas UU PDP akan sangat ditentukan oleh seberapa jelas dan terukur petunjuk teknis (juknis) yang dikeluarkan sebagai turunan dari UU tersebut. Beberapa elemen teknis yang wajib diatur secara detail meliputi:

1. Standar enkripsi untuk data *in-transit* dan *at-rest*.
2. Durasi maksimal penyimpanan data dan mekanisme pemusnahan.
3. Pengelolaan hak akses pengguna dan *audit trail*.
4. Penanganan data spesifik dalam sistem berbasis AI atau *big data*.
5. Sistem pelaporan pelanggaran data secara daring, real time, dan terintegrasi.

Efektivitas perlindungan data pribadi yang bersifat spesifik spesifik juga berkaitan erat dengan mekanisme kontrol internal dan audit rutin yang diterapkan oleh institusi. Audit keamanan informasi harus dilakukan tidak hanya saat terjadi insiden, tetapi secara berkala dengan dokumentasi yang dapat diawasi oleh lembaga otoritatif. Setiap institusi penyelenggara sistem elektronik (PSE) harus memiliki:[267]

1. Tim pengendali risiko dan perlindungan data internal.
2. Protokol penilaian dampak privasi (*Privacy Impact Assessment*).

---

[266] Jefri Ronald Parulian Siagian, *Meningkatkan Sumber Daya Manusia Yang Berdaya Saing Di Era Teknologi Digital Guna Mendukung Transformasi Digital Nasional*, *Lemhannas RI* (Jakarta, 2024).

[267] Solechan, *loc.cit*.

3. Catatan perubahan sistem dan log akses pengguna.
4. Rencana peningkatan keamanan tahunan berdasarkan temuan audit.

Tanpa mekanisme ini, institusi hanya akan bersifat reaktif dan tidak adaptif terhadap ancaman digital yang terus berkembang. Aspek lain yang penting dalam efektivitas perlindungan data adalah transparansi dan akuntabilitas institusi terhadap publik. UU PDP mengamanatkan bahwa subjek data berhak mengetahui tujuan, dasar hukum, dan pihak ketiga mana saja yang menerima data mereka. Untuk itu, setiap lembaga wajib memiliki kebijakan privasi yang:[268]

1. Ditulis dengan bahasa yang mudah dimengerti oleh pengguna umum.
2. Memuat kontak pengelola data dan cara mengajukan pengaduan.
3. Diperbaharui secara berkala seiring perubahan sistem.
4. Tersedia dalam format daring dan mudah diakses.
5. Memberikan pilihan *(opt-in/opt-out)* bagi pengguna atas jenis data yang dikumpulkan.

Teknologi kecerdasan buatan (AI) menjadi tantangan baru bagi efektivitas perlindungan data karena membutuhkan data spesifik dalam jumlah besar (wajah, suara, kebiasaan pengguna), sehingga Indonesia perlu segera merumuskan etika penggunaan AI berbasis privasi seperti *AI Act* di Uni Eropa, mencakup larangan profiling sensitif tanpa persetujuan eksplisit, audit algoritma independen, transparansi penggunaan AI, dan penghapusan data pasca pelatihan agar AI tidak berubah menjadi alat pelanggaran privasi massal.

[268] Layla Intan Rahayu, Tri Wahyudiono, and Dewi Ulfa Lailatul Fitria, "Efektivitas Kebijakan Hukum Dalam Penanganan Pandemi," *Jurnal Online Mahasiswa (Jom) Hukum Tata Negara* 1, no. 2 (2023), hlm. 80-112.

Efektivitas perlindungan data spesifik juga menuntut pendekatan *risk-based approach*, dengan proteksi tertinggi bagi data medis pasien, data biometrik, informasi keuangan lengkap, data anak, serta data lokasi *real-time*. Pendekatan ini mengharuskan pengendali dan prosesor data melakukan penilaian risiko berkala (*data protection impact assessment*) untuk memastikan tingkat pengamanan sebanding dengan potensi dampak kebocoran data. Untuk memperkuat sistem, dapat diterapkan skema pelabelan keamanan digital (misalnya *Basic Security, Advanced Encryption, Privacy Shielded*, dan *Compliant with PDP Law*) agar pengguna memahami tingkat perlindungan yang diberikan dan mendorong kompetisi sehat antar penyedia layanan. Oleh karena itu, Indonesia perlu menyusun kebijakan *adequacy status* untuk:

1. Mendapatkan pengakuan sistem perlindungan data dari negara mitra.
2. Memudahkan perusahaan lokal bersaing di pasar internasional.
3. Menjaga kedaulatan data warga negara dalam skema kerja sama digital.
4. Menghindari isolasi digital akibat rendahnya standar perlindungan data.

Ketentuan ini menandakan bahwa perlindungan data tidak hanya urusan domestik, tapi juga hubungan internasional. Evaluasi efektivitas perlindungan data spesifik juga dapat dilakukan melalui kajian akademik berbasis *evidence*. Perguruan tinggi dapat menjadi mitra pemerintah dalam menyusun indeks nasional perlindungan data dengan melibatkan:[269]

1. Survei persepsi masyarakat dan pelaku industri.

[269] "Dewan Perlindungan Data Eropa – EDPB | Uni Eropa," accessed May 9, 2025, https://european--union-europa-eu.translate.goog/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_en?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sge.

2. Analisis jumlah dan pola kebocoran data tahunan.
3. Penelitian dampak sosial akibat pelanggaran privasi.
4. Simulasi respons terhadap insiden digital.

Data ini akan membantu pengambilan kebijakan berbasis fakta, bukan asumsi. Penguatan efektivitas perlindungan data juga harus dilakukan melalui revisi dan harmonisasi peraturan sektoral yang tumpang tindih. Sebelum adanya UU PDP, sektor-sektor seperti perbankan, pertelekomunikasian, dan kesehatan telah memiliki regulasi masing-masing tentang data. Beberapa di antaranya bersifat kontradiktif, sehingga menimbulkan ketidakpastian hukum. Pemerintah perlu melakukan:

1. Penyusunan peta regulasi sektoral yang bersinggungan dengan data pribadi.
2. Harmonisasi definisi dan lingkup data di seluruh regulasi.
3. Pencabutan atau revisi regulasi lama yang tidak sejalan dengan UU PDP.
4. Dialog terbuka antara regulator sektoral dan Kominfo sebagai koordinator pusat.

Sistem perlindungan data akan lebih efektif dan tidak membingungkan pelaku usaha dengan harmonisasi ini. Di Indonesia, belum terbentuk norma sosial yang kuat mengenai penghormatan atas privasi digital. Banyak masyarakat yang membagikan data pribadi orang lain tanpa izin, seperti menyebarkan KTP, rekam medis, atau alamat pribadi di media sosial. Untuk itu, pendidikan etika digital sejak

dini menjadi keharusan. Tanpa perubahan budaya, segala sistem perlindungan akan mudah runtuh oleh kelalaian kolektif.[270]

Indonesia perlu mengembangkan sistem reward and punishment yang proporsional dalam upaya meningkatkan efektivitas perlindungan data pribadi yang bersifat spesifik spesifik. Penerapan sanksi administratif dan pidana sebagaimana diatur dalam UU PDP memang sudah menjadi langkah maju. Namun, pemberian penghargaan bagi institusi yang patuh dan aktif menerapkan prinsip perlindungan data juga penting sebagai insentif moral dan reputasi. Skema ini dapat meliputi:

1. Penghargaan tahunan "*Digital Privacy Excellence Award*."
2. Publikasi daftar institusi terbaik dalam perlindungan data oleh Kominfo.
3. Sertifikasi khusus bagi perusahaan yang menyampaikan laporan audit keamanan secara transparan.
4. Prioritas akses dalam program transformasi digital pemerintah.

Insentif semacam ini akan mendorong budaya kepatuhan dan tanggung jawab yang lebih kuat. Efektivitas perlindungan data spesifik juga terkait erat dengan pemberdayaan *whistleblower* atau pelapor pelanggaran. Hingga saat ini, Indonesia belum memiliki sistem yang memungkinkan pelapor kebocoran atau penyalahgunaan data di institusinya sendiri untuk mendapatkan perlindungan

[270] Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital : Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023), hlm. 132-146.

hukum yang memadai. Padahal, banyak insiden besar terungkap justru dari pihak internal. Untuk memperkuat sistem ini, pemerintah dapat:[271]

1. Membangun *platform* pelaporan daring anonim dan terenkripsi.
2. Menjamin kerahasiaan identitas pelapor secara hukum.
3. Memberikan penghargaan kepada pelapor yang menyelamatkan publik dari kebocoran data.
4. Menyediakan bantuan hukum dan psikologis bagi pelapor.

Deteksi dini atas pelanggaran bisa dilakukan lebih cepat dengan sistem pelaporan yang aman. Efektivitas sistem perlindungan data pribadi yang bersifat spesifik juga sangat bergantung pada kerja sama antarnegara dan organisasi internasional, terutama dalam menghadapi kejahatan siber lintas batas. Penjahat digital dapat beroperasi dari luar yurisdiksi Indonesia, memanfaatkan kelemahan sistem hukum dan kerja sama antarnegara yang belum optimal. Oleh karena itu, Indonesia perlu memperkuat:[272]

1. Keikutsertaan dalam konvensi internasional seperti *Budapest Convention on Cybercrime*.
2. MoU bilateral terkait ekstradisi pelaku kejahatan siber.
3. Integrasi sistem pelacakan digital bersama Interpol dan ASEAN CERT.

---

[271] Vidya Loka Santi and Zaenal Wafa, "Pengaruh Sistem Pengendalian Internal, Komite Audit, Dan Whistleblowing System Terhadap Pencegahan Fraud," *Value : Jurnal Manajemen dan Akuntansi* 19, no. 3 (2024), hlm. 919-936.

[272] Dewi Asri Puanandini, Muhammad Syahid Syidiq, and Jihan Pasha Noevera, "Efektivitas Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang," *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum* 2, no. 2 (2023), hlm. 39-49.

4. Kegiatan pertukaran data dan praktik terbaik antar otoritas perlindungan data global.

Kerja sama ini akan meningkatkan efektivitas perlindungan secara menyeluruh. Penilaian atas efektivitas perlindungan data pribadi yang bersifat spesifik spesifik juga dapat dilakukan melalui survei nasional kepuasan pengguna digital terhadap sistem keamanan data. Survei ini bisa dilakukan secara tahunan oleh lembaga independen dan hasilnya dipublikasikan secara terbuka. Indikator yang dapat digunakan dalam survei tersebut antara lain:[273]

1. Persepsi publik terhadap keamanan data dalam layanan pemerintah.
2. Tingkat kepercayaan terhadap platform fintech dan *e-commerce*.
3. Pengalaman pengguna dalam mengakses hak mereka atas data.
4. Tingkat kepuasan terhadap respons lembaga saat terjadi pelanggaran.
5. Keinginan publik untuk tetap menggunakan layanan digital.

Data ini menjadi masukan penting bagi perumusan kebijakan yang lebih responsif terhadap kebutuhan publik. Kebijakan perlindungan data yang efektif juga harus memperhatikan kelompok rentan seperti anak-anak, lansia, dan penyandang disabilitas. Data mereka seringkali bersifat spesifik dan sensitif, tetapi perlindungannya belum terakomodasi secara khusus. Oleh karena itu, perlu dirancang pedoman teknis khusus untuk kelompok rentan yang mencakup:

1. Persetujuan orang tua atau wali dalam pengumpulan data anak.
2. Pelarangan profiling iklan terhadap anak di bawah usia tertentu.

[273] Ade Risna Sari and M Si SH, *Reformasi Pelayanan Publik* (Jakarta: PT Indonesia Delapan Kreasi Nusa, 2024). hlm. 127.

3. Aksesibilitas kebijakan privasi dalam bahasa isyarat atau format audio.
4. Pengawasan khusus terhadap aplikasi pendidikan anak yang mengumpulkan data lokasi.

Kesiapan dunia usaha untuk menerapkan perlindungan data juga dapat dilihat dari tingkat sertifikasi dan pelatihan internal karyawan. Perusahaan yang memiliki pelatihan rutin tentang privasi dan keamanan data menunjukkan tingkat kepatuhan yang lebih tinggi dibandingkan yang tidak memiliki program tersebut. Elemen pelatihan yang penting untuk meningkatkan efektivitas antara lain:[274]

1. Simulasi kebocoran data dan prosedur respons.
2. Etika penggunaan data pelanggan.
3. Pencegahan social engineering dan serangan phishing.
4. Penggunaan perangkat kerja yang aman.
5. Pengenalan sistem audit internal dan pelaporan pelanggaran.

Pemerintah pusat dan daerah perlu membangun hub digital regional yang berfungsi sebagai pusat data, pusat pelatihan keamanan siber, serta pusat koordinasi penanggulangan insiden kebocoran data. Dengan pendekatan desentralisasi ini, efektivitas perlindungan dapat diperluas ke daerah-daerah yang selama ini kurang mendapat perhatian. Fasilitas yang bisa dikembangkan dalam hub digital tersebut meliputi:[275]

1. *Data Center* tersertifikasi *Tier III* ke atas.
2. Laboratorium keamanan siber dan digital forensik.

---

[274] Rika Yuliana, "Laporan Penelitian Best Practice Framework for Information Technology Security in Indonesia" (Aceh: UIN Ar-Raniry Banda Aceh, 2023).

[275] Nur Rochmah Dyah Puji Astuti et al., *Keamanan Data Dalam Revolusi Teknologi* (Banjarnegara: PT Penerbit Qriset Indonesia, 2025). hlm. 60.

3. Ruang tanggap darurat (*emergency response center*).
4. Kantor otoritas perlindungan data regional.

Evaluasi berkala terhadap efektivitas perlindungan data spesifik sebaiknya dijadikan sebagai bagian dari Rencana Pembangunan Jangka Menengah Nasional (RPJMN). Pemerintah bisa menetapkan target-target konkret yang terukur, seperti:

1. Penurunan jumlah insiden kebocoran data sebesar 50% dalam 5 tahun.
2. 100% lembaga publik memiliki DPO (*Data Protection Officer*).
3. 80% masyarakat mengetahui hak-haknya atas data pribadi.
4. Sertifikasi keamanan digital untuk 60% perusahaan teknologi.
5. Pengoperasian penuh lembaga pelindung data independen.

Efektivitas perlindungan data spesifik di Indonesia adalah refleksi dari kesiapan bangsa memasuki masyarakat digital yang beradab dan adil. Regulasi yang kuat harus didampingi dengan kapasitas kelembagaan yang mumpuni, partisipasi masyarakat yang aktif, serta teknologi yang mendukung. Tanpa sinergi seluruh elemen ini, perlindungan data akan mudah runtuh dan menjadi krisis kepercayaan di tengah masyarakat yang semakin digital.[276]

Kehadiran UU PDP secara normatif telah menggeser arsitektur perlindungan data indonesia menuju konvergensi global melalui pengklasifikasian data spesifik dan pengenaan sanksi. realitas empiris justru menunjukkan kondisi yang sangat kontradiktif dengan capaian normatif tersebut. analisis menggunakan pisau teori perlindungan hukum (*middle range theory*) terhadap tingginya insiden kebocoran data spesifik pasca-pengesahan uu pdp membuktikan kegagalan fungsi

[276] *Idem*. hlm. 73.

perlindungan preventif maupun represif negara. efektivitas perlindungan di indonesia masih tersandera oleh lemahnya kapasitas kelembagaan, rendahnya kultur kepatuhan pelaku usaha, serta tumpulnya instrumen sanksi. fakta ini sangat tertinggal jika dibandingkan dengan yurisdiksi seperti thailand yang telah memiliki otoritas pengawas independen dengan orientasi penegakan (*enforcement*) agresif.

Kegagalan sistemik ini menghadirkan urgensi yang sangat mendesak berdasarkan tinjauan teori keadilan sosial (*grand theory*). pembiaran terhadap kerentanan data berakibat pada beralihnya beban risiko secara tidak proporsional kepada kelompok masyarakat berpendapatan rendah. dampak lanjutan dari pembiaran ini adalah pengkhianatan terhadap dimensi keadilan distributif sekaligus pencederaan terhadap penghormatan martabat manusia sebagai subjek hukum. teori hukum pembangunan (*applied theory*) menuntut agar hukum tidak tertinggal oleh dinamika era digital. rekonstruksi hukum perlindungan data spesifik merupakan langkah mutlak agar hukum benar-benar berfungsi sebagai sarana rekayasa sosial (*law as a tool of social engineering*) yang responsif dalam menjamin kepastian dan keamanan masyarakat.

Urgensi rekonstruksi hukum ini memperoleh legitimasi absolut dari perspektif data kewahyuan dalam ajaran islam. al-qur'an secara tegas melarang eksploitasi ruang privat tanpa hak, sebagaimana diamanatkan dalam surah al-hujurat ayat 12 mengenai larangan perbuatan *tajassus* (mencari-cari informasi pribadi) dan surah an-nur ayat 27 mengenai prinsip keizinan, yang dalam diskursus modern diartikulasikan sebagai prinsip persetujuan (*consent*).

Penguatan prinsip perlindungan ini dikukuhkan lebih lanjut melalui hadis riwayat imam muslim yang menegaskan inviolabilitas (kesucian) atas harta, darah, dan kehormatan setiap muslim. ekosistem digital saat ini menempatkan data pribadi yang bersifat spesifik sebagai wujud konkret dari kehormatan individu tersebut. penguatan perlindungan terhadap data spesifik pada akhirnya bukan semata-mata tuntutan ilmu hukum modern, melainkan sebuah keharusan mendesak demi menjaga martabat kemanusiaan (*ḥifẓ al-'irḍ*) sesuai dengan prinsip hak asasi dalam hukum islam.

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik tidak dapat lagi ditunda atau dipahami sebagai agenda teknis semata, melainkan harus ditempatkan sebagai bagian dari pembaruan hukum nasional yang menyentuh inti relasi antara negara, teknologi, dan warga negara. Negara berkewajiban memastikan bahwa setiap perkembangan teknologi digital berlangsung dalam koridor keadilan, sehingga pemanfaatan data tidak berubah menjadi sarana dominasi, eksploitasi, atau penghilangan kendali individu atas identitas pribadinya.

Rekonstruksi hukum yang diperlukan harus mampu membangun norma yang adaptif, kelembagaan yang kuat, dan budaya hukum yang sadar privasi, agar perlindungan terhadap data pribadi yang bersifat spesifik benar-benar efektif. Dengan demikian, urgensi perlindungan data pribadi di era digital tidak hanya lahir dari meningkatnya ancaman kebocoran data, tetapi juga dari tuntutan konstitusional dan moral untuk menjaga kehormatan, keamanan, dan hak asasi setiap warga negara. Pada titik ini, hukum harus berfungsi sebagai pelindung yang nyata, bukan sekadar simbol normatif.

BAB III
KEBIJAKAN PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI YANG BERSIFAT SPESIFIK AKIBAT PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL

A. Perlindungan Hukum Terhadap Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi di Era Digital

Pancasila sebagai *rechtsidee* (cita hukum) dan landasan filosofis bernegara merupakan akar utama dalam setiap proses pembentukan serta penegakan hukum di Indonesia. Nilai keadilan dalam Sila Kedua "Kemanusiaan yang Adil dan Beradab" mengamanatkan penghormatan penuh terhadap hak asasi manusia melalui keseimbangan antara hak dan kewajiban. Landasan filosofis tersebut menemukan urgensi transformatifnya pada perlindungan data pribadi yang bersifat spesifik di tengah kompleksitas era digital saat ini. Eksploitasi terhadap data spesifik dengan tingkat sensitivitas tinggi bukan sekadar bentuk pelanggaran privasi, melainkan serangan langsung terhadap harkat dan martabat individu. Negara memegang mandat utama untuk hadir sebagai otoritas pelindung dengan memastikan tidak ada entitas korporasi maupun penyelenggara teknologi yang menyalahgunakan posisi dominannya untuk mengeksploitasi data warga negara. Kehadiran negara dalam fungsi proteksi ini menjadi syarat mutlak bagi terwujudnya tatanan digital yang setara dan berkeadilan bagi seluruh lapisan masyarakat.[277]

Keadilan sosial dalam Pancasila menekankan pada pemerataan hak dan perlindungan bagi seluruh lapisan masyarakat. Dalam hal ini, perlindungan data pribadi yang bersifat spesifik merupakan bagian dari penerapan keadilan sosial,

[277] Uu Nurul Huda et al., *Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital* (Bandung: Penerbit Widina, 2024). hlm. 58.

dimana setiap individu berhak untuk mendapatkan perlindungan yang sama terhadap data pribadinya tanpa adanya ketidakadilan, baik oleh negara, korporasi, maupun pihak lain yang mengelola data.[278] Keberadaan UU PDP adalah bentuk nyata dari penerapan keadilan sosial ini, dimana regulasi tersebut memastikan bahwa data pribadi yang bersifat sensitif mendapat perlindungan khusus, serta mengatur kewajiban pihak yang mengendalikan data untuk menjaga kerahasiaan dan keamanannya.

Regulasi perlindungan data pribadi yang bersifat spesifik di Indonesia harus senantiasa diselaraskan dengan nilai-nilai Pancasila. Nilai keadilan yang terkandung dalam Pancasila mengharuskan setiap kebijakan dan regulasi terkait perlindungan data pribadi yang bersifat spesifik mengutamakan prinsip-prinsip keadilan, kesetaraan, dan penghormatan terhadap hak asasi manusia.[279] Sebagai dasar negara, Pancasila memberikan pedoman yang jelas bagi negara dan masyarakat untuk menciptakan sistem hukum yang adil, transparan, dan responsif terhadap perubahan sosial dan teknologi.

Pelindungan data pribadi yang bersifat spesifik pada hakikatnya tidak dapat dilepaskan dari tanggung jawab negara untuk menjamin hadirnya keadilan yang nyata di ruang digital. Negara tidak cukup hanya membentuk peraturan yang bersifat normatif, tetapi juga wajib memastikan bahwa setiap ketentuan dapat dijalankan secara efektif oleh seluruh pihak yang mengelola data pribadi. Keadilan

---

[278] Humairah Almahdali et al., *Pendidikan Pancasila Dan Kewarganegaraan* (Agam: Yayasan Tri Edukasi Ilmiah, 2024). hlm. 6.

[279] Mohammad Wira Utama, "Rekonstruksi Regulasi Perlindungan Data Pribadi Bagi Nasabah Perbankan Yang Berbasis Nilai Keadilan" (Universitas Islam Sultan Agung (Indonesia), 2024). hlm. 163.

yang diidealkan oleh Pancasila menuntut agar warga negara tidak ditempatkan sebagai pihak yang lemah ketika berhadapan dengan korporasi digital, lembaga publik, maupun penyelenggara sistem elektronik yang memiliki kapasitas teknologi, modal, dan akses informasi yang jauh lebih besar. Oleh karena itu, perlindungan hukum terhadap data pribadi yang bersifat spesifik harus diarahkan untuk memperbaiki ketimpangan tersebut melalui penguatan hak subjek data, penegasan kewajiban pengendali data, serta penegakan hukum yang konsisten dan tidak diskriminatif. Dalam konteks ini, negara harus hadir sebagai penjamin keseimbangan antara kepentingan inovasi, kebutuhan pelayanan publik, dan perlindungan martabat manusia sebagai inti dari hak privasi.

Keadilan dalam perlindungan data pribadi yang bersifat spesifik juga harus dimaknai secara substantif, bukan hanya formal. Perlindungan formal hanya akan menghasilkan daftar hak dan kewajiban di dalam undang-undang, tetapi belum tentu menjamin bahwa hak tersebut benar-benar dapat dinikmati oleh masyarakat.[280] Sebaliknya, keadilan substantif menuntut agar setiap individu benar-benar memiliki kemampuan untuk menggunakan haknya, seperti hak memberikan atau menolak persetujuan, hak mengakses dan memperbaiki data, hak menghapus data, serta hak memperoleh pemulihan ketika terjadi pelanggaran. Dalam praktiknya, banyak subjek data masih belum memiliki posisi tawar yang memadai karena mereka berhadapan dengan syarat layanan digital yang rumit, kebijakan privasi yang tidak mudah dipahami, dan mekanisme pengaduan yang tidak

[280] Fauzan Hanafi, Abdul Balgis Hi Talib, and Musaddi Din, "Analisis Keadilan Substansial Pada Penerapan Undang-Undang Perlindungan Data Pribadi Terhadap Hak Pemilik Data Dalam Perspektif Hukum Positif Dan Hukum Islam," *Qadauna: Jurnal Ilmiah Mahasiswa Hukum Keluarga Islam* 6, no. 3 (2025): hlm. 274-291.

sederhana. Karena itu, hukum perlindungan data pribadi yang bersifat spesifik harus dirancang agar tidak hanya memberikan pengakuan normatif, tetapi juga menjamin adanya akses nyata, prosedur yang sederhana, serta mekanisme penyelesaian sengketa yang cepat dan terjangkau. Dengan cara demikian, keadilan tidak berhenti sebagai prinsip abstrak, melainkan hadir sebagai pengalaman hukum yang dapat dirasakan secara langsung oleh warga negara.

Pendekatan perlindungan hukum dalam perspektif Pancasila harus menempatkan data pribadi yang bersifat spesifik sebagai bagian dari kehormatan dan martabat manusia. Data kesehatan, data biometrik, data genetika, data keuangan pribadi, dan data anak bukan sekadar rangkaian informasi teknis, melainkan representasi dari identitas pribadi yang melekat pada eksistensi seseorang.[281] Penyalahgunaan atau kebocoran data tersebut dapat mengakibatkan kerugian yang tidak berhenti pada aspek ekonomi, tetapi juga dapat menimbulkan stigma sosial, diskriminasi, tekanan psikologis, hingga hilangnya rasa aman dalam kehidupan sehari-hari. Karena itu, perlindungan terhadap data pribadi yang bersifat spesifik harus diperlakukan sebagai bagian dari kewajiban konstitusional negara dalam menjamin hak asasi manusia. Pandangan ini sejalan dengan sila kedua Pancasila yang menempatkan manusia sebagai makhluk yang harus diperlakukan secara adil dan beradab. Dengan demikian, setiap tindakan pengumpulan, penyimpanan, pemrosesan, pemanfaatan, dan penghapusan data wajib tunduk pada prinsip penghormatan terhadap martabat manusia, sehingga tidak ada satu pun

[281] Sidi A Wiraguna and Megawati Barthos, *Hukum Privasi Dan Pelindungan Data Pribadi Di Indonesia*, ed. Neng Rismawati (Bandung: CV Widina Media Utama, 2025). hlm. 25-70.

pihak yang dapat menjadikan data pribadi sebagai alat eksploitasi atau dominasi atas individu lain.

Dalam hubungannya dengan tanggung jawab penyelenggara sistem elektronik, keadilan Pancasila menuntut adanya standar akuntabilitas yang lebih tinggi terhadap pihak-pihak yang mengelola data pribadi yang bersifat spesifik. Setiap pengendali data harus memiliki kewajiban untuk membuktikan bahwa data dikumpulkan untuk tujuan yang sah, diproses secara transparan, disimpan dengan aman, dan tidak diberikan kepada pihak ketiga tanpa dasar hukum yang jelas.[282] Prinsip akuntabilitas ini penting karena dalam banyak kasus, pelanggaran data terjadi bukan semata-mata karena serangan dari luar, tetapi karena lemahnya tata kelola internal, minimnya pengamanan teknis, dan rendahnya kesadaran etis dalam tubuh organisasi. Oleh sebab itu, hukum tidak boleh hanya berhenti pada larangan penyalahgunaan, melainkan harus mengharuskan setiap pengendali data untuk membangun sistem pengamanan yang memadai, melakukan audit secara berkala, menyediakan notifikasi insiden secara cepat, dan bertanggung jawab atas setiap kerugian yang timbul akibat kelalaiannya. Dalam perspektif Pancasila, tanggung jawab hukum seperti itu merupakan bentuk nyata dari keadilan sosial, karena memastikan bahwa pihak yang memperoleh manfaat dari pemrosesan data juga memikul beban tanggung jawab yang sebanding terhadap perlindungan hak masyarakat.

[282] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *Jurnal Yuridis* 7, no. 1 (2020): hlm. 105-119.

Prinsip musyawarah yang terkandung dalam sila keempat Pancasila mengajarkan bahwa pembentukan kebijakan publik tidak boleh dilakukan secara sepihak, tetapi harus melibatkan masyarakat sebagai pihak yang terdampak langsung.[283] Dalam konteks perlindungan data, hal ini berarti bahwa penyusunan regulasi, pedoman teknis, dan kebijakan pengawasan harus membuka ruang partisipasi yang luas bagi akademisi, masyarakat sipil, pelaku usaha, komunitas teknologi, serta kelompok-kelompok rentan yang datanya paling berisiko disalahgunakan. Partisipasi ini penting agar hukum yang dibentuk tidak hanya mencerminkan kepentingan institusional negara atau pasar, tetapi juga mencerminkan kebutuhan riil masyarakat. Dengan pendekatan yang partisipatif, kebijakan perlindungan data akan memiliki legitimasi sosial yang lebih kuat, sekaligus lebih adaptif terhadap perubahan teknologi dan praktik pemrosesan data yang terus berkembang. Dalam arti ini, demokratisasi tata kelola data bukan hanya soal prosedur, tetapi juga soal menciptakan keadilan dalam distribusi kekuasaan informasi.

Sanksi tegas terhadap pelanggaran data pribadi juga harus dipahami dalam kerangka keadilan korektif dan restoratif. Keadilan korektif menuntut agar setiap pelanggaran diikuti dengan upaya nyata untuk memperbaiki kerugian yang dialami korban, sedangkan keadilan restoratif mendorong agar hukum tidak hanya menghukum, tetapi juga memulihkan keseimbangan yang terganggu akibat pelanggaran tersebut. Dalam kasus data pribadi yang bersifat spesifik, pemulihan

[283] Nofita Rudiani Asbanu, Claudina Margarida Freitas Belo, and Yakobus Adi Saingo, "Analisis Peran DPR Dalam Menyuarakan Kepentingan Rakyat Berdasarkan Sila Keempat Pancasila," *MUTIARA: Jurnal Ilmiah Multidisiplin Indonesia* 3, no. 1 (January 15, 2025): hlm. 120-134.

semacam ini sangat penting karena kerugian korban sering kali bersifat multidimensi, meliputi kerugian finansial, reputasi, psikologis, dan sosial. Oleh sebab itu, mekanisme ganti rugi, permintaan maaf resmi, penghentian pemrosesan, penghapusan data yang diperoleh secara melawan hukum, serta kewajiban perbaikan sistem keamanan harus menjadi bagian dari respon hukum yang terstruktur. Penegakan hukum yang hanya berfokus pada denda administratif tanpa memulihkan korban akan sulit mencerminkan keadilan yang utuh. Pancasila menuntut agar hukum tidak hanya menjaga keteraturan, tetapi juga menghadirkan pemulihan yang berkeadilan bagi pihak yang dirugikan. Dengan demikian, sanksi yang tegas harus selalu dihubungkan dengan kewajiban pemulihan yang nyata dan dapat dirasakan oleh korban.

Budaya hukum masyarakat juga memegang peranan besar dalam mewujudkan perlindungan data pribadi yang bersifat spesifik yang berkeadilan. Sebaik apa pun regulasi yang dibentuk, hukum akan sulit berjalan efektif apabila masyarakat tidak memahami nilai penting privasi, pengendali data tidak memandang kepatuhan sebagai kewajiban etik, dan aparatur negara tidak memiliki sensitivitas terhadap hak subjek data.[284] Oleh karena itu, pendidikan hukum digital, literasi privasi, dan penguatan etika pengelolaan data harus menjadi bagian tak terpisahkan dari kebijakan nasional. Masyarakat perlu didorong untuk lebih sadar dalam memberikan data pribadi, lebih kritis terhadap praktik pengumpulan data, dan lebih berani menuntut transparansi dari pihak-pihak yang memproses data

[284] Yacinta Tira Varany and Listyowati Sumanto, "Dinamika Sistem Hukum Pelindungan Data Pribadi: Analisis Interaksi Struktur, Substansi, Dan Kultur Hukum Di Era Big Data," *Jurnal Impresi Indonesia* 4, no. 11 (2025): hlm. 5172-5185.

mereka. Di sisi lain, pelaku usaha dan institusi publik harus meninggalkan paradigma lama yang memandang perlindungan data sebagai beban administratif, lalu beralih kepada paradigma tata kelola yang menempatkan privasi sebagai nilai dasar dalam setiap desain sistem dan layanan. Dengan terbentuknya budaya hukum seperti ini, perlindungan data pribadi tidak hanya dijalankan karena takut sanksi, tetapi karena lahir dari kesadaran bersama bahwa data pribadi adalah bagian dari kehormatan manusia yang wajib dijaga.

Perlindungan hukum terhadap data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital harus diarahkan pada terwujudnya sistem hukum yang adil, adaptif, dan berorientasi pada manusia. Sistem tersebut harus mampu memastikan bahwa kemajuan teknologi tidak berakhir pada penguatan dominasi oleh pihak yang menguasai data, tetapi justru mendukung terciptanya ruang digital yang aman, transparan, dan berkeadilan bagi seluruh warga negara.[285] Nilai-nilai Pancasila memberikan arah yang jelas dalam mewujudkan tujuan tersebut, yakni dengan menempatkan perlindungan martabat manusia, keadilan sosial, musyawarah, tanggung jawab negara, dan keseimbangan kepentingan sebagai fondasi utama tata kelola data di Indonesia. Dengan demikian, perlindungan data pribadi yang bersifat spesifik bukan hanya soal kepatuhan terhadap hukum positif, tetapi merupakan bagian dari upaya menjaga harkat manusia, memperkuat kepercayaan publik, dan membangun peradaban digital nasional yang beretika.

---

[285] Ramadhina Eka Putri Sugiarto, Nita Afriani, and Rendy Kurniawan, "Analisis Yuridis Normatif Efektivitas Konvensi Kecerdasan Buatan Terhadap Perlindungan Hak Asasi Manusia," *Littera Legis: Journal of Law, Society, and Justice* 1, no. 2 (2026): hlm. 15-31.

1. Perlindungan Pemerintah terhadap Warga Negara dalam Pengelolaan Data Pribadi yang Bersifat Spesifik

Implementasi keadilan berdasarkan Pancasila dalam perlindungan data pribadi yang bersifat spesifik membutuhkan pengawasan yang ketat dan penegakan hukum yang konsisten, dimana pemerintah bersama lembaga terkait wajib memastikan ketentuan UU PDP diterapkan secara efektif dan dipatuhi oleh perusahaan maupun penyelenggara sistem elektronik demi kepentingan masyarakat. Proses penegakan hukum harus berlangsung adil, tanpa diskriminasi, serta memberikan perlindungan maksimal bagi individu yang datanya disalahgunakan atau dibocorkan. Dalam kerangka tersebut, hubungan antara hak asasi manusia dan keadilan Pancasila sangat erat, karena Pancasila menempatkan hak atas privasi dan martabat manusia sebagai hak yang wajib dihormati dan dilindungi. Oleh karena itu, setiap regulasi terkait perlindungan data pribadi yang bersifat spesifik tidak hanya berfokus pada pengamanan informasi, tetapi juga harus dirancang sedemikian rupa agar mencegah penyalahgunaan data, menjaga hak asasi manusia, dan mewujudkan keadilan sosial secara substantif.[286]

Pihak penyelenggara sistem elektronik yang mengelola data pribadi harus bertanggung jawab untuk menjaga keamanan data tersebut, sesuai dengan prinsip keadilan yang terkandung dalam sila kelima Pancasila, yaitu "Keadilan Sosial bagi seluruh Rakyat Indonesia." Agar perlindungan data pribadi yang bersifat spesifik dapat terlaksana dengan adil, perlu ada pengawasan yang ketat terhadap

[286] Sri Yunita et al., "Peranan Hukum Dalam Penegakan Hak Asasi Manusia (Ham) Di Era Digital," *Jurnal Review Pendidikan dan Pengajaran* 7, no. 4 (2024), hlm. 16726-16731.

pengelolaan data pribadi. Pengawasan ini bukan hanya tugas pemerintah, tetapi juga bagian dari tanggung jawab sosial seluruh elemen masyarakat.[287] Dalam penerapan Pancasila, keadilan sosial menuntut agar pengelolaan data pribadi dilakukan dengan transparansi dan akuntabilitas yang tinggi. Pengawasan ini bertujuan untuk memastikan bahwa tidak ada pihak yang menyelewengkan data pribadi untuk kepentingan pribadi atau korporasi yang merugikan masyarakat.

Regulasi perlindungan data pribadi yang bersifat spesifik harus direkonstruksi secara berkelanjutan untuk menjaga relevansinya dengan tantangan zaman seiring dengan perkembangan teknologi dan meningkatnya ancaman terhadap privasi individu. Rekonstruksi hukum ini harus disesuaikan dengan kebutuhan masyarakat yang semakin terhubung dengan dunia digital. Pancasila sebagai dasar negara memberikan prinsip dasar untuk menciptakan hukum yang berkeadilan, yang menyesuaikan dengan perkembangan zaman namun tetap menghormati hak-hak dasar manusia. Dalam hal ini, rekonstruksi hukum akan memastikan bahwa perlindungan data pribadi yang bersifat spesifik tidak hanya responsif terhadap perubahan teknologi, tetapi juga tetap adil dan merata bagi seluruh rakyat Indonesia.

Kebijakan perlindungan data pribadi yang bersifat spesifik harus disusun dengan memperhatikan dinamika sosial dan perkembangan teknologi yang terus berubah.[288] Negara harus mampu menghadirkan kebijakan yang responsif, yang

---

[287] Loso Judijanto and Al-Amin, "Transformasi Digital Dalam Pelayanan Publik: Implikasi Dan Tantangan Hukum Administrasi Negara," *Jurnal Administrasi Negara* 3, no. 2 (2025), hlm. 1-7.

[288] Aullia Vivi Yulianingrum and Muhammad Nurcholis, "Poltik Hukum Pengaturan Dan Pembangunan Hukum Transportasi Online Di Era Disrupsi Berbasis E- Governance Dan Dynamic Governance," *Jurnal Rectum* 7, no. 1 (2025), hlm. 18-33.

tidak hanya melindungi data pribadi, tetapi juga menciptakan ruang bagi inovasi teknologi.[289] Pancasila mengajarkan bahwa kebijakan harus berpihak kepada kepentingan masyarakat luas, bukan hanya segelintir pihak. Oleh karena itu, kebijakan yang mengatur perlindungan data pribadi yang bersifat spesifik perlu menyeimbangkan antara kebutuhan untuk melindungi privasi individu dengan kebutuhan untuk mendorong kemajuan teknologi yang bermanfaat bagi masyarakat.

Pelindungan data pribadi yang bersifat spesifik bukan hanya menyangkut aspek keamanan informasi, tetapi juga terkait langsung dengan pemeliharaan martabat dan hak setiap individu, sehingga menjadi bagian integral dari keadilan sosial dalam sistem hukum Indonesia yang berlandaskan Pancasila. Negara, melalui kebijakan dan regulasi, berkewajiban memastikan setiap orang memperoleh perlindungan yang setara atas data pribadinya, sekaligus menjamin terpenuhinya hak untuk mengakses dan mengoreksi data pribadi sebagai perwujudan prinsip transparansi dalam pengolahan data. Pancasila menegaskan pentingnya hak individu untuk mengetahui dan mengontrol data yang berkaitan dengan dirinya, serta memastikan bahwa data yang disimpan dan diproses akurat, tidak merugikan, dan dikelola melalui mekanisme yang memadai, mudah diakses, dan tidak menimbulkan hambatan bagi masyarakat.[290]

---

[289] Akhmad Zaki Yamani, "Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak," *Journal of Law and Nation (JOLN) Vol.* 4, no. 2 (2025), hlm. 312-324.

[290] Wyanda Kinanti Syauqi Ramadhani and Sidi Ahyar Wiraguna, "Implementasi Pelindungan data pribadi yang bersifat spesifik Dalam Sistem Informasi Pada Perusahaan Jasa Keuangan," *Perspektif Administrasi Publik dan hukum* 2, no. 2 (2025), hlm. 158-175.

Keputusan yang diambil oleh pengelola data pribadi harus berlandaskan prinsip keadilan, dengan mengutamakan kepentingan subjek data dan memastikan bahwa setiap tindakan pengumpulan, penggunaan, maupun penghapusan data tidak merugikan pihak mana pun. Dalam perspektif Pancasila, khususnya sila keempat, proses pengambilan keputusan idealnya dilakukan secara bijaksana, transparan, dan mencerminkan semangat musyawarah untuk mufakat dalam merumuskan kebijakan perlindungan data pribadi yang bersifat spesifik. Untuk menjamin keadilan tersebut, diperlukan pengawasan yang ketat dan efektif oleh lembaga yang berwenang dan independen, baik dari unsur pemerintah maupun lembaga mandiri, guna mencegah pelanggaran hak individu, mendorong kepatuhan terhadap regulasi, serta memastikan tidak terjadinya penyalahgunaan data pribadi.[291]

Transparansi adalah salah satu prinsip keadilan dalam Pancasila yang relevan dengan perlindungan data pribadi yang bersifat spesifik, yakni hak setiap individu untuk mengetahui bagaimana data mereka dikumpulkan, diproses, dan digunakan oleh pihak lain, sehingga mereka tidak merasa ditipu dan dapat menilai apakah penggunaan data tersebut sudah adil. Regulasi perlindungan data pribadi yang bersifat spesifik karenanya harus mewajibkan keterbukaan penuh dalam pengelolaan data, sekaligus mampu merespons tantangan baru yang muncul akibat pesatnya perkembangan teknologi, termasuk penggunaan *algoritma* dan *kecerdasan buatan* yang berpotensi mengancam hak privasi. Dalam konteks ini, Pancasila memberikan landasan etis agar setiap pemanfaatan teknologi di bidang

[291] Mahameru et al., *loc.cit*.

data pribadi diatur secara bijaksana dan adil, tanpa mengorbankan hak asasi manusia dan keadilan sosial.[292]

Penggunaan data pribadi untuk kepentingan ekonomi harus dilaksanakan dengan berlandaskan prinsip keadilan, yakni tidak merugikan konsumen dan tetap menghormati hak privasi individu, sejalan dengan ajaran Pancasila tentang keseimbangan antara kepentingan individu dan kepentingan kolektif. Dalam perspektif konstitusional, Pasal 28G ayat (1) UUD 1945 menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, serta rasa aman dari ancaman terhadap pelaksanaan hak-haknya, sehingga perlindungan data pribadi yang bersifat spesifik merupakan bagian integral dari perlindungan hak asasi manusia yang wajib dijamin negara. Dengan demikian, negara tidak hanya berkewajiban membentuk regulasi perlindungan data pribadi yang bersifat spesifik, tetapi juga memastikan pengawasan dan penegakan hukum yang efektif terhadap setiap pelanggaran, agar seluruh pihak yang mengelola data pribadi mematuhi ketentuan yang berlaku demi terwujudnya keadilan dan kesejahteraan sosial sesuai dengan nilai-nilai Pancasila.[293]

Kebijakan perlindungan data pribadi yang bersifat spesifik harus disusun secara berkelanjutan agar adaptif terhadap perkembangan teknologi dan dinamika sosial, namun tetap berlandaskan prinsip keadilan dan kesejahteraan rakyat dalam Pancasila, sehingga mampu menjaga hak privasi sekaligus menyeimbangkan

---

[292] Marsya Indah Yunita et al., "Tantangan Etika Dan Privasi Terhadap Perspektif Global Pendidikan Teknologi Bagi Generasi Mendatang," *EDUCREATIVA: Jurnal Seputar Isu dan Inovasi Pendidikan* 1, no. 1 (2025), hlm. 64-74.

[293] Moh Bagas Fadhli Dzil Ikrom and Badrut Tamam, "Perlindungan Hukum Hak Privasi Warga Negara Terhadap Kebocoran Data Pribadi Di Indonesia," *Constituion Journal* 3, no. 2 (2024), hlm. 139-154.

kemajuan teknologi dengan perlindungan data. Untuk mewujudkannya, masyarakat perlu diedukasi mengenai hak-hak atas data pribadi, cara melindunginya, dan langkah yang dapat ditempuh ketika terjadi penyalahgunaan, sementara teknologi dimanfaatkan untuk mendeteksi dan mencegah kebocoran serta mengamankan transaksi digital demi kepentingan bersama. Seluruh upaya tersebut harus ditopang oleh penegakan hukum yang tegas dan konsisten, dengan sanksi yang proporsional dan menimbulkan efek jera, agar prinsip keadilan Pancasila dalam menjaga martabat dan hak setiap individu benar-benar terimplementasi dalam praktik perlindungan data pribadi yang bersifat spesifik.[294]

Penegakan hukum yang efektif dalam perlindungan data pribadi yang bersifat spesifik tidak hanya bertumpu pada pemberian sanksi, tetapi juga pada pengawasan dan upaya pencegahan agar regulasi yang ada dapat diterapkan secara konsisten, serta setiap pelanggaran diproses dengan cepat dan adil. Dalam perspektif Pancasila, keadilan tidak semata-mata lahir dari hukuman, tetapi juga dari tindakan preventif yang melibatkan seluruh elemen masyarakat. Pelindungan data pribadi yang bersifat spesifik yang berkeadilan dapat terwujud apabila prinsip-prinsip Pancasila seperti keadilan, kesetaraan, dan penghormatan terhadap hak asasi manusia diintegrasikan dalam pengelolaan data pribadi.[295]

[294] Satria dan Yusuf, *loc.cit*.
[295] Ikrom dan Tamam, *loc.cit*.

2. Perlindungan Hak-Hak Warga Negara sebagai Subjek Data

Hak Asasi Manusia (HAM) merupakan landasan utama dalam penerapan keadilan berdasarkan Pancasila.[296] Pancasila mengakui hak-hak dasar setiap individu, termasuk hak atas privasi, yang dijamin dalam Pasal 28G UUD 1945. Dalam konteks perlindungan data pribadi yang bersifat spesifik, HAM berperan penting untuk melindungi hak setiap individu terhadap penyalahgunaan data pribadi. Oleh karena itu, regulasi perlindungan data pribadi yang bersifat spesifik di Indonesia, termasuk UU PDP, harus berpihak pada perlindungan hak-hak individu tersebut.[297] Dalam hal ini, keadilan Pancasila mengharuskan negara dan masyarakat untuk menghormati dan melindungi hak setiap individu atas data pribadinya dengan memberikan akses yang adil terhadap pengelolaan dan penggunaan data tersebut.

Keadilan dalam pengolahan data pribadi mencakup prinsip bahwa setiap individu harus memiliki kontrol penuh terhadap data pribadinya. Prinsip ini bertentangan dengan praktik pengumpulan data secara massal tanpa izin atau transparansi.[298] Dalam konteks Pancasila, pengolahan data pribadi harus dilakukan dengan menghormati hak-hak individu dan tidak merugikan mereka. Ini mencerminkan sila kelima Pancasila, yaitu "Keadilan Sosial bagi seluruh Rakyat

---

[296] Safira Kanaya, Iffat Husna, and Fatma Ulfatun Najicha, "Pancasila Dan Hubungannya Dengan Hak Asasi Manusia Di Indonesia Safira," *JCE: Jurnal Civic Education* 7, no. 2 (2023), hlm. 104-112.

[297] Ridho Pakina and Mohammad Solekhan, "Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia," *Journal of Scientech Research and Development* 6, no. 1 (2024), hlm. 273-286.

[298] Nur Rochmah Dyah Puji Astuti et al., *op.cit*. hlm. 46.

Indonesia," yang mendorong pemerataan perlindungan hak atas data pribadi bagi seluruh masyarakat, tanpa memandang status sosial, ekonomi, atau politik.

Data pribadi yang bersifat spesifik atau sensitif memerlukan perlindungan yang lebih ketat dibandingkan data pribadi biasa. Keberadaan data seperti informasi medis, agama, atau orientasi seksual, misalnya, membutuhkan pengaturan khusus dalam hal pengumpulan, penggunaan, dan penyimpanan[299]. Keadilan dalam hal ini berarti bahwa negara dan pihak yang mengelola data harus memastikan bahwa data sensitif tersebut hanya digunakan untuk tujuan yang sah dan dengan persetujuan eksplisit dari subjek data. UU PDP mengatur ketat tentang hal ini, memberikan perlindungan ekstra terhadap data yang berpotensi menimbulkan kerugian besar jika disalahgunakan.[300]

Bentuk implementasi keadilan dalam perlindungan data pribadi yang bersifat spesifik adalah pemberian hak kepada setiap individu untuk mengakses dan menghapus data pribadinya, sehingga ia memiliki kontrol atas informasi yang dikelola pihak ketiga. Pancasila sebagai dasar negara memberikan landasan filosofis bagi kebijakan perlindungan data pribadi yang bersifat spesifik, khususnya melalui sila kedua tentang *Kemanusiaan yang Adil dan Beradab*, yang menuntut agar setiap orang diperlakukan secara adil dalam pengelolaan data pribadinya. Konsekuensinya, perumusan undang-undang dan peraturan, seperti UU PDP, harus

[299] Shinta Hadiyantina et al., *Perlindungan Data Pribadi Dalam Bidang Rekam Medis* (Malang: Universitas Brawijaya Press, 2023). hlm. 89.

[300] Muhammad Kamarulzaman Satria and Hudi Yusuf, "Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *JICN: Jurnal Intelek dan Cendikiawan Nusantara* 1, no. 2 (2024), hlm. 2442-2456.

secara konsisten mencerminkan nilai keadilan, transparansi, perlindungan hak asasi manusia, serta keadilan sosial bagi setiap individu tanpa terkecuali.[301]

Setiap individu berhak memperoleh perlindungan atas data pribadinya, dimana sila kedua, *"*Kemanusiaan yang Adil dan Beradab*,"* menjadi dasar bagi perlindungan yang adil dan setara terhadap privasi dan pengelolaan data pribadi. Hukum perlindungan data pribadi yang bersifat spesifik di Indonesia, khususnya melalui UU PDP, bertujuan memastikan bahwa setiap warga negara tanpa kecuali memperoleh jaminan perlindungan yang efektif dan adil, sekaligus menegaskan bahwa perlindungan data pribadi yang bersifat spesifik bukan hanya hak individu, tetapi juga tanggung jawab negara dan para pengelola data. Dengan demikian, regulasi tersebut diharapkan mampu mencegah ketidakadilan sosial yang dapat timbul dari penyalahgunaan data pribadi, termasuk oleh pihak-pihak yang memiliki kekuatan ekonomi atau teknologi yang lebih besar.[302]

Implementasi penting dari keadilan dalam Pancasila terkait data pribadi adalah hak individu untuk memberikan persetujuan yang jelas sebelum data mereka dikumpulkan atau diproses. Dalam konteks UU PDP, persetujuan eksplisit adalah prinsip utama yang mengedepankan keadilan dalam pemrosesan data pribadi.[303] Tanpa persetujuan yang sah, data pribadi tidak dapat dikumpulkan atau digunakan,

---

[301] Ibnu Abdillah et al., "Pancasila Sebagai Pedoman Dasar Dalam Perlindungan Hukum Terhadap Hak Asasi Manusia," *Jurnal Moralita: Jurnal Pendidikan Pancasila dan Kewarganegaraan* 5, no. 2 (2024), hlm. 57-63.

[302] Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *Justisi* 10, no. 1 (2024).

[303] Masitoh Indriani and Annida Aqiila Putri, "Persetujuan Dinamis Sebagai Sarana Optimalisasi Pelindungan data pribadi yang bersifat spesifik Dan Hak Atas Privasi (The Dynamic Consent for Optimizing Personal Data Protection and The Right to Privacy)," *Jurnal HAM* 14, no. 2 (2023).

yang mencerminkan hak setiap individu untuk mengontrol data mereka. Ini adalah penerapan dari sila keempat Pancasila.[304]

Pancasila mengajarkan bahwa setiap individu berhak untuk mengakses data pribadi mereka dan menghapusnya jika tidak lagi diperlukan. Hal ini merupakan salah satu bentuk perlindungan yang memberikan kontrol penuh kepada individu atas data pribadi mereka. UU PDP memberikan hak ini sebagai bagian dari keadilan dalam penggunaan data pribadi. Negara bertanggung jawab untuk menciptakan sistem yang memudahkan akses tersebut, sehingga setiap orang dapat melindungi privasinya sesuai dengan prinsip keadilan yang diusung oleh Pancasila. [305] Keamanan data pribadi adalah bagian integral dari perlindungan yang adil dalam Pancasila. Data pribadi yang tidak dilindungi dengan baik dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, yang dapat mengarah pada ketidakadilan sosial.[306] Dalam hal ini, negara harus menjamin bahwa setiap individu memperoleh keamanan yang setara terhadap data pribadi mereka.

Pelindungan data pribadi yang bersifat spesifik bukan hanya menyangkut aspek keamanan informasi, tetapi juga terkait langsung dengan pemeliharaan martabat dan hak setiap individu, sehingga menjadi bagian integral dari keadilan sosial dalam sistem hukum Indonesia yang berlandaskan Pancasila. Negara, melalui kebijakan dan regulasi, berkewajiban memastikan setiap orang memperoleh

---

[304] Denindah Olivia, Sinta Dewi Rosadi, and Rika Ratna Permata, "Perlindungan Data Pribadi Dalam Penyelenggaraan Aplikasi Surveilans Kesehatan Pedulilindungi Dan Covidsafe Di Indonesia Dan Australia," *DATIN Law Jurnal* 1, no. 2 (2020), hlm. 1-15.

[305] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi," *Borneo Law Review* 5, no. 1 (2021), hlm. 46-68.

[306] Muh. Arhanul Ilham, Haslindah, and Muh. Arafah, "Jual Beli Online Di Masa Kini Ditinjau Dalam Perspektif Islam (Studi Pada Pengguna Online Shop Di Kecamatan Tanete Riattang Kabupaten Bone)," *Jurnal Ilmiah Multidisiplin Terpadu* 8, no. 9 (2024), hlm. 213-241.

perlindungan yang setara atas data pribadinya, sekaligus menjamin terpenuhinya hak untuk mengakses dan mengoreksi data pribadi sebagai perwujudan prinsip transparansi dalam pengolahan data. Pancasila menegaskan pentingnya hak individu untuk mengetahui dan mengontrol data yang berkaitan dengan dirinya, serta memastikan bahwa data yang disimpan dan diproses akurat, tidak merugikan, dan dikelola melalui mekanisme yang memadai, mudah diakses, dan tidak menimbulkan hambatan bagi masyarakat.[307]

3. Sanksi Tegas terhadap Pelanggaran Data Pribadi

Negara perlu memastikan penegakan hukum yang konsisten dan adil untuk mewujudkan keadilan dalam perlindungan data pribadi yang bersifat spesifik. Pelanggaran terhadap hak privasi individu yang berkaitan dengan data pribadi harus dikenakan sanksi yang tegas. Dalam hal ini, keadilan Pancasila mengajarkan bahwa hukum harus ditegakkan tanpa memandang status sosial atau kekuasaan individu yang bersangkutan. Penegakan hukum yang adil akan memberikan efek jera kepada pihak yang melanggar, sekaligus memastikan bahwa setiap individu dilindungi haknya secara setara.

Kebijakan perlindungan data pribadi yang bersifat spesifik harus disusun secara berkelanjutan agar adaptif terhadap perkembangan teknologi dan dinamika sosial, namun tetap berlandaskan prinsip keadilan dan kesejahteraan rakyat dalam Pancasila, sehingga mampu menjaga hak privasi sekaligus menyeimbangkan kemajuan teknologi dengan perlindungan data. Untuk mewujudkannya, masyarakat

[307] Wyanda Kinanti Syauqi Ramadhani and Sidi Ahyar Wiraguna, "Implementasi Pelindungan data pribadi yang bersifat spesifik Dalam Sistem Informasi Pada Perusahaan Jasa Keuangan," *Perspektif Administrasi Publik dan hukum* 2, no. 2 (2025), hlm. 158-175.

perlu diedukasi mengenai hak-hak atas data pribadi, cara melindunginya, dan langkah yang dapat ditempuh ketika terjadi penyalahgunaan, sementara teknologi dimanfaatkan untuk mendeteksi dan mencegah kebocoran serta mengamankan transaksi digital demi kepentingan bersama. Seluruh upaya tersebut harus ditopang oleh penegakan hukum yang tegas dan konsisten, dengan sanksi yang proporsional dan menimbulkan efek jera, agar prinsip keadilan Pancasila dalam menjaga martabat dan hak setiap individu benar-benar terimplementasi dalam praktik perlindungan data pribadi yang bersifat spesifik.[308]

Penegakan hukum yang efektif dalam perlindungan data pribadi yang bersifat spesifik tidak hanya bertumpu pada pemberian sanksi, tetapi juga pada pengawasan dan upaya pencegahan agar regulasi yang ada dapat diterapkan secara konsisten, serta setiap pelanggaran diproses dengan cepat dan adil. Dalam perspektif Pancasila, keadilan tidak semata-mata lahir dari hukuman, tetapi juga dari tindakan preventif yang melibatkan seluruh elemen masyarakat. Pelindungan data pribadi yang bersifat spesifik yang berkeadilan dapat terwujud apabila prinsip-prinsip Pancasila seperti keadilan, kesetaraan, dan penghormatan terhadap hak asasi manusia diintegrasikan dalam pengelolaan data pribadi.[309]

Data pribadi menjadi komoditas penting bagi banyak sektor di era digital. Penerapan keadilan dalam perlindungannya menjadi sangat krusial. Pancasila mengajarkan bahwa setiap individu berhak untuk mendapatkan perlindungan yang adil terhadap hak-haknya, termasuk data pribadi yang sering kali dieksploitasi

[308] Satria dan Yusuf, *loc.cit*.
[309] Ikrom dan Tamam, *loc.cit*.

untuk kepentingan ekonomi atau politik.[310] Dalam hal ini, regulasi yang adil tidak hanya mengatur hak individu untuk melindungi data pribadinya tetapi juga mengatur tanggung jawab pihak yang mengumpulkan, mengelola, dan mengolah data tersebut, agar tidak merugikan pihak yang memiliki data. Keberadaan UU PDP memberikan dasar hukum yang kuat untuk mewujudkan keadilan dalam perlindungan data pribadi yang bersifat spesifik, dengan mengedepankan prinsip transparansi, persetujuan yang jelas, dan hak untuk mengakses data.

Masyarakat memiliki peran penting dalam menciptakan ekosistem yang adil dalam pengelolaan data pribadi. Pancasila mengajarkan pentingnya gotong royong dan partisipasi aktif dalam menjaga keadilan sosial.[311] Dalam konteks ini, masyarakat harus dilibatkan dalam pengawasan dan pengambilan keputusan yang berkaitan dengan perlindungan data pribadi. Selain itu, kesadaran masyarakat tentang pentingnya perlindungan data pribadi dan hak-hak privasi juga menjadi kunci untuk memastikan keadilan dalam dunia digital.

Penyusunan regulasi yang adil mengenai perlindungan data pribadi yang bersifat spesifik harus berlandaskan prinsip musyawarah dan mufakat sebagaimana diajarkan Pancasila, dengan melibatkan berbagai pemangku kepentingan agar kebijakan yang dihasilkan benar-benar mencerminkan kepentingan seluruh masyarakat. Kebijakan tersebut wajib berpihak pada keadilan sosial dengan memberikan perlindungan yang setara bagi seluruh lapisan masyarakat, sehingga tidak ada individu atau kelompok yang terpinggirkan atau dirugikan. Selain itu,

---

[310] Efraim Mangaluk, Sepriano Sepriano, and Agus Nasrullah, *Buku Referensi Wawasan Pancasila* (Jambi: PT. Sonpedia Publishing Indonesia, 2025). hlm. 29.

[311] Alfath Roziq and Fatma Ulfatun Najicha, *Peran Nilai Pancasila Dan Semangat Bela Negara Bagi Generasi Muda Dalam Era Transformasi Digital* (Surakarta, 2023).

keamanan data pribadi harus mempertimbangkan keadilan antargenerasi, yakni memastikan bahwa data yang dikumpulkan dan disimpan tidak disalahgunakan sehingga generasi mendatang tetap dapat menikmati hak yang sama atas privasi.[312]

B. Jaminan Kepastian Hukum Terhadap Data Pribadi yang Bersifat Spesifik di Era Digital

Pancasila sebagai dasar negara menuntut agar pengelolaan data pribadi mencerminkan nilai-nilai luhur dalam setiap sila. Sila pertama, *Ketuhanan Yang Maha Esa*, mengajarkan penghormatan terhadap martabat manusia sehingga pengelolaan data pribadi harus berbasis nilai moral, dilakukan secara etis, hati-hati, dengan persetujuan eksplisit dan transparansi mengenai tujuan serta cara pemrosesan data. [313] Sila kedua, *Kemanusiaan yang Adil dan Beradab*, menegaskan hak setiap individu untuk mengontrol data pribadinya, termasuk hak untuk mengakses, mengubah, dan menghapus data, serta mewajibkan negara memberikan perlindungan efektif terhadap pelanggaran privasi melalui sanksi yang menimbulkan efek jera. [314] Sila ketiga, *Persatuan Indonesia*, menuntut keseimbangan antara kepentingan negara (misalnya demi keamanan nasional) dan hak privasi individu, sehingga pengumpulan dan penggunaan data pribadi hanya boleh untuk tujuan yang sah dan diawasi dengan ketat agar tidak disalahgunakan oleh lembaga negara maupun pihak lain yang memiliki akses terhadap data tersebut. Pengelolaan data pribadi juga harus mengedepankan transparansi, dimana individu

---

[312] "Perlindungan Data Pribadi Di Era Digital - ITEBA," *Iteba.Ac.Id*, accessed May 9, 2025, https://iteba.ac.id/berita/perlindungan-data-pribadi-di-era-digital/.

[313] Ellen Diva Ibanez, "Etika Data : Pengumpulan Dan Pengolahan Bertanggung Jawab," *Ftmm.Unair.Ac.Id*, accessed May 9, 2025, https://ftmm.unair.ac.id/etika-data-pengumpulan-dan-pengolahan-bertanggung-jawab/.

[314] Suari dan Sarjana, *loc.cit*.

harus mengetahui dengan jelas bagaimana data mereka akan digunakan dan diproses. [315]

Pelindungan data pribadi yang bersifat spesifik membutuhkan regulasi yang tidak hanya ketat dan tegas, tetapi juga fleksibel dan adaptif terhadap perkembangan teknologi dan dinamika sosial. Regulator harus memastikan bahwa aturan yang ada dapat menanggapi perubahan cepat di dunia digital dan tetap relevan dalam mengatur pengelolaan data pribadi. Di samping itu, kebijakan perlindungan data pribadi yang bersifat spesifik harus mempertimbangkan inovasi yang dapat bermanfaat bagi masyarakat, seperti penggunaan teknologi untuk meningkatkan pelayanan publik atau kemudahan dalam bertransaksi.

Di era digital yang serba terhubung ini, perlindungan data pribadi yang bersifat spesifik menjadi semakin penting dan semakin sulit untuk diatur. Seiring dengan pesatnya perkembangan teknologi, semakin banyak platform dan aplikasi yang mengumpulkan data pribadi penggunanya. Dalam konteks ini, peraturan yang mengatur perlindungan data pribadi yang bersifat spesifik harus selalu diperbarui untuk mengimbangi perubahan yang terjadi di dunia digital. Penggunaan teknologi canggih seperti kecerdasan buatan (AI), *Internet of Things* (IoT), dan big data memerlukan kebijakan perlindungan data yang lebih canggih dan adaptif agar data pribadi yang dikumpulkan tetap terlindungi.[316]

---

[315] Naylawati Bahtiar, "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)* 2, no. 1 (2024), hlm. 85-100.

[316] Prado Dian Firmansyah et al., "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan," *Jurnal Kewirausahaan dan Multi Talenta* 2, no. 2 (2024), hlm. 112-125.

Masa depan regulasi perlindungan data pribadi yang bersifat spesifik di Indonesia akan bergantung pada kemampuan negara untuk beradaptasi dengan perkembangan teknologi yang cepat. Dengan pesatnya kemajuan di bidang teknologi, terutama di dunia digital, regulasi perlindungan data pribadi yang bersifat spesifik harus mampu menanggapi tantangan baru dan memberikan perlindungan yang memadai bagi individu.[317] Oleh karena itu, peraturan yang ada harus bersifat dinamis, yang memungkinkan penyesuaian dengan teknologi baru tanpa mengorbankan prinsip dasar perlindungan data. Selain itu, peran pemerintah dan sektor swasta akan semakin penting dalam menciptakan sistem pengelolaan data pribadi yang efektif dan aman. Kolaborasi yang erat antara kedua sektor ini akan memungkinkan Indonesia untuk memajukan industri digital sambil tetap menjaga standar tinggi dalam perlindungan data pribadi yang bersifat spesifik. Untuk itu, perlu ada investasi berkelanjutan dalam pengembangan infrastruktur digital yang mendukung keamanan data dan melibatkan masyarakat dalam pengawasan untuk memastikan kebijakan ini dijalankan dengan efektif.[318]

1. Konsep Kepastian Hukum dalam Perlindungan Data Pribadi

Penegakan hukum terhadap pelanggaran data pribadi adalah aspek yang sangat penting dalam memastikan efektivitas perlindungan data pribadi yang bersifat spesifik. Di Indonesia, meskipun sudah ada regulasi seperti Undang-Undang Pelindungan data pribadi (UU PDP), implementasi penegakan hukum

---

[317] Nuraisah Masita Utiarahman, "Peraturan Hukum Perdata Nasional Di Era Digital Hambatan Dan Kesempatan Dalam Melindungi Data Pribadi," *Ganec Swara* 19, no. 1 (2025), hlm. 147-154.

[318] Dede Al Mustaqim, "Strategi Pengembangan Pariwisata Halal Sebagai Pendorong Ekonomi Berkelanjutan Berbasis Maqashid Syariah," *AB-JOIEC: Al-Bahjah Journal of Islamic Economics* 1, no. 1 (2023), hlm. 26-43.

sering kali terkendala oleh berbagai faktor. Salah satunya adalah kurangnya pengawasan yang memadai dan sumber daya manusia yang terlatih untuk menangani kasus pelanggaran data pribadi.[319] Oleh karena itu, penting bagi negara untuk memperkuat lembaga yang bertanggung jawab dalam penegakan hukum dan memastikan bahwa mereka memiliki kapasitas yang memadai untuk menangani kasus pelanggaran data pribadi.

Pelindungan data pribadi yang efektif menuntut kerja sama erat antara pemerintah, sektor swasta, dan masyarakat untuk meningkatkan kesadaran akan pelanggaran data, mendorong pelaporan, serta memastikan adanya tindak lanjut yang tegas melalui sanksi yang menimbulkan efek jera. Partisipasi publik perlu difasilitasi melalui forum konsultasi, mekanisme pengaduan, dan ruang dialog lain agar kebijakan benar-benar mencerminkan kebutuhan semua pihak. Di saat yang sama, edukasi dan kampanye literasi privasi harus diprioritaskan agar masyarakat memahami hak-haknya dan mampu melindungi diri dari penyalahgunaan data. Perkembangan teknologi termasuk *big data* dan kecerdasan buatan memang menghadirkan efisiensi bagi berbagai sektor, tetapi juga memperbesar risiko pengumpulan dan pemrosesan data tanpa izin eksplisit, sehingga regulasi perlindungan data pribadi yang bersifat spesifik harus terus diperbarui dan diperkuat agar tetap relevan dengan dinamika teknologi.[320]

---

[319] Muhammad Yudistira and Ramadani Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh KOMINFO," *UNES Law Review* 5, no. 4 (2023), hlm. 3917-3929.

[320] Berto Purnomo Sidik and Sidi Ahyar Wiraguna, "Tinjauan Hukum Terhadap Aplikasi Digital Sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora* 2, no. 2 (2025), hlm. 219-232.

Lembaga pengawas memiliki peran yang sangat penting dalam memastikan bahwa regulasi perlindungan data pribadi yang bersifat spesifik dijalankan dengan baik dan efektif. Lembaga ini bertanggung jawab untuk memantau pelaksanaan kebijakan, menangani pengaduan, dan menindaklanjuti pelanggaran data pribadi.[321] Penting bagi lembaga pengawas untuk memiliki kewenangan yang cukup untuk melakukan audit terhadap perusahaan atau organisasi yang mengelola data pribadi, serta memberikan sanksi yang sesuai jika terjadi pelanggaran.

Hukum memiliki peran yang sangat penting dalam menjaga keamanan data pribadi. Dalam hal ini, sanksi yang tegas terhadap pelanggaran data pribadi akan memberikan efek jera kepada pihak-pihak yang tidak bertanggung jawab. Penegakan hukum yang adil dan konsisten sangat diperlukan agar regulasi yang ada dapat berjalan dengan efektif. Hukum juga berfungsi untuk memastikan bahwa hak-hak privasi individu tetap dilindungi, dan bahwa pelanggaran terhadap data pribadi akan mendapat sanksi yang sesuai.[322]

Sistem peradilan yang berpihak pada perlindungan data pribadi yang bersifat spesifik akan memberikan rasa aman bagi masyarakat bahwa hak privasi mereka dihormati, sehingga dibutuhkan pengaturan hukum yang jelas, baik di tingkat nasional maupun internasional, agar setiap individu yang dirugikan akibat pelanggaran data dapat memperoleh keadilan. Dalam konteks layanan keuangan

---

[321] Muhammad Fadel Adhyputra, Thoriq Ahmadi, and Mohammad Rifqi, "Analisis Komparatif Rancangan LPPDP Indonesia Dengan Otoritas Pelindungan Data Singapura Dalam Penegakan Hukum Pelanggaran Data Pribadi: The Notion Of Personal Data Protection By Indonesia's Lppdp: A Comparative Study With The Singapore Personal Data Prot," *Jurnal Nomokrasi* 2, no. 2 (2024), hlm. 56-74.

[322] Ananta Fadli Sutarli and Shelly Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *Innovative: Journal Of Social Science Research* 3, no. 2 (2023), hlm. 4208-4221.

digital yang berkembang pesat, perlindungan data pribadi yang bersifat spesifik menjadi sangat krusial karena menyangkut informasi sensitif seperti rekening, nomor kartu kredit, dan riwayat transaksi; karena itu, penyedia layanan wajib menerapkan teknologi keamanan yang kuat dan kebijakan pengelolaan data yang tegas. Penerapan prinsip *data minimization* penting dijalankan dengan cara hanya mengumpulkan dan menyimpan data yang benar-benar diperlukan untuk keperluan transaksi, sementara pengawasan yang lebih ketat terhadap penyelenggara layanan keuangan digital diperlukan untuk memastikan kepatuhan terhadap regulasi perlindungan data pribadi yang bersifat spesifik dan mencegah penyalahgunaan data untuk kepentingan yang tidak sah.[323]

Penegakan hukum yang efektif menjadi kunci agar regulasi perlindungan data pribadi benar-benar dipatuhi, melalui sistem hukum yang transparan, efisien, dan menyediakan mekanisme yang jelas bagi individu ketika hak privasinya dilanggar. Setiap pelanggaran harus segera ditindak dengan sanksi yang tegas dan proporsional mulai dari denda administratif, sanksi pidana, hingga upaya pemulihan bagi subjek data sehingga kepercayaan publik terhadap sistem perlindungan data pribadi dapat diperkuat. Upaya ini perlu diiringi pendidikan berkelanjutan kepada masyarakat mengenai pentingnya menjaga privasi, hak-hak mereka atas data pribadi (termasuk hak akses, perbaikan, dan penghapusan), serta kesadaran akan risiko kebocoran dan penyalahgunaan data, agar pencegahan pelanggaran dapat berjalan lebih efektif.[324]

---

[323] Sidik dan Wiraguna, *loc.cit*.

[324] Ahmad Fachri Yamin et al., "Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi," *Meraja journal* 7, no. 2 (2024), hlm. 138-155.

Pancasila sebagai dasar negara menuntut agar pengelolaan data pribadi mencerminkan nilai-nilai luhur dalam setiap sila. Sila pertama, *Ketuhanan Yang Maha Esa*, mengajarkan penghormatan terhadap martabat manusia sehingga pengelolaan data pribadi harus berbasis nilai moral, dilakukan secara etis, hati-hati, dengan persetujuan eksplisit dan transparansi mengenai tujuan serta cara pemrosesan data. [325] Sila kedua, *Kemanusiaan yang Adil dan Beradab*, menegaskan hak setiap individu untuk mengontrol data pribadinya, termasuk hak untuk mengakses, mengubah, dan menghapus data, serta mewajibkan negara memberikan perlindungan efektif terhadap pelanggaran privasi melalui sanksi yang menimbulkan efek jera. [326] Sila ketiga, *Persatuan Indonesia*, menuntut keseimbangan antara kepentingan negara (misalnya demi keamanan nasional) dan hak privasi individu, sehingga pengumpulan dan penggunaan data pribadi hanya boleh untuk tujuan yang sah dan diawasi dengan ketat agar tidak disalahgunakan oleh lembaga negara maupun pihak lain yang memiliki akses terhadap data tersebut. Pengelolaan data pribadi juga harus mengedepankan transparansi, dimana individu harus mengetahui dengan jelas bagaimana data mereka akan digunakan dan diproses. [327]

Sila keempat, Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan, memberikan landasan normatif bahwa tata kelola perlindungan data pribadi yang bersifat spesifik harus diselenggarakan melalui proses yang akuntabel, partisipatif, dan berbasis alasan yang dapat diuji. Perumusan

---

[325] Ellen Diva Ibanez, "Etika Data : Pengumpulan Dan Pengolahan Bertanggung Jawab."
[326] Suari dan Sarjana, *loc.cit*.
[327] Naylawati Bahtiar, "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)* 2, no. 1 (2024), hlm. 85-100.

norma turunan UU PDP, pedoman teknis, serta standar kepatuhan sektoral selayaknya membuka ruang konsultasi publik yang bermakna, tidak sekadar formalitas prosedural. Mekanisme partisipasi tersebut perlu menjamin keterwakilan kelompok rentan, pelaku usaha, akademisi, dan masyarakat sipil, sehingga kebijakan yang lahir tidak bersifat elitis serta mampu menjawab risiko nyata di lapangan. [328] Prinsip musyawarah juga menuntut adanya akses informasi yang memadai mengenai rancangan kebijakan, analisis dampak, dan argumentasi pembatasan hak, agar masyarakat dapat menilai proporsionalitas serta urgensi pengolahan data yang diusulkan.

Sila kelima, Keadilan Sosial bagi Seluruh Rakyat Indonesia, memperluas makna perlindungan data pribadi yang bersifat spesifik dari sekadar kepatuhan administratif menuju pencegahan ketidakadilan struktural di ruang digital. Pengolahan data yang masif, termasuk pemrofilan, penilaian kredit, penentuan harga dinamis, dan seleksi otomatis berbasis algoritma, berpotensi menimbulkan diskriminasi terselubung terhadap kelompok tertentu. [329] Prinsip keadilan sosial menuntut regulasi yang memastikan adanya perlindungan khusus bagi subjek data yang memiliki keterbatasan literasi digital, kondisi ekonomi lemah, atau posisi tawar rendah terhadap korporasi platform. Hak atas penjelasan yang dapat dipahami, hak untuk menolak pemrosesan otomatis tertentu, serta hak atas pemulihan efektif harus dirumuskan secara operasional agar tidak berhenti sebagai

[328] Denindah Olivia, Sinta Dewi Rosadi, dan Rika Ratna Permata, "Perlindungan Data Pribadi Dalam Penyelenggaraan Aplikasi Surveilans Kesehatan Pedulilindungi Dan Covidsafe Di Indonesia Dan Australia," *Datin Law Jurnal* Vol. 1, no. 2 (2020), hlm. 1-15.

[329] Iwan Irawan, "Penerapan Etika Pancasila Dalam Pengembangan Kecerdasan Buatan Yang Bertanggung Jawab Di Indonesia," *Journal Bit-Tech* Vol. 7, no. 2 (2024), hlm. 263-271.

deklarasi. Orientasi keadilan juga mensyaratkan akses prosedural yang setara terhadap mekanisme pengaduan, bantuan hukum, dan penyelesaian sengketa.

Prinsip utama Pancasila adalah demokrasi yang menegaskan hak setiap individu untuk terlibat dalam pengambilan keputusan yang menyangkut kehidupannya, termasuk dalam perumusan kebijakan perlindungan data pribadi yang bersifat spesifik. Oleh karena itu, negara perlu menjamin adanya partisipasi publik dan transparansi dalam pengelolaan data, dengan memberikan informasi yang jelas tentang cara data pribadi dikumpulkan, diproses, dan digunakan, sehingga menumbuhkan kepercayaan masyarakat dan memastikan hak mereka terlindungi. Dalam kerangka keadilan sosial, negara juga wajib memastikan bahwa seluruh lapisan masyarakat memiliki akses dan kontrol yang setara terhadap data pribadinya, tanpa diskriminasi berdasarkan latar belakang sosial, ekonomi, maupun pendidikan.[330]

2. Eksistensi Dan Peran Undang-Undang Pelindungan Data Pribadi

Kepatuhan perlindungan data pribadi yang bersifat spesifik memerlukan penguatan prinsip akuntabilitas melalui instrumen hukum dan tata kelola internal yang terukur. Pengendali data perlu diwajibkan menyusun catatan kegiatan pemrosesan, menetapkan dasar pemrosesan yang sah, serta membangun kebijakan retensi dan pemusnahan data yang konsisten dengan prinsip minimalisasi. Kewajiban penilaian dampak perlindungan data untuk pemrosesan berisiko tinggi dapat diposisikan sebagai standar kehati-hatian, terutama pada penggunaan AI,

[330] Robby Nurtresna and Mabsuti Mabsuti, "Peran Hukum Dalam Mewujudkan Keadilan Sosial Di Masyarakat," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 4, no. 2 (2024), hlm. 1581-1596.

biometrik, dan pemantauan berbasis lokasi. [331] Penunjukan pejabat atau fungsi perlindungan data di organisasi menjadi relevan untuk memastikan kepatuhan berkelanjutan, bukan reaktif setelah insiden. Standar kontraktual dengan pemroses dan pihak ketiga perlu memuat pembatasan tujuan, larangan penggunaan ulang tanpa dasar hukum, kewajiban keamanan, serta audit kepatuhan. Rangkaian instrumen tersebut memperjelas pertanggungjawaban dan memudahkan pembuktian ketika terjadi sengketa atau pelanggaran.

Fragmentasi kebijakan sektoral seperti di perbankan, kesehatan, pendidikan, dan *e-commerce* menjadi persoalan serius karena menimbulkan standar perlindungan yang tidak konsisten dan sering kali tidak selaras dengan regulasi umum. Idealnya, seluruh sektor tunduk pada satu regulasi utama, yaitu UU PDP, yang kemudian diperkuat dengan peraturan teknis sektoral yang sejalan dengan prinsip-prinsip dasarnya. Penyusunan regulasi yang komprehensif dan lintas sektor, dengan memastikan harmonisasi antara aturan umum dan aturan sektoral, menjadi kunci untuk mencegah tumpang tindih, mengurangi kebingungan implementasi di lapangan, serta mewujudkan perlindungan data pribadi yang bersifat spesifik yang efektif dan efisien di semua sektor.[332]

Salah satu tantangan utama dalam penerapan kebijakan perlindungan data pribadi yang bersifat spesifik di Indonesia adalah fragmentasi kebijakan sektoral

[331] Tuulia Karjalainen, "All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm," *European Data Protection Law Review* Vol. 8, no. 1 (2022): hlm. 19-30.

[332] Fitri Novia Heriani, "Empat Kunci Implementasi UU PDP Bagi Pelaku Bisnis," *Hukumonline.Com*, last modified 2023, accessed May 9, 2025, https://www.hukumonline.com/berita/a/empat-kunci-implementasi-uu-pdp-bagi-pelaku-bisnis-lt63d05bd4d167c.

yang berbeda-beda. Beberapa sektor seperti perbankan, kesehatan, dan *e-commerce* memiliki regulasi yang tidak seragam, sehingga menimbulkan kebingungannya dalam implementasi pengelolaan data. Untuk menyelesaikan masalah ini, kebijakan perlindungan data pribadi yang bersifat spesifik perlu terintegrasi dengan baik. Beberapa langkah yang perlu dilakukan, antara lain:[333]

1. Penyusunan regulasi yang seragam di seluruh sektor untuk memastikan kebijakan perlindungan data pribadi yang bersifat spesifik diterapkan dengan cara yang konsisten.
2. Peningkatan koordinasi antar sektor untuk menjamin bahwa semua sektor menerapkan standar perlindungan data pribadi yang bersifat spesifik yang sama.
3. Penguatan peraturan teknis sektoral yang dapat menyesuaikan dengan kebutuhan dan karakteristik masing-masing sektor, namun tetap mengikuti regulasi utama yang sudah ditetapkan.
4. Peningkatan kapasitas pengawasan, untuk memastikan bahwa semua sektor mematuhi regulasi perlindungan data pribadi yang bersifat spesifik yang telah ditetapkan dan menghindari adanya penyalahgunaan data.

Edukasi terhadap perusahaan dan lembaga, untuk memastikan bahwa mereka memahami kewajiban dan tanggung jawab mereka dalam mengelola data pribadi sesuai dengan peraturan yang berlaku.

[333] Agus Wibowo and Sri Yulianingsih, *Hukum Teknologi Informasi* (Semarang: Yayasan Prima Agus Teknik, 2023). hlm. 150.

Lembaga pengawas memiliki peran yang sangat penting dalam memastikan bahwa regulasi perlindungan data pribadi yang bersifat spesifik dijalankan dengan baik dan efektif. Lembaga ini bertanggung jawab untuk memantau pelaksanaan kebijakan, menangani pengaduan, dan menindaklanjuti pelanggaran data pribadi.[334] Penting bagi lembaga pengawas untuk memiliki kewenangan yang cukup untuk melakukan audit terhadap perusahaan atau organisasi yang mengelola data pribadi, serta memberikan sanksi yang sesuai jika terjadi pelanggaran

Lembaga pengawas perlindungan data pribadi yang bersifat spesifik harus bekerja secara independen, objektif, dan adil, serta memiliki kapasitas dan kompetensi yang memadai untuk mengawasi penggunaan teknologi baru seperti *artificial intelligence* (*AI*), *blockchain*, dan *big data* dalam pengumpulan dan pemrosesan data pribadi. Pemerintah Indonesia memikul tanggung jawab besar untuk memastikan pelanggaran data pribadi ditangani secara serius melalui penegakan hukum yang konsisten, tegas, dan berkeadilan sosial, didukung oleh kerangka hukum yang jelas, aparatur penegak hukum yang terlatih, serta mekanisme pelaporan dan perlindungan hukum yang mudah diakses masyarakat. Di saat yang sama, regulasi perlindungan data pribadi yang bersifat spesifik harus dirancang secara antisipatif terhadap perkembangan teknologi, dengan pengaturan yang lebih spesifik terhadap penggunaan teknologi, misalnya AI untuk pemasaran

[334] Muhammad Fadel Adhyputra, Thoriq Ahmadi, and Mohammad Rifqi, "Analisis Komparatif Rancangan LPPDP Indonesia Dengan Otoritas Pelindungan Data Singapura Dalam Penegakan Hukum Pelanggaran Data Pribadi: The Notion Of Personal Data Protection By Indonesia's Lppdp: A Comparative Study With The Singapore Personal Data Prot," *Jurnal Nomokrasi* 2, no. 2 (2024), hlm. 56-74.

atau penentuan harga, agar manfaat efisiensi tetap dapat diraih tanpa mengorbankan hak privasi dan perlindungan data pribadi individu.[335]

Kementerian Komunikasi dan Informatika (Kominfo) memegang peranan penting dalam pengawasan dan implementasi regulasi perlindungan data pribadi yang bersifat spesifik di Indonesia. Sebagai lembaga yang bertanggung jawab dalam pengelolaan informasi dan komunikasi, Kominfo harus memastikan bahwa kebijakan dan peraturan yang ada sesuai dengan perkembangan teknologi dan kebutuhan masyarakat. Kominfo juga perlu memperkuat kerjasama dengan sektor swasta dalam memastikan bahwa pelaksanaan regulasi perlindungan data pribadi yang bersifat spesifik berjalan sesuai dengan yang diharapkan.[336] Selain itu, Kominfo juga harus memastikan bahwa ada sistem pelaporan yang efisien bagi masyarakat jika terjadi pelanggaran data pribadi. Kemampuan Kominfo untuk mengawasi pelaksanaan kebijakan dan memberikan penegakan hukum yang tegas terhadap pelanggaran yang terjadi akan sangat membantu dalam mewujudkan sistem pengelolaan data pribadi yang aman dan dapat diandalkan.

Indonesia telah memiliki UU PDP, tetapi tantangan utama terletak pada penegakan hukum yang belum optimal akibat keterbatasan pemahaman, kapasitas, dan sumber daya di berbagai sektor, sehingga diperlukan pendampingan, pelatihan, penguatan struktur pengawasan, serta sosialisasi regulasi kepada masyarakat agar pelanggaran dapat dilaporkan dan ditindak secara efektif. Perkembangan pesat *e-*

---

[335] Rayyan Jamal et al., "Penggunaan Teknologi Informasi Dalam Mengoptimalisasi Supply Chain Management," *Jurnal Inovasi Global* 2, no. 7 (2024), hlm. 737-750.

[336] Fadil Isam Yusuf Endiputra, Adrian Pratama Nasution, and Akbar Dwi Febrian, "Blockchain: Inovasi Pembaruan Dalam Sektor Pengamanan E-Government Dalam Meningkatkan Sistem Akuntabilitas Pemerintahan Di Indonesia," *Journal of Legal Reform* 1, no. 1 (2025), hlm. 1-14.

commerce membuat pengumpulan dan pemrosesan data pribadi kian masif untuk keperluan pemasaran dan peningkatan pengalaman pengguna, yang berpotensi melanggar hak privasi bila tidak dikendalikan dengan baik. Pelaku *e-commerce* harus menjamin bahwa pengelolaan data dilakukan secara sah, transparan, dan aman, sementara regulasi di sektor ini perlu diperbarui secara berkala agar selaras dengan perkembangan teknologi dan tetap memastikan hak konsumen untuk mengakses serta menghapus data pribadi mereka.[337]

Tantangan penting dalam implementasi perlindungan data pribadi yang bersifat spesifik di Indonesia adalah fragmentasi kebijakan antarsektor dan daerah, karena setiap sektor seperti kesehatan, perbankan, pendidikan, dan *e-commerce* sering memiliki aturan pengelolaan data yang berbeda sehingga menimbulkan kebingungan dalam kepatuhan. UU PDP perlu ditegaskan sebagai regulasi payung yang menjadi kerangka dasar bagi seluruh sektor, yang kemudian diperinci melalui aturan teknis sektoral yang tetap selaras, agar standar perlindungan data menjadi lebih seragam, efektif, dan konsisten. Isu lain yang krusial adalah menjaga keseimbangan antara keamanan dan akses terhadap data pribadi, dimana pengendali data wajib melindungi informasi dari ancaman siber dan penyalahgunaan, sementara individu tetap dijamin haknya untuk mengakses, mengelola, memperbaiki, dan menghapus data mereka. Regulasi perlindungan data karena itu harus sekaligus menjamin penghormatan hak privasi dan menyediakan mekanisme

[337] Rachel Milafebina, Idham Putra Lesmana, and Moody Rizqy Syailendra, "Perlindungan Data Pribadi Terhadap Kebocoran Data Pelanggan E-Commerence Di Indonesia," *Jurnal Tana Mana* 4, no. 1 (2023), hlm. 157-169.

yang jelas serta mudah diakses agar subjek data dapat menggunakan hak-haknya tanpa mengurangi kewajiban pengelola data untuk menjaga keamanan informasi.[338]

Pemerintah Indonesia berperan sentral dalam merumuskan dan menerapkan kebijakan pengelolaan data pribadi melalui regulasi yang mampu melindungi individu sekaligus mendukung perkembangan ekonomi digital, antara lain dengan menyempurnakan dan memperbarui UU PDP secara berkala agar selaras dengan dinamika teknologi dan kebutuhan masyarakat. Tanggung jawab ini mencakup penguatan kerja sama dengan sektor swasta melalui pelatihan mengenai kewajiban perlindungan data, pengawasan ketat untuk mencegah kebocoran dan penyalahgunaan, serta sosialisasi hak-hak masyarakat terkait data pribadi dan cara melindunginya di ruang digital.[339] Selain itu, kerja sama internasional dalam hal pengawasan dan penegakan hukum sangat penting untuk memastikan bahwa pelanggaran data pribadi yang melibatkan negara lain dapat segera ditindaklanjuti.

3. Kepastian Hukum dalam Regulasi Data Pribadi di Indonesia

Sektor kesehatan memiliki peran penting dalam pengelolaan data pribadi, mengingat data medis merupakan jenis data yang sangat sensitif. Regulasi perlindungan data pribadi yang bersifat spesifik di sektor ini harus dirancang dengan hati-hati agar bisa memenuhi kebutuhan untuk melindungi data pribadi

[338] Ajisatria Suleiman, Pingkan Audrine, and Thomas Dewaranu, *Pengaturan Bersama Dalam Perlindungan Data Pribadi: Potensi Peran Asosiasi Industri Sebagai Organisasi Regulator Mandiri* (Center for Indonesian Policy Studies, 2022).

[339] Ayiliani dan Farida, *loc.cit*.

pasien sekaligus memungkinkan inovasi dalam penyediaan layanan kesehatan.[340] Di sektor ini, beberapa hal yang perlu diperhatikan adalah:

1. Kerahasiaan data medis, yang harus dijaga dengan ketat agar data pasien tidak disalahgunakan oleh pihak yang tidak berkepentingan.
2. Hak akses pasien terhadap data medis mereka, yang memungkinkan mereka untuk melihat dan mengontrol data medis yang dimiliki oleh rumah sakit atau penyedia layanan kesehatan.
3. Penggunaan teknologi dalam penyimpanan data medis, yang harus memenuhi standar keamanan tinggi, termasuk enkripsi data dan autentikasi yang kuat.
4. Koordinasi antara lembaga kesehatan dan pemerintah untuk memastikan bahwa setiap kebijakan terkait perlindungan data medis diterapkan dengan baik di seluruh fasilitas kesehatan.

Dalam sektor kesehatan, kepastian hukum harus diwujudkan melalui pengaturan yang ketat mengenai kerahasiaan, akses, pemrosesan, dan penggunaan lanjutan terhadap data medis pasien. Data kesehatan memiliki karakteristik yang sangat sensitif karena berkaitan langsung dengan kondisi fisik, riwayat penyakit, tindakan medis, hasil laboratorium, hingga prognosis kesehatan seseorang. Apabila data semacam ini diproses tanpa dasar hukum yang jelas atau dibuka kepada pihak yang tidak berwenang, dampaknya tidak hanya berupa pelanggaran privasi, tetapi juga berpotensi menimbulkan diskriminasi sosial, penolakan asuransi, stigma, bahkan kerugian psikologis bagi pasien. Oleh karena itu, kepastian hukum dalam

[340] Susy Ariyanie Yusuf, Christine Herlina, and Liston Sibarani, "Aspek Legal Dan Etika Penggunaan Data Pasien Dalam Teknologi Big Data Dan Kecerdasan Buatan Di Sektor Kesehatan," *Proceeding Masyarakat Hukum Kesehatan Indonesia* 1, no. 1 (2024), hlm. 381-393.

sektor kesehatan harus menegaskan bahwa setiap pemrosesan data medis hanya dapat dilakukan untuk tujuan yang sah, proporsional, dan terbatas, misalnya untuk diagnosis, pelayanan kesehatan, administrasi rumah sakit, atau penelitian medis yang telah memenuhi persyaratan etik dan hukum. Dalam kerangka ini, regulasi juga harus menjamin hak pasien untuk mengetahui data apa saja yang dikumpulkan, hak untuk mengakses rekam medisnya, hak untuk mengoreksi data yang tidak akurat, serta hak untuk memperoleh penjelasan jika datanya digunakan untuk kepentingan lain di luar pelayanan kesehatan langsung. Selain itu, kepastian hukum juga memerlukan kewajiban bagi penyedia layanan kesehatan untuk menerapkan sistem keamanan yang dapat dipertanggungjawabkan, seperti enkripsi, autentikasi berlapis, pembatasan hak akses internal, dan pencatatan jejak akses (access log), agar setiap penggunaan data dapat diaudit secara jelas.

Kepastian hukum pada sektor kesehatan digital juga harus menjawab persoalan baru yang muncul seiring berkembangnya telemedicine, rekam medis elektronik, aplikasi kesehatan, dan integrasi data antarpenyedia layanan. Dalam ekosistem digital, data pasien semakin mudah dipertukarkan lintas platform, rumah sakit, laboratorium, perusahaan asuransi, bahkan pihak ketiga penyedia teknologi. Kondisi ini menimbulkan kebutuhan akan kepastian prosedural yang lebih kuat, terutama mengenai persetujuan pasien, standar interoperabilitas, serta batas penggunaan data oleh mitra teknologi. Regulasi yang baik harus memastikan bahwa persetujuan pasien tidak cukup hanya formal, tetapi harus diberikan secara sadar, spesifik, dan didasarkan pada informasi yang memadai. Dengan demikian, pasien benar-benar memahami apakah datanya hanya digunakan untuk kepentingan

pengobatan, atau juga untuk analisis layanan, penelitian, maupun pengembangan produk kesehatan digital. Di samping itu, kepastian hukum juga memerlukan mekanisme yang jelas mengenai tanggung jawab apabila terjadi kebocoran data kesehatan, termasuk kewajiban notifikasi kepada pasien, tindakan mitigasi, dan bentuk pertanggungjawaban hukum dari pengendali maupun pemroses data. Dengan pengaturan yang demikian, sektor kesehatan tidak hanya menjamin perlindungan privasi pasien, tetapi juga menciptakan kepercayaan terhadap transformasi layanan kesehatan digital.

Kepastian hukum dalam regulasi data pribadi di Indonesia pada dasarnya tidak hanya menuntut adanya aturan yang tertulis, tetapi juga menuntut adanya kejelasan norma, konsistensi penerapan, dan jaminan perlindungan yang dapat dirasakan secara nyata oleh subjek data. Dalam konteks data pribadi yang bersifat spesifik, kepastian hukum menjadi semakin penting karena data yang dikelola tidak sekadar berkaitan dengan identitas umum seseorang, melainkan menyangkut informasi yang sangat sensitif, seperti kondisi kesehatan, data biometrik, informasi keuangan, dan data yang diproses oleh institusi publik. Oleh karena itu, regulasi perlindungan data pribadi yang bersifat spesifik harus mampu memberikan batasan yang tegas mengenai siapa yang berwenang memproses data, untuk tujuan apa data digunakan, berapa lama data dapat disimpan, dan bagaimana tanggung jawab hukum dibebankan ketika terjadi pelanggaran. Tanpa kejelasan mengenai hal-hal tersebut, pengelolaan data pribadi akan rentan menimbulkan ketidakpastian bagi masyarakat, sekaligus memperlemah posisi hukum subjek data dalam mempertahankan hak-haknya.

Pelindungan data pribadi dalam penelitian medis, yang memungkinkan penggunaan data medis untuk penelitian tanpa melanggar privasi pasien. Sektor perbankan dan keuangan merupakan sektor yang sangat sensitif terkait dengan pengelolaan data pribadi, mengingat data yang dikelola mencakup informasi keuangan dan identitas pribadi pelanggan.[341] Kehadiran kebijakan perlindungan data pribadi yang bersifat spesifik, diharapkan sektor perbankan dapat meningkatkan transparansi mengenai bagaimana data pelanggan digunakan dan memastikan bahwa pelanggan selalu diberi kontrol penuh atas data mereka. Selain itu, sektor perbankan juga perlu mengimplementasikan teknologi enkripsi dan autentikasi yang lebih kuat untuk melindungi data transaksi dan identitas pelanggan dari potensi ancaman peretasan.[342] Oleh karena itu, pengelolaan data di sektor ini harus dilakukan dengan sangat hati-hati dan aman. Penggunaan data pribadi dalam sektor perbankan harus dipatuhi dengan standar yang tinggi untuk melindungi privasi dan keamanan pelanggan. Pemerintah juga harus mengawasi sektor ini secara ketat dengan melakukan audit berkala terhadap pengelolaan data pribadi untuk memastikan bahwa tidak ada kebocoran atau penyalahgunaan data yang merugikan nasabah.

Regulasi perlindungan data pribadi yang bersifat spesifik harus memberikan kejelasan mengenai penggunaan data pribadi oleh pemerintah. Data pribadi yang dikumpulkan oleh pemerintah sering kali digunakan untuk kepentingan yang lebih

---

[341] Catherine Wijaya et al., "Perlindungan Data Pribadi Konsumen Dalam Layanan Keuangan Digital: Tinjauan Dari UU PDP," *Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara* 3, no. 2 (2025), hlm. 30-42.

[342] Dewi Fatmala Putri, Widya Ratna Sari, and Faricha Lita Nabbila, "Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking," *Jurnal Ilmiah Ekonomi Dan Manajemen* 1, no. 4 (2023), hlm. 173-181.

besar, seperti untuk perencanaan pembangunan atau analisis statistik. Meskipun demikian, privasi individu harus tetap dijaga, dan penggunaan data pribadi oleh pemerintah harus sesuai dengan prinsip keadilan dan transparansi.[343]

Pemerintah perlu menetapkan regulasi yang jelas tentang batasan penggunaan data pribadi, serta memastikan bahwa data yang dikumpulkan tidak disalahgunakan. Hal ini termasuk memastikan bahwa data pribadi yang digunakan untuk keperluan administrasi publik tidak jatuh ke tangan pihak ketiga yang tidak berwenang. Pemerintah juga harus memberikan transparansi mengenai bagaimana data pribadi digunakan, serta memberikan hak kepada individu untuk mengakses data mereka dan mengoreksi informasi yang tidak akurat.[344]

Sektor publik memegang peran krusial dalam pengelolaan data pribadi, karena lembaga pemerintahan mengumpulkan data sensitif seperti identitas, catatan pajak, dan informasi kesehatan yang harus digunakan hanya untuk tujuan yang sah dengan izin yang jelas dari pemilik data, dijaga kerahasiaannya, dan dilindungi dari penyalahgunaan. Pada saat yang sama, pemerintah tetap perlu membuka akses terhadap data publik yang tidak sensitif, seperti data statistik dan informasi umum, dengan tetap menjunjung prinsip transparansi dan pembatasan akses terhadap data yang bersifat pribadi atau sensitif. Seiring pesatnya perkembangan teknologi dan dinamika dunia digital, regulasi perlindungan data pribadi yang bersifat spesifik di

[343] Beni Kharisma Arrasuli and Khairul Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *UNES Journal of Swara Justisia* 7, no. 2 (2023), hlm. 369-392.

[344] Florianus Yudhi Priyo Amboro and Viona Puspita, "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)," in *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, vol. 1, 2021, hlm. 415-427.

sektor publik harus secara berkala diperbarui agar tetap relevan, mampu mengantisipasi risiko baru, dan efektif dalam melindungi hak privasi masyarakat.[345]

Dalam sektor publik dan pemerintahan, kepastian hukum menuntut adanya kejelasan yang lebih ketat karena negara memiliki akses yang sangat luas terhadap data pribadi warga negara. Pemerintah dan lembaga publik menghimpun berbagai data sensitif, seperti identitas kependudukan, catatan pajak, data kesehatan, informasi bantuan sosial, hingga data administrasi layanan publik. Luasnya cakupan data tersebut membuat negara berada pada posisi yang sangat kuat, sehingga tanpa pembatasan hukum yang jelas, terdapat risiko besar terjadinya penyalahgunaan, pengawasan berlebihan, atau penggunaan data di luar tujuan awal pengumpulannya. Oleh karena itu, regulasi harus menegaskan bahwa setiap pengumpulan dan pemrosesan data pribadi oleh pemerintah hanya boleh dilakukan atas dasar kewenangan hukum yang jelas, untuk tujuan yang sah, dan dengan memperhatikan prinsip pembatasan tujuan, minimalisasi data, akurasi, keamanan, serta akuntabilitas.

Kepastian hukum juga menuntut agar warga negara diberi hak untuk mengetahui data apa yang disimpan oleh pemerintah, bagaimana data itu digunakan, serta kepada siapa data tersebut dibagikan. Dalam konteks ini, prinsip transparansi menjadi elemen sentral agar negara tidak menggunakan alasan pelayanan publik untuk memperluas pemrosesan data secara berlebihan tanpa kontrol hukum yang memadai.

---

[345] Budi Tri Wijayanto, "Regulasi Konflik Kepentingan Di Era Disrupsi: Tantangan Dan Urgensi Pembaharuan Di Indonesia," *Jurnal Globalisasi Hukum* 2, no. 1 (2025), hlm. 148-174.

Sistem pemerintahan digital, e-government, dan integrasi layanan publik memang dapat meningkatkan efisiensi, namun juga memperbesar kemungkinan pertukaran data antarinstansi secara luas. Karena itu, perlu ada aturan yang jelas mengenai interoperabilitas data, standar keamanan minimum, pembatasan akses antarinstansi, dan kewajiban pencatatan setiap pertukaran data yang terjadi. Negara tidak cukup hanya menjadi pengumpul dan pengelola data, tetapi juga harus menjadi penjamin utama bahwa data warga negara tidak jatuh ke tangan pihak yang tidak berwenang. Dalam perspektif ini, kepastian hukum bukan hanya bertujuan menciptakan tertib administrasi, melainkan juga menjaga kepercayaan publik terhadap negara. Ketika warga yakin bahwa data mereka dikelola secara sah, aman, dan transparan, maka legitimasi pemerintahan digital akan semakin kuat. Sebaliknya, jika negara gagal memberikan kepastian hukum, maka kebocoran atau penyalahgunaan data publik akan menimbulkan krisis kepercayaan yang serius terhadap institusi pemerintahan.

Sektor kesehatan merupakan bidang yang sangat sensitif dalam pengelolaan data pribadi, karena data medis bersifat sangat pribadi dan rentan disalahgunakan sehingga pengelolaannya harus mengikuti standar perlindungan data yang ketat, termasuk dalam penggunaan rekam medis elektronik yang hanya dapat diakses tenaga medis berwenang dengan dukungan sistem keamanan canggih serta jaminan hak pasien untuk mengakses dan mengoreksi data mereka. Sektor perbankan dan keuangan digital menyimpan data yang sama sensitifnya, seperti informasi rekening, transaksi, dan identitas, sehingga wajib mematuhi regulasi ketat serta menerapkan keamanan siber yang kuat melalui enkripsi dan autentikasi berlapis

untuk mencegah pencurian dan akses tidak sah. Nasabah perlu dijamin hak penuh atas data pribadi mereka, termasuk hak untuk mengakses, memperbaiki, dan menghapus informasi yang tidak relevan, sementara pemerintah bersama lembaga keuangan harus menetapkan standar keamanan yang seragam dan melakukan pengawasan ketat guna mencegah kebocoran maupun penyalahgunaan data.[346]

Regulasi perlindungan data pribadi yang bersifat spesifik di sektor kesehatan digital harus menjamin bahwa hanya penyedia layanan yang berwenang yang dapat mengakses data medis pasien, data tidak dibagikan kepada pihak ketiga tanpa persetujuan eksplisit, serta didukung sistem keamanan yang kuat agar kebocoran dan penyalahgunaan dapat dicegah, sekaligus memberi hak penuh kepada pasien untuk melihat, memperbaiki, atau menghapus data mereka. Pemerintah sebagai pengelola infrastruktur digital, termasuk portal layanan publik dan sistem *e-government* yang menghimpun data sangat sensitif seperti identitas, status perpajakan, dan informasi keuangan, wajib menempatkan keamanan siber sebagai prioritas utama agar seluruh data pribadi warga negara tetap terlindungi secara optimal.[347]

Regulasi perlindungan data pribadi yang bersifat spesifik di sektor layanan keuangan *digital* harus memastikan penyedia jasa mematuhi standar keamanan yang ketat, membatasi penggunaan data hanya untuk tujuan yang sah, serta memberikan hak kontrol penuh kepada konsumen, termasuk akses dan

---

[346] Veronika Christiana, Didik Suahriyanto, and Ismail Ismail, "Perlindungan Data Nasabah Perbankan Dengan Perjanjian Pembukaan Rekening," *Mutiara: Multidiciplinary Scientifict Journal* 3, no. 1 (2025), hlm. 1-16.

[347] Anastasia Vienessa Putri et al., "Tarakan Smart City: Meningkatkan Transparansi Dan Akuntabilitas Layanan Publik Melalui E-Government," *Tumoutou Social Science Journal* 2, no. 1 (2025), hlm. 61-73.

penghapusan data yang disimpan perusahaan, sehingga perluasan akses keuangan tetap sejalan dengan perlindungan privasi. Pemerintah memikul tanggung jawab untuk menjamin pelaksanaan hukum melalui penguatan lembaga pengawas, penerapan sanksi tegas yang menimbulkan efek jera, dan penyediaan pendidikan serta pelatihan bagi aparat penegak hukum agar mampu menangani pelanggaran data pribadi secara profesional dan konsisten, sehingga masyarakat merasa hak privasinya benar-benar terlindungi.[348]

Dalam sektor perbankan dan keuangan digital, kepastian hukum harus diletakkan pada pengakuan bahwa data keuangan merupakan salah satu bentuk data pribadi yang bersifat spesifik karena sangat erat kaitannya dengan keamanan ekonomi, identitas, dan stabilitas kehidupan seseorang. Informasi rekening, riwayat transaksi, pola konsumsi, data kartu pembayaran, profil kredit, hingga data autentikasi nasabah merupakan data yang apabila disalahgunakan dapat mengakibatkan kerugian langsung dalam bentuk pencurian dana, penipuan digital, pembobolan akun, hingga perampasan identitas finansial. Oleh sebab itu, regulasi dalam sektor ini harus memastikan adanya standar hukum yang lebih tegas mengenai prinsip kehati-hatian, keamanan sistem, dan tanggung jawab lembaga jasa keuangan dalam mengelola data nasabah.

Kepastian hukum bukan hanya berarti bahwa bank atau penyedia jasa keuangan memiliki kewajiban menjaga rahasia bank, tetapi juga berarti bahwa nasabah memiliki posisi hukum yang jelas untuk mengetahui bagaimana data mereka dikumpulkan, digunakan, dibagikan, dan disimpan. Regulasi harus

[348] Azmi et al., *loc.cit*.

menegaskan bahwa penggunaan data keuangan hanya boleh dilakukan untuk kepentingan yang sah, seperti penyediaan layanan, manajemen risiko, pencegahan fraud, atau pemenuhan kewajiban hukum, dan tidak dapat diperluas secara sepihak untuk kepentingan komersial lain tanpa dasar persetujuan yang jelas. Selain itu, standar pengamanan seperti enkripsi, autentikasi multi-faktor, deteksi anomali transaksi, serta audit keamanan berkala harus ditempatkan sebagai kewajiban hukum, bukan sekadar pilihan kebijakan internal perusahaan.

Kepastian hukum di sektor keuangan juga harus mampu menjawab tantangan yang muncul dari digital banking, fintech, dompet digital, pinjaman online, serta pemanfaatan kecerdasan buatan dalam analisis kredit dan profil risiko nasabah. Dalam praktiknya, semakin banyak keputusan finansial yang dibuat melalui proses otomatis, termasuk penilaian kelayakan kredit, pembatasan akses layanan, hingga deteksi transaksi mencurigakan. Kondisi ini menuntut adanya kepastian hukum mengenai sejauh mana data nasabah boleh diproses secara otomatis dan bagaimana hak nasabah dijamin ketika keputusan tersebut berdampak signifikan terhadap dirinya. Regulasi yang memberi kepastian harus menjamin hak untuk memperoleh informasi yang jelas mengenai logika dasar pemrosesan, hak untuk mengajukan keberatan, serta hak untuk meminta peninjauan ulang secara manusiawi apabila keputusan otomatis dianggap merugikan. Di samping itu, pengawasan negara terhadap sektor keuangan tidak cukup hanya berorientasi pada stabilitas sistem, tetapi juga harus menempatkan perlindungan data nasabah sebagai bagian dari perlindungan hukum konsumen. Dengan demikian, kepastian hukum dalam sektor keuangan digital harus dipahami sebagai jaminan bahwa modernisasi layanan

keuangan tidak boleh mengorbankan privasi, keamanan, dan kendali hukum nasabah atas data pribadinya.

Sektor perbankan memproses data pribadi spesifik yang rentan, seperti identitas dan riwayat transaksi, sehingga diwajibkan mematuhi standar keamanan tingkat tinggi. Regulasi perlindungan data harus mewajibkan perbankan menerapkan protokol teknis yang ketat, meliputi enkripsi data, autentikasi berlapis, serta notifikasi seketika atas transaksi mencurigakan. Pemenuhan hak nasabah untuk mengakses, mengoreksi, dan mengetahui transparansi pemrosesan datanya juga wajib dijamin sepenuhnya.[349] Sebagai langkah preventif terhadap kebocoran, pemanfaatan sistem pemantauan canggih menjadi sebuah keharusan. Implementasi pengawasan otomatis berbasis kecerdasan buatan (AI) sangat esensial untuk mendeteksi anomali akses ilegal dan memberikan peringatan dini atas ancaman siber. Melalui pendekatan ini, lembaga keuangan dapat merespons insiden dengan lebih cepat, efisien, dan proaktif, guna memastikan data nasabah senantiasa terlindungi secara optimal di ruang digital.

Kepastian hukum dalam regulasi data pribadi di Indonesia harus dipahami sebagai upaya untuk membangun sistem perlindungan yang tidak parsial, melainkan terintegrasi lintas sektor. Sektor kesehatan, keuangan, dan sektor publik memang memiliki karakteristik tersendiri, tetapi semuanya memerlukan landasan umum yang sama, yaitu kejelasan norma, standar keamanan minimum, jaminan hak subjek data, pengawasan yang efektif, dan mekanisme pertanggungjawaban yang

[349] Muhammad Wildan, Daud Renata Candra Ramadhan, and Zulfa Rena Wijayanti, "Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan," *Media Hukum Indonesia (MHI)* 2, no. 4 (2024).

dapat dijalankan secara nyata. Kepastian hukum baru dapat dikatakan terwujud apabila subjek data tidak hanya diakui haknya dalam teks undang-undang, tetapi juga memiliki akses yang nyata untuk menggunakan hak tersebut, memperoleh perlindungan saat terjadi pelanggaran, dan mendapatkan pemulihan ketika hak privasinya dirugikan. Oleh karena itu, penguatan regulasi di Indonesia harus diarahkan pada harmonisasi antara aturan umum dan aturan sektoral, sehingga tidak terjadi fragmentasi standar perlindungan data. Dengan kerangka hukum yang jelas, konsisten, dan berkeadilan, pengelolaan data pribadi yang bersifat spesifik di era digital akan lebih mampu menjamin keamanan, kepastian, dan perlindungan yang seimbang bagi seluruh warga negara.

4. Kepastian Hukum Berbasis Nilai-Nilai Pancasila

Pengelolaan data pribadi tidak hanya harus mengikuti regulasi yang ada, tetapi juga harus berlandaskan pada etika yang kuat. Sistem yang mengelola data pribadi harus mengutamakan keadilan, keamanan, dan privasi individu. Perusahaan dan organisasi yang mengelola data pribadi harus berkomitmen untuk menjaga etika dalam pengumpulan dan penggunaan data. Ini mencakup penggunaan data yang adil, tidak mengekspolitasi kelemahan individu, dan selalu mendapatkan persetujuan eksplisit dari pemilik data sebelum data mereka digunakan untuk tujuan lain.[350]

Etika dalam pengelolaan data pribadi menuntut transparansi atas setiap proses pengumpulan dan pemanfaatan data, sehingga individu berhak mengetahui apa

[350] Sudanto Sudanto, "Transformasi Digital Dan Automasi Proses Bisnis Syariah Melalui Artificial Intelligence," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (2025), hlm. 14-23.

yang terjadi dengan data mereka, yang kemudian harus dituangkan dalam kode etik dan pedoman etika yang jelas baik oleh pemerintah maupun tiap sektor pengelola data. Sejalan dengan itu, prinsip *privacy by design* mengharuskan perlindungan dan privasi data dipertimbangkan sejak tahap awal perancangan sistem dan produk, misalnya dengan membatasi akses hanya pada pihak yang berwenang, memastikan penggunaan data sesuai tujuan yang disetujui pemilik data, serta menerapkan penyimpanan yang aman melalui enkripsi dan pengaturan hak akses yang ketat. Integrasi prinsip ini sejak awal tidak hanya meminimalkan risiko pelanggaran data dan kerugian bagi konsumen, tetapi juga menjaga kepercayaan publik dan reputasi perusahaan.[351]

Pelindungan data pribadi yang bersifat spesifik yang efektif memerlukan kolaborasi yang erat antara pemerintah, sektor swasta, dan masyarakat. Setiap pihak memiliki peran yang sangat penting dalam memastikan bahwa data pribadi dikelola dengan aman dan sesuai dengan regulasi yang berlaku. Pemerintah harus menyediakan regulasi yang jelas dan pengawasan yang efektif, sementara sektor swasta harus memastikan bahwa kebijakan perlindungan data pribadi yang bersifat spesifik diterapkan dengan baik di perusahaan mereka. Masyarakat, di sisi lain, harus sadar akan hak-hak mereka dan berpartisipasi aktif dalam pengawasan terhadap penggunaan data pribadi.[352]

---

[351] Ni Putu Ega Maha Wiryanthi, "Peran Hukum Dalam Meningkatkan Etika Bisnis Di Perusahaan Media Online," *Kertha Wicaksana* 19, no. 1 (2025), hlm. 18-28.

[352] Kevin Bramantya Fristanto and Sultoni Fikri, "Perlindungan Hukum Terhadap Penggunaan Data Pribadi Oleh Partai Politik Tanpa Izin," *Journal Evidence Of Law* 4, no. 1 (2025), hlm. 266-271.

Lembaga pendidikan berperan strategis dalam membekali generasi muda dengan pemahaman tentang pentingnya perlindungan data pribadi yang bersifat spesifik dan hak privasi di era digital. Sejalan dengan itu, Kementerian Hukum dan HAM memegang peran kunci dalam merumuskan dan mengoordinasikan kebijakan hukum perlindungan data pribadi yang bersifat spesifik serta memastikan implementasinya berjalan efektif dan konsisten di seluruh sektor. Kementerian ini juga bertanggung jawab menegakkan hukum terhadap pelanggaran data pribadi dengan sanksi yang tepat, sekaligus memastikan bahwa regulasi tidak hanya mengatur aspek teknis, tetapi juga memuat dimensi etika dan moral, sehingga perlindungan data pribadi yang bersifat spesifik benar-benar menghadirkan rasa keadilan sosial bagi setiap individu.[353]

Pemerintah Indonesia berperan sentral dalam merumuskan dan menerapkan kebijakan pengelolaan data pribadi melalui regulasi yang mampu melindungi individu sekaligus mendukung perkembangan ekonomi digital, antara lain dengan menyempurnakan dan memperbarui UU PDP secara berkala agar selaras dengan dinamika teknologi dan kebutuhan masyarakat. Tanggung jawab ini mencakup penguatan kerja sama dengan sektor swasta melalui pelatihan mengenai kewajiban perlindungan data, pengawasan ketat untuk mencegah kebocoran dan penyalahgunaan, serta sosialisasi hak-hak masyarakat terkait data pribadi dan cara melindunginya di ruang digital.[354] Selain itu, kerja sama internasional dalam hal

[353] Juliantio Dwi Pramana et al., "Law Enforcement Of Criminal Acts Of Dissemination Of Population Document Data By Dinas Dukcapil Kab. Mukomuko (Study Of Mukomuko District Police Legal Area," *Jurnal Hukum Sehasen* 10, no. 1 (2024), hlm. 329-338.

[354] Ayiliani dan Farida, *loc.cit*.

pengawasan dan penegakan hukum sangat penting untuk memastikan bahwa pelanggaran data pribadi yang melibatkan negara lain dapat segera ditindaklanjuti.

Kepastian hukum berbasis nilai-nilai Pancasila menuntut agar setiap pengaturan mengenai perlindungan data pribadi yang bersifat spesifik dirumuskan secara jelas, tegas, dan tidak menimbulkan multitafsir dalam pelaksanaannya. Dalam negara hukum, kepastian hukum merupakan jaminan bahwa hak dan kewajiban setiap pihak dapat diketahui dan dipahami secara pasti, baik oleh subjek data, pengendali data, pemroses data, maupun oleh negara sebagai regulator dan pengawas. Oleh karena itu, nilai-nilai Pancasila harus tercermin dalam pembentukan norma hukum yang mampu memberikan pedoman yang konsisten mengenai bagaimana data pribadi dikumpulkan, digunakan, disimpan, dipindahkan, dan dimusnahkan. Kepastian hukum yang demikian akan mencegah terjadinya penyalahgunaan kewenangan, mengurangi potensi pelanggaran hak privasi, serta memperkuat kepercayaan masyarakat terhadap sistem hukum dan tata kelola data di era digital.

Kepastian hukum tidak dapat dipisahkan dari perlindungan terhadap martabat manusia. Data pribadi yang bersifat spesifik melekat secara langsung pada identitas, kondisi, dan kehidupan pribadi seseorang, sehingga penyalahgunaannya dapat menimbulkan kerugian yang tidak hanya bersifat materiil, tetapi juga psikologis, sosial, dan moral.[355] Oleh sebab itu, kepastian hukum harus diwujudkan melalui norma yang menjamin bahwa setiap pemrosesan data dilakukan atas dasar yang sah,

[355] Nurmalasari Nurmalasari, "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum," *Syntax Idea* 3, no. 8 (2021): hlm. 1947-1966.

untuk tujuan yang jelas, dan dengan batasan yang proporsional. Kejelasan norma ini penting agar tidak ada pihak yang memanfaatkan kekaburan hukum untuk mengumpulkan atau menggunakan data pribadi secara sewenang-wenang. Dengan demikian, kepastian hukum yang berlandaskan Pancasila pada hakikatnya merupakan bentuk penghormatan negara terhadap harkat dan martabat warga negara.

Kepastian hukum berbasis Pancasila juga menghendaki adanya keseimbangan yang adil antara kepentingan negara, kepentingan pelaku usaha, dan kepentingan individu sebagai subjek data. Negara memang memiliki kepentingan untuk menggunakan data tertentu dalam rangka pelayanan publik, keamanan, dan pembangunan nasional, sedangkan pelaku usaha memerlukan data untuk menjalankan kegiatan ekonomi dan inovasi teknologi. Namun, seluruh kepentingan tersebut tidak boleh mengesampingkan hak privasi individu. Oleh karena itu, kepastian hukum diperlukan untuk menetapkan batas-batas yang tegas mengenai ruang lingkup penggunaan data pribadi, syarat persetujuan, jangka waktu penyimpanan, mekanisme akses, serta tanggung jawab ketika terjadi pelanggaran. Melalui pengaturan yang pasti dan berkeadilan, nilai Pancasila hadir sebagai dasar untuk mencegah dominasi salah satu kepentingan atas kepentingan lainnya.

Kepastian hukum yang berlandaskan nilai-nilai Pancasila harus diwujudkan melalui mekanisme pengawasan dan penegakan hukum yang efektif, transparan, dan dapat diakses oleh masyarakat. Kepastian hukum tidak akan tercapai apabila norma hanya berhenti pada tataran tertulis, tetapi tidak disertai dengan pelaksanaan

yang konsisten.[356] Dalam konteks ini, negara harus memastikan adanya lembaga yang berwenang untuk menerima pengaduan, melakukan pemeriksaan, menjatuhkan sanksi, serta memberikan pemulihan kepada korban pelanggaran data pribadi. Penegakan hukum yang konsisten merupakan bentuk nyata dari sila kelima Pancasila, karena memberikan jaminan bahwa setiap orang memperoleh perlindungan yang sama di hadapan hukum. Dengan adanya mekanisme tersebut, masyarakat tidak hanya mengetahui hak-haknya secara normatif, tetapi juga memiliki kepastian mengenai cara mempertahankan hak tersebut ketika dilanggar.

Nilai moral dan nilai hukum dalam Pancasila juga menegaskan bahwa kepastian hukum dalam perlindungan data pribadi tidak boleh hanya dipahami secara formal, melainkan harus mengandung dimensi etis dan keadilan substantif.[357] Artinya, hukum tidak cukup hanya jelas dalam rumusan, tetapi juga harus adil dalam penerapan dan bermanfaat bagi masyarakat. Dalam pengelolaan data pribadi yang bersifat spesifik, hal ini berarti bahwa setiap kebijakan dan tindakan pemrosesan data harus selalu mempertimbangkan kepatutan, itikad baik, perlindungan terhadap pihak yang lemah, serta dampaknya terhadap kehidupan individu. Dengan demikian, kepastian hukum berbasis Pancasila merupakan kepastian hukum yang tidak kaku dan legalistik semata, melainkan kepastian hukum yang hidup dalam kerangka moralitas, kemanusiaan, dan keadilan sosial.

---

[356] Ratih Mega Puspa Sari et al., *Kewarganegaraan Dan Pranata Hukum Di Indonesia* (Yogyakarta: Penerbit KBM Indonesia, 2026). hlm. 23.

[357] Agam Ibnu Asa and M Mukhtasar Syamsuddin, "Rekontruksi Makna Pancasila Dalam Konteks Sumber Tertib Hukum (Tinjauan Filsafat Hukum)," *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKN* 12, no. 1 (2025): hlm. 59-77.

Kepastian hukum berbasis nilai-nilai Pancasila dalam perlindungan data pribadi yang bersifat spesifik merupakan fondasi penting untuk membangun tata kelola data yang beradab, adil, dan terpercaya di era digital. Kepastian hukum tersebut harus mampu menjamin bahwa perkembangan teknologi tidak mengurangi perlindungan terhadap hak privasi warga negara, melainkan justru berjalan seiring dengan penguatan martabat manusia, keadilan sosial, dan tanggung jawab negara. Dengan demikian, perlindungan data pribadi yang bersifat spesifik tidak hanya menjadi persoalan teknis atau administratif, tetapi juga menjadi bagian dari perwujudan cita hukum Indonesia yang berlandaskan Pancasila.

C. Kebijakan Perlindungan Hukum Terhadap Data Pribadi Yang Bersifat Spesifik Akibat Perkembangan Teknologi Di Era Digital

UU PDP di Indonesia merupakan regulasi yang masih relatif baru dan sedang dalam tahap implementasi, dengan keunggulan berupa pendekatan yang adaptif dan kontekstual terhadap kondisi nasional yang beragam, serta pembentukan Komisi Pelindungan data pribadi yang bersifat spesifik (KPDP) sebagai lembaga pengawas. Tantangan utama regulasi ini meliputi lemahnya pengawasan pada praktik implementasi, rendahnya kesadaran masyarakat terhadap hak perlindungan data pribadi yang bersifat spesifik, dan tingkat sanksi yang belum keras, sehingga efek jeranya terhadap pelanggar masih terbatas.[358]

[358] Indonesia, "UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." https://www.dpr.go.id/dokjdih/document/uu/UU_2022_27.pdf

Tabel 3. 1. Perbandingan Undang-Undang Pelindungan data pribadi yang bersifat spesifik di Uni Eropa, Amerika Serikat, Singapura, dan Indonesia sebagai Rujukan Integrasi Keadilan Pancasila dalam Regulasi yang Bersifat Spesifik

Dimensi / Aspek	Singapura – *PDPA*	Indonesia – UU PDP	Rujukan Integrasi Keadilan Pancasila
Pendekatan umum regulasi	Regulasi nasional tunggal yang mengikat sektor publik dan privat dengan pengecualian tertentu.	Regulasi nasional yang bersifat umum, dilengkapi aturan sektoral (*lex specialis*).	Menunjukkan pentingnya satu kerangka umum nasional yang memberi kepastian hukum, tetapi tetap memberi ruang pengaturan khusus yang mencerminkan keadilan kontekstual Indonesia.
Orientasi nilai & hak asasi	Menyeimbangkan perlindungan individu dengan kebutuhan inovasi dan iklim usaha.	Menempatkan perlindungan data sebagai hak warga sekaligus mendukung kepentingan pembangunan nasional.	Dapat diintegrasikan dengan sila kedua dan kelima Pancasila: perlindungan martabat manusia (privasi) dan keadilan sosial, bukan hanya kepentingan pasar.
Hak subjek data	Hak pemberitahuan, akses, koreksi, dan penarikan persetujuan.	Hak akses, koreksi, penghapusan, keberatan, pembatasan pemrosesan, dan gugatan ganti rugi.	Menjadi dasar penguatan "hak kontrol" warga atas data sebagai pengejawantahan keadilan, kesetaraan, dan penghormatan martabat manusia dalam Pancasila.
Dasar pemrosesan & persetujuan	Menekankan persetujuan yang diinformasikan, kewajiban pemberitahuan, dan tujuan pemrosesan yang jelas.	Mengatur persetujuan, tujuan yang spesifik, pembatasan pemrosesan, dan kewajiban menjaga keakuratan data.	Dapat diarahkan agar persetujuan sejalan dengan etika Pancasila: jujur, transparan, tidak menipu, serta menjamin posisi tawar yang adil bagi subjek data.
Otoritas pengawas dan penegakan	*Personal Data Protection Commission* (*PDPC*) sebagai otoritas pusat dengan mandat jelas.	Komisi Pelindungan data pribadi yang bersifat spesifik (KPDP) dirancang sebagai lembaga pengawas nasional, masih dalam tahap penguatan kelembagaan.	Menjadi rujukan untuk membangun lembaga pengawas yang independen, akuntabel, dan berkeadilan sesuai sila keempat (musyawarah, representasi) dan sila kelima.
Sanksi dan efek jera	Denda administratif yang signifikan	Sanksi administratif, pidana, dan ganti kerugian, tetapi tingkat dan konsistensi penegakan masih berkembang.	Dapat diarahkan untuk menerapkan sanksi yang tegas namun proporsional, mencerminkan keadilan Pancasila: melindungi korban, mendorong pemulihan, dan memberi efek jera tanpa sewenang-wenang.
Kelemahan utama	Sanksi relatif lebih ringan, respons terhadap	Tantangan pada penegakan, kesadaran publik yang masih	Menjadi peringatan agar integrasi keadilan Pancasila tidak hanya kuat di norma

	perkembangan teknologi kadang tertinggal.	rendah, serta kesiapan lembaga dan pelaku usaha.	tertulis, tetapi juga realistis terhadap kapasitas nasional dan tidak menambah kesenjangan digital.
Relevansi sebagai rujukan bagi Indonesia	Contoh negara kawasan yang menyeimbangkan perlindungan dan kemudahan berbisnis.	Menjadi titik awal untuk mengembangkan Unsur-unsur khas Indonesia yang berlandaskan Pancasila.	Kombinasi unsur terbaik dari keempat Unsur-unsur dapat dipadukan menjadi desain regulasi spesifik yang adil, manusiawi, demokratis, dan berorientasi keadilan sosial sesuai nilai-nilai Pancasila.

Data dalam tabel di atas mengilustrasikan keragaman filosofis (*ratio legis*) yang melandasi rezim perlindungan data di berbagai negara, mulai dari pendekatan hak asasi yang ketat hingga orientasi pasar yang fleksibel. Indonesia, sebagaimana terlihat pada kolom rujukan integrasi, tidak sekadar mengadopsi struktur hukum asing secara mentah, tetapi melakukan harmonisasi dengan Sila Kedua dan Kelima Pancasila. Pendekatan ini menempatkan perlindungan privasi sebagai instrumen fundamental untuk menjaga martabat manusia sekaligus mewujudkan keadilan sosial bagi seluruh rakyat. Arah pengaturan spesifik di masa depan karenanya harus mencerminkan keseimbangan proporsional antara hak kontrol individu atas data pribadi dan kepentingan kolektif nasional yang dikelola secara jujur, transparan, dan akuntabel.

Kurangnya regulasi federal yang komprehensif membuat perlindungan data pribadi di seluruh negeri menjadi sangat bervariasi dan sering kali tidak memadai untuk menghadapi ancaman di era digital yang terus berkembang. [359] Singapura melalui *Personal Data Protection Act* (PDPA) memiliki pendekatan yang lebih

[359] State of California Department of Justice, "California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General," *Oag.ca.Gov*, accessed May 9, 2025, https://www.oag.ca.gov/privacy/ccpa. https://www.oag.ca.gov/privacy/ccpa.

terfokus dan komprehensif dalam perlindungan data pribadi dengan tujuan untuk menyeimbangkan antara perlindungan data pribadi dan kemajuan teknologi. Kelebihannya adalah fokus pada transparansi dan penegakan yang tegas melalui mekanisme pengawasan oleh *Personal Data Protection Commission* (PDPC). [360]

Perbandingan antar negara menunjukkan bahwa meskipun negara-negara tersebut memiliki sistem perlindungan data pribadi yang kuat, masing-masing memiliki kelebihan dan kekurangannya. Uni Eropa unggul dalam perlindungan hak individu dengan regulasi yang ketat, namun sering menghadapi tantangan dalam hal implementasi yang kompleks. Amerika Serikat, dengan pendekatan sektoralnya, memberikan fleksibilitas namun memiliki kekurangan dalam ketidakmerataan regulasi. Singapura, dengan pendekatan yang lebih terfokus, memberikan standar yang jelas, tetapi masih kurang dalam hal sanksi yang lebih keras. Indonesia, meskipun memiliki regulasi yang baru dan adaptif, masih menghadapi tantangan besar dalam hal pengawasan, kesadaran masyarakat, dan implementasi yang efektif. Keterbukaan antar sektor dan kerjasama internasional dapat membantu memperkuat perlindungan data pribadi yang bersifat spesifik di seluruh dunia, termasuk di Indonesia.

Integrasi nilai-nilai Pancasila ke dalam regulasi perlindungan data pribadi yang bersifat spesifik merupakan manifestasi konkret dari Teori Keadilan Sosial (*Grand Theory*), dimana sila Kemanusiaan yang Adil dan Beradab serta Keadilan Sosial menjadi landasan filosofis agar distribusi hak dan kewajiban antara subjek

[360] Singapore Statutes Online, "Personal Data Protection Act 2012 - Singapore Statutes Online." https://sso.agc.gov.sg/Act/PDPA2012.

data dan pengendali data berjalan seimbang. Dalam tataran Teori Perlindungan Hukum (*Middle Range Theory*), integrasi ini memperkuat substansi perlindungan hukum bagi rakyat dengan memastikan bahwa adopsi standar global tidak sekadar menjadi transplantasi hukum, melainkan disesuaikan dengan kebutuhan perlindungan hak warga negara Indonesia yang spesifik. Proses integrasi ini sekaligus mengukuhkan Teori Hukum Pembangunan (*Applied Theory*), dimana pembangunan hukum nasional harus berakar pada nilai budaya bangsa (Pancasila) untuk menciptakan sistem hukum yang responsif dan mampu mengarahkan pembangunan ekosistem digital Indonesia ke arah yang berkeadaban dan berkeadilan.

Nilai-nilai keadilan yang terkandung dalam Pancasila juga memiliki koherensi dengan nilai-nilai universal yang bersumber dari data kewahyuan dalam ajaran Islam, khususnya terkait penghormatan terhadap martabat manusia dan perlindungan terhadap privasi individu. Al-Qur'an menegaskan larangan melakukan pelanggaran terhadap ruang privat seseorang sebagaimana tercantum dalam Surah Al-Hujurat ayat 12 yang melarang perbuatan *tajassus* atau mencari-cari informasi pribadi orang lain tanpa hak. Larangan tersebut mencerminkan prinsip dasar penghormatan terhadap kehormatan dan privasi manusia yang dalam konteks modern dapat dimaknai sebagai kewajiban untuk menjaga kerahasiaan data pribadi. Dalam perspektif ini, perlindungan terhadap data pribadi yang bersifat spesifik tidak hanya dipahami sebagai kewajiban hukum administratif semata, tetapi juga sebagai kewajiban moral yang berakar pada nilai penghormatan terhadap martabat manusia sebagai makhluk yang memiliki hak atas privasinya.

Prinsip persetujuan (*consent*) yang menjadi salah satu asas penting dalam regulasi perlindungan data pribadi yang bersifat spesifik modern juga memiliki landasan normatif dalam ajaran Islam. Surah An-Nur ayat 27 menegaskan kewajiban meminta izin sebelum memasuki ruang privat orang lain, yang secara substantif mencerminkan prinsip bahwa setiap individu memiliki hak untuk mengendalikan akses terhadap ruang pribadi yang dimilikinya. Dalam konteks pengelolaan data pribadi di era digital, prinsip ini dapat dimaknai sebagai kewajiban bagi pengendali data untuk memperoleh persetujuan yang sah dan sadar dari subjek data sebelum melakukan pemrosesan data pribadi. Nilai ini selaras dengan prinsip kemanusiaan yang adil dan beradab dalam Pancasila yang menempatkan manusia sebagai subjek utama yang harus dihormati hak dan martabatnya.

Penguatan perlindungan hukum terhadap privasi individu juga tercermin dalam hadis Nabi Muhammad SAW yang diriwayatkan oleh Imam Muslim yang menyatakan bahwa setiap Muslim memiliki kehormatan atas darah, harta, dan kehormatannya yang tidak boleh dilanggar oleh orang lain. Dalam konteks masyarakat digital modern, data pribadi dapat dipandang sebagai bagian dari kehormatan dan identitas individu yang harus dijaga dari penyalahgunaan. Oleh karena itu, integrasi nilai-nilai Pancasila dalam regulasi perlindungan data pribadi yang bersifat spesifik tidak hanya memiliki legitimasi filosofis dalam kerangka negara hukum Indonesia, tetapi juga memperoleh penguatan nilai dari perspektif etika keagamaan yang menempatkan perlindungan terhadap martabat manusia sebagai prinsip fundamental dalam kehidupan bermasyarakat. Sinergi antara nilai Pancasila dan prinsip-prinsip yang bersumber dari data kewahyuan tersebut

menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik merupakan bagian dari upaya menjaga kehormatan manusia, mewujudkan keadilan sosial, serta membangun tata kelola ruang digital yang beretika dan berkeadaban.

Perspektif *maqāṣid al-syarī'ah* juga memperkuat urgensi perlindungan terhadap data pribadi sebagai bagian dari upaya menjaga lima tujuan pokok syariat, khususnya perlindungan terhadap kehormatan dan martabat manusia (*ḥifẓ al-'ird*) serta perlindungan terhadap harta (*ḥifẓ al-māl*). Penyalahgunaan data pribadi dalam era digital berpotensi menimbulkan kerugian ekonomi, pencemaran nama baik, hingga pelanggaran terhadap identitas seseorang. Oleh karena itu, rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik dapat dipandang sebagai upaya untuk menghadirkan sistem hukum yang tidak hanya memenuhi tuntutan perkembangan teknologi modern, tetapi juga selaras dengan nilai-nilai etika dan moral yang bersumber dari ajaran agama, sehingga tercipta tata kelola ruang digital yang menjunjung tinggi keadilan, tanggung jawab, dan penghormatan terhadap martabat manusia.

Rekonstruksi perlindungan data pribadi yang bersifat spesifik yang dimaksud tidak hanya memiliki landasan yuridis dan filosofis dalam nilai-nilai Pancasila, tetapi juga memperoleh legitimasi etis dari ajaran Islam. Keselarasan antara nilai ketuhanan, kemanusiaan, keadilan, dan tanggung jawab menunjukkan bahwa perlindungan data pribadi merupakan kebutuhan fundamental dalam era digital, maka penguatan regulasi perlindungan data pribadi yang bersifat spesifik menjadi langkah penting untuk mewujudkan kepastian hukum, perlindungan hak warga negara, serta tata kelola digital yang berkeadilan dan berkeadaban.

BAB IV
REKONSTRUKSI HUKUM PELINDUNGAN DATA PRIBADI YANG BERSIFAT SPESIFIK TERHADAP PERKEMBANGAN TEKNOLOGI DI ERA DIGITAL YANG SESUAI DENGAN NILAI-NILAI KEADILAN BERDASARKAN PANCASILA

A. Dasar Kebutuhan Rekonstruksi Hukum Perlindungan Data Pribadi yang Bersifat Spesifik di Era Digital untuk Mewujudkan Keadilan Berdasarkan Pancasila

Dasar kebutuhan rekonstruksi hukum terhadap perlindungan data pribadi yang bersifat spesifik di era digital lahir dari adanya kesenjangan antara perkembangan teknologi yang semakin masif dengan kemampuan instrumen hukum dalam memberikan perlindungan yang efektif, adaptif, dan berkeadilan. Perlindungan terhadap data pribadi yang bersifat spesifik menjadi isu fundamental karena jenis data tersebut memiliki tingkat sensitivitas yang tinggi dan berhubungan langsung dengan identitas, kehormatan, martabat, keamanan, serta hak privasi subjek data.[361] Tanpa adanya kerangka hukum yang kuat dan adaptif, individu rentan terekspos pada risiko penyalahgunaan data yang merugikan, seperti penipuan, pencurian identitas, hingga eksploitasi privasi. Oleh karena itu, pembaruan dan rekonstruksi norma hukum mutlak diperlukan bukan sekadar untuk mengejar ketertinggalan dari disrupsi teknologi, melainkan untuk memastikan bahwa tata kelola ruang digital di Indonesia secara nyata menjamin keadilan sosial,

[361] Disemadi et al., *loc.cit.*

kesetaraan hak, dan penghormatan terhadap martabat masyarakat sesuai dengan nilai-nilai luhur Pancasila.[362]

Konsepsi keadilan sosial Pancasila menempatkan perlindungan data pribadi yang bersifat spesifik spesifik sebagai bagian dari perlindungan martabat manusia dan jaminan kesetaraan warga negara dalam ruang digital. Data kesehatan, biometrik, genetika, data anak, data keuangan, serta data yang mengungkap keyakinan atau orientasi tertentu memiliki daya rusak yang lebih tinggi apabila diproses tanpa batas, karena dapat menimbulkan stigma, eksklusi sosial, diskriminasi layanan, hingga pemerasan.[363] Urgensi rekonstruksi hukum terletak pada kebutuhan untuk memutus rantai ketimpangan kekuasaan informasi antara pengendali data dan subjek data, terutama ketika subjek data berada pada posisi tawar yang lemah. Kerangka hukum yang berorientasi Pancasila perlu memastikan penguatan hak substantif dan prosedural bagi pemilik data, sehingga perlindungan tidak hanya bersifat deklaratif, melainkan efektif mencegah ketidakadilan yang muncul akibat pemrosesan data sensitif dalam skala besar.

Perusahaan swasta yang mengelola data pribadi harus mengambil langkah-langkah proaktif untuk meningkatkan sistem keamanan mereka. Mereka harus berinvestasi dalam sistem perlindungan yang kuat, memastikan bahwa data pengguna tidak hanya disimpan dengan aman, tetapi juga hanya dapat diakses oleh pihak yang berwenang. Perusahaan juga perlu melaksanakan audit dan pengujian

---

[362] U Darmanto Soer and Nining Yurista Prawitasari, "Perlindungan Hukum Data Pribadi Konsumen Dalam Transaksi E-Commerce Di Indonesia," *SABAJAYA Jurnal Pengabdian Kepada Masyarakat* 3, no. 01 (2025), hlm. 49-55.

[363] Levina Yustitianingtyas, Anang Dony Irawan, and Dedy Stansyah, "Human Rights Enforcement in Indonesia towards the Implementation of Pancasila Values," *JUSTISI* Vol. 11, no. 2 (2025): Hlm. 387-405.

secara berkala untuk mendeteksi potensi celah dalam sistem mereka. Lembaga pengawas, seperti OJK, memiliki peran yang sangat penting dalam memastikan bahwa data pribadi masyarakat terlindungi dengan baik.[364] Lembaga-lembaga ini perlu meningkatkan fungsi pengawasan mereka terhadap implementasi regulasi perlindungan data pribadi. Selain itu, lembaga pengawas juga harus memberikan pelatihan dan fasilitas untuk membantu perusahaan dalam memenuhi standar perlindungan data.

Pelindungan data pribadi yang bersifat spesifik merupakan aspek penting dalam menjaga hak asasi manusia, terutama di era digital. Ketika perlindungan data pribadi tidak memadai, individu menghadapi risiko kehilangan kontrol terhadap informasi yang sangat personal dan sensitif.[365] Regulasi yang ada di Indonesia, seperti UU PDP, telah mencanangkan upaya untuk menjaga data pribadi, namun masih terdapat kesenjangan signifikan antara regulasi tersebut dan prinsip keadilan sosial yang terkandung dalam Pancasila. Kesenjangan ini mengarah pada ketidakadilan dalam pengelolaan dan pengawasan data pribadi yang menguntungkan pihak tertentu sementara merugikan individu yang seharusnya dilindungi.

Kelemahan besar dalam perlindungan data pribadi yang bersifat spesifik di Indonesia adalah ketidakmampuan regulasi yang ada dalam menangani kebocoran data. Meskipun Indonesia telah memiliki UU PDP, implementasinya masih sangat

---

[364] Rizqika Farah Isnugraheny, Zahra Ekasiwi Megawati, and Siti Susilawati, "Optimalisasi Prinsip Kerahasiaan Data Nasabah Dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi," *Media Hukum Indonesia (Mhi)* 2, no. 4 (2024).

[365] Muhammad Hanan Nuhi et al., "Tinjauan Hak Asasi Manusia Terhadap Perlindungan Data Pribadi Dan Kepastian Hukumnya Di Indonesia," in *National Conference on Law Studies (NCOLS)*, vol. 6, 2024, hlm. 433-447.

terbatas. Banyak kasus kebocoran data yang terjadi karena kelemahan dalam pengawasan serta penegakan hukum yang tidak konsisten. Kasus kebocoran data di sektor publik maupun swasta menjadi semakin sering, menunjukkan adanya celah dalam sistem perlindungan data pribadi. Hal ini memperlihatkan bahwa meskipun regulasi telah ada, masih banyak kekurangan dalam hal implementasi dan pengawasan yang efektif.[366]

UU PDP di Indonesia memiliki ketentuan mengenai sanksi bagi pihak yang melakukan pelanggaran terkait pengelolaan data pribadi. Namun, penerapan sanksi hukum ini sering kali tidak efektif, dan terkadang tidak memberikan efek jera. Ketidakjelasan mengenai mekanisme penegakan hukum dan sanksi terhadap pelanggaran yang terjadi menunjukkan adanya kelemahan dalam sistem hukum Indonesia terkait dengan perlindungan data pribadi yang bersifat spesifik. [367] Perusahaan atau lembaga yang mengelola data pribadi sering kali tidak takut untuk melanggar aturan karena rendahnya penegakan hukum yang ada. Untuk itu, penerapan sanksi yang lebih jelas dan tegas harus menjadi perhatian dalam reformasi regulasi perlindungan data pribadi yang bersifat spesifik.

Pemberlakuan terhadap UU PDP masih memiliki banyak kendala. Kurangnya detail dan ketegasan dalam peraturan pelaksanaan sering kali menjadi hambatan dalam menegakkan kebijakan yang efektif. Meskipun Indonesia telah memiliki UU PDP, penegakan hukum terhadap kebocoran data sering kali terhambat oleh ketidakjelasan peraturan pelaksanaan. Kurangnya sanksi yang jelas dan efektif bagi

---

[366] Althea Serafim Kriswandaru, Berliant Pratiwi, and Suwardi Suwardi, "Efektivitas Kebijakan Perlindungan Data Pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus," *Hakim: Jurnal Ilmu Hukum dan Sosial* 2, no. 4 (2024), hlm. 740-756.

[367] Yudistira dan Ramadani, *loc.cit*.

pelanggar serta tidak adanya mekanisme pengawasan yang kuat membuat kebocoran data sering kali tidak direspons secara serius. Hal ini menunjukkan perlunya memperkuat penegakan hukum dalam hal perlindungan data pribadi.

Pelindungan data pribadi di Indonesia menjadi semakin penting di era digital ini, namun implementasinya menghadapi banyak kendala. UU PDP merupakan langkah penting untuk melindungi data pribadi warga negara. Namun, pelaksanaannya tidak semudah yang diharapkan. Banyak hambatan yang menghalangi implementasi yang efektif dari regulasi ini. Salah satunya adalah kurangnya koordinasi antar lembaga pemerintah yang terlibat dalam pengawasan dan penegakan hukum. Tanpa kerjasama yang kuat antar lembaga, efektivitas regulasi ini akan terus terhambat.[368]

Kebocoran data merujuk pada insiden dimana data pribadi yang bersifat sensitif, seperti identitas, informasi keuangan, atau data kesehatan, dapat diakses oleh pihak yang tidak berwenang. Dalam konteks ini, kebocoran data merupakan ancaman serius terhadap privasi individu. Data pribadi yang bocor dapat digunakan untuk berbagai tindakan yang merugikan, seperti pencurian identitas, penipuan, atau bahkan kejahatan siber lainnya.[369]

Penyebab utama kebocoran data di Indonesia dapat dikategorikan menjadi dua aspek: pertama, faktor teknis yang berkaitan dengan kelemahan sistem keamanan dan kedua, faktor manusia atau kelalaian dalam pengelolaan data.[370]

---

[368] Erikha dan Hoesein, *loc.cit*.

[369] Disemadi et al., *loc.cit*

[370] Maichle Delpiero et al., "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," *Padjadjaran Law Review* 9, no. 1 (2021), hlm. 1-22.

Secara teknis, kebocoran data dapat terjadi jika infrastruktur sistem informasi yang digunakan untuk menyimpan data tidak dilengkapi dengan perlindungan yang memadai, seperti enkripsi atau kontrol akses yang ketat. Faktor manusia sering kali mencakup kesalahan operasional, kelalaian dalam pengelolaan data, atau kurangnya kesadaran akan pentingnya keamanan data.

Regulasi yang tidak memadai ini berkontribusi pada kebocoran data karena tidak adanya kontrol yang cukup ketat terhadap perusahaan atau lembaga yang mengelola data pribadi.Salah satu contoh kebocoran data yang paling mencolok di Indonesia adalah kasus kebocoran data yang melibatkan BPJS Kesehatan. Pada tahun 2020, terungkap bahwa data pribadi lebih dari 20 juta peserta BPJS Kesehatan bocor dan dijual di pasar gelap.[371] Data tersebut meliputi informasi sensitif seperti nama, alamat, nomor kartu BPJS, dan data medis lainnya. Kasus ini mencerminkan adanya kekurangan dalam sistem keamanan dan pengawasan yang memadai terhadap lembaga yang mengelola data pribadi masyarakat.

Kebocoran data di Indonesia juga terjadi pada *platform digital*, salah satunya adalah Gojek. Pada tahun 2020, sebuah data pribadi yang melibatkan informasi pelanggan dan mitra Gojek, termasuk nama, nomor telepon, dan informasi transaksi, dilaporkan bocor. Penyebab utama kebocoran ini adalah kelalaian dalam pengelolaan akses data dan tidak adanya sistem pengamanan data yang memadai dalam aplikasi yang digunakan.[372] Pada tahun 2020, Tokopedia, salah satu platform

[371] Bahtiar, *loc.cit*.

[372] Wahyunanda Kusuma Pertiwi and Oik Yusuf, "Data Tokopedia, Gojek, Dan Bukalapak Bocor Di Tengah Absennya RUU PDP," *Tekno.Kompas.Com*, accessed May 12, 2025, https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp.

e-commerce terbesar di Indonesia, juga mengalami kebocoran data.[373] Data lebih dari 90 juta pengguna, termasuk nama, email, nomor telepon, dan data transaksi, bocor ke internet. Kebocoran ini terjadi akibat celah dalam sistem keamanan yang tidak terdeteksi dengan cepat. Kasus ini menunjukkan pentingnya implementasi pengamanan yang lebih ketat dalam platform *e-commerce* untuk melindungi data pengguna. Penyalahgunaan data pribadi sering kali terjadi dalam sektor pinjaman online (pinjol) ilegal.

Kelalaian dalam pengelolaan data pribadi oleh perusahaan sering kali menjadi faktor utama penyebab kebocoran data. Banyak perusahaan pinjol yang memperoleh dan memanfaatkan data pribadi tanpa izin dari pihak yang bersangkutan.[374] Penggunaan data pribadi ini sering kali melibatkan ancaman dan intimidasi untuk menagih utang. Hal ini menambah keprihatinan terhadap perlindungan data pribadi di Indonesia, mengingat rentannya individu terhadap eksploitasi data. Banyak perusahaan yang tidak memberikan perhatian cukup terhadap keamanan data pelanggan mereka. Penyebab kelalaian ini bisa beragam, mulai dari kurangnya pelatihan karyawan mengenai pentingnya keamanan data hingga kurangnya investasi pada sistem perlindungan yang memadai.[375]

Lembaga-lembaga yang ada sering kali tidak memiliki kewenangan atau sumber daya yang cukup untuk melakukan pengawasan yang mendalam dan

---

[373] Yudha Pratomo and Reza Wahyudi, "Kebocoran Data 15 Juta Pengguna, Pengakuan Tokopedia, Dan Analisis Ahli," *Tekno.Kompas.Com*, accessed May 12, 2025, https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli.

[374] Abdurrazaq Triansyah et al., "Peran Otoritas Jasa Keuangan Dalam Perlindungan Hukum Bagi Pengguna Pinjaman Online Ilegal (Studi Kasus Pinjol Ilegal Di Yogyakarta)," *Cross-border* 5, no. 2 (2022), hlm. 1090-1104.

[375] Erikha dan Hoesein, *loc.cit*.

menyeluruh terhadap pengelolaan data pribadi oleh pihak ketiga. Kelemahan ini menyebabkan banyak pelanggaran yang terjadi tanpa mendapatkan perhatian yang memadai. Pengawasan yang independen dan berkelanjutan sangat penting untuk memastikan bahwa hak individu terkait dengan data pribadi dilindungi dengan baik.[376]

Kebocoran data di Indonesia banyak disebabkan oleh sistem keamanan yang lemah pada penyelenggara sistem elektronik. Misalnya, penggunaan perangkat lunak yang usang, kurangnya pemeliharaan sistem yang rutin, serta ketidakmampuan dalam mendeteksi celah-celah keamanan.[377] Hal ini menunjukkan perlunya peningkatan investasi pada teknologi dan infrastruktur yang dapat melindungi data pribadi. Salah satu faktor yang menyebabkan kebocoran data adalah kurangnya pengawasan terhadap pihak yang mengelola data pribadi. Pengawasan yang lemah oleh lembaga yang berwenang atau oleh pihak yang bertanggung jawab terhadap data pribadi menyebabkan celah-celah dalam sistem yang rentan terhadap kebocoran. Pengawasan yang efektif harus dilakukan secara berkala untuk memastikan bahwa setiap pengelolaan data memenuhi standar keamanan yang ketat.

Pemerintah Indonesia juga memiliki peran penting dalam menanggulangi kebocoran data dengan merumuskan kebijakan yang lebih ketat terkait perlindungan data pribadi. Salah satu langkah yang perlu diambil adalah

---

[376] Erikha dan Hoesein, *loc.cit*.

[377] Inaz Indra Nugroho, Reza Pratiwi, and Salsabila Rahma Az Zahro, "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia," *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 1, no. 2 (2021), hlm. 115-129.

memperkuat regulasi dan meningkatkan pengawasan terhadap lembaga-lembaga yang mengelola data pribadi. Pemerintah juga perlu memberikan sanksi yang lebih tegas terhadap pelanggar untuk mencegah terjadinya kebocoran data di masa depan.

Implementasi regulasi perlindungan data pribadi di Indonesia masih menghadapi tantangan besar dalam hal penegakan hukum. Meskipun telah ada UU PDP yang menyatakan bahwa data pribadi harus dilindungi, penegakan hukum terhadap kebocoran atau penyalahgunaan data pribadi sering kali tidak dilakukan secara tegas. Menurut laporan dari Komisi Pelindungan data pribadi (KPDP), pengawasan dan penegakan hukum yang lemah terhadap pelanggaran terkait data pribadi menyebabkan ketidakadilan dalam sistem perlindungan data di Indonesia. Penegakan yang tidak konsisten ini menyebabkan banyak pihak merasa bahwa regulasi ini tidak memadai untuk memberikan perlindungan yang sejajar dengan nilai-nilai yang terkandung dalam Pancasila.[378]

Penegakan hukum yang lemah menjadi salah satu masalah utama dalam implementasi UU PDP. Banyak pelanggaran yang tidak ditindaklanjuti dengan sanksi yang tegas, yang seharusnya memberikan efek jera kepada pelaku. Penegakan hukum yang lemah ini menciptakan ketidakadilan, dimana pelanggaran data pribadi tidak mendapatkan perhatian yang semestinya. Hal ini semakin diperburuk oleh kurangnya transparansi dalam proses penegakan hukum. Publik

[378] Barli Tomia, "Perlindungan Hukum Terhadap Data Pribadi Di Indonesia Tantangan Dan Solusi Dalam Era Digital - Kompasiana.Com," *Kompasiana.Com*, accessed May 12, 2025, https://www.kompasiana.com/adityasaputra3664/67814681c925c459f631bfe2/perlindungan-hukum-terhadap-data-pribadi-di-indonesia-tantangan-dan-solusi-dalam-era-digital.

tidak selalu mengetahui bagaimana pelanggaran data pribadi diproses, dan apakah pelaku pelanggaran benar-benar mendapat sanksi yang sesuai.379

Perbaikan dalam sistem pengawasan digital juga diperlukan. Diperlukan standar yang lebih konsisten dan menyeluruh untuk memastikan perlindungan data yang lebih efektif. Perusahaan dan lembaga yang mengelola data pribadi harus memiliki sistem pengawasan yang lebih canggih dan terintegrasi untuk memastikan bahwa data yang mereka kelola terlindungi dengan baik. Implementasi sistem yang lebih transparan dan berbasis teknologi akan membantu memperbaiki pengawasan yang ada saat ini dan membuat pelanggaran lebih mudah terdeteksi. Penerapan teknologi keamanan yang lebih baik di seluruh sektor adalah langkah yang penting. Teknologi seperti enkripsi dan autentikasi dua faktor harus diterapkan secara lebih luas di semua sektor yang mengelola data pribadi.

Pelindungan data pribadi yang bersifat spesifik di Indonesia mengalami tantangan signifikan dalam hal implementasi, terutama terkait dengan penegakan hukum dan pengawasan yang lemah. Meskipun UU PDP telah dirancang untuk melindungi data pribadi warga negara, banyak hambatan dalam implementasinya yang menghambat pencapaian tujuan hukum tersebut. Salah satu masalah utama adalah kurangnya koordinasi antar lembaga pemerintah yang terlibat dalam pengawasan dan penegakan hukum. Tanpa kerjasama yang kuat antar lembaga, efektivitas regulasi ini akan terus terhambat.

---

379 Nansya Janaika Safalla, "Perlindungan Hukum Konsumen Terhadap Tindak Pidana Pencurian Data Pribadi Dalam Transaksi E-Commerce Di Indonesia" (Semarang: Universitas Islam Sultan Agung Semarang, 2024).

Perkembangan teknologi informasi dan komunikasi di Indonesia berjalan dengan sangat cepat, namun regulasi yang ada sering kali tertinggal. Teknologi baru seperti AI, IoT, dan big data memberikan tantangan baru dalam hal perlindungan data pribadi. Sementara itu, peraturan yang ada belum sepenuhnya dapat mengakomodasi perubahan cepat ini. Banyak celah yang belum diatur dalam regulasi yang ada, yang menyebabkan ketidakmampuan untuk mengatasi tantangan yang muncul akibat kemajuan teknologi. Pembaruan dan perbaikan regulasi yang lebih adaptif terhadap perkembangan teknologi sangat dibutuhkan.[380]

Kebutuhan rekonstruksi hukum juga berangkat dari karakter teknologi modern yang memungkinkan pemrosesan data spesifik dilakukan melalui pemrofilan, korelasi lintas basis data, serta pengambilan keputusan otomatis yang berdampak hukum atau berdampak signifikan bagi individu. Risiko ketidakadilan meningkat ketika algoritma menilai kelayakan kredit, premi asuransi, seleksi kerja, atau akses layanan publik dengan menggunakan data sensitif secara langsung maupun tidak langsung melalui variabel proksi. Norma hukum yang berbasis keadilan sosial Pancasila perlu menegaskan pembatasan terhadap pemrosesan otomatis berisiko tinggi, kewajiban penilaian dampak perlindungan data, serta hak subjek data untuk memperoleh penjelasan yang dapat dipahami dan mekanisme keberatan yang efektif. [381] Instrumen tersebut harus disertai standar audit algoritmik

[380] Andi Ahmad Munajat and Hudi Yusuf, "Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus : Studi Tentang Kejahatan Keuangan Berbasis Digital The Role of Information Technology in the Prevention and Disclosure of Special Economic Crimes : A Study of Digita," *JIIC: Jurnal Intelek Insan Cendikia* 1, no. 9 (2024), hlm. 4853-4865.

[381] Lucilla Gatt and Ilaria Amelia Caggiano, "Consumers and Digital Environments as a Structural Vulnerability Relationship," *European Journal of Privacy Law & Technologies* Vol. 1, no. 2 (2022), hlm. 8-16.

dan kewajiban transparansi minimal agar pengambilan keputusan digital tidak melahirkan diskriminasi sistemik. Perumusan norma yang adaptif akan mencegah ketertinggalan regulasi dan memperkuat perlindungan terhadap kelompok rentan.

Integrasi antara regulasi perlindungan data pribadi dengan sistem hukum yang lebih luas juga hal yang penting. Meskipun UU PDP sudah ada, peraturan pelaksanaannya masih terbatas, dan seringkali tidak sejalan dengan undang-undang lain yang mengatur perlindungan data di Indonesia.382 Koordinasi antar peraturan ini perlu diperkuat agar tidak ada kesenjangan antara satu regulasi dengan yang lainnya, sehingga perlindungan data pribadi dapat dilaksanakan secara menyeluruh dan efisien. Sistem perlindungan data pribadi yang terpisah di setiap sektor juga menambah kerumitan dalam implementasi UU PDP. Sektor kesehatan, pendidikan, perbankan, dan sektor lainnya memiliki sistem perlindungan data pribadi yang berbeda-beda. Hal ini menimbulkan masalah koordinasi, karena setiap sektor sering kali memiliki standar dan prosedur yang berbeda dalam menangani data pribadi.

Regulasi perlindungan data pribadi harus lebih fleksibel namun tetap adil untuk mencakup perkembangan teknologi yang cepat. Negara harus mampu menyusun kebijakan yang dapat beradaptasi dengan perubahan zaman dan perkembangan teknologi yang terus berkembang. Teknologi informasi dan komunikasi yang semakin canggih mempengaruhi cara data pribadi dikumpulkan, disimpan, dan digunakan. Negara harus memastikan bahwa regulasi yang ada selalu

[382] Syarifuddin Syarifuddin et al., "Reformasi Hukum Di Era Digital:: Tantangan Dan Peluang Di Indonesia," *Indonesian Research Journal on Education* 4, no. 4 (2024), hlm. 3206-3215.

relevan dengan perkembangan teknologi, sehingga perlindungan data pribadi tetap optimal di tengah perubahan yang pesat.

Penyelenggara sistem elektronik yang mengelola data pribadi di Indonesia sering kali tidak memadai dalam hal infrastruktur keamanan siber. Banyak perusahaan dan lembaga yang belum sepenuhnya memperhatikan kebutuhan pengamanan data, terutama data yang bersifat spesifik dan sensitif. Misalnya, infrastruktur yang lemah dapat menyebabkan akses yang tidak sah terhadap data pribadi, atau bahkan kebocoran yang terjadi akibat peretasan sistem yang tidak dilengkapi dengan proteksi yang memadai. Keamanan siber yang kuat sangat penting untuk mencegah pelanggaran data pribadi, dan kelemahan infrastruktur ini menjadi salah satu faktor utama dalam tingginya angka kebocoran data di Indonesia.

Risiko terbesar yang dihadapi oleh individu ketika data pribadi mereka bocor adalah pencurian identitas.[383] Data yang bocor, seperti nomor KTP, nomor rekening, dan informasi pribadi lainnya, dapat digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan penipuan atau bahkan kejahatan lainnya. Dalam beberapa kasus, pencurian identitas ini juga digunakan untuk mendapatkan keuntungan finansial atau untuk melakukan aktivitas kriminal yang merugikan korban. Penyalahgunaan data pribadi ini menjadi salah satu masalah besar yang harus diatasi dalam sistem perlindungan data pribadi yang bersifat spesifik di Indonesia.

[383] Irvin Atara, Sharron Syallomeita, and Raffi Aqil Baihaqi Haksoro, "Analisis Kriminologi Terhadap Pencurian Data Pribadi Di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023," *Jurnal Ilmiah Penelitian Mahasiswa* 3, no. 2 (2025), hlm. 129-140.

Masalah lain yang sering terjadi dalam perlindungan data pribadi yang bersifat spesifik di Indonesia adalah penggunaan data pribadi tanpa persetujuan yang jelas dan eksplisit dari pemilik data. Banyak perusahaan dan lembaga yang mengumpulkan data pribadi tanpa memberitahukan dengan jelas tujuan pengumpulan tersebut atau bahkan tanpa meminta izin dari individu yang bersangkutan.[384] Praktik seperti ini sering kali terjadi pada *platform digital* dan layanan online, yang mengumpulkan data pengguna secara otomatis dan tidak transparan. Tanpa persetujuan yang jelas, penggunaan data pribadi tersebut dapat melanggar hak privasi individu dan menambah ketidakadilan dalam pengelolaan data.

Perusahaan yang mengumpulkan data pribadi sering kali menggunakan data tersebut untuk tujuan yang tidak sesuai dengan kepentingan individu atau bahkan melanggar hak privasi. Sebagai contoh, data pribadi yang dikumpulkan untuk tujuan pemasaran sering kali digunakan untuk menjual informasi kepada pihak ketiga tanpa persetujuan eksplisit dari individu yang bersangkutan. Hal ini tidak hanya melanggar hak individu atas data mereka, tetapi juga menciptakan ketidakadilan sosial, karena beberapa pihak mendapatkan keuntungan dari data pribadi orang lain tanpa memberikan manfaat yang setara kepada pemilik data.

Pelindungan data pribadi yang bersifat spesifik merupakan aspek penting dalam menjaga hak asasi manusia, terutama di era digital. Ketika perlindungan data pribadi tidak memadai, individu menghadapi risiko kehilangan kontrol terhadap

[384] Arrasuli dan Fahmi, *loc.cit*.

informasi yang sangat personal dan sensitif.[385] Regulasi yang ada di Indonesia, seperti UU PDP, telah mencanangkan upaya untuk menjaga data pribadi, namun masih terdapat kesenjangan signifikan antara regulasi tersebut dan prinsip keadilan sosial yang terkandung dalam Pancasila. Kesenjangan ini mengarah pada ketidakadilan dalam pengelolaan dan pengawasan data pribadi yang menguntungkan pihak tertentu sementara merugikan individu yang seharusnya dilindungi.

Keadilan sosial sebagai nilai utama dalam Pancasila mengharuskan adanya pemerataan dalam perlindungan hak privasi setiap individu. Namun, dalam implementasi UU PDP, masih ditemukan banyak celah yang menyebabkan sebagian masyarakat, khususnya mereka yang memiliki akses terbatas terhadap teknologi, kurang terlindungi. Penelitian oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa hanya sebagian kecil masyarakat Indonesia yang memiliki pemahaman mendalam tentang hak mereka terkait dengan perlindungan data pribadi.[386] Hal ini menciptakan ketidaksetaraan dalam akses terhadap perlindungan data pribadi yang seharusnya diatur secara merata untuk semua kalangan.

Kepercayaan publik terhadap pengelolaan data pribadi sangat tergantung pada sejauh mana perusahaan dan lembaga pemerintah dapat menunjukkan komitmen mereka dalam melindungi data. Peningkatan transparansi dalam

---

[385] Muhammad Hanan Nuhi et al., "Tinjauan Hak Asasi Manusia Terhadap Perlindungan Data Pribadi Dan Kepastian Hukumnya Di Indonesia," in *National Conference on Law Studies (NCOLS)*, vol. 6, 2024, hlm. 433-447.

[386] Budi Praptawismacaya Amir, "Pengaruh Globalisasi Terhadap Perekonomian Ditinjau Dari Hukum Niaga," *Syntax Literate; Jurnal Ilmiah Indonesia* 9, no. 5 (2024), hlm. 2967-2975.

pengelolaan data, diikuti dengan langkah-langkah pengamanan yang jelas dan efektif, akan membantu membangun kepercayaan masyarakat. Kepercayaan ini sangat penting agar masyarakat tidak enggan berbagi data pribadi yang diperlukan dalam transaksi digital. Salah satu contoh nyata ketidakadilan ini adalah kurangnya pengawasan terhadap perusahaan besar yang mengelola data pribadi, seperti perusahaan *e-commerce* atau *platform digital* lainnya. Di sisi lain, individu atau kelompok masyarakat yang memiliki akses terbatas pada teknologi dan informasi, sering kali tidak memahami sepenuhnya hak mereka terkait data pribadi mereka. Kebijakan yang ada belum dapat menjamin perlindungan yang setara bagi seluruh masyarakat Indonesia, terutama bagi mereka yang kurang teredukasi mengenai pentingnya privasi digital.[387]

Kesenjangan antara regulasi yang ada dengan prinsip keadilan sosial juga tercermin dalam kelemahan pengawasan terhadap pengelolaan data pribadi oleh pihak ketiga. Banyak perusahaan yang mengumpulkan data pribadi tanpa memberikan informasi yang cukup kepada individu mengenai bagaimana data mereka akan digunakan.[388] Praktik ini bertentangan dengan prinsip transparansi yang diharapkan dalam UU PDP dan Pancasila. Kurangnya pengawasan yang independen memungkinkan perusahaan-perusahaan ini untuk melakukan praktik yang dapat merugikan individu tanpa adanya konsekuensi yang jelas.

---

[387] Aurelia Elma Adriana Surya Wibawa, "Etika Dan Hukum Penggunaan Ai Untuk Pemasaran Digital Dalam Prespektif Hukum Bisnis Di Indonesia" (Yogyakarta: Universitas Atma Jaya Yogyakarta, 2024).

[388] Fauzi Rifa and Maslihati Nur Hidayati, "Kebijakan Penal Dalam Perlindungan Data Pribadi Nasabah Fintech Lending Di Indonesia," *Binamulia Hukum* 13, no. 2 (2024), hlm. 461-481.

Pengaruh ekonomi terhadap perlindungan data pribadi juga menjadi faktor yang mempengaruhi kesenjangan antara regulasi yang ada dengan prinsip keadilan sosial. Korporasi besar, yang memiliki sumber daya lebih banyak, sering kali lebih mudah memenuhi persyaratan untuk perlindungan data pribadi, sementara perusahaan kecil dan menengah seringkali tidak memiliki cukup dana untuk menerapkan kebijakan keamanan yang memadai.[389] Hal ini menciptakan ketimpangan dalam perlindungan data pribadi, dimana individu yang bertransaksi dengan perusahaan besar mungkin mendapatkan perlindungan yang lebih baik daripada mereka yang berurusan dengan perusahaan kecil atau usaha lokal.

Pelindungan data pribadi yang bersifat spesifik juga memerlukan keterlibatan lebih besar dari sektor swasta. Banyak perusahaan yang memiliki data pribadi konsumen tidak selalu mematuhi regulasi yang ada. 390 Penyalahgunaan data sering kali terjadi tanpa sepengetahuan konsume n, yang menunjukkan bahwa perlindungan data pribadi di sektor swasta masih sangat lemah. Pemerintah perlu lebih tegas dalam mengawasi sektor swasta untuk memastikan bahwa perusahaan yang mengelola data pribadi mematuhi regulasi yang berlaku. Kurangnya mekanisme pengaduan yang efektif di Indonesia juga menghambat penegakan UU PDP. Masyarakat tidak selalu tahu dimana dan bagaimana mengadukan pelanggaran terkait data pribadi mereka. Sistem pengaduan yang ada saat ini masih belum sepenuhnya efisien, dan banyak laporan tidak ditindaklanjuti dengan segera. Diperlukan penguatan mekanisme pengaduan agar masyarakat dapat melaporkan

[389] I Wayan Sudira, "Keadilan Digital: Tantangan Hukum Dalam Era Disrupsi Teknologi," *Kertha Widya* 12, no. 2 (2025), hlm. 35-59.

[390] Erikha dan Hoesein, *loc.cit*.

pelanggaran dengan mudah dan efektif. 391 Sanksi yang lebih berat harus diterapkan kepada perusahaan yang tidak mematuhi aturan perlindungan data pribadi.

Negara perlu menyediakan sistem pelaporan yang mudah diakses oleh masyarakat agar mereka dapat melaporkan pelanggaran data pribadi dengan cepat. Sistem pelaporan yang efisien dan responsif akan mempercepat proses pengambilan tindakan terhadap pelanggaran yang terjadi. Tanpa sistem pelaporan yang efektif, banyak pelanggaran yang tidak terdeteksi dan dibiarkan tanpa tindakan yang sesuai. Negara harus menciptakan sistem yang memfasilitasi pengaduan masyarakat dan menangani masalah ini dengan cepat dan tepat.

Mekanisme pelaporan yang efektif sangat diperlukan untuk mempermudah masyarakat melaporkan pelanggaran terhadap data pribadi mereka. Tanpa adanya saluran pelaporan yang jelas dan mudah diakses, masyarakat akan kesulitan untuk melaporkan penyalahgunaan data mereka. 392 Penguatan pengawasan dan penegakan hukum juga memerlukan peran serta sektor swasta yang lebih besar dalam memastikan kepatuhan terhadap regulasi yang ada. Perusahaan-perusahaan yang mengelola data pribadi harus dilibatkan dalam proses pengawasan dan diberi pemahaman yang lebih mendalam mengenai kewajiban mereka untuk melindungi

[391] Bovin Tri Mahendra et al., "Kebijakan Hukum Pidana Terhadap Penyebaran Data Pribadi Oleh Jurnalis Dalam Rangka Perlindungan Data Pribadi Di Indonesia" (Jambi: Universitas Jambi, 2025).

[392] Cecep Sutrisna, "Aspek Hukum Perlindungan Data Pribadi Dan Kondisi Darurat Kebocoran Atas Data Pribadi Di Indonesia," *Wacana Paramarta: Jurnal Ilmu Hukum* 20, no. 5 (2021), hlm. 1-10.

data.393 Pengusaha harus memiliki komitmen untuk menjaga data pribadi yang mereka kelola dan harus siap untuk diawasi secara ketat oleh lembaga yang berwenang.

Desain sanksi yang berkeadilan menuntut diferensiasi berdasarkan tingkat risiko, skala pemrosesan, dan akibat yang ditimbulkan bagi subjek data, sehingga penegakan hukum tidak berhenti pada formalitas administratif. Rekonstruksi hukum perlu merumuskan parameter penilaian pelanggaran yang operasional, mencakup kelalaian pengendali data, kegagalan menerapkan standar keamanan minimum, kegagalan notifikasi insiden, serta keuntungan ekonomi yang diperoleh dari pemrosesan yang melanggar hukum. Sanksi yang proporsional harus menggabungkan denda administratif yang signifikan, perintah penghentian sementara pemrosesan, kewajiban pemulihan, serta eskalasi ke sanksi pidana pada pelanggaran yang disengaja atau berdampak luas.[394] Kepastian mengenai prosedur pembuktian dan tata cara penjatuhan sanksi menjadi krusial untuk mencegah disparitas dan menguatkan efek jera. Konstruksi ini selaras dengan keadilan sosial karena menempatkan perlindungan korban sebagai orientasi utama, bukan semata kepentingan institusional.

---

[393] Thiara Octaviani Putri and Muhamad Farudin, "Pelindungan data pribadi yang bersifat spesifik Konsumen Pada Perusahaan E-Commerce Yang Mengalami Kepailitan Di Indonesia Ditinjau Berdasarkan Hukum Positif Indonesia," *Politika Progresif: Jurnal Hukum, Politik dan Humaniora* 2, no. 1 (2025), hlm. 260-279.

[394] Tina Marjanov et al., "Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR," *Proceedings on Privacy Enhancing Technologies* Vol. 1, no. 3 (2023), hlm. 405-417.

Poin-poin penting yang perlu diperhatikan dalam kesenjangan antara regulasi dan Pancasila adalah sebagai berikut:[395]

a) Kesenjangan antara teori dan praktik regulasi

   UU PDP memberikan dasar hukum untuk perlindungan data pribadi, penerapannya masih sangat terbatas dalam banyak sektor, baik itu publik maupun swasta.

b) Ketidakjelasan mengenai penerapan sanksi

   Ketentuan mengenai sanksi, pengawasan terhadap pelanggaran tidak dilakukan secara tegas dan konsisten.

c) Ketimpangan dalam pengelolaan data pribadi

   Perusahaan besar yang memiliki sumber daya lebih mudah untuk mematuhi regulasi terkait perlindungan data pribadi, sementara perusahaan kecil dan menengah kesulitan untuk menyediakan sistem perlindungan yang setara.

Tantangan dalam harmonisasi ini adalah ketidakadilan yang timbul dari adanya regulasi yang hanya menguntungkan pihak tertentu, seperti korporasi besar atau mereka yang memiliki kekuatan politik. Misalnya, dalam regulasi perlindungan data pribadi, sering kali perusahaan memiliki hak untuk mengakses dan memanfaatkan data pribadi masyarakat tanpa persetujuan yang jelas. Hal ini bertentangan dengan prinsip keadilan sosial yang mengharuskan perlindungan hak individu. Dalam hal ini, regulasi harus lebih mengutamakan perlindungan bagi

[395] Ajisatria Suleiman, Pingkan Audrine, and Thomas Dewaranu, "Menjelaskan Kesenjangan Regulasi : Mengapa Pengaturan Bersama Dalam," *Center for Indonesian Policy Studies*, no. 1 May 2025 (2022), hlm. 1-15.

masyarakat luas, bukan hanya bagi kepentingan segelintir pihak yang memiliki kekuatan.

Regulasi perlindungan data pribadi harus lebih fleksibel namun tetap adil untuk mencakup perkembangan teknologi yang cepat. Negara harus mampu menyusun kebijakan yang dapat beradaptasi dengan perubahan zaman dan perkembangan teknologi yang terus berkembang. Teknologi informasi dan komunikasi yang semakin canggih mempengaruhi cara data pribadi dikumpulkan, disimpan, dan digunakan. Negara harus memastikan bahwa regulasi yang ada selalu relevan dengan perkembangan teknologi, sehingga perlindungan data pribadi tetap optimal di tengah perubahan yang pesat.

Perusahaan swasta yang mengelola data pribadi harus mengambil langkah-langkah proaktif untuk meningkatkan sistem keamanan mereka. Mereka harus berinvestasi dalam sistem perlindungan yang kuat, memastikan bahwa data pengguna tidak hanya disimpan dengan aman, tetapi juga hanya dapat diakses oleh pihak yang berwenang. Perusahaan juga perlu melaksanakan audit dan pengujian secara berkala untuk mendeteksi potensi celah dalam sistem mereka. Lembaga pengawas, seperti OJK, memiliki peran yang sangat penting dalam memastikan bahwa data pribadi masyarakat terlindungi dengan baik.[396] Lembaga-lembaga ini perlu meningkatkan fungsi pengawasan mereka terhadap implementasi regulasi perlindungan data pribadi. Selain itu, lembaga pengawas juga harus memberikan

[396] Rizqika Farah Isnugraheny, Zahra Ekasiwi Megawati, and Siti Susilawati, "Optimalisasi Prinsip Kerahasiaan Data Nasabah Dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi," *Media Hukum Indonesia (Mhi)* 2, no. 4 (2024).

pelatihan dan fasilitas untuk membantu perusahaan dalam memenuhi standar perlindungan data.

Masalah lain yang menyebabkan kesenjangan adalah ketimpangan dalam kapasitas dan kemampuan lembaga pengawas yang ada. Lembaga seperti OJK yang memiliki tugas untuk mengawasi pelaksanaan regulasi, tidak memiliki kapasitas yang cukup untuk memantau seluruh pelaksanaan kebijakan perlindungan data pribadi di sektor publik maupun swasta.[397] Oleh karena itu, ketidakmampuan lembaga pengawas dalam melaksanakan tugas mereka menambah kesenjangan yang ada, sehingga masyarakat tidak dapat merasakan perlindungan yang maksimal terhadap data pribadi mereka.

Kekurangan sumber daya pada lembaga pengawas menjadi tantangan besar dalam memastikan UU PDP diterapkan dengan baik. Kurangnya infrastruktur teknologi yang memadai menjadi salah satu faktor penghambat dalam implementasi UU PDP. Lembaga yang bertugas untuk mengawasi pengelolaan data pribadi sering kali kekurangan tenaga ahli yang berkompeten dalam bidang ini. Keterbatasan sumber daya manusia dan anggaran yang dimiliki oleh lembaga pengawas memperburuk masalah ini, sehingga pengawasan terhadap pengelolaan data pribadi di Indonesia menjadi sangat terbatas. Tanpa pengawasan yang memadai, kemungkinan pelanggaran terhadap perlindungan data pribadi akan terus meningkat. Banyak lembaga atau perusahaan yang tidak memiliki sistem keamanan data yang cukup untuk menghindari kebocoran data pribadi. Sistem keamanan yang

[397] Elda Septi Darmayanti dan Sidi Ahyar Wiraguna, "Tanggung Jawab Hukum Pinjaman Online Terhadap Penyebaran Data Nasabah Secara Ilegal," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025), hlm. 233-251.

lemah ini memberikan peluang besar bagi pelanggaran terhadap data pribadi untuk terjadi. Oleh karena itu, investasi dalam teknologi yang dapat melindungi data pribadi menjadi sangat penting untuk memastikan regulasi ini dapat diterapkan dengan efektif.

Kurangnya sumber daya pada lembaga pengawas menjadi tantangan besar dalam memastikan UU PDP diterapkan dengan baik. Lembaga yang bertugas untuk mengawasi pengelolaan data pribadi sering kali kekurangan tenaga ahli yang berkompeten dalam bidang ini. Keterbatasan sumber daya manusia dan anggaran yang dimiliki oleh lembaga pengawas memperburuk masalah ini, sehingga pengawasan terhadap pengelolaan data pribadi di Indonesia menjadi sangat terbatas. Tanpa pengawasan yang memadai, kemungkinan pelanggaran terhadap perlindungan data pribadi akan terus meningkat.[398]

Sistem pengawasan dan penegakan hukum yang efektif tidak hanya mengandalkan regulasi yang ada, tetapi juga pada integritas dan kompetensi lembaga pengawas. Lembaga pengawas yang independen dan profesional sangat penting untuk memastikan bahwa regulasi dilaksanakan dengan baik. Negara harus memberikan dukungan yang cukup kepada lembaga ini agar mereka dapat melakukan tugas mereka secara efektif dan tidak terbatas oleh keterbatasan sumber daya atau tekanan dari pihak lain.

Masalah utama yang dihadapi oleh lembaga pengawas saat ini adalah keterbatasan sumber daya manusia dan anggaran. Lembaga seperti OJK memiliki kewenangan untuk mengawasi sektor tertentu, namun pengawasan terhadap data

[398] Alfitri, Rahmawati, dan Firmansyah, *loc.cit*.

pribadi yang mencakup berbagai sektor, baik publik maupun swasta, sering kali terhambat karena kurangnya personel yang terlatih di bidang perlindungan data. Penambahan jumlah tenaga ahli yang memiliki pemahaman tentang teknologi informasi dan regulasi data pribadi harus menjadi prioritas. Selain itu, lembaga pengawas perlu diberikan anggaran yang memadai untuk menjalankan fungsinya dengan efektif.

Pengawasan yang efektif memerlukan independensi lembaga pengawas. Lembaga yang bertanggung jawab dalam mengawasi perlindungan data pribadi harus bebas dari pengaruh eksternal, baik dari pihak pemerintah maupun sektor swasta. 399 Tanpa adanya independensi yang kuat, proses pengawasan akan menjadi kurang transparan, dan kemungkinan terjadinya konflik kepentingan akan semakin besar. Oleh karena itu, untuk menciptakan sistem yang adil, lembaga pengawas harus diberikan kewenangan yang cukup serta dilengkapi dengan mekanisme yang memungkinkan mereka untuk bertindak tanpa adanya tekanan dari pihak lain.

Lembaga khusus yang memiliki otoritas lebih besar dalam hal perlindungan data pribadi yang bersifat spesifik menjadi penting. Lembaga ini tidak hanya akan bertanggung jawab untuk mengawasi penerapan UU PDP, tetapi juga akan memiliki wewenang untuk menetapkan standar dan pedoman yang jelas bagi semua pihak yang mengelola data pribadi. Pembentukan lembaga pengawas yang lebih

[399] Irfan Setiawan, *Pengawasan Pemerintahan Dalam Ulasan Teori Dan Praktek* (Bandung: CV. Rtujuh Media Printing, 2024). hlm. 41.

terfokus pada data pribadi akan mempercepat respons terhadap pelanggaran dan meningkatkan pengawasan terhadap pengelolaan data di berbagai sektor.

Lembaga pengawas yang ada perlu diberikan akses yang lebih besar untuk melakukan audit terhadap pengelolaan data pribadi. Pemerintah harus memastikan bahwa lembaga pengawas memiliki wewenang untuk melakukan audit secara reguler terhadap sektor-sektor yang mengelola data pribadi, baik itu sektor publik maupun swasta. Hal ini akan membantu mendeteksi pelanggaran lebih dini dan mencegah kebocoran data yang dapat merugikan masyarakat.400 Tanpa adanya audit yang transparan, potensi kebocoran atau penyalahgunaan data pribadi akan sulit dikendalikan.

Penerapan nilai-nilai Pancasila dalam perlindungan data pribadi juga mengharuskan adanya peran aktif pemerintah dalam memastikan bahwa kebijakan dan regulasi perlindungan data yang ada tidak hanya menguntungkan pihak tertentu, tetapi juga memastikan bahwa hak-hak individu terjaga secara adil.[401] Pemerintah harus bertanggung jawab untuk mengatasi kesenjangan ini dengan menyediakan mekanisme pengawasan yang lebih efektif, serta menjamin bahwa sanksi terhadap pelanggaran data pribadi ditegakkan dengan tegas. Penerapan prinsip-prinsip yang terkandung dalam Pancasila akan membantu menciptakan sistem perlindungan data yang lebih adil dan transparan.

---

[400] Yaffa Ivana Faustina and Sidi Ahyar Wiraguna, "Perlindungan Data Pengguna Oleh Marketplace Shopee Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882* 2, no. 2 (2025), hlm. 1037-1044.

[401] Ida Wahyuliana et al., "Pendidikan Karakter Melalui Pendidikan Pancasila Sebagai Upaya Preventif Penyalahgunaan Data Pribadi Dalam Perkembangan Iptek," *Jurnal Pancasila* 3, no. 1 (2022), hlm. 1-11.

Pemerintah perlu memperkuat regulasi dengan memberikan pedoman yang jelas tentang bagaimana perusahaan dan lembaga publik harus mengelola data pribadi sebagai bagian dari solusi untuk mengatasi kesenjangan ini. Regulasi yang ada perlu lebih berfokus pada hak-hak individu dan memastikan bahwa seluruh lapisan masyarakat mendapatkan perlindungan yang setara, tanpa terkecuali. Dengan demikian, kesenjangan antara regulasi yang ada dengan prinsip keadilan Pancasila dapat diminimalkan, menciptakan sistem perlindungan data yang lebih adil dan merata bagi seluruh rakyat Indonesia.

Penguatan regulasi dan pengawasan menjadi aspek yang sangat penting dalam memperbaiki sistem perlindungan data pribadi yang bersifat spesifik di Indonesia. Penyusunan regulasi yang lebih komprehensif dan penegakan hukum yang lebih tegas terhadap pelanggaran data pribadi sangat diperlukan untuk memastikan bahwa hak individu terhadap data pribadi terlindungi. Penyusunan regulasi ini harus disesuaikan dengan perkembangan teknologi yang sangat cepat, serta dengan mempertimbangkan perlindungan terhadap data pribadi yang bersifat spesifik.[402] Sanksi yang lebih berat harus diterapkan kepada perusahaan yang tidak mematuhi aturan perlindungan data pribadi.

Harmonisasi antara regulasi yang ada dengan prinsip-prinsip yang terkandung dalam Pancasila menjadi aspek yang sangat penting dalam pembangunan hukum di Indonesia. Pancasila, sebagai dasar negara, mengandung nilai-nilai yang harus diintegrasikan dalam setiap kebijakan dan regulasi yang

[402] Ridho Pakina and Mohammad Solekhan, "Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia," *Journal of Scientech Research and Development* 6, no. 1 (2024), hlm. 273-286.

dihasilkan. Namun, seringkali terdapat ketimpangan antara tujuan normatif yang tercantum dalam regulasi dengan implementasi di lapangan, yang berisiko mengabaikan kepentingan rakyat. Oleh karena itu, perlu adanya upaya untuk menyelaraskan setiap regulasi dengan nilai-nilai yang terkandung dalam Pancasila, khususnya dalam hal keadilan sosial.

Keadilan sosial perlu dijaga dalam regulasi juga membutuhkan evaluasi terhadap regulasi yang ada. Regulasi yang tidak mengutamakan keadilan sosial dapat menyebabkan ketimpangan sosial, dimana hanya segelintir pihak yang diuntungkan. Oleh karena itu, evaluasi regulasi yang ada harus dilakukan secara terus-menerus untuk melihat apakah regulasi tersebut sudah mencerminkan prinsip Pancasila, terutama dalam hal keadilan sosial, atau justru menguntungkan pihak-pihak tertentu yang memiliki kekuatan ekonomi lebih.[403]

Penguatan penegakan hukum merupakan langkah penting dalam memastikan kebijakan perlindungan data pribadi dapat dijalankan dengan efektif. Negara harus menerapkan sanksi yang tegas bagi pelanggar regulasi yang berkaitan dengan data pribadi. Tanpa penegakan hukum yang konsisten dan transparan, banyak pihak yang mungkin merasa tidak ada konsekuensi nyata terhadap pelanggaran data pribadi. Negara harus memastikan bahwa setiap pelanggaran terhadap data pribadi mendapat perhatian yang tepat dan dihukum sesuai dengan tingkat pelanggaran yang terjadi.

---

[403] Anang Dony Irawan, *Pancasila Sebagai Dasar Pembentukan Peraturan Perundang-Undangan Di Indonesia*, *Pengantar Hukum Indonesia* (CV. Gita Lentera, 2025). hlm. 28.

Negara juga harus memastikan bahwa sanksi yang diberikan kepada pelanggar data pribadi bersifat adil dan efektif. Sanksi yang diberikan harus memberikan perlindungan yang maksimal bagi individu yang hak privasinya dilanggar. Penerapan sanksi yang tidak konsisten atau tidak setimpal dengan tingkat pelanggaran dapat menurunkan tingkat kepatuhan terhadap regulasi yang ada. Oleh karena itu, negara memiliki kewajiban untuk memastikan bahwa setiap pelanggaran ditindak dengan cara yang adil dan transparan.

Negara harus terus berupaya untuk memperbaiki sistem perlindungan data pribadi yang bersifat spesifik, dengan menjadikan perlindungan data pribadi sebagai prioritas dalam kebijakan publik.[404] Negara harus terus melakukan evaluasi terhadap regulasi yang ada dan memastikan bahwa kebijakan perlindungan data pribadi tidak hanya sesuai dengan perkembangan zaman, tetapi juga mencerminkan nilai-nilai keadilan yang terkandung dalam Pancasila.

Penegakan hukum yang lemah menjadi hambatan besar dalam implementasi kebijakan perlindungan data pribadi. Banyak pelanggaran terhadap data pribadi yang tidak mendapat perhatian yang memadai, dan pelaku pelanggaran sering kali tidak diberikan sanksi yang setimpal.405 Penerapan sanksi yang jelas dan tegas terhadap pelanggaran data pribadi harus menjadi salah satu fokus utama dalam memperkuat pengawasan dan penegakan hukum. Tanpa adanya sanksi yang jelas, regulasi perlindungan data pribadi akan menjadi tidak efektif karena tidak ada efek jera bagi pelaku yang melanggar.

---

[404] Yuyut Prayuti, "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik e-Commerce Dan Perlindungan Data Konsumen Di Indonesia," *Jurnal Interpretasi Hukum* 5, no. 1 (2024), hlm. 903-913.

[405] Kriswandaru, Pratiwi, dan Suwardi, *loc.cit*.

Sanksi yang dikenakan terhadap pelanggar juga harus berimbang dan adil. Sering kali, pelanggaran terhadap data pribadi dilakukan oleh perusahaan besar yang memiliki sumber daya lebih banyak, sementara individu atau organisasi kecil yang melakukan pelanggaran mendapatkan sanksi yang lebih berat. Hal ini menimbulkan ketidakadilan dalam penegakan hukum dan membuat perlindungan data pribadi tampak tidak merata. Oleh karena itu, diperlukan sistem sanksi yang dapat menanggapi berbagai jenis pelanggaran dengan cara yang adil, sesuai dengan tingkat kerugian yang ditimbulkan.

Prinsip keadilan sosial dalam Pancasila harus dijadikan dasar untuk mengatur regulasi yang lebih mengutamakan kepentingan rakyat. Selama ini, banyak regulasi yang lebih menguntungkan pihak-pihak tertentu, seperti korporasi besar, ketimbang rakyat kecil yang seharusnya menjadi prioritas. Prinsip keadilan sosial dalam Pancasila mengharuskan regulasi yang mengatur hak dan kewajiban data pribadi juga mencerminkan keadilan bagi seluruh masyarakat.

Prinsip keadilan sosial dalam Pancasila juga mengandung pemahaman bahwa setiap individu harus diperlakukan dengan adil, tanpa adanya diskriminasi. Harmonisasi regulasi harus mempertimbangkan akses yang setara bagi semua kalangan, termasuk mereka yang memiliki akses terbatas terhadap informasi atau teknologi. Misalnya, dalam sektor pendidikan atau kesehatan, akses yang setara terhadap informasi dan layanan harus dijamin melalui regulasi yang berpihak pada masyarakat.

Negara memegang peran yang sangat penting dalam perlindungan data pribadi yang bersifat spesifik sebagai hak dasar setiap warga negara. Dalam konteks

ini, negara tidak hanya bertanggung jawab untuk menyusun dan menerapkan regulasi yang mengatur pengelolaan data pribadi, tetapi juga memastikan bahwa regulasi tersebut dapat memberikan perlindungan yang setara bagi seluruh lapisan masyarakat.[406] UU PDP yang telah disahkan menjadi landasan hukum yang diharapkan dapat menjamin hak setiap individu atas data pribadi mereka. Namun, implementasi regulasi ini memerlukan perhatian dan upaya yang lebih serius dari negara agar prinsip keadilan dapat terwujud dengan baik.

Pelindungan data pribadi yang bersifat spesifik mencakup lebih dari sekadar pengaturan siapa yang memiliki hak untuk mengakses data tersebut. Negara harus memastikan bahwa pengelolaan data pribadi dilakukan dengan penuh tanggung jawab oleh semua pihak yang terlibat.[407] Negara juga harus memperkuat pengawasan terhadap lembaga atau entitas yang mengelola data pribadi agar mereka mematuhi regulasi yang ada dan mengelola data dengan cara yang aman. Tanpa pengawasan yang efektif, risiko kebocoran data atau penyalahgunaan data akan tetap tinggi.

Rekonstruksi hukum yang berorientasi keadilan sosial perlu memuat skema kepatuhan berbasis risiko yang tetap menjamin standar minimum perlindungan bagi seluruh masyarakat, tanpa menciptakan beban yang tidak proporsional bagi pelaku usaha kecil. Pengaturan yang membedakan tingkat kewajiban berdasarkan volume pemrosesan, jenis data spesifik, dan profil risiko dapat disertai mekanisme pembinaan, pedoman teknis, serta insentif kepatuhan bagi UKM, termasuk

[406] Endiputra, Nasution, dan Febrian, *loc.cit*.
[407] Disemadi et al., *loc.cit*.

dukungan adopsi enkripsi, autentikasi berlapis, dan tata kelola retensi data. Keadilan sosial menuntut agar subjek data tidak dirugikan hanya karena bertransaksi dengan pelaku usaha yang kapasitasnya terbatas, sehingga negara wajib memastikan tersedianya standar keamanan minimum yang mengikat serta fasilitas kepatuhan yang realistis. [408] Pola ini menjaga keseimbangan antara perlindungan hak privasi dan keberlanjutan ekonomi, sekaligus mencegah lahirnya "kelas perlindungan" yang berbeda antara pengguna layanan korporasi besar dan pengguna layanan pelaku usaha kecil.

Kerjasama internasional dalam perlindungan data pribadi juga menjadi penting, mengingat banyaknya perusahaan global yang mengelola data pribadi masyarakat Indonesia. Dalam era globalisasi ini, penegakan hukum perlindungan data pribadi tidak dapat hanya mengandalkan hukum domestik. Oleh karena itu, Indonesia perlu memperkuat kerjasama dengan negara-negara lain untuk melindungi data pribadi warganya yang melibatkan perusahaan atau lembaga yang beroperasi di luar negeri.409

Pelindungan data pribadi juga memerlukan keterlibatan lebih besar dari sektor swasta. Banyak perusahaan yang memiliki data pribadi konsumen tidak selalu mematuhi regulasi yang ada. Penyalahgunaan data sering kali terjadi tanpa sepengetahuan konsumen, yang menunjukkan bahwa perlindungan data pribadi di sektor swasta masih sangat lemah. Pemerintah perlu lebih tegas dalam mengawasi

---

[408] Muhamad Rizal, Sinta Dewi Rosadi, and Agus Taryana, "Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia," *Journal of Law and Sustainable Development* Vol. 12, no. 1 (2024): hlm. 1-30.

[409] Jonathan Manurung and Tom Finaldin, "Peran ASEAN Melalui *Cybersecurity Cooperation Strategy* (ACCS) Dalam Menangani Kejahatan Siber Di Indonesia," *Global Mind* 7, no. 1 (2025), hlm. 31-38.

sektor swasta untuk memastikan bahwa perusahaan yang mengelola data pribadi mematuhi regulasi yang berlaku.[410] Pengawasan yang lebih ketat terhadap perusahaan yang mengelola data pribadi sangat penting agar data pribadi konsumen tidak jatuh ke tangan yang salah.

Penerapan teknologi keamanan yang lebih baik di seluruh sektor adalah elemen penting. Teknologi seperti enkripsi dan autentikasi dua faktor harus diterapkan secara lebih luas di semua sektor yang mengelola data pribadi. Ini akan membantu meningkatkan keamanan data pribadi dan mencegah terjadinya kebocoran data yang dapat merugikan individu. Dengan mengadopsi teknologi yang lebih canggih, sektor publik dan swasta dapat memberikan perlindungan yang lebih baik bagi data pribadi masyarakat.

Harmonisasi regulasi dengan Pancasila dapat tercapai dengan merekonstruksi undang-undang yang sudah ada. Beberapa undang-undang yang ada saat ini masih belum sepenuhnya mencerminkan prinsip keadilan sosial, sehingga perlu dilakukan pembaruan untuk memastikan bahwa regulasi tersebut lebih mengakomodasi kepentingan masyarakat luas.[411] Pembaruan ini juga harus melibatkan partisipasi masyarakat untuk memastikan bahwa suara rakyat didengar dalam proses penyusunan undang-undang.

Rekonstruksi undang-undang yang ada perlu dilakukan untuk memastikan bahwa regulasi tersebut lebih mengakomodasi kepentingan masyarakat luas. Pembaruan ini harus melibatkan partisipasi masyarakat. Partisipasi masyarakat

---

[410] Wardhono, Badrawani, Deviana, Pramudyastuti, et al., *loc.cit*.

[411] Firman Freaddy Busroh, Fatria Khairo, and Putri Difa Zhafirah, "Harmonisasi Regulasi Di Indonesia: Simplikasi Dan Sinkronisasi Untuk Peningkatan Efektivitas Hukum," *Jurnal Interpretasi Hukum* 5, no. 1 (2024), hlm. 699-711.

dalam perumusan regulasi sangat penting untuk memastikan bahwa regulasi tersebut sesuai dengan harapan masyarakat.

Pembaruan regulasi yang berfokus pada kesejahteraan sosial harus dilaksanakan dengan memperhatikan kemajuan teknologi dan dinamika sosial yang berkembang. Dalam hal ini, regulasi yang mengatur teknologi digital dan data pribadi harus dapat mengakomodasi perubahan zaman, sementara tetap berpegang pada nilai-nilai dasar dalam Pancasila.[412] Teknologi dapat menjadi alat yang sangat bermanfaat bagi kemajuan masyarakat, namun tanpa regulasi yang tepat, teknologi juga dapat disalahgunakan untuk kepentingan tertentu yang merugikan masyarakat.

Harmonisasi ini harus mempertimbangkan kebutuhan untuk menciptakan sistem hukum yang responsif terhadap perubahan sosial. Dalam dunia yang terus berubah, sistem hukum harus mampu mengadaptasi dengan cepat terhadap kebutuhan masyarakat. Oleh karena itu, regulasi yang ada harus mampu merespons tantangan sosial dan ekonomi yang muncul di masyarakat, dengan tetap memperhatikan prinsip-prinsip Pancasila, terutama dalam hal pemerataan dan keadilan.

Penerapan teknologi yang tepat sangat penting untuk mendukung pengawasan yang lebih efektif terhadap pengelolaan data pribadi.[413] Negara harus memastikan bahwa teknologi yang digunakan dalam pengelolaan data pribadi aman dan sesuai dengan regulasi yang ada. Teknologi seperti enkripsi dan sistem audit

---

[412] Iskandar Iskandar et al., "Analisis Kritis Terhadap Teori Hukum Murni Dalam Perkembangan Hukum Kontemporer," *TERAJU* 7, no. 01 (2025), hlm. 48-65.

[413] Desi Julianti, "Strategi Kebijakan Penguatan Pelayanan Publik Dan Pengawasan Perizinan Berusaha Dengan Aplikasi Berbasis Teknologi Informasi," *Kybernology Jurnal Ilmu Pemerintahan Dan Administrasi Publik* 2, no. 2 (2024), hlm. 324-363.

yang canggih dapat membantu meningkatkan pengawasan dan mencegah kebocoran data. Negara perlu mendukung penggunaan teknologi ini untuk memastikan perlindungan data pribadi yang lebih baik di semua sektor.

Penerapan teknologi juga harus disertai dengan pelatihan bagi lembaga-lembaga yang terlibat dalam pengelolaan data pribadi.[414] Banyak lembaga, baik sektor publik maupun swasta, yang tidak memiliki pemahaman yang cukup tentang cara melindungi data pribadi sesuai dengan regulasi. Tanpa pelatihan yang memadai, lembaga-lembaga ini mungkin tidak dapat mengelola data pribadi dengan baik, sehingga meningkatkan risiko kebocoran atau penyalahgunaan data.

Harmonisasi regulasi yang ada dengan kebutuhan masyarakat dan perkembangan teknologi sangat diperlukan. Negara tidak dapat mengabaikan tantangan yang ditimbulkan oleh globalisasi dan kemajuan teknologi yang terus berkembang. Oleh karena itu, regulasi yang ada harus fleksibel dan responsif terhadap perubahan yang terjadi dalam masyarakat dan dunia digital. Negara harus memastikan bahwa setiap regulasi yang diterapkan dapat mencerminkan keadilan sosial dan hak asasi manusia, sesuai dengan nilai-nilai Pancasila.

Kerja sama antara pemerintah, sektor swasta, dan masyarakat sangat diperlukan untuk memperkuat perlindungan data pribadi yang bersifat spesifik. Masyarakat harus diberdayakan untuk memahami hak mereka terkait dengan data pribadi, dan sektor swasta harus lebih transparan dalam pengelolaan data tersebut.[415] Negara harus memfasilitasi kolaborasi ini agar sistem perlindungan data

[414] Farhan A Yunani and Andi Aina Ilmih, "Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Perlindungan Data Pribadi," *Media Hukum Indonesia (MHI)* 2, no. 3 (2024).
[415] Fristanto dan Fikri, *loc.cit*.

pribadi dapat terlaksana dengan baik dan lebih efektif. Dengan adanya kerjasama yang solid antara berbagai pihak, perlindungan data pribadi dapat lebih terjamin dan menciptakan kepercayaan masyarakat terhadap sistem hukum yang ada.

Kolaborasi internasional juga tidak kalah penting dalam era globalisasi ini. Banyak perusahaan besar yang mengelola data pribadi di banyak negara, dan mereka beroperasi lintas batas negara. Negara harus memperkuat kerja sama dengan negara-negara lain untuk memastikan bahwa data pribadi masyarakat Indonesia terlindungi dengan baik, meskipun data tersebut dikelola oleh entitas asing. Penguatan kerja sama internasional ini juga akan mempermudah penegakan hukum terhadap pelanggaran data pribadi yang melibatkan perusahaan multinasional.

Pengawasan dan penegakan hukum data pribadi di Indonesia secara mutlak memerlukan sinergi kokoh antara pemerintah, swasta, dan masyarakat.[416] Negara wajib memfasilitasi ini melalui penguatan regulasi demi sistem perlindungan yang berkeadilan. [417] Kolaborasi internasional juga krusial mengingat masifnya perusahaan global yang memproses data warga Indonesia. Regulasi ketat dari negara lain dapat menjadi perbaikan tata kelola nasional. Terakhir, negara harus segera menyediakan sistem pelaporan terintegrasi yang mudah diakses bagi setiap korban pelanggaran data pribadi.

---

[416] Pakina dan Solekhan, *loc.cit*.

[417] Dwi Sinta Wati et al., "Dampak Cyber Crime Terhadap Keamanan Nasional Dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum," *Jurnal Bevinding* 2, no. 01 (2024), hlm. 44-55.

B. Unsur-unsur Rekonstruksi Sistem Hukum Perlindungan Data Pribadi yang Bersifat Spesifik Berbasis Nilai Keadilan Pancasila

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik memerlukan pendekatan sistemik dan komprehensif. Pendekatan ini secara mutlak harus membedah elemen-elemen sistem hukum yang mencakup substansi, struktur, dan budaya hukum, sekaligus mensinergikannya dengan asas kemanfaatan, keadilan, serta nilai-nilai dasar Pancasila.

Pelindungan data pribadi yang bersifat spesifik di era digital tidak lagi dapat dipahami semata-mata sebagai persoalan teknis keamanan informasi, melainkan telah berkembang menjadi persoalan hukum yang kompleks dan multidimensional.[418] Data yang bersifat spesifik, seperti data kesehatan, data biometrik, data genetika, data keuangan pribadi, data anak, dan data lain yang memiliki tingkat sensitivitas tinggi, memiliki karakter yang berbeda dari data pribadi yang bersifat umum. Perbedaan tersebut terletak pada besarnya potensi kerugian yang dapat timbul apabila data dimaksud diakses, diproses, disebarluaskan, atau disalahgunakan tanpa dasar yang sah. Dalam konteks inilah, hukum dituntut untuk hadir bukan hanya sebagai instrumen pengaturan formal, tetapi juga sebagai sarana perlindungan yang mampu memberikan kepastian, keadilan, dan kemanfaatan secara seimbang bagi seluruh warga negara.

Kebutuhan akan rekonstruksi hukum semakin mendesak ketika perkembangan teknologi digital berlangsung jauh lebih cepat dibandingkan

[418] Erni Muzairoh et al., "Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital Dalam Prespektif Hak Asasi Manusia," *Borobudur Law and Society Journal* 3, no. 1 (2024): hlm. 31-36.

kemampuan sistem hukum dalam menyesuaikan diri. Pemanfaatan artificial intelligence, big data, cloud computing, internet of things, serta integrasi sistem digital antar lembaga telah menciptakan cara-cara baru dalam pengumpulan, penyimpanan, analisis, dan pemrosesan data pribadi.[419] Perubahan tersebut membawa manfaat besar bagi efisiensi pelayanan publik, inovasi bisnis, dan pertumbuhan ekonomi digital. Namun di sisi lain, perubahan tersebut juga menimbulkan bentuk-bentuk kerentanan baru, seperti pemrosesan otomatis tanpa kendali yang memadai, kebocoran data lintas sistem, profiling yang diskriminatif, penyebaran data sensitif tanpa persetujuan yang bermakna, dan lemahnya akuntabilitas para pengendali data. Apabila hukum tidak direkonstruksi secara tepat, maka perkembangan teknologi justru berpotensi memperluas ketimpangan antara pihak yang menguasai teknologi dan data dengan masyarakat sebagai pemilik data.

Dalam perspektif tersebut, rekonstruksi hukum harus diarahkan untuk memperbaiki kelemahan mendasar yang masih terdapat dalam sistem perlindungan data pribadi yang bersifat spesifik di Indonesia. Kelemahan tersebut tidak hanya terletak pada tataran norma, tetapi juga pada kelembagaan penegakannya dan budaya hukum masyarakat maupun pelaku usaha. Pada sisi substansi, regulasi yang ada masih memerlukan penyempurnaan agar lebih operasional, adaptif, dan sensitif terhadap perkembangan teknologi baru. Pada sisi struktur, pengawasan dan penegakan hukum masih memerlukan penguatan kelembagaan yang independen,

[419] Muslimah, "Integrasi Ilmu Hukum Dan Teknologi Etika Dan Regulasi Dalam Era Digital," *Jurnal Hukum Dan Kolaborasi Keilmuan* 1, no. 1 (2025): hlm. 27-34.

profesional, dan memiliki kewenangan yang memadai. Sementara pada sisi budaya hukum, tantangan besar masih terlihat pada rendahnya literasi privasi, belum tumbuhnya budaya kepatuhan di sektor swasta, serta masih terbatasnya kesadaran masyarakat mengenai hak-hak mereka sebagai subjek data. Karena itu, rekonstruksi hukum tidak dapat dilakukan secara parsial, melainkan harus memandang ketiga unsur tersebut sebagai satu kesatuan yang saling memengaruhi.

Pendekatan yang berbasis substansi, struktur, dan budaya hukum menjadi penting karena hukum pada hakikatnya bukan hanya kumpulan norma tertulis, tetapi juga mencakup kelembagaan yang menjalankan norma tersebut dan kesadaran sosial yang menopangnya.[420] Norma yang baik tidak akan efektif apabila tidak didukung oleh struktur penegakan yang kuat. Sebaliknya, lembaga yang kuat juga tidak akan mampu bekerja optimal apabila norma yang menjadi dasar tindakannya masih kabur, tumpang tindih, atau tidak relevan dengan perkembangan zaman. Demikian pula, baik norma maupun struktur hukum akan kehilangan daya guna apabila masyarakat tidak memahami haknya, pelaku usaha tidak menginternalisasi kepatuhan sebagai kewajiban etik, dan negara tidak membangun budaya tata kelola data yang bertanggung jawab. Oleh sebab itu, unsur-unsur rekonstruksi yang ideal harus memadukan pembaruan norma, penguatan institusi, dan transformasi kesadaran hukum dalam satu kerangka kebijakan yang terpadu.

Dalam kerangka filsafat hukum Indonesia, rekonstruksi tersebut tidak boleh dilepaskan dari nilai-nilai Pancasila sebagai dasar negara dan cita hukum nasional.

---

[420] Maulana Syafi'i and Surya Sukti, "Transformasi Hukum Dalam Ruang Sosial: Relasi Antara Masyarakat, Nilai Keadilan, Dan Pembinaan Hukum," *AT-TAKLIM: Jurnal Pendidikan Multidisiplin* 2, no. 6 (2025): hlm. 689-701.

Pancasila menempatkan manusia sebagai makhluk bermartabat yang harus diperlakukan secara adil dan beradab. Oleh karena itu, perlindungan data pribadi yang bersifat spesifik harus dimaknai sebagai bagian dari penghormatan terhadap martabat manusia, bukan sekadar urusan administratif atau kepentingan teknokratis. Sila Kemanusiaan yang Adil dan Beradab menuntut agar setiap pemrosesan data dilakukan dengan penghormatan terhadap hak privasi dan otonomi individu. Sila Keadilan Sosial bagi Seluruh Rakyat Indonesia menegaskan bahwa perlindungan tersebut harus dinikmati secara setara oleh seluruh lapisan masyarakat, tanpa diskriminasi berdasarkan status ekonomi, akses teknologi, atau kedudukan sosial. Dengan demikian, unsur-unsur rekonstruksi hukum yang dibangun harus memastikan bahwa hukum benar-benar berpihak pada perlindungan warga negara sebagai subjek utama, bukan semata-mata mengakomodasi kepentingan negara atau korporasi.[421]

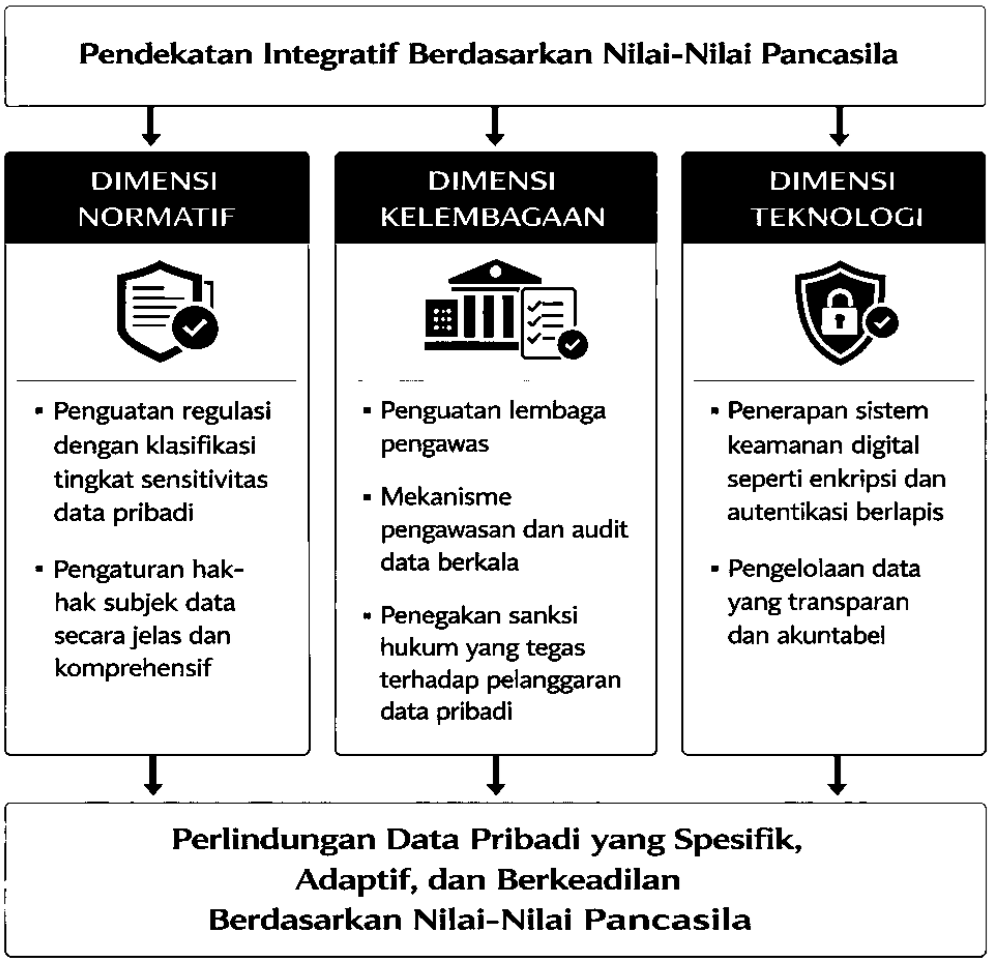
Perspektif keadilan Pancasila juga menghendaki agar rekonstruksi hukum tidak berhenti pada pendekatan formalistik, tetapi bergerak menuju keadilan substantif. Dalam konteks perlindungan data pribadi, keadilan substantif berarti bahwa regulasi harus mampu mencegah ketimpangan kekuasaan antara pengendali data dan subjek data, memberi ruang bagi pemulihan korban, dan menjamin adanya tanggung jawab nyata ketika terjadi pelanggaran. Rekonstruksi hukum juga harus memberi manfaat yang luas bagi masyarakat digital, yakni dengan menciptakan sistem yang aman, terpercaya, dan tetap membuka ruang bagi inovasi yang

[421] Iwandi Agung Manalu, Usman Usman Lubis, and Yati Sharfina Desiandri, "Hak Asasi Manusia Dan Keadilan Sosial: Analisis Implementasi Nilai-Nilai Pancasila Dalam Sistem Peradilan," *Innovative: Journal of Social Science Research* 4, no. 6 (2024): hlm. 5308-5316.

bertanggung jawab. Oleh karena itu, pembahasan mengenai unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik tidak cukup dilakukan hanya dari sudut peraturan perundang-undangan, tetapi juga harus dilihat sebagai bagian dari upaya besar membangun tata kelola hukum digital nasional yang berkeadilan, beretika, dan berorientasi pada perlindungan hak asasi manusia. Berangkat dari pemahaman tersebut, maka unsur-unsur rekonstruksi hukum yang dibahas selanjutnya perlu dianalisis melalui dimensi substansi hukum, struktur hukum, budaya hukum, serta integrasi nilai keadilan dan kemanfaatan dalam perspektif Pancasila.

Unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik dalam penelitian ini dibangun melalui pendekatan integratif yang mensinergikan dimensi normatif, kelembagaan, dan teknologi dengan berlandaskan nilai-nilai Pancasila. Dimensi normatif diwujudkan melalui penguatan regulasi yang mengatur klasifikasi tingkat sensitivitas data pribadi serta menjamin hak-hak subjek data secara jelas dan komprehensif. Dimensi kelembagaan diwujudkan melalui penguatan peran dan kewenangan lembaga pengawas, penerapan mekanisme pengawasan dan audit data secara berkala, serta penegakan sanksi hukum yang tegas terhadap pelanggaran data pribadi. Sementara itu, dimensi teknologi diwujudkan melalui penerapan standar keamanan digital seperti enkripsi, autentikasi berlapis, dan sistem pengelolaan data yang transparan dan akuntabel. Sinergi ketiga dimensi tersebut diharapkan mampu membentuk sistem perlindungan data pribadi yang lebih komprehensif, adaptif terhadap perkembangan teknologi, dan berkeadilan berdasarkan nilai-nilai Pancasila.

Bagan 4. 1. Bagan Unsur-unsur Rekonstruksi Hukum Pelindungan Data Pribadi Yang Bersifat Spesifik di Era Digital Untuk Mewujudkan Keadilan Berdasarkan Pancasila



Unsur-unsur ini mensinergikan tiga dimensi utama, yaitu dimensi normatif melalui penguatan regulasi dan pengaturan hak subjek data, dimensi kelembagaan melalui penguatan pengawasan, audit, dan penegakan sanksi, serta dimensi teknologi melalui penerapan sistem keamanan digital dan pengelolaan data yang transparan. Sinergi ketiga dimensi tersebut diarahkan untuk mewujudkan sistem perlindungan data pribadi yang lebih adaptif, efektif, dan berkeadilan berdasarkan Pancasila.

1. Rekonstruksi Substansi Hukum (*Legal Substance*)

Rekonstruksi substansi hukum menitikberatkan pada pembaruan norma tertulis agar lebih operasional dan proporsional. Formulasi kewajiban pengendali dan pemroses data wajib mengadopsi pendekatan berbasis risiko (*risk-based approach*). Pendekatan ini memungkinkan diferensiasi tingkat kewajiban berdasarkan skala pemrosesan, sensitivitas data, serta potensi dampak terhadap subjek data. Pembaruan norma mengharuskan penerapan *Data Protection Impact Assessment* (DPIA) bagi pemrosesan berisiko tinggi, serta merekonstruksi Pasal 4 UU PDP untuk mengklasifikasikan data kesehatan, biometrik, dan keuangan sebagai kategori dengan perlindungan ekstra mutlak.[422]

Tingkat sensitivitas data pribadi yang bersifat spesifik menuntut pembatasan yang sangat ketat karena dampak kebocorannya bersifat permanen dan merusak. Kebocoran data rekam medis dan genetika berisiko tinggi memicu diskriminasi sistemik, seperti penolakan klaim asuransi kesehatan atau eksklusi dalam rekrutmen tenaga kerja berdasarkan profil kerentanan penyakit masa depan.[423] Eksploitasi terhadap data keuangan pribadi turut membuka celah kejahatan siber yang berujung pada kehancuran finansial dan pencurian identitas (*identity theft*). Fakta empiris ini mendesak adanya rumusan substansi hukum yang mewajibkan pemrosesan data spesifik hanya dapat dilakukan dengan persetujuan eksplisit (*explicit consent*) dan standar enkripsi tertinggi.

---

[422] Muhammad Taufik and Fatimah Zahara, "Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)," *Jurnal Ilmu Hukum, Humaniora dan Politik* 4, no. 6 (September 14, 2024): hlm. 2378-2392.

[423] Rospita Siregar and Haposan Sinaga, "Aspek Hukum Perlindungan Data Pasien Dalam Penyelenggaraan Rekam Medis Elektronik Di Indonesia," *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 11, no. 1 (April 28, 2025): hlm. 106-116.

Perumusan ulang sanksi dan mekanisme ganti rugi menjadi bagian penting dalam rekonstruksi substansi hukum perlindungan data pribadi yang bersifat spesifik. Sanksi tidak boleh hanya diposisikan sebagai ancaman normatif, melainkan harus dirumuskan secara operasional, proporsional, dan efektif agar mampu menimbulkan efek jera bagi setiap pelanggar. Dalam konteks ini, pelanggaran terhadap data pribadi yang bersifat spesifik harus dibedakan berdasarkan tingkat kesalahan, skala dampak, serta jenis data yang diproses, sehingga dimungkinkan adanya pengenaan sanksi administratif, perdata, maupun pidana secara bertingkat. Di samping itu, hukum juga harus menjamin adanya mekanisme ganti rugi yang jelas bagi korban, baik berupa kompensasi finansial, pemulihan hak, maupun tindakan korektif lain yang dapat memulihkan posisi subjek data. Dengan demikian, rekonstruksi hukum tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada pemulihan yang adil bagi pihak yang dirugikan.

Rekonstruksi substansi hukum perlu mempertegas batasan tujuan pemrosesan, jangka waktu penyimpanan, serta kewajiban penghapusan data setelah tujuan pemrosesan terpenuhi. Kejelasan norma mengenai prinsip purpose limitation, data minimization, dan storage limitation menjadi penting agar pengendali data tidak memproses atau mempertahankan data pribadi yang bersifat spesifik secara berlebihan. Di samping itu, hukum harus mewajibkan transparansi yang utuh kepada subjek data mengenai dasar hukum pemrosesan, risiko yang mungkin timbul, serta pihak-pihak yang dapat menerima akses atas data tersebut.

2. Rekonstruksi Struktur Hukum (*Legal Structure*)

Efektivitas norma hukum perlindungan data sangat bergantung pada kekuatan struktur kelembagaan yang menegakkannya. Penguatan kelembagaan pengawas menuntut desain tata kelola yang menjamin independensi struktural, fungsional, dan anggaran. Independensi struktural mengharuskan lembaga pengawas ini terbebas dari subordinasi langsung kementerian teknis guna menghindari konflik kepentingan. Independensi fungsional memberikan jaminan bahwa kewenangan investigasi, pemeriksaan, audit kepatuhan, dan penjatuhan sanksi dapat dijalankan tanpa intervensi politik atau tekanan ekonomi.[424] Rekonstruksi hukum perlu merumuskan secara eksplisit kewenangan lembaga tersebut dalam memberikan perintah penghentian pemrosesan serta menjatuhkan denda administratif yang mengikat, sehingga penegakan hukum berjalan secara operasional.

Rekonstruksi struktur hukum juga menuntut adanya koordinasi kelembagaan yang kuat antarinstansi yang memiliki keterkaitan dengan perlindungan data pribadi. Dalam praktiknya, penanganan pelanggaran data pribadi tidak dapat dibebankan hanya pada satu lembaga, karena persoalan ini menyentuh aspek keamanan siber, tata kelola sistem elektronik, penegakan hukum, dan pengawasan sektoral secara bersamaan. Oleh karena itu, diperlukan koordinasi yang jelas antara lembaga pengawas independen, kementerian atau otoritas teknis seperti Kominfo, BSSN, aparat penegak hukum, serta lembaga pengawas sektoral lainnya. Koordinasi tersebut harus mencakup pertukaran informasi, standar respons insiden,

[424] Dwiky Arianto and Wafda Vivid Izziyana, "Peran Strategis Dewan Pengawas Syariah (DPS) Dalam Struktur Kelembagaan Keuangan Syariah," *Ghanimah: Journal of Sharia Economics and Business* 2, no. 1 (2026): hlm. 26-39.

mekanisme audit bersama, serta pembagian kewenangan yang tegas agar tidak terjadi tumpang tindih maupun kekosongan tindakan. Dengan struktur koordinasi yang demikian, penegakan hukum terhadap pelanggaran data pribadi akan menjadi lebih cepat, efektif, dan terintegrasi.

Penguatan struktur hukum tidak hanya berhenti pada pembentukan dan koordinasi kelembagaan, tetapi juga harus memastikan tersedianya mekanisme kerja yang transparan, akuntabel, dan mudah diakses oleh masyarakat. Dalam konteks perlindungan data pribadi yang bersifat spesifik, struktur hukum yang efektif harus mampu menyediakan jalur pengaduan yang sederhana, cepat, dan responsif bagi subjek data yang haknya dilanggar. Masyarakat harus memiliki kepastian ke mana pengaduan diajukan, bagaimana proses penanganannya berlangsung, serta bentuk pemulihan apa yang dapat diperoleh apabila terbukti terjadi pelanggaran. Oleh karena itu, lembaga pengawas tidak hanya berfungsi sebagai institusi pengawasan administratif, tetapi juga sebagai simpul utama dalam penyelesaian sengketa data pribadi, pemberian rekomendasi korektif, serta fasilitator pemulihan korban.

Penguatan struktur hukum juga memerlukan dukungan sumber daya manusia yang profesional dan memiliki kompetensi lintas bidang, baik di bidang hukum, keamanan siber, audit sistem elektronik, maupun forensik digital. Tanpa kapasitas teknis yang memadai, lembaga pengawas akan sulit menjalankan fungsi pengawasan secara optimal, terutama dalam menghadapi modus pelanggaran data yang semakin kompleks.

3. Rekonstruksi Kemanfaatan dan Keadilan

Hukum yang direkonstruksi wajib menghadirkan keseimbangan antara perlindungan hak privasi dan keberlanjutan inovasi. Formulasi norma berbasis risiko berfungsi menciptakan ekosistem ekonomi digital yang tumbuh secara inklusif tanpa mengorbankan keamanan masyarakat. Keadilan distributif menuntut perlindungan ekstra bagi kelompok rent[425] an seperti pemilik data medis dan biometrik agar mereka tidak menjadi korban eksploitasi oleh pemegang kendali teknologi. Rekonstruksi ini memastikan bahwa negara tidak menciptakan beban kepatuhan yang mematikan pelaku usaha mikro dan kecil, melainkan memberikan skema pembinaan dan dukungan teknis agar kepatuhan standar keamanan minimum dapat dicapai oleh seluruh lapisan industri.

Integrasi nilai keadilan dalam rekonstruksi hukum perlindungan data pribadi perlu mencakup keadilan korektif dan keadilan restoratif secara seimbang. Keadilan korektif menghendaki agar setiap pelanggaran terhadap data pribadi diikuti dengan tindakan hukum yang dapat memperbaiki kerugian yang timbul, baik melalui penghentian pemrosesan yang melanggar, penghapusan data yang diperoleh secara tidak sah, maupun pemberian kompensasi kepada korban. Sementara itu, keadilan restoratif menekankan pentingnya pemulihan hubungan hukum dan sosial yang terganggu akibat pelanggaran data, termasuk melalui kewajiban pelaku untuk memulihkan rasa aman, memperbaiki sistem pengelolaan data, dan menjamin tidak terulangnya pelanggaran serupa. Dalam konteks masyarakat digital, kedua

[425] Bagus Hermanto et al., "Diskursus Epistemologis Dalam Pembentukan Hukum Digital: Quo Vadis Navigasi Perundang-Undangan Indonesia Kedepan," *Jurnal Ilmu Perundang-Undangan* 2, no. 1 (2026): hlm. 14-26.

pendekatan ini menjadi penting karena kerugian akibat kebocoran atau penyalahgunaan data tidak selalu berhenti pada aspek ekonomi, tetapi juga menyentuh reputasi, martabat, dan kepercayaan publik. Oleh sebab itu, rekonstruksi hukum harus memastikan bahwa keadilan tidak hanya hadir dalam bentuk sanksi, tetapi juga dalam bentuk pemulihan yang nyata dan berkelanjutan.

Pelindungan Pelindungan data pribadi yang bersifat spesifik pada hakikatnya merupakan bagian dari perlindungan hak asasi manusia, khususnya hak atas privasi sebagai hak dasar yang melekat pada setiap individu. Dalam perspektif ini, data pribadi bukan sekadar objek administratif atau komoditas ekonomi, melainkan bagian dari identitas, kehormatan, dan otonomi pribadi yang wajib dihormati dan dilindungi oleh negara. Oleh karena itu, rekonstruksi hukum perlindungan data pribadi harus menempatkan *privacy as a human right* sebagai landasan utama dalam perumusan norma, kelembagaan, dan mekanisme penegakan hukumnya.

Negara berkewajiban memastikan bahwa setiap orang memiliki kendali atas data pribadinya, memperoleh perlindungan dari pemrosesan yang sewenang-wenang, serta mendapatkan akses terhadap upaya hukum yang efektif ketika hak privasinya dilanggar. Dengan menempatkan privasi sebagai bagian dari hak asasi manusia, rekonstruksi hukum perlindungan data pribadi tidak hanya memperkuat kepastian hukum dan perlindungan hak warga negara, tetapi juga mempertegas komitmen konstitusional negara dalam menjunjung tinggi martabat manusia di tengah perkembangan teknologi dan transformasi digital yang semakin pesat. Dengan demikian, hak privasi terlindungi.

4. Rekonstruksi Budaya Hukum (*Legal Culture*)

Keberhasilan rekonstruksi hukum bertumpu pada terbangunnya budaya kepatuhan dan kesadaran privasi. Peningkatan literasi privasi dan edukasi publik mengenai risiko serta hak-hak atas data pribadi menjadikan masyarakat lebih sadar, kritis, dan berdaya di ruang digital. Masyarakat yang teredukasi akan secara aktif menuntut transparansi dan menolak eksploitasi datanya. Sektor swasta dan korporasi pada saat yang bersamaan didorong untuk meninggalkan paradigma lama yang memandang perlindungan data sekadar beban regulasi (*regulatory burden*). Korporasi wajib menginternalisasi perlindungan data sebagai standar etika tata kelola bisnis dan menerapkan prinsip *privacy by design* sejak tahap awal perancangan sistem teknologi mereka.[426]

Budaya hukum dalam perlindungan data pribadi yang bersifat spesifik juga menuntut keterlibatan aktif lembaga pendidikan, pemerintah, media, dan masyarakat sipil dalam membangun kesadaran kolektif mengenai pentingnya privasi di era digital. Literasi digital tidak cukup hanya dipahami sebagai kemampuan menggunakan teknologi, tetapi juga harus mencakup kemampuan memahami risiko pemrosesan data, membaca kebijakan privasi secara kritis, serta mengetahui langkah hukum yang dapat ditempuh apabila terjadi pelanggaran. Dalam konteks ini, pembentukan budaya hukum berarti menumbuhkan kebiasaan untuk tidak memberikan data pribadi secara sembarangan, meningkatkan kehati-

[426] Nurul Hidayati Indra Ningsih et al., *Hukum Ekonomi Digital: Regulasi Bisnis Di Era Teknologi* (PT. Nawala Gama Education, 2025), hlm. 149.

hatian dalam penggunaan layanan digital, serta memperkuat keberanian masyarakat untuk menuntut akuntabilitas dari pengendali data.

Budaya hukum yang kuat juga mensyaratkan perubahan orientasi dalam tubuh korporasi dan institusi publik. Kepatuhan terhadap perlindungan data tidak boleh dipandang semata-mata sebagai kewajiban administratif, melainkan sebagai bagian dari integritas kelembagaan dan tanggung jawab sosial. Setiap organisasi yang memproses data pribadi harus membangun tata kelola internal yang mendukung etika perlindungan data, mulai dari pelatihan sumber daya manusia, penguatan standar operasional, hingga pembentukan mekanisme pengawasan internal yang konsisten. Dengan demikian, budaya hukum yang terbentuk akan menjadi landasan penting bagi efektivitas rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik secara berkelanjutan.

Penguatan substansi hukum ini menemukan pijakan moralitasnya dalam perspektif *maqāṣid al-syarī'ah*, khususnya prinsip *ḥifẓ al-'irḍ* (perlindungan kehormatan) dan *ḥifẓ al-māl* (perlindungan harta). Ajaran Islam secara tegas menempatkan data pribadi sebagai wujud nyata dari ruang privat dan martabat kemanusiaan yang kesuciannya haram untuk dilanggar secara eksploitatif.[427] Rekonstruksi substansi hukum perlindungan data pada akhirnya bukan sekadar pemenuhan standar regulasi global, melainkan manifestasi kewajiban negara untuk mencegah kezaliman digital. Formulasi norma hukum positif harus mencerminkan

[427] Sinta Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (June 28, 2018): hlm. 88-110.

penghormatan absolut terhadap martabat manusia agar hak asasi subjek data terjamin secara substantif.

Pancasila sebagai *rechtsidee* (cita hukum) merupakan fondasi filosofis mutlak dalam seluruh tahapan rekonstruksi ini. Sila "Kemanusiaan yang Adil dan Beradab" mengamanatkan bahwa perlindungan data spesifik merupakan bagian tak terpisahkan dari perlindungan martabat manusia. Eksploitasi data sensitif merupakan serangan langsung terhadap harkat kemanusiaan. Sila "Keadilan Sosial bagi Seluruh Rakyat Indonesia" menuntut agar setiap individu mendapatkan perlindungan yang setara tanpa adanya diskriminasi status ekonomi maupun sosial. Sinergi nilai-nilai dasar ini dengan hukum modern menempatkan perlindungan data pribadi sebagai instrumen rekayasa sosial (*law as a tool of social engineering*) yang mewujudkan tata kelola ruang digital yang beretika dan beradab.[428]

Unsur-unsur rekonstruksi hukum yang ideal dalam perspektif Pancasila harus dibangun tidak hanya atas kepastian norma, tetapi juga keberpihakan pada manusia sebagai subjek hukum. Rekonstruksi ini perlu mengintegrasikan moral, keadilan sosial, dan tanggung jawab negara agar perlindungan data pribadi spesifik menjamin keamanan, kemanfaatan, dan penghormatan hak privasi warga digital.

Dalam kerangka tersebut, unsur-unsur rekonstruksi hukum yang ideal tidak boleh berhenti pada perumusan norma yang bersifat deklaratif, tetapi harus diarahkan pada pembentukan sistem perlindungan yang benar-benar operasional, efektif, dan responsif terhadap dinamika perkembangan teknologi. Hukum harus

[428] Muhammad Yasir, "Rekonstruksi Regulasi Pemeriksaan Tersangka Yang Berbasis Nilai Keadilan Pancasila" (Semarang: Universitas Islam Sultan Agung (Indonesia), 2024).

mampu hadir sebagai instrumen yang memberikan kepastian sekaligus perlindungan nyata, terutama ketika data pribadi yang bersifat spesifik diproses dalam lingkungan digital yang kompleks, terhubung, dan rentan terhadap penyalahgunaan. Oleh karena itu, unsur-unsur rekonstruksi hukum yang dibangun harus menempatkan subjek data bukan sebagai objek administrasi semata, melainkan sebagai pemilik hak yang memiliki kedudukan utama dalam keseluruhan proses pemrosesan data. Dalam perspektif ini, setiap mekanisme pengumpulan, penyimpanan, penggunaan, pemindahan, dan penghapusan data pribadi harus selalu berorientasi pada penghormatan terhadap hak privasi, keamanan, dan martabat manusia.

Unsur-unsur rekonstruksi hukum yang ideal juga harus menegaskan bahwa keadilan dalam perlindungan data pribadi yang bersifat spesifik tidak hanya dimaknai sebagai perlakuan yang sama secara formal, tetapi sebagai perlindungan yang proporsional sesuai dengan tingkat kerentanan dan risiko yang melekat pada jenis data tersebut. Data kesehatan, data biometrik, data genetika, data keuangan pribadi, dan data anak tidak dapat diperlakukan sama dengan data pribadi umum, karena kebocoran atau penyalahgunaannya memiliki dampak yang lebih berat, lebih sensitif, dan lebih sulit dipulihkan.[429] Oleh sebab itu, hukum yang direkonstruksi harus memberi perlindungan berlapis melalui pengaturan klasifikasi data yang lebih tegas, standar keamanan yang lebih tinggi, persyaratan persetujuan yang lebih ketat, serta mekanisme pengawasan yang lebih tajam. Dengan demikian,

[429] Johan Wijaya, Aji Titin Roswitha Nursanthy, and Muhammad Arganata Thamrin, "Perlindungan Terhadap Data Pribadi Dalam Berselancar Di Dunia Maya," *The Juris* 8, no. 2 (2024): hlm. 638-644.

keadilan tidak hanya hadir pada tataran konsep, tetapi benar-benar diwujudkan dalam bentuk perlakuan hukum yang memberikan perhatian khusus terhadap data yang paling rentan menimbulkan ketidakadilan.

Unsur-unsur rekonstruksi hukum yang ideal harus mengintegrasikan tanggung jawab negara secara lebih nyata dan terukur. Negara tidak cukup hanya berperan sebagai pembentuk regulasi, tetapi juga harus menjadi penjamin aktif atas efektivitas perlindungan data pribadi. Tanggung jawab tersebut mencakup penyediaan kerangka hukum yang adaptif, pembentukan lembaga pengawas yang independen, penegakan hukum yang konsisten, penyediaan mekanisme pengaduan yang mudah diakses, serta jaminan pemulihan bagi korban pelanggaran data pribadi.[430] Dalam perspektif Pancasila, negara tidak boleh membiarkan warga negara menghadapi risiko digital secara sendiri-sendiri, terlebih ketika ketimpangan teknologi dan informasi membuat posisi masyarakat jauh lebih lemah dibandingkan korporasi atau institusi yang menguasai data. Oleh karena itu, unsur-unsur rekonstruksi hukum yang ideal harus menempatkan negara sebagai pelindung yang aktif, adil, dan bertanggung jawab dalam menjaga keseimbangan antara kepentingan inovasi digital, pertumbuhan ekonomi, dan perlindungan hak-hak warga negara.

Dalam masyarakat digital, data memang menjadi sumber daya yang penting bagi pengembangan layanan, efisiensi kebijakan, dan kemajuan ekonomi. Namun, pemanfaatan data tidak boleh dibenarkan apabila mengorbankan kebebasan

[430] Muhammad Putra Syawal Al Mahdi and Irwan Triadi, "Dari Rectsvaccum Menuju Kepastian Hukum: Pembentukan Lembaga Perlindungan Data Pribadi Sebagai Penemuan Hukum Di Era Digital," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 12, no. 11 (2025): hlm. 4416-4430.

individu, menghilangkan kontrol subjek data atas informasinya, atau membuka ruang bagi eksploitasi tersembunyi.[431] Karena itu, rekonstruksi hukum yang ideal harus membangun keseimbangan yang wajar antara perlindungan hak privasi dengan kepentingan pemanfaatan data yang sah. Keseimbangan tersebut dapat dicapai melalui prinsip pembatasan tujuan, minimalisasi data, akuntabilitas pengendali data, audit kepatuhan, serta kewajiban transparansi yang memungkinkan masyarakat memahami bagaimana datanya digunakan. Dengan rekonstruksi seperti ini, hukum tidak menjadi penghambat kemajuan, tetapi justru menjadi pagar normatif agar kemajuan teknologi tetap berada dalam jalur yang beradab.

Perlindungan yang efektif tidak akan pernah tercapai apabila masyarakat tidak memahami hak-haknya, korporasi tidak menginternalisasi kepatuhan sebagai nilai etis, dan aparatur negara tidak memandang privasi sebagai hak asasi yang harus dijaga.[432] Oleh karena itu, rekonstruksi hukum harus disertai dengan pembangunan kesadaran kolektif mengenai pentingnya privasi, literasi digital, serta pembentukan tata kelola yang transparan dan akuntabel. Dalam hal ini, Pancasila memberikan landasan yang kuat, karena nilai kemanusiaan, keadilan sosial, tanggung jawab moral, dan semangat gotong royong sesungguhnya dapat menjadi dasar pembentukan budaya perlindungan data yang lebih bermartabat. Dengan demikian, unsur-unsur rekonstruksi hukum yang ideal bukan hanya menghasilkan

[431] Gerasela et al., "Perkembangan Ilmu Pengetahuan Dan Teknologi: Menyongsong Era Baru Dalam Prespektif Ilmu Sosial," *PESHUM : Jurnal Pendidikan, Sosial dan Humaniora* 4, no. 4 (June 4, 2025): hlm. 5983-5989.

[432] Yusuf Daeng et al., "Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi," *Innovative: Journal Of Social Science Research* 3, no. 6 (November 30, 2023): hlm. 2898-2905.

aturan yang lebih baik, tetapi juga membentuk ekosistem hukum digital yang berkeadilan, beretika, dan berpihak pada manusia sebagai subjek utama dalam kehidupan bernegara.

Unsur-unsur rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik dalam perspektif Pancasila harus dipahami sebagai upaya membangun sistem hukum yang utuh, yaitu sistem yang mampu menyatukan dimensi moral, normatif, kelembagaan, dan sosial dalam satu kerangka perlindungan yang berkeadilan. Rekonstruksi tersebut harus memastikan bahwa hukum tidak sekadar hadir sebagai teks, tetapi sebagai sarana nyata untuk mencegah ketidakadilan digital, memulihkan kerugian korban, mengendalikan kekuasaan pengelola data, dan menjaga martabat warga negara.

C. Rekonstruksi Hukum Pelindungan Data Pribadi Yang Bersifat Spesifik Terhadap Perkembangan Teknologi Di Era Digital Yang Sesuai Dengan Nilai-Nilai Keadilan Berdasarkan Pancasila

Pelindungan data pribadi yang bersifat spesifik telah menjadi isu yang semakin penting di era digital saat ini. Banyaknya kasus kebocoran data yang melibatkan berbagai pihak, baik itu lembaga publik maupun swasta, menunjukkan bahwa sistem perlindungan data pribadi yang ada saat ini belum cukup memadai.[433] Rekonstruksi hukum yang lebih kuat dan jelas diperlukan untuk memastikan bahwa data pribadi setiap individu terlindungi dengan baik. Rekonstruksi hukum ini memberi dampak signifikan terhadap sektor swasta yang mengelola data pribadi. Pihak-pihak swasta yang memiliki akses ke data pribadi harus lebih berhati-hati

[433] Erikha and Hoesein, *loc.cit*.

dalam mengelola data yang mereka kumpulkan. Dengan adanya regulasi yang ketat, perusahaan harus memastikan bahwa data pribadi yang mereka miliki dilindungi dengan baik dan digunakan hanya untuk tujuan yang sah. Hal ini akan menuntut perusahaan untuk meningkatkan sistem pengamanan data mereka. Rekonstruksi hukum ini akan memperkenalkan mekanisme pelaporan yang lebih efektif bagi masyarakat.

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik juga perlu menegaskan asas proporsionalitas, legalitas, dan pembatasan tujuan sebagai prinsip fundamental dalam setiap tindakan pemrosesan data. Asas proporsionalitas menuntut agar setiap pembatasan hak privasi dilakukan secara sah, diperlukan, dan seimbang dengan tujuan yang hendak dicapai, khususnya dalam konteks kepentingan umum atau keamanan nasional. Asas legalitas mengharuskan seluruh kegiatan pemrosesan memiliki dasar hukum yang jelas dan dapat diuji, sehingga tidak membuka ruang diskresi yang berlebihan bagi pengendali data. Pembatasan tujuan *(purpose limitation)* menghendaki agar data pribadi hanya digunakan sesuai dengan tujuan awal pengumpulannya dan tidak diperluas tanpa persetujuan yang sah dari subjek data.[434] Penegasan asas-asas tersebut akan memperkuat kepastian hukum serta mencegah praktik penyalahgunaan kewenangan, baik oleh sektor publik maupun privat.

Penegakan hukum yang tegas dan konsisten menjadi pilar utama keberhasilan perlindungan data pribadi yang bersifat spesifik. Sistem sanksi perlu mencakup

[434] Dwi Ratna Indri Hapsari and Kukuh Dwi Kurniawan, "Consumer Protection: Principle of Proportionality in Banking Credit Agreement under the Indonesian Law," *Fiat Justisia: Jurnal Ilmu Hukum* 14, no. 4 (2020), 337–352.

sanksi administratif (misalnya pencabutan izin atau pembatasan operasional) dan sanksi pidana (denda dan hukuman penjara) yang proporsional dengan tingkat pelanggaran dan dampaknya, terutama pada kebocoran massal atau penyalahgunaan untuk penipuan dan pencurian identitas. Proses peradilan yang cepat, transparan, dan didukung alat teknologi yang memadai memungkinkan deteksi dini pelanggaran, penindakan yang efektif, serta peningkatan kepercayaan publik terhadap sistem hukum. Kerja sama internasional juga krusial mengingat arus data lintas batas dan keterlibatan perusahaan multinasional.[435]

Strategi implementasi yang tepat sangat penting untuk mengatasi masalah ini, termasuk dengan memperbaiki regulasi yang ada dan memperkenalkan mekanisme baru yang lebih efektif.[436] Salah satu langkah pertama dalam strategi implementasi adalah pembentukan regulasi yang lebih komprehensif. Pembaruan regulasi ini harus dapat mengakomodasi berbagai jenis data pribadi yang lebih beragam dan lebih sensitif, seperti data medis, data biometrik, dan data keuangan. Regulasi yang lebih komprehensif juga harus mencakup penyusunan aturan mengenai siapa yang dapat mengakses data pribadi, serta dengan tujuan apa data tersebut digunakan. Masyarakat yang merasa hak-haknya dilanggar akan lebih mudah untuk melaporkan penyalahgunaan data pribadi. Pemerintah harus memastikan bahwa setiap pelaporan yang diterima dapat ditindaklanjuti dengan cepat dan efisien.

---

[435] Shafa Salsabila and Sidi Ahyar Wiraguna, "Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan data pribadi yang bersifat spesifik Indonesia," *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 2, no. 2 (2025), hlm. 145-157.

[436] Mahameru et al, *loc.cit.*

Strategi implementasi harus mencakup penyusunan pedoman dan standar pengelolaan data pribadi yang jelas bagi semua pihak yang terlibat. Pengelola data pribadi harus memiliki pedoman yang dapat mereka ikuti dalam setiap tahap pengelolaan data. Pedoman ini mencakup cara pengumpulan, penyimpanan, penggunaan, dan penghapusan data pribadi. Standar pengelolaan data yang jelas akan membantu menghindari penyalahgunaan data dan memberikan perlindungan yang lebih kuat terhadap privasi individu. [437] Mekanisme pengaduan dan penyelesaian sengketa yang efektif harus tersedia untuk masyarakat. Ketika individu merasa bahwa hak data pribadi mereka telah dilanggar, mereka harus memiliki saluran yang jelas untuk mengajukan keluhan dan mendapatkan penyelesaian yang adil.

Rekonstruksi hukum yang bersifat spesifik juga harus mengintegrasikan kewajiban penerapan *Data Protection Impact Assessment* (DPIA) atau penilaian dampak perlindungan data bagi kegiatan pemrosesan yang berisiko tinggi terhadap hak dan kebebasan individu. Kewajiban ini penting terutama dalam penggunaan teknologi kecerdasan buatan, sistem pemantauan berskala besar, pemrosesan data biometrik, serta penggabungan basis data lintas sektor. Penilaian dampak tersebut harus dilakukan sebelum pemrosesan dimulai dan didokumentasikan secara akuntabel, termasuk identifikasi risiko, langkah mitigasi, serta mekanisme pengawasan internal. [438] Konstruksi norma yang mewajibkan DPIA akan

[437] Tiara Shafa Putri and Moody Rizqy Syailendra Putra, "Implementasi Undang-Undang Pelindungan data pribadi yang bersifat spesifik: Peran Manajemen Risiko Hukum Bagi Prosesor Data Pribadi," *Jurnal Hukum Lex Generalis* 5, no. 4 (2024).

[438] Laurens Vandercruysse, Caroline Buts, and Michaël Dooms, "A Typology of Smart City Services: The Case of Data Protection Impact Assessment," *Cities* Vol. 104, no. 1 (2020), hlm. 1-15.

mendorong budaya kehati-hatian *(due diligence)* dan pencegahan dini, sehingga perlindungan hukum tidak bersifat reaktif setelah terjadi pelanggaran. Pendekatan preventif ini sejalan dengan nilai kemanusiaan yang adil dan beradab, karena menempatkan perlindungan hak individu sebagai pertimbangan utama sejak tahap perencanaan sistem.

Sinergi antara pemerintah, korporasi, dan masyarakat menjadi kunci terwujudnya keadilan pada era digital. Pemerintah berperan sebagai pembuat kebijakan dan pengawas, korporasi sebagai pengelola data yang wajib patuh regulasi sekaligus menjunjung etika penggunaan data, sedangkan masyarakat sebagai pemilik data yang aktif menjaga dan menuntut haknya. [439] Proses penyusunan kebijakan yang inklusif, berbasis musyawarah, serta didukung pedoman dan standar yang jelas bagi lembaga pengawas akan menciptakan sistem perlindungan data pribadi yang bersifat spesifik yang lebih responsif, adil, dan adaptif terhadap perkembangan teknologi, sekaligus memperkuat kepercayaan pada ekosistem digital dan perekonomian nasional.

Pengelola data harus menyediakan mekanisme penyelesaian sengketa yang dapat diakses oleh semua pihak yang terlibat dalam pengelolaan data pribadi. Mekanisme ini akan membantu menyelesaikan masalah tanpa harus melalui jalur peradilan yang rumit. Penetapan sanksi administratif yang efektif juga merupakan bagian penting dari strategi ini. Pengelola data pribadi yang tidak mematuhi regulasi harus dikenakan sanksi administratif, seperti denda atau pembatasan izin

[439] Alfredo Nainggolan, Ivo E Lumbantoruan, and Sahata Manalu, "Eksistensi Negara Hukum Dalam Era Digital," *MIMBAR KEADILAN: Jurnal Ilmu Hukum* 1, no. 3 (2024): hlm. 62-70.

operasional. Sanksi ini harus cukup berat untuk memberikan efek jera dan memastikan bahwa pengelolaan data pribadi dilakukan dengan penuh tanggung jawab.

Sanksi administratif dapat meningkatkan keseriusan perusahaan dalam melindungi data pribadi yang mereka kelola.[440] Pengawasan terhadap lembaga pemerintah yang mengelola data pribadi juga perlu diperkuat. Data pribadi yang dikelola oleh sektor publik sering kali memiliki tingkat sensitivitas yang tinggi. Oleh karena itu, lembaga pemerintah harus diawasi dengan ketat untuk memastikan bahwa data pribadi masyarakat dikelola sesuai dengan regulasi yang berlaku. Pengawasan ini akan meningkatkan akuntabilitas lembaga publik dalam pengelolaan data pribadi.

Partisipasi masyarakat dalam pengelolaan data pribadi adalah hal enting untuk diutamakan. Masyarakat harus diberdayakan untuk mengontrol data pribadi mereka dan untuk melaporkan pelanggaran yang terjadi. Partisipasi aktif masyarakat dalam pengelolaan data pribadi akan menciptakan sistem perlindungan yang lebih efektif, dimana masyarakat memiliki peran penting dalam menjaga privasi mereka.[441] Oleh karena itu, partisipasi masyarakat harus menjadi bagian dari strategi implementasi yang ada.

Ketersediaan mekanisme audit dan evaluasi secara berkala juga diperlukan. Pengelola data pribadi harus menjalani audit untuk memastikan bahwa pengelolaan

---

[440] Budiandru Budiandru and Rahmad Sujud Hidayat, "Tanggung Jawab Hukum Marketplace Terhadap Kebocoran Data Pribadi Pengguna Dalam Perspektif UU ITE Dan UU Perlindungan Data Pribadi," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 3 (2025), 7738–7743.

[441] Angnesia and Wiraguna, *loc.cit*.

data dilakukan sesuai dengan regulasi yang berlaku. Audit ini harus dilakukan secara rutin dan melibatkan pihak yang independen untuk memastikan transparansi dalam pengelolaan data pribadi. Evaluasi juga akan membantu dalam mengidentifikasi kelemahan yang ada dalam sistem perlindungan data dan mencari solusi untuk perbaikan.

Penyusunan rencana darurat dalam menghadapi kebocoran data atau serangan siber juga harus menjadi bagian dari strategi implementasi. Pengelola data pribadi harus memiliki prosedur yang jelas untuk mengatasi kebocoran data dan serangan siber yang dapat merusak integritas data pribadi. Prosedur ini harus mencakup langkah-langkah mitigasi yang cepat dan efektif untuk mengurangi dampak dari kebocoran data.[442] Pengembangan dan penerapan teknologi baru yang dapat meningkatkan efisiensi pengelolaan data pribadi akan menjadi faktor kunci dalam strategi. Teknologi baru seperti *blockchain* dan kecerdasan buatan dapat digunakan untuk meningkatkan keamanan data dan efisiensi pengelolaan data pribadi.[443] Dengan memanfaatkan teknologi ini, pengelolaan data pribadi dapat dilakukan dengan lebih aman, efisien, dan transparan, sehingga memberikan perlindungan yang lebih kuat terhadap privasi individu.

Penguatan lembaga pengawas yang independen dan memiliki kewenangan yang cukup juga merupakan bagian penting dari strategi implementasi ini. Tanpa adanya lembaga pengawas yang kuat, pengelolaan data pribadi akan terus

---

[442] Mohamad Soleh and Zubakhrum Tjenreng, "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital," *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics* 11, no. 1 (2025), hlm. 1-10.

[443] Alwi Al Hadad, "Keamanan Data Dalam Proses Pemilu 2024: Identifikasi Dan Mitigasi Ancaman Kebocoran Data Elektoral," *Jurnal Keadilan Pemilu* 4, no. 2 (2023), hlm. 86-98.

menghadapi tantangan besar.[444] Lembaga ini harus diberi kewenangan untuk melakukan audit, mengawasi pengelolaan data, serta memberikan sanksi yang tegas jika terjadi pelanggaran terhadap data pribadi. Penguatan lembaga pengawas ini akan memastikan bahwa pengelola data pribadi dapat mematuhi regulasi yang ada.

Penerapan teknologi yang aman dan dapat diandalkan juga merupakan aspek penting dalam strategi. Penggunaan teknologi yang canggih untuk melindungi data pribadi harus menjadi standar yang diterapkan oleh semua pihak yang terlibat dalam pengelolaan data. Enkripsi, sistem autentikasi yang kuat, dan proteksi yang lebih baik terhadap data yang disimpan harus diimplementasikan untuk memastikan bahwa data pribadi tidak jatuh ke tangan yang salah. Teknologi harus diperbarui secara berkala untuk mengatasi potensi ancaman yang muncul seiring dengan perkembangan teknologi.[445]

Pengembangan sistem pelaporan yang efisien dan cepat sangat penting dalam strategi implementasi ini. Masyarakat harus diberi saluran yang jelas dan mudah diakses untuk melaporkan pelanggaran atau kebocoran data pribadi. Tanpa sistem pelaporan yang efisien, banyak pelanggaran yang tidak dapat segera ditangani.[446] Oleh karena itu, sistem pelaporan yang responsif dan mudah digunakan oleh masyarakat akan mempermudah penegakan hukum dan memberikan perlindungan yang lebih baik terhadap data pribadi.

---

[444] Muhamad Adri Rinjani and Ricky Firmansyah, "Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 8, no. 1 (2025), hlm. 70-83.

[445] Indryana Widi Ardhianty, "Tantangan Dan Strategi Perlindungan Konsumen Pada Layanan Perbankan Di Tengah Kemajuan Teknologi," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 2 (2025), hlm. 151-162.

[446] Erikha and Hoesein, *loc.cit*.

Rekonstruksi hukum dalam perlindungan data pribadi yang bersifat spesifik merupakan langkah krusial dalam memastikan bahwa hak individu atas data pribadi terlindungi dengan baik di era digital.[447] Mengingat pentingnya data pribadi dalam kehidupan sehari-hari, masyarakat berhak untuk merasa aman dan terlindungi dari potensi penyalahgunaan data mereka oleh pihak yang tidak bertanggung jawab.[448] Proses rekonstruksi hukum ini tidak hanya berdampak pada pengelolaan data pribadi, tetapi juga membawa implikasi signifikan terhadap masyarakat dan pemerintah. Oleh karena itu, pemahaman yang mendalam tentang dampak tersebut sangat penting untuk membangun kebijakan yang efektif dan adil.[449]

Rekonstruksi hukum yang baik dapat memperkuat sistem perlindungan data pribadi, yang pada gilirannya akan memberikan dampak positif pada hak individu. Perlindungan yang kuat terhadap data pribadi akan mengurangi risiko kebocoran atau penyalahgunaan data yang dapat merugikan individu secara sosial dan ekonomi. Melalui regulasi yang jelas, setiap individu dapat lebih mengontrol data pribadi mereka dan merasa lebih aman dalam berbagi informasi di ruang digital.

Penguatan kelembagaan pengawas perlu disertai dengan desain tata kelola yang menjamin independensi struktural, fungsional, dan anggaran. Independensi struktural menuntut agar lembaga pengawas tidak berada di bawah subordinasi langsung kementerian teknis yang berpotensi menimbulkan konflik kepentingan. Independensi fungsional mengharuskan kewenangan investigasi, pemeriksaan, dan

---

[447] Ahmad Ihsan Amri and Y A Triana Ohoiwutun, "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana," *Opinia de Journal* 4, no. 1 (2024), hlm. 13-26.

[448] Fuad, Baskara, dan Urbaningrum, *loc.cit*.

[449] Cindy Gladys Pratiwi Sianturi, Roida Nababan, and Ria Juliana Siregar, "Peran Hukum Dalam Melindungi Data Pribadi," *Innovative: Journal Of Social Science Research* 4, no. 5 (2024), hlm. 2607-2624.

penjatuhan sanksi dapat dijalankan tanpa intervensi politik atau tekanan ekonomi. Dukungan anggaran yang memadai menjadi syarat agar fungsi pengawasan, audit kepatuhan, serta edukasi publik dapat terlaksana secara efektif. [450] Rekonstruksi hukum perlu merumuskan secara eksplisit kewenangan lembaga tersebut dalam memerintahkan penghentian pemrosesan, menjatuhkan denda administratif yang signifikan, serta mengeluarkan rekomendasi kebijakan yang mengikat. Pengaturan demikian akan memperkuat prinsip akuntabilitas dan menjamin bahwa perlindungan data pribadi yang bersifat spesifik tidak sekadar normatif, melainkan operasional dan dapat ditegakkan.

Implikasi rekonstruksi hukum dapat membawa dampak positif bagi masyarakat, terutama dalam hal kesadaran terhadap hak privasi. Masyarakat akan lebih memahami pentingnya melindungi data pribadi mereka dari penyalahgunaan, serta memahami mekanisme yang tersedia untuk melaporkan jika hak mereka dilanggar.[451] Peningkatan kesadaran ini akan menciptakan masyarakat yang lebih waspada terhadap ancaman terkait data pribadi dan lebih aktif dalam melindungi hak mereka. Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik memperkuat tanggung jawab negara dalam menjaga hak privasi warga, baik terhadap pengelolaan data oleh sektor publik maupun swasta.

Negara berkewajiban menyediakan regulasi yang jelas, mekanisme pengawasan yang efektif, serta kebijakan yang menyeimbangkan kebutuhan pengelolaan data dengan hak privasi individu. Peningkatan transparansi menjadi

---

[450] Sonny Langingi and Rochmad Abu Bakar, "Pengawasan Terhadap Lembaga Negara Independen: Antara Independensi Dan Akuntabilitas," *Lentera: Multidisciplinary Studies* Vol. 3, no. 4 (2025), hlm. 749-766.

[451] Pakina and Solekhan, *loc.cit*.

dampak penting, karena pemerintah dan pelaku usaha harus menjelaskan secara terbuka bagaimana data dikumpulkan, digunakan, disimpan, dan kepada siapa data dibagikan, sehingga kepercayaan masyarakat terhadap sistem perlindungan data meningkat.[452]

Peningkatan transparansi dalam pengelolaan data akan menjadi salah satu dampak dari rekonstruksi hukum ini. Pemerintah dan sektor swasta yang mengelola data pribadi akan diwajibkan untuk memberikan informasi yang jelas dan terbuka mengenai bagaimana data pribadi digunakan. Hal ini akan mendorong rasa saling percaya antara masyarakat dan lembaga yang mengelola data pribadi.

Mekanisme pelaporan yang baik akan mempercepat proses penyelesaian sengketa terkait data pribadi dan memberikan rasa aman kepada masyarakat.[453] Penegakan hukum yang tegas sangat dibutuhkan untuk memberikan efek jera kepada pihak-pihak yang tidak mematuhi regulasi perlindungan data pribadi yang bersifat spesifik. Pihak yang melanggar regulasi harus dikenakan sanksi yang sesuai, agar tidak terjadi pelanggaran yang serupa di masa depan. Dengan adanya regulasi yang lebih jelas, masyarakat akan memperoleh perlindungan yang lebih besar terhadap penyalahgunaan data pribadi. Pemerintah dapat menciptakan mekanisme yang memudahkan masyarakat untuk mengetahui hak-hak mereka dan bagaimana cara mereka dapat melaporkan pelanggaran terkait data pribadi. Hal ini

---

[452] Asep Mahbub Junaedi, "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian dan Pengembangan* 5, no. 2 (2025), hlm. 247-257.

[453] Alvian Dwiangga Wijaya and Teddy Prima Anggriawan, "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi Di Smartphone," *Inicio Legis* 3, no. 1 (2022), hlm. 63-72.

berpotensi mengurangi jumlah kasus penyalahgunaan data pribadi yang sering terjadi di sektor publik dan swasta. [454]

Dampak terhadap pemerintah juga mencakup kebutuhan untuk meningkatkan kapasitas lembaga pengawas. Lembaga pengawas harus dilengkapi dengan alat dan sumber daya yang memadai agar dapat menjalankan fungsi mereka dengan efisien. Pengawasan yang lemah akan mengurangi efektivitas dari regulasi yang ada, sehingga penting bagi pemerintah untuk terus memperkuat lembaga pengawas agar mereka dapat bertindak secara efektif. [455] Pendidikan publik terkait pentingnya perlindungan data pribadi juga menjadi salah satu aspek yang perlu ditekankan dalam rekonstruksi hukum ini. Masyarakat perlu diberi pengetahuan yang cukup mengenai hak-hak mereka terkait dengan data pribadi dan cara untuk melindungi data mereka di dunia maya. Peningkatan literasi mengenai hak privasi akan membuat masyarakat lebih sadar akan pentingnya melindungi informasi pribadi mereka.

Peningkatan literasi privasi dan edukasi publik mengenai risiko serta hak-hak atas data pribadi menjadikan masyarakat lebih sadar, kritis, dan berdaya dalam menjaga keamanan informasi pribadinya di ruang digital.[456] Regulasi yang lebih tegas memberikan perlindungan lebih besar terhadap penyalahgunaan data pribadi sekaligus menyediakan mekanisme pengaduan yang mudah diakses bagi

---

[454] Muhammad Gustryan and Zainal Arifin Hoesein, "Peran Undang-Undang ITE Dan Undang-Undang Perlindungan Data Pribadi Dalam Perlindungan Data Dan Privasi Di Era Ekonomi Digital," *Jurnal Minfo Polgan* Vol. 14, no. 2 (2025): hlm. 3333-3343.

[455] Irvita et al., *loc.cit*.

[456] Friska Yulanda Pratiwi and Fajar Rachmad Dwi Miarsa, "Urgensi Edukasi Publik Dalam Menangkal Penyalahgunaan Data Pribadi," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (2025), hlm. 1342-1349.

masyarakat. Masyarakat memperoleh kepastian mengenai hak untuk mengetahui, mengakses, memperbaiki, dan meminta penghapusan data pribadi mereka, serta cara melaporkan pelanggaran yang terjadi.

Pengawasan yang lebih ketat akan memastikan bahwa sektor swasta mematuhi regulasi yang ada dan menjaga transparansi dalam pengelolaan data pribadi. Sektor swasta terdorong untuk meningkatkan standar tata kelola dan keamanan data melalui rekonstruksi hukum ini. Perusahaan harus memastikan bahwa data pribadi hanya digunakan untuk tujuan yang sah, dilindungi dengan infrastruktur dan teknologi yang memadai, serta dikelola secara transparan.[457] Lembaga pengawas yang dibentuk dalam rangka implementasi rekonstruksi hukum ini akan memiliki kewenangan yang lebih besar untuk mengaudit dan memantau penggunaan data pribadi. Pengawasan terhadap pengelolaan data pribadi oleh sektor swasta juga harus diperketat.

Pengawasan yang lebih ketat oleh lembaga pengawas, melalui audit dan pemantauan berkelanjutan, memastikan kepatuhan terhadap regulasi dan mencegah praktik pengelolaan data yang melanggar hak privasi individu. Penerapan standar teknis yang lebih jelas juga membantu mengurangi celah pelanggaran.[458] Dari perspektif ekonomi, rekonstruksi hukum ini dapat menciptakan pasar yang lebih sehat. Pelindungan data pribadi yang kuat akan meningkatkan kepercayaan konsumen terhadap layanan yang ditawarkan oleh sektor swasta. Konsumen yang

[457] Pakina and Solekhan, *loc.cit*.
[458] *Ibid*.

merasa aman dalam berbagi data pribadi mereka dengan perusahaan akan lebih cenderung untuk menggunakan layanan yang ditawarkan.

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik juga perlu memperhatikan pendekatan berbasis risiko *(risk-based approach)* dalam merumuskan kewajiban pengendali dan pemroses data. Pendekatan ini memungkinkan diferensiasi tingkat kewajiban berdasarkan skala pemrosesan, sensitivitas data, serta potensi dampak terhadap subjek data. Pengendali data dengan volume besar dan risiko tinggi harus dikenakan standar kepatuhan yang lebih ketat, termasuk kewajiban audit eksternal, pelaporan berkala, dan penunjukan pejabat perlindungan data. Pelaku usaha mikro dan kecil tetap wajib mematuhi prinsip dasar perlindungan data, namun dapat diberikan skema pembinaan dan dukungan teknis agar kepatuhan tidak menjadi beban yang tidak proporsional. [459] Formulasi norma berbasis risiko akan menciptakan keseimbangan antara perlindungan hak privasi dan keberlanjutan pertumbuhan ekonomi digital, sekaligus mencerminkan keadilan substantif sebagaimana diamanatkan dalam nilai-nilai Pancasila.

Rekonstruksi Pasal 4 UU PDP yang mengklasifikasikan data pribadi menjadi data umum dan data pribadi yang bersifat spesifik perlu dilakukan dengan merujuk pada pengaturan *special categories of personal data*, yang secara eksplisit memasukkan data kesehatan, biometrik, genetika, orientasi seksual, dan keyakinan sebagai kategori yang mendapat perlindungan ekstra dan hanya boleh diproses

[459] Gunsu Nurmansyah, Rudi Natamiharja, and Ikhsan Setiawan, "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach," *Pancasila and Law Review* Vol. 6, no. 1 (2025): hlm. 15-44.

dengan syarat yang jauh lebih ketat. Sementara itu, *PDPA* Singapura tidak membagi secara eksplisit ke dalam kategori "umum" dan "spesifik", tetapi mengenakan kewajiban yang lebih ketat pada organisasi melalui *consent obligation*, *purpose limitation*, dan *protection obligation* terhadap seluruh data yang berpotensi menimbulkan dampak serius bagi individu.[460]

Penguatan Pasal 4 harus memastikan keadilan distributif dan pengakuan (*à la Nancy Fraser*) dengan menjamin bahwa kelompok rentan misalnya pemilik data kesehatan, biometrik, dan keyakinan mendapat perlindungan yang lebih tinggi sejalan dengan nilai kemanusiaan yang adil dan beradab dalam Pancasila. Melalui *Middle Range Theory* (Teori Perlindungan Hukum), klasifikasi ulang ini harus menghadirkan rumusan norma yang lebih jelas, operasional, dan dapat ditegakkan, sehingga aparat penegak dan pelaku usaha memiliki kepastian mengenai standar pengelolaan data spesifik. Adapun dalam kerangka *Applied Theory* (Teori Hukum Pembangunan), Pasal 4 yang direkonstruksi perlu dirancang sebagai instrumen rekayasa sosial yang mendorong ekosistem ekonomi *digital* Indonesia tumbuh secara inklusif, tetap diselaraskan dengan nilai keadilan sosial Pancasila dan kebutuhan pembangunan nasional.

Rekonstruksi Pasal 28 sampai dengan Pasal 32 UU PDP yang mengatur hak-hak subjek data pribadi perlu mengadopsi, *PDPA* Singapura memfokuskan pada *access and correction obligation*, yaitu kewajiban organisasi untuk memberikan akses dan melakukan koreksi atas data pribadi bila diminta, disertai kewajiban

[460] Sinta Dewi et al., "The Role of International Mediation in Data Protection and Privacy Law-Can It Be Effective?," *University of New South Wales Law Research Series* Vol. 1, no. 1 (2019): hlm. 61-73.

keamanan dan pembatasan retensi.[461] Penguatan hak-hak subjek data ini mencerminkan keadilan prosedural dan partisipatoris: warga tidak lagi menjadi objek pasif, melainkan subjek yang berdaya untuk menentukan nasib data pribadinya, sejalan dengan sila Kerakyatan dan Keadilan Sosial. Dalam *Middle Range Theory* (Teori Perlindungan Hukum), rekonstruksi Pasal 28–32 harus diterjemahkan ke dalam mekanisme yang konkret misalnya batas waktu respon permohonan akses/koreksi, prosedur sederhana dan murah, serta kewajiban dokumentasi sehingga perlindungan hukum tidak berhenti pada teks, tetapi efektif di tingkat implementasi. Sementara itu, *Applied Theory* (Teori Hukum Pembangunan) menuntut agar hak-hak ini dirumuskan dengan mempertimbangkan kapasitas infrastruktur *digital* Indonesia: desainnya harus mendorong transformasi *digital* yang berkeadilan (misalnya melalui *privacy by design* dan sistem *dashboard* hak privasi), bukan justru menjadi beban administratif yang menghambat inovasi, sehingga lahir rekonstruksi hukum yang khas dengan citra Indonesia namun sejajar dengan praktik terbaik global.

Analisis rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik juga memperoleh legitimasi nilai dari perspektif data kewahyuan dalam ajaran Islam. Al-Qur'an menegaskan pentingnya menjaga kehormatan dan privasi individu sebagai bagian dari perlindungan terhadap martabat manusia. Hal ini tercermin dalam Surah Al-Hujurat ayat 12 yang melarang perbuatan *tajassus* atau mencari-cari informasi pribadi orang lain tanpa hak. Larangan tersebut

[461] Muchamad Taufiq and Ananda Salsabila Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR," *International Journal of Business, Law, and Education,* Vol. 6, no. 2 (2025): hlm. 1260-1268.

menunjukkan bahwa pengambilan atau penyebaran informasi pribadi tanpa izin merupakan tindakan yang bertentangan dengan prinsip etika dalam Islam. Dalam konteks era digital, tindakan mengakses, mengumpulkan, atau menyebarkan data pribadi yang bersifat sensitif tanpa persetujuan yang sah dapat dipandang sebagai bentuk modern dari pelanggaran privasi yang dilarang oleh ajaran tersebut.

Prinsip persetujuan (*consent*) yang menjadi salah satu asas utama dalam perlindungan data pribadi yang bersifat spesifik modern juga memiliki dasar normatif dalam Al-Qur'an. Surah An-Nur ayat 27 menegaskan kewajiban meminta izin sebelum memasuki ruang privat seseorang, yang secara substantif mencerminkan prinsip penghormatan terhadap hak individu untuk mengendalikan akses terhadap wilayah pribadinya. Dalam konteks pengelolaan data pribadi di era digital, prinsip ini dapat dimaknai sebagai kewajiban bagi pengendali data untuk memperoleh persetujuan yang sah dari subjek data sebelum melakukan pemrosesan terhadap data pribadi yang bersifat spesifik. Prinsip tersebut sejalan dengan asas legalitas dan pembatasan tujuan dalam regulasi perlindungan data pribadi yang bersifat spesifik, dimana setiap pemrosesan data harus memiliki dasar hukum yang jelas dan tujuan yang sah.

Penguatan perlindungan terhadap data pribadi juga sejalan dengan hadis Nabi Muhammad SAW yang diriwayatkan oleh Imam Muslim yang menyatakan bahwa darah, harta, dan kehormatan seorang Muslim adalah suci dan tidak boleh dilanggar oleh orang lain. Dalam masyarakat digital modern, data pribadi dapat dipahami sebagai bagian dari kehormatan dan identitas individu yang harus dijaga dari penyalahgunaan. Dengan demikian, rekonstruksi hukum perlindungan data pribadi

yang bersifat spesifik tidak hanya memiliki dasar dalam teori hukum modern dan nilai keadilan Pancasila, tetapi juga memperoleh penguatan dari nilai etika keagamaan yang menempatkan penghormatan terhadap martabat manusia sebagai prinsip fundamental dalam kehidupan bermasyarakat.

Perspektif data kewahyuan tersebut juga dapat dipahami dalam kerangka tujuan syariat (*maqāṣid al-syarī'ah*), khususnya prinsip *ḥifẓ al-'irdh* (perlindungan kehormatan) dan *ḥifẓ al-māl* (perlindungan harta). Dalam konteks masyarakat digital, data pribadi yang bersifat spesifik sering kali memiliki nilai ekonomi dan sosial yang tinggi sehingga memerlukan perlindungan yang kuat agar tidak disalahgunakan. Oleh karena itu, rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik dapat dipandang sebagai bagian dari upaya menjaga kehormatan, keamanan, dan hak individu dalam kehidupan modern. Sinergi antara nilai-nilai Pancasila, teori hukum modern, dan prinsip etika yang bersumber dari data kewahyuan menunjukkan bahwa perlindungan data pribadi yang bersifat spesifik merupakan bagian dari upaya mewujudkan keadilan sosial serta membangun tata kelola ruang digital yang beretika, berkeadaban, dan berorientasi pada penghormatan terhadap martabat manusia.

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik dalam penelitian ini diarahkan pada penguatan norma yang mengatur klasifikasi data pribadi, jaminan hak subjek data, serta efektivitas mekanisme penegakan hukum terhadap pelanggaran pengelolaan data pribadi. Fokus rekonstruksi ditempatkan pada Pasal 4 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan data pribadi yang bersifat spesifik yang mengatur klasifikasi data pribadi, Pasal 28

hingga Pasal 32 yang mengatur hak-hak subjek data, serta Pasal 58 hingga Pasal 64 yang mengatur sanksi administratif. Ketiga kelompok norma tersebut memiliki keterkaitan langsung dengan perlindungan data pribadi yang bersifat spesifik yang memiliki tingkat sensitivitas lebih tinggi dibandingkan data pribadi yang bersifat umum. Penguatan norma tersebut diperlukan agar perlindungan terhadap data pribadi yang bersifat spesifik mampu memberikan kepastian hukum serta perlindungan yang efektif bagi individu di era digital.

Pasal 4 ayat (2) UU PDP mengatur klasifikasi data pribadi menjadi data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Data pribadi yang bersifat spesifik meliputi data kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, serta data keuangan pribadi. Pengaturan tersebut menunjukkan pengakuan bahwa terdapat jenis data yang memiliki tingkat sensitivitas lebih tinggi dibandingkan dengan data lainnya. Rumusan norma yang ada belum memberikan definisi yang jelas mengenai kriteria data pribadi yang bersifat spesifik. Norma yang berlaku juga belum menetapkan standar perlindungan yang lebih ketat terhadap pengelolaan data pribadi yang sensitif. Kondisi tersebut menunjukkan adanya kelemahan pengaturan yang berpotensi menimbulkan kerentanan terhadap penyalahgunaan data pribadi yang bersifat spesifik.

Rekonstruksi terhadap Pasal 4 ayat (2) diarahkan pada penegasan definisi data pribadi yang bersifat spesifik sebagai data yang memiliki tingkat sensitivitas tinggi dan berpotensi menimbulkan kerugian serius bagi subjek data apabila disalahgunakan. Rekonstruksi norma juga diarahkan pada penambahan kategori data sensitif yang relevan dengan perkembangan teknologi digital seperti data

identitas digital, data lokasi presisi, serta data yang berkaitan dengan keyakinan atau identitas pribadi. Rumusan norma hasil rekonstruksi perlu memuat kewajiban bagi pengendali data untuk menerapkan standar keamanan yang lebih tinggi terhadap pemrosesan data pribadi yang bersifat spesifik. Ketentuan tersebut memberikan perlindungan yang lebih kuat terhadap data sensitif serta mencegah potensi penyalahgunaan yang dapat merugikan individu secara sosial maupun ekonomi.

Pasal 28 hingga Pasal 32 UU PDP mengatur hak-hak subjek data yang meliputi hak memperoleh informasi mengenai pemrosesan data pribadi, hak mengakses data pribadi, hak memperbaiki data yang tidak akurat, serta hak untuk menghapus data pribadi. Pengaturan tersebut menunjukkan bahwa UU PDP telah mengakui posisi subjek data sebagai pihak yang memiliki kendali atas data pribadinya. Implementasi norma tersebut dalam praktik masih menghadapi berbagai kendala. Mekanisme pelaksanaan hak subjek data belum sepenuhnya mudah diakses oleh masyarakat. Ketentuan mengenai batas waktu pemenuhan permohonan subjek data juga belum diatur secara rinci dalam undang-undang.

Rekonstruksi terhadap Pasal 28 hingga Pasal 32 diarahkan pada penguatan mekanisme pelaksanaan hak-hak subjek data secara lebih operasional. Rumusan norma perlu menetapkan batas waktu yang jelas bagi pengendali data untuk menanggapi permohonan subjek data. Mekanisme pengajuan hak subjek data perlu disederhanakan melalui sistem digital yang mudah diakses oleh masyarakat. Pengendali data juga perlu diwajibkan untuk memberikan informasi yang transparan mengenai proses pengumpulan, penggunaan, penyimpanan, dan penghapusan data pribadi. Penguatan hak subjek data tersebut akan meningkatkan

perlindungan terhadap privasi individu serta memperkuat posisi masyarakat sebagai pemilik data dalam ekosistem digital.

Pasal 58 hingga Pasal 64 UU PDP mengatur sanksi administratif bagi pelanggaran terhadap pengelolaan data pribadi. Sanksi administratif yang diatur meliputi teguran tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan data, serta denda administratif. Pengaturan tersebut bertujuan untuk memastikan bahwa pengendali data mematuhi kewajiban yang ditetapkan dalam regulasi perlindungan data pribadi yang bersifat spesifik. Efektivitas sanksi administratif dalam praktik masih menghadapi berbagai kendala. Besaran sanksi yang ada belum sepenuhnya memberikan efek jera terhadap pelaku pelanggaran, terutama bagi perusahaan besar yang mengelola data dalam jumlah besar.

Rekonstruksi terhadap Pasal 58 hingga Pasal 64 diarahkan pada penguatan mekanisme penegakan hukum melalui penetapan sanksi yang lebih proporsional terhadap tingkat pelanggaran yang terjadi. Rumusan norma perlu memberikan sanksi yang lebih berat terhadap pelanggaran yang melibatkan kebocoran data dalam skala besar atau penyalahgunaan data pribadi yang bersifat spesifik. Penguatan kewenangan lembaga pengawas juga diperlukan agar pengawasan terhadap pengelolaan data pribadi dapat berjalan secara efektif. Kewenangan tersebut meliputi audit kepatuhan, investigasi terhadap pelanggaran, serta penjatuhan sanksi administratif secara independen.

Rekonstruksi norma terhadap Pasal 4, Pasal 28 hingga Pasal 32, serta Pasal 58 hingga Pasal 64 UU PDP bertujuan memperkuat sistem perlindungan data pribadi yang bersifat spesifik agar lebih efektif dan responsif terhadap

perkembangan teknologi digital. Penguatan norma tersebut diarahkan pada peningkatan perlindungan terhadap data pribadi yang bersifat spesifik yang memiliki tingkat sensitivitas tinggi, sekaligus menjamin kepastian hukum dan perlindungan hak privasi individu. Rekonstruksi ini juga mencerminkan penerapan nilai-nilai keadilan berdasarkan Pancasila yang menempatkan penghormatan terhadap martabat manusia sebagai prinsip fundamental dalam pengelolaan data pribadi di ruang digital.

Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik pada hakikatnya merupakan upaya pembaruan hukum nasional yang bertujuan memperkuat kapasitas sistem hukum dalam merespons dinamika perkembangan teknologi digital sekaligus menjamin perlindungan hak asasi manusia. Perkembangan teknologi informasi, kecerdasan buatan, komputasi awan, serta analisis big data telah mengubah secara signifikan cara data pribadi dikumpulkan, diproses, dan dimanfaatkan dalam berbagai sektor kehidupan. Penguatan klasifikasi data pribadi yang bersifat sensitif, jaminan yang lebih efektif terhadap hak-hak subjek data, serta mekanisme penegakan hukum yang tegas dan proporsional menjadi elemen penting dalam membangun tata kelola data yang adil, akuntabel, dan bertanggung jawab.

Rekonstruksi norma yang lebih responsif terhadap risiko pemrosesan data pribadi yang bersifat spesifik diharapkan mampu menciptakan ekosistem digital yang aman, transparan, dan berkeadilan, sekaligus memastikan bahwa perkembangan ekonomi digital berjalan selaras dengan prinsip kepastian hukum, penghormatan terhadap martabat manusia, serta nilai-nilai keadilan sosial yang

terkandung dalam Pancasila. Upaya rekonstruksi ini mengamanatkan pergeseran paradigma dari pendekatan yang semata-mata bersifat administratif prosedural menuju pendekatan berbasis risiko (*risk-based approach*) yang lebih substantif. Kewajiban perlindungan data tidak lagi direduksi oleh korporasi sebagai sekadar beban regulasi (*regulatory burden*), melainkan terinternalisasi sebagai standar etika tata kelola teknologi yang esensial. Manifestasi dari nilai-nilai keadilan ini akan berfungsi secara efektif dalam mengeliminasi asimetri kekuasaan antara subjek data selaku pihak yang rentan direifikasi dengan penyelenggara sistem elektronik selaku pemegang kendali teknologi.

Rekonstruksi norma dalam ketentuan perlindungan data pribadi sebagaimana tercermin dalam perubahan terhadap Pasal 4, Pasal 28 sampai dengan Pasal 32, serta Pasal 57 sampai dengan Pasal 59 menunjukkan adanya upaya sistematis untuk memperkuat struktur hukum yang sebelumnya masih menyisakan berbagai kelemahan normatif. Fokus utama rekonstruksi terletak pada penajaman konsep data pribadi yang bersifat spesifik, yang sebelumnya hanya dirumuskan secara enumeratif tanpa disertai parameter yuridis yang jelas. Rumusan baru memberikan batasan berbasis tingkat sensitivitas dan potensi dampak kerugian terhadap subjek data pribadi apabila terjadi penyalahgunaan. Perluasan kategori data pribadi spesifik mencakup tidak hanya data kesehatan dan biometrik, tetapi juga data lokasi presisi, identitas unik, serta informasi keyakinan pribadi. Pengaturan tambahan mengenai kewajiban persetujuan eksplisit dan standar keamanan yang lebih tinggi menegaskan adanya diferensiasi perlindungan berdasarkan tingkat risiko data. Perubahan ini sekaligus mengisi kekosongan norma yang sebelumnya

menimbulkan ketidakpastian hukum dalam praktik pemrosesan data digital. Keseluruhan rekonstruksi tersebut diarahkan untuk membangun sistem perlindungan data pribadi yang lebih adaptif terhadap perkembangan teknologi informasi .

Rekonstruksi juga menyasar ketentuan mengenai kewajiban pengendali data pribadi dalam proses pemrosesan data sebagaimana diatur dalam Pasal 28 hingga Pasal 32. Norma sebelumnya dinilai belum memberikan pedoman operasional yang memadai dalam menjamin terpenuhinya hak subjek data. Ketentuan baru memperkenalkan prinsip pemrosesan yang sah, transparan, terbatas, dan akuntabel sebagai landasan utama kegiatan pengolahan data. Pengendali data diwajibkan memastikan akurasi, kelengkapan, serta kemutakhiran data melalui mekanisme verifikasi dan validasi berkala. Kewajiban untuk menyediakan sarana akses yang mudah dan transparan bagi subjek data menjadi elemen penting dalam memperkuat kontrol individu atas data pribadinya. Pengaturan mengenai batas waktu pembaruan data tetap dipertahankan, namun dilengkapi dengan kewajiban pemberitahuan apabila diperlukan verifikasi tambahan. Pencatatan aktivitas pemrosesan juga diperluas dengan memasukkan unsur tujuan, pihak yang mengakses, serta tindakan pengamanan yang diterapkan.

Tabel 4. 2. Rekonstruksi Hukum Pelindungan Data Pribadi Yang Bersifat Spesifik di Era Digital Untuk Mewujudkan Keadilan Berdasarkan Pancasila

Sebelum Rekonstruksi	Norma Sebelum Rekonstruksi	Permasalahan Norma	Setelah Rekonstruksi

Pasal 4 Ayat (2) (2) Data pribadi yang bersifat spesifik meliputi: a. data dan informasi kesehatan; b. data biometrik; c. data genetika; d. catatan kejahatan; e. data anak; f. data keuangan pribadi; dan g. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.	Data pribadi dibagi menjadi data pribadi umum dan data pribadi spesifik. Data pribadi spesifik meliputi data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, serta data lain sesuai peraturan perundang-undangan.	Norma dalam Pasal 4 belum memberikan definisi yuridis yang jelas mengenai kriteria data pribadi yang bersifat spesifik, sehingga menimbulkan ketidakpastian hukum dalam menentukan tingkat sensitivitas suatu data. Selain itu, ketentuan tersebut belum menetapkan standar perlindungan yang berbeda secara tegas antara data pribadi umum dan data pribadi spesifik. Akibatnya, data yang memiliki tingkat sensitivitas tinggi dan berpotensi menimbulkan kerugian serius bagi subjek data pribadi apabila disalahgunakan belum memperoleh perlindungan hukum yang memadai, terutama dalam konteks pemrosesan data pada ekosistem digital.	Pasal 4 Ayat (2) dan tambahan Ayat (3), Ayat (4), dan Ayat (5) (Rekonstruksi) (2) Data pribadi yang bersifat spesifik adalah data pribadi yang memiliki tingkat sensitivitas tinggi yang apabila diproses, diungkapkan, atau disalahgunakan dapat menimbulkan kerugian serius terhadap hak, kebebasan, keamanan, atau kepentingan subjek data pribadi. (3) Data pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (2) meliputi: a. data kesehatan; b. data biometrik; c. data genetika; d. catatan kejahatan; e. data anak; f. data keuangan pribadi; g. nomor identitas kependudukan atau identitas unik lainnya yang digunakan dalam sistem administrasi negara; h. data lokasi presisi yang dapat mengidentifikasi pergerakan individu secara spesifik; i. data mengenai keyakinan atau pandangan pribadi; dan j. data lainnya yang ditetapkan berdasarkan peraturan perundang-undangan. (4) Setiap pemrosesan data pribadi yang bersifat spesifik wajib dilakukan berdasarkan persetujuan eksplisit dari subjek data pribadi serta

			dilaksanakan dengan standar perlindungan dan keamanan yang lebih tinggi dibandingkan dengan pemrosesan data pribadi yang bersifat umum. (5) Pengendali data pribadi yang memproses data pribadi yang bersifat spesifik wajib menerapkan langkah-langkah pengamanan tambahan yang meliputi enkripsi, pembatasan akses, pencatatan aktivitas pemrosesan, serta mekanisme pengawasan dan akuntabilitas yang ketat.
Pasal 28 Pengendali Data Pribadi wajib melakukan pemrosesan Data Pribadi sesuai dengan tujuan pemrosesan Data Pribadi. Pasal 29 (1) Pengendali Data Pribadi wajib memastikan akurasi, kelengkapan, dan konsistensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan. (2) Dalam memastikan akurasi, kelengkapan, dan konsistensi Data Pribadi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib melakukan verifikasi. Pasal 30 (1) Pengendali Data Pribadi wajib memperbarui dan/atau	Pasal 28 mengatur bahwa pengendali data pribadi wajib melakukan pemrosesan data sesuai tujuan pemrosesan data pribadi. Pasal 29 mewajibkan pengendali data memastikan akurasi, kelengkapan, dan konsistensi data pribadi serta melakukan verifikasi. Pasal 30 mewajibkan pengendali data memperbarui atau memperbaiki data pribadi paling lambat 3 × 24 jam setelah menerima permintaan pembaruan. Pasal 31 mewajibkan pengendali data melakukan perekaman seluruh kegiatan pemrosesan data	Ketentuan Pasal 28–32 telah mengatur kewajiban pengendali data dalam pemrosesan data pribadi, namun norma tersebut belum sepenuhnya menjamin efektivitas pelaksanaan hak subjek data. Undang-undang belum mengatur secara rinci mekanisme operasional permohonan akses, koreksi, maupun pengendalian pemrosesan data oleh subjek data. Selain itu, belum terdapat kewajiban bagi pengendali data untuk menyediakan sistem layanan digital yang transparan dan mudah diakses oleh masyarakat dalam pelaksanaan hak tersebut. Ketiadaan	Pasal 28 (Rekonstruksi) (1) Pengendali Data Pribadi wajib melakukan pemrosesan Data Pribadi secara sah, transparan, terbatas, dan sesuai dengan tujuan pemrosesan Data Pribadi yang telah ditentukan sebelumnya. (2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) harus dilakukan berdasarkan prinsip pelindungan Data Pribadi yang meliputi kepastian tujuan, proporsionalitas, keamanan, dan akuntabilitas. (3) Setiap perubahan tujuan pemrosesan Data Pribadi wajib diberitahukan terlebih dahulu kepada Subjek Data Pribadi dan memperoleh persetujuan kembali dari Subjek Data

memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 3 × 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan pembaruan dan/atau perbaikan Data Pribadi. (2) Pengendali Data Pribadi wajib memberitahukan hasil pembaruan dan/atau perbaikan Data Pribadi kepada Subjek Data Pribadi. Pasal 31 Pengendali Data Pribadi wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan Data Pribadi. Pasal 32 (1) Pengendali Data Pribadi wajib memberikan akses kepada Subjek Data Pribadi terhadap Data Pribadi yang diproses beserta rekam jejak pemrosesan Data Pribadi sesuai dengan jangka waktu penyimpanan Data Pribadi. (2) Akses sebagaimana dimaksud pada ayat (1) diberikan paling lambat 3 × 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan akses.	pribadi. Pasal 32 mewajibkan pengendali data memberikan akses kepada subjek data terhadap data pribadi dan rekam jejak pemrosesan dalam waktu paling lambat 3 × 24 jam setelah permintaan diterima.	standar prosedural yang lebih operasional berpotensi menimbulkan hambatan administratif dan ketidakpastian hukum dalam pelaksanaan hak subjek data pribadi.	Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan. Pasal 29 (Rekonstruksi) (1) Pengendali Data Pribadi wajib memastikan akurasi, kelengkapan, konsistensi, dan kemutakhiran Data Pribadi yang diproses. (2) Dalam memastikan akurasi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib melakukan verifikasi, validasi, dan pembaruan Data Pribadi secara berkala. (3) Pengendali Data Pribadi wajib menyediakan mekanisme yang mudah diakses oleh Subjek Data Pribadi untuk mengajukan permintaan pembaruan atau perbaikan Data Pribadi. Pasal 30 (Rekonstruksi) (1) Pengendali Data Pribadi wajib memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 3 × 24 (tiga kali dua puluh empat) jam sejak menerima permintaan pembaruan atau perbaikan dari Subjek Data Pribadi. (2) Dalam hal permintaan pembaruan memerlukan proses verifikasi tambahan, Pengendali Data Pribadi wajib memberikan

			pemberitahuan kepada Subjek Data Pribadi mengenai alasan dan jangka waktu penyelesaian. (3) Pengendali Data Pribadi wajib memberitahukan hasil pembaruan atau perbaikan Data Pribadi kepada Subjek Data Pribadi secara elektronik atau nonelektronik. Pasal 31 (Rekonstruksi) (1) Pengendali Data Pribadi wajib melakukan pencatatan dan perekaman seluruh aktivitas pemrosesan Data Pribadi secara sistematis. (2) Pencatatan sebagaimana dimaksud pada ayat (1) paling sedikit memuat: a. jenis Data Pribadi yang diproses; b. tujuan pemrosesan Data Pribadi; c. waktu pemrosesan Data Pribadi; d. pihak yang memiliki akses terhadap Data Pribadi; dan e. tindakan pengamanan yang diterapkan dalam pemrosesan Data Pribadi. (3) Pencatatan kegiatan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) wajib disimpan sebagai bukti pertanggungjawaban. Pasal 32 (Rekonstruksi) (1) Pengendali Data Pribadi wajib memberikan akses

			kepada Subjek Data Pribadi terhadap Data Pribadi yang diproses beserta informasi mengenai aktivitas pemrosesan Data Pribadi. (2) Akses sebagaimana dimaksud pada ayat (1) diberikan paling lambat 3 × 24 (tiga kali dua puluh empat) jam sejak permintaan akses diterima. (3) Pengendali Data Pribadi wajib menyediakan sistem layanan yang transparan, sederhana, dan mudah diakses, baik secara elektronik maupun nonelektronik, untuk pelaksanaan hak akses Subjek Data Pribadi. (4) Dalam hal permintaan akses tidak dapat dipenuhi, Pengendali Data Pribadi wajib memberikan penjelasan secara tertulis disertai alasan yang sah sesuai dengan ketentuan peraturan perundang-undangan.
Pasal 57 (1) Pelanggaran terhadap ketentuan Pasal 20 ayat (1), Pasal 21, Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (3), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, Pasal 39 ayat (1), Pasal 40 ayat (1),	Undang-Undang mengatur bahwa pelanggaran terhadap ketentuan pemrosesan data pribadi dikenakan sanksi administratif berupa: peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan denda	Besaran sanksi administratif belum sepenuhnya memberikan efek jera bagi pelanggar, khususnya korporasi besar yang mengelola data dalam skala besar. Selain itu, mekanisme penegakan sanksi masih sangat bergantung pada kapasitas pengawasan	Pasal 57 (Rekonstruksi) (1) Setiap pelanggaran terhadap ketentuan pemrosesan Data Pribadi sebagaimana diatur dalam Undang-Undang ini dikenai sanksi administratif oleh lembaga pengawas Pelindungan Data Pribadi. (2) Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat

Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1) dan ayat (3), Pasal 47, Pasal 48 ayat (1), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (1), Pasal 55 ayat (2), dan Pasal 56 ayat (2) sampai dengan ayat (4) dikenai sanksi administratif. (2) Sanksi administratif sebagaimana dimaksud pada ayat (1) berupa: a. peringatan tertulis; b. penghentian sementara kegiatan pemrosesan Data Pribadi; c. penghapusan atau pemusnahan Data Pribadi; dan/atau d. denda administratif. (3) Sanksi administratif berupa denda administratif sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2% (dua persen) dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. (4) Penjatuhan sanksi administratif sebagaimana dimaksud pada ayat (2) diberikan oleh lembaga. (5) Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif	administratif paling tinggi 2% dari pendapatan tahunan. Penjatuhan sanksi administratif dilakukan oleh lembaga pengawas pelindungan data pribadi.	lembaga yang belum sepenuhnya independen dan belum memiliki kewenangan investigatif yang kuat. Kondisi ini berpotensi menimbulkan lemahnya penegakan hukum dalam kasus pelanggaran pelindungan data pribadi, termasuk kebocoran data berskala besar.	berupa: a. peringatan tertulis; b. penghentian sementara sebagian atau seluruh kegiatan pemrosesan Data Pribadi; c. penghapusan atau pemusnahan Data Pribadi; d. denda administratif; dan/atau e. pembatasan kegiatan pemrosesan Data Pribadi. (3) Penjatuhan denda administratif sebagaimana dimaksud pada ayat (2) huruf d ditentukan secara proporsional berdasarkan tingkat pelanggaran, jumlah subjek data yang terdampak, dan skala pemrosesan Data Pribadi. (4) Dalam hal pelanggaran menimbulkan kebocoran Data Pribadi dalam skala besar atau dilakukan secara berulang, lembaga pengawas dapat mengenakan denda administratif yang lebih tinggi serta penghentian kegiatan pemrosesan Data Pribadi secara permanen. (5) Ketentuan lebih lanjut mengenai tata cara penjatuhan sanksi administratif diatur dalam Peraturan Pemerintah. Pasal 58 (Rekonstruksi) (1) Penyelenggaraan Pelindungan Data Pribadi dilaksanakan

sebagaimana dimaksud pada ayat (3) diatur dalam Peraturan Pemerintah. Pasal 58 (1) Pemerintah berperan dalam penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini. (2) Penyelenggaraan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga. (3) Lembaga sebagaimana dimaksud pada ayat (2) ditetapkan oleh Presiden. (4) Lembaga sebagaimana dimaksud pada ayat (2) bertanggung jawab kepada Presiden. (5) Ketentuan lebih lanjut mengenai lembaga sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Presiden. Pasal 59 Lembaga sebagaimana dimaksud dalam Pasal 58 ayat (2) melaksanakan: a. perumusan dan penetapan kebijakan dan strategi Pelindungan Data Pribadi; b. pengawasan terhadap			oleh lembaga pengawas Pelindungan Data Pribadi yang bersifat independen. (2) Lembaga sebagaimana dimaksud pada ayat (1) memiliki kewenangan untuk melakukan pengawasan, pemeriksaan, dan penegakan hukum administratif terhadap pelanggaran pelindungan Data Pribadi. (3) Lembaga sebagaimana dimaksud pada ayat (1) bertanggung jawab secara langsung kepada Presiden dalam menjalankan tugas dan kewenangannya. (4) Ketentuan lebih lanjut mengenai kedudukan, tugas, dan kewenangan lembaga diatur dengan Peraturan Presiden. Pasal 59 (Rekonstruksi) Lembaga pengawas Pelindungan Data Pribadi memiliki kewenangan untuk: a. merumuskan dan menetapkan kebijakan nasional di bidang pelindungan Data Pribadi; b. melakukan pengawasan terhadap pemrosesan Data Pribadi oleh Pengendali Data Pribadi dan Prosesor Data Pribadi; c. melakukan audit kepatuhan dan investigasi terhadap dugaan pelanggaran pelindungan Data

penyelenggaraan Pelindungan Data Pribadi; c. penegakan hukum administratif terhadap pelanggaran Undang-Undang ini; dan d. fasilitasi penyelesaian sengketa di luar pengadilan.			Pribadi; d. menjatuhkan sanksi administratif terhadap pelanggaran ketentuan Undang-Undang ini; dan e. memfasilitasi penyelesaian sengketa pelindungan Data Pribadi melalui mekanisme non-litigasi.

Aspek lain yang direkonstruksi mencakup penguatan sistem sanksi administratif dan kelembagaan pengawas perlindungan data pribadi. Ketentuan sebelumnya dinilai belum memberikan efek jera yang optimal, khususnya bagi entitas korporasi besar dengan kapasitas ekonomi yang tinggi. Rekonstruksi memperkenalkan pendekatan sanksi yang lebih fleksibel dan proporsional berdasarkan tingkat pelanggaran, jumlah subjek data yang terdampak, serta skala pemrosesan data. Penambahan jenis sanksi berupa pembatasan kegiatan pemrosesan serta kemungkinan penghentian permanen dalam kasus pelanggaran berat menunjukkan peningkatan ketegasan norma. Di sisi kelembagaan, pembentukan lembaga pengawas yang bersifat independen menjadi langkah strategis dalam memastikan efektivitas penegakan hukum. Lembaga tersebut diberikan kewenangan untuk melakukan audit, investigasi, serta penjatuhan sanksi administratif. Penguatan fungsi pengawasan ini diharapkan mampu mengatasi kelemahan sebelumnya yang terlalu bergantung pada kapasitas lembaga yang belum optimal. Rekonstruksi ini mencerminkan pergeseran paradigma dari sekadar regulasi normatif menuju penegakan hukum yang lebih aktif dan responsif.

Analisis rekonstruksi tersebut pada tataran *grand theory* menunjukkan keterkaitannya dengan konsep negara hukum dan perlindungan hak asasi manusia. Negara hukum menuntut adanya kepastian hukum, keadilan, serta perlindungan terhadap hak-hak fundamental warga negara. Pelindungan data pribadi merupakan bagian integral dari hak atas privasi yang diakui secara universal. Rekonstruksi norma memberikan kejelasan mengenai klasifikasi data pribadi dan standar perlindungan yang berbeda sesuai tingkat risiko. Hal ini mencerminkan penerapan prinsip *legal certainty* yang menjadi salah satu pilar utama dalam negara hukum. Penguatan sanksi dan kelembagaan pengawas juga mencerminkan adanya jaminan terhadap prinsip *rule of law*, di mana setiap pelanggaran harus dapat ditindak secara efektif. Pengaturan mengenai persetujuan eksplisit memperkuat posisi subjek data sebagai pemegang hak atas informasi pribadinya. Dengan demikian, rekonstruksi ini tidak hanya bersifat teknis, tetapi juga memiliki dimensi filosofis yang kuat dalam kerangka perlindungan hak asasi manusia.

Pendekatan *middle theory* dalam analisis ini dapat dilihat melalui penerapan teori perlindungan data dan teori regulasi responsif. Teori perlindungan data menekankan pentingnya prinsip-prinsip dasar dalam pengolahan data, seperti *lawful, fair, and transparent processing*. Rekonstruksi Pasal 28 sampai dengan Pasal 32 menunjukkan adopsi prinsip tersebut melalui kewajiban transparansi, akuntabilitas, dan keterbukaan akses bagi subjek data. Teori regulasi responsif menekankan bahwa hukum harus mampu menyesuaikan diri dengan perkembangan sosial dan teknologi. Penambahan ketentuan mengenai enkripsi, pembatasan akses, serta pencatatan aktivitas menunjukkan adanya respons terhadap risiko keamanan

data di era digital. Pengaturan mengenai sistem layanan yang mudah diakses mencerminkan kebutuhan akan pendekatan yang lebih user-oriented. Norma tidak lagi hanya bersifat represif, tetapi juga preventif dan edukatif dalam mengatur perilaku pengendali data. Pendekatan ini memperlihatkan bahwa rekonstruksi telah mengintegrasikan dimensi normatif dan praktis dalam satu kerangka yang koheren.

Rekonstruksi norma mencerminkan penerapan prinsip *good data governance* dan *risk-based approach* dalam pengelolaan data pribadi. Prinsip *good data governance* menekankan pentingnya tata kelola data yang transparan, akuntabel, dan berorientasi pada perlindungan hak individu. Kewajiban pencatatan aktivitas pemrosesan dan penyediaan akses bagi subjek data merupakan bentuk konkret dari prinsip tersebut. Pendekatan berbasis risiko terlihat dalam diferensiasi perlindungan antara data pribadi umum dan data pribadi spesifik. Data dengan tingkat sensitivitas tinggi diberikan perlindungan yang lebih ketat, termasuk kewajiban persetujuan eksplisit dan penerapan standar keamanan tambahan. Pengendali data juga diwajibkan melakukan evaluasi berkala terhadap akurasi dan relevansi data yang diproses. Mekanisme ini menunjukkan adanya integrasi antara norma hukum dan praktik manajemen risiko dalam pengelolaan data. Dengan demikian, rekonstruksi tidak hanya memperkuat aspek regulasi, tetapi juga meningkatkan kualitas praktik operasional di lapangan.

Novelty dalam rekonstruksi ini terletak pada pendekatan konseptual yang lebih maju dibandingkan dengan norma sebelumnya. Perumusan definisi data pribadi spesifik berbasis tingkat risiko dan potensi kerugian merupakan inovasi yang memberikan kejelasan sekaligus fleksibilitas dalam penerapan hukum.

Pendekatan ini memungkinkan adaptasi terhadap jenis data baru yang terus berkembang seiring kemajuan teknologi. Penguatan kewajiban pengendali data melalui mekanisme transparansi dan aksesibilitas menciptakan keseimbangan antara kepentingan bisnis dan perlindungan hak individu. Pengenalan kewajiban sistem layanan digital yang mudah diakses merupakan langkah progresif dalam mendekatkan hukum kepada masyarakat. Penguatan sanksi berbasis proporsionalitas dan dampak pelanggaran memberikan dimensi keadilan yang lebih substantif. Pembentukan lembaga pengawas independen dengan kewenangan investigatif juga menjadi terobosan penting dalam sistem penegakan hukum.

Rekonstruksi tidak hanya mengatur prinsip-prinsip umum, tetapi juga memberikan panduan operasional yang jelas bagi pengendali data. Pengaturan mengenai enkripsi, pembatasan akses, serta pencatatan aktivitas menunjukkan adanya pengakuan terhadap pentingnya aspek teknis dalam perlindungan data. Pendekatan ini mencerminkan pergeseran dari regulasi berbasis teks menuju regulasi berbasis sistem. Norma hukum tidak lagi berdiri sendiri, tetapi terintegrasi dengan praktik teknologi informasi yang berkembang pesat. Hal ini memberikan kepastian hukum sekaligus meningkatkan efektivitas implementasi di lapangan. Rekonstruksi ini juga membuka ruang bagi pengembangan kebijakan turunan yang lebih spesifik dan kontekstual. Dengan demikian, sistem perlindungan data pribadi menjadi lebih adaptif dan berkelanjutan.

Implikasi dari rekonstruksi ini sangat signifikan terhadap praktik perlindungan data pribadi di Indonesia. Pengendali data dituntut untuk meningkatkan kapasitas teknis dan kelembagaan dalam memenuhi kewajiban yang

diatur. Subjek data memperoleh posisi yang lebih kuat dalam mengontrol penggunaan data pribadinya. Lembaga pengawas memiliki peran strategis dalam memastikan kepatuhan dan menegakkan hukum secara efektif. Keseluruhan perubahan ini diharapkan mampu meningkatkan kepercayaan masyarakat terhadap sistem digital. Rekonstruksi juga memberikan landasan bagi pengembangan ekosistem ekonomi digital yang lebih aman dan berkelanjutan. Dengan demikian, perlindungan data pribadi tidak hanya dilihat sebagai kewajiban hukum, tetapi juga sebagai bagian dari tata kelola yang baik dalam era digital.

Implikasi rekonstruksi pengaturan perlindungan data pribadi ini memberikan penguatan terhadap perlindungan hak subjek data, peningkatan kewajiban pengendali data, serta optimalisasi peran lembaga pengawas dalam menjamin kepatuhan terhadap peraturan perundang-undangan. Perubahan tersebut diharapkan dapat meningkatkan kepercayaan masyarakat terhadap sistem digital dan mendukung terciptanya ekosistem ekonomi digital yang aman, transparan, dan berkelanjutan. Dengan demikian, perlindungan data pribadi tidak hanya menjadi kewajiban hukum, tetapi juga bagian dari tata kelola yang baik di era digital.

BAB V
KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pembahasan tersebut, kesimpulan dari penelitian ini adalah:

1. Inefektivitas perlindungan data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital menunjukkan bahwa regulasi yang ada saat ini belum sepenuhnya mampu menjamin keamanan dan hak privasi individu. Kebocoran data, penyalahgunaan informasi, serta rendahnya literasi digital masyarakat menegaskan perlunya penguatan hukum yang lebih adaptif dan komprehensif. Rekonstruksi hukum diperlukan untuk mengintegrasikan prinsip-prinsip keadilan sosial berdasarkan Pancasila, memperkuat efektivitas pengawasan, sanksi, serta mekanisme pemulihan hak subjek data. Dengan langkah-langkah tersebut, perlindungan data pribadi yang bersifat spesifik dapat dilaksanakan secara lebih efektif, responsif terhadap perkembangan teknologi, serta selaras dengan nilai-nilai keadilan dan martabat manusia.
2. Kebijakan perlindungan hukum terhadap data pribadi yang bersifat spesifik akibat perkembangan teknologi di era digital telah memperoleh dasar normatif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta didukung oleh berbagai ketentuan hukum lain yang berkaitan dengan hak privasi, keamanan sistem elektronik, perlindungan konsumen, dan administrasi kependudukan. Kebijakan tersebut pada dasarnya telah mengatur klasifikasi data

pribadi, hak subjek data, kewajiban pengendali data, prinsip persetujuan, keamanan pemrosesan data, serta sanksi terhadap pelanggaran. Namun, pelaksanaannya belum sepenuhnya efektif karena masih terdapat kelemahan dalam pengawasan, rendahnya kepatuhan pengendali data, belum optimalnya pelaksanaan hak subjek data, serta belum kuatnya mekanisme pemulihan bagi korban penyalahgunaan atau kebocoran data. Dengan demikian, kebijakan perlindungan hukum yang berlaku masih memerlukan penguatan agar tidak hanya memberikan kepastian hukum secara normatif, tetapi juga mampu menjamin perlindungan yang nyata, adaptif, dan berkeadilan bagi subjek data pribadi yang bersifat spesifik.

3. Rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik terhadap perkembangan teknologi di era digital yang sesuai dengan nilai-nilai keadilan berdasarkan Pancasila harus diarahkan pada penyempurnaan substansi, struktur, dan budaya hukum secara terpadu. Pada aspek substansi, rekonstruksi perlu dilakukan terhadap Pasal 4 ayat (2) UU PDP agar klasifikasi data pribadi spesifik lebih dinamis, terhadap Pasal 28 sampai dengan Pasal 32 agar hak subjek data benar-benar efektif, serta terhadap Pasal 58 sampai dengan Pasal 64 agar sanksi dan ganti rugi berorientasi pada keadilan restoratif. Pada aspek struktur, diperlukan lembaga pengawas independen yang memiliki kewenangan pengawasan, audit, investigasi, penjatuhan sanksi, dan fasilitasi penyelesaian sengketa. Pada aspek budaya hukum, diperlukan

peningkatan literasi privasi, kepatuhan pelaku usaha, dan internalisasi etika pengelolaan data. Seluruh rekonstruksi tersebut harus berlandaskan penghormatan terhadap martabat manusia, keadilan sosial, akuntabilitas, dan keseimbangan antara perlindungan hak privasi dengan perkembangan teknologi digital.

B. Saran

Berdasarkan kesimpulan tersebut, saran dari penelitian ini adalah:

1. Sebaiknya pemerintah melakukan penguatan dan rekonstruksi hukum perlindungan data pribadi yang bersifat spesifik secara menyeluruh, baik dari aspek substansi regulasi, kelembagaan pengawas, penegakan sanksi, maupun mekanisme pemulihan hak korban. Penguatan tersebut harus diarahkan agar perlindungan data pribadi tidak hanya bersifat administratif, tetapi benar-benar mampu menjamin keamanan, privasi, martabat, dan keadilan bagi setiap subjek data di era digital sesuai dengan nilai-nilai Pancasila.
2. Sebaiknya, pemerintah dan pembentuk undang-undang memperkuat kebijakan perlindungan hukum terhadap data pribadi yang bersifat spesifik dengan memperjelas standar perlindungan terhadap data yang memiliki tingkat sensitivitas tinggi, memperkuat kewajiban pengendali data dalam memperoleh persetujuan yang sah dan bermakna, menjamin pelaksanaan hak subjek data secara sederhana dan efektif, serta meningkatkan pengawasan terhadap pemrosesan data pribadi di sektor publik maupun privat. Penguatan kebijakan tersebut juga perlu

diarahkan pada pembentukan mekanisme sanksi dan pemulihan yang lebih proporsional, sehingga korban kebocoran atau penyalahgunaan data tidak hanya memperoleh pengakuan atas pelanggaran haknya, tetapi juga mendapatkan ganti rugi dan pemulihan yang adil sesuai dengan kerugian yang dialami.

3. Sebaiknya rekonstruksi hukum yang diterapkan dibangun secara terpadu melalui penguatan substansi hukum, pembentukan lembaga pengawas independen yang efektif, peningkatan budaya hukum masyarakat dan pelaku usaha, serta penerapan teknologi pengamanan data yang akuntabel, dengan tetap menempatkan nilai-nilai Pancasila sebagai landasan utama agar perlindungan data pribadi yang bersifat spesifik benar-benar mewujudkan keadilan sosial, penghormatan martabat manusia, dan keseimbangan kepentingan dalam masyarakat digital.

DAFTAR PUSTAKA

A. Buku

Abas, M., Mia Amalia, Ridwan Malik, Abdul Aziz, and Safrin Salam. 2023. *Sosiologi Hukum: Pengantar Teori-Teori Hukum Dalam Ruang Sosial*. Jambi: PT. Sonpedia Publishing Indonesia.

Achmad Ali. 2010. *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence) Termasuk Interpretasi Undang-Undang (Legisprudence). Cetakan ke-3*. Jakarta: Kencana.

Achmad Solechan. 2021. *Audit Sistem Informasi Audit Sistem Informasi*. Semarang: Yayasan Prima Agus Teknik.

Ade Risna Sari and M Si SH. 2024. Reformasi Pelayanan Publik. Jakarta: PT Indonesia Delapan Kreasi Nusa.

Adriaman, Mahlil. 2024. *Pengantar Metode Penelitian Ilmu Hukum*. Agam: Yayasan Tri Edukasi Ilmiah.

Agus Raharjo. 2021. *Perlindungan Hukum terhadap Privasi dan Data Pribadi di Indonesia.* Jakarta: Sinar Grafika.

Agus Wibowo and Sri Yulianingsih. 2023. *Hukum Teknologi Informasi.* Semarang: Yayasan Prima Agus Teknik.

Ahmad Azhar Basyir. 1999. *Prinsip-Prinsip Hukum Islam tentang Hak Asasi Manusia.* Yogyakarta: UII Press.

Ajisatria Suleiman, Pingkan Audrine, and Thomas Dewaranu. 2022. *Pengaturan Bersama Dalam Perlindungan Data Pribadi: Potensi Peran Asosiasi Industri Sebagai Organisasi Regulator Mandiri.* Center for Indonesian Policy Studies.

Ali, A. 2012. *Menguak Teori Hukum dan Teori Peradilan*. Jakarta: Kencana.

Ali, Mohammad Daud. 2010. *Hukum Islam: Pengantar Ilmu Hukum dan Tata Hukum Islam di Indonesia*. Jakarta: Rajawali Pers.

Alfath Roziq and Fatma Ulfatun Najicha. 2023. *Peran Nilai Pancasila Dan Semangat Bela Negara Bagi Generasi Muda Dalam Era Transformasi Digital.* Surakarta.

Allan F. Westin. 2003. *Privacy dan Freedom, dalam Edmon Makarim, Kompasi Hukum Telematika.* Jakarta: Raja Grafindo Persada.

Almahdali, Humairah, Jana Milia, Pristiyanto Pristiyanto, Budi Juliardi, Susi Anita Patmawati, Dwi Riyanti, Yongker Baali, La Ode Muhammad Rauda Agus Udaya, Imam Rozikin, and Zuhdi Arman. 2024. *Pendidikan Pancasila Dan Kewarganegaraan*. Agam: Yayasan Tri Edukasi Ilmiah

Andri Yanto. 2021. *Mazhab-Mazhab Hukum: Suatu Pengantar Memahami Dimensi Pemikiran Hukum.* Penerbit Segap Pustaka.

Al-Qaradawi, Yusuf. 2010. Halal dan Haram dalam Islam. Jakarta: Gema Insani.

Arifuddin, Qadriani, Riswan Riswan, Muhammad Adam HR, Bulkis Bulkis, Abdul Latif, Salma Salma, Hasnawati Hasnawati, A. Ariani Hidayat, and Nur Indah. 2025. *Metodologi Penelitian Hukum*. Jambi: PT. Sonpedia Publishing Indonesia.

Asep Dedi Suwasta and Ujuh Juhana. 2024. *Pengantar Ilmu Hukum.* Tohar Media.

Asshiddiqie, J. 2014. *Gagasan Konstitusi Sosial: Negara Kesejahteraan dan Konstitusi Indonesia*. Jakarta: Konstitusi Press.

_____. 2021. *Konstitusi dan Konstitusionalisme Indonesia*. Jakarta: Sinar Grafika.

Az-Zuhaili, Wahbah. 2011. *Al-Fiqh Al-Islami wa Adillatuhu*. Jakarta: Gema Insani.

Badriyah, S. M. 2022. *Sistem Penemuan Hukum dalam Masyarakat Prismatik*. Jakarta: Sinar Grafika.

Basyir, Ahmad Azhar. 1999. *Prinsip-Prinsip Hukum Islam tentang Hak Asasi Manusia*. Yogyakarta: UII Press.

Bernard Arief Sidharta. 2000. *"Refleksi Tentang Struktur Ilmu Hukum."* II Bandung: Mandar Maju (2000).

Busyro. 2019. *Maqāṣid al-Syarī'ah: Pengetahuan Mendasar Memahami Maslahah*. Jakarta: Kencana.

Damanik, P., S. Nugraha, and F. Nur. 2024. *Hukum Administrasi Negara: Teori, Prinsip, dan Praktik Tata Kelola Pemerintahan*. PT. Media Penerbit Indonesia.

Efraim Mangaluk, Sepriano Sepriano, and Agus Nasrullah. 2025. *Buku Referensi Wawasan Pancasila.* Jambi: PT. Sonpedia Publishing Indonesia.

Erlina Puspitaloka Mahadewi. 2025. *Pemasaran Internasional.* Jambi: PT. Sonpedia Publishing Indonesia.

Evi, Tiolina. 2023. *Transformasi Transaksi Tunai Ke Digital Di Indonesia*. CV. AA. Rizky.

Fara Amalia Lutfi Pratama et al. 2023. *Implementasi Nilai Pancasila Dalam Bhinneka Tunggal Ika Sebagai Alat Pemersatu Bangsa Di Era Generasi Milenial.* Unisri Press.

Farid Wajdi and Diana Susanti. 2023. *Hukum Pelindungan Konsumen.* Malang: Setara Press.

Gani, Taufiq A. 2023. *Kedaulatan Data Digital Untuk Integritas Bangsa*. Syiah Kuala: Syiah Kuala University Press.

Hadiyantina, Shinta, Zainal Amin Ayub, Dewi Cahyandari, Amelia Ayu Paramitha, Sinta Devi Ambarwati, Yusuf Mustofa, Xaviera Qatrunnada Djana Sudjati, and Nur Auliya Rahmatika. 2023. *Pelindungan data pribadi Dalam Bidang Rekam Medis*. Malang: Universitas Brawijaya Press

Hadjon, P. M. 1987. *Pelindungan Hukum bagi Rakyat di Indonesia: Sebuah Studi tentang Prinsip-prinsipnya, Penanganannya oleh Pengadilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*. Surabaya: Bina Ilmu.

Harahap, Yahya. 2020. *Hukum tentang Perlindungan Privasi dan Data Pribadi*. Jakarta: Sinar Grafika.

Hatta, Mohammad. 1966. *Demokrasi Kita*. Djakarta: Pustaka Antara.

Huda, Uu Nurul, Tatang Astaruddin, Muhammad Irsan Nasution, Alwi Al Haddad, and Dian Rachmat Gumelar. 2024. *Data Pribadi, Hak Warga, Dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital*. Bandung: Penerbit Widina.

Irawan, Anang Dony. 2025. *Pancasila Sebagai Dasar Pembentukan Peraturan Perundang-Undangan Di Indonesia*. CV. Gita Lentera.

Efendi, Jonaedi. 2018. *Rekonstruksi Dasar Pertimbangan Hukum Hakim*. Jakarta: Prenada Media.

Kaelan. 2016. *Pancasila sebagai Ideologi dan Dasar Negara*. Yogyakarta: Paradigma.

Khairandy, Ridwan. 2019. *Hak Asasi Manusia dalam Perspektif Hukum*. Yogyakarta: FH UII Press.

Khoir, Qoidul, Josepin Harianja, Cartes Asbit Rangotwat, Henny Saida Flora, Suparwi, Sardjana Orba Manullang, and Prisko Yanuarius Djawaria Pare. 2023. *Pancasila & Kewarganegaraan*. Batam: Cendikia Mulia Mandiri.

Kusumaatmadja, M. 2002. *Konsep-konsep Hukum dalam Pembangunan*. Bandung: Penerbit Alumni.

_____. *Hukum, Masyarakat, dan Pembinaan Hukum Nasional*. Bandung: Penerbit Bina Cipta.

Kristiawanto. 2024. *Pengantar Mudah Memahami Metode Penelitian Hukum*. Klaten: Nas Media Pustaka.

Latif, Yudi. 2011. *Negara Paripurna: Historisitas, Rasionalitas, dan Aktualitas Pancasila*. Jakarta: Gramedia Pustaka Utama.

_____. 2018. "Identitas Keindonesiaan dan Aktualisasi Pancasila bagi Generasi Milenial di Era Digital." *Jurnal Lemhannas RI* 6(1):5–19.

Lubis, Todung Mulya. 2023. *In Search of Human Rights: Legal-Political Dilemmas of Indonesia New Order, 1966-1990*. Dalam Bunyamin, F.X. Watkat, dkk. *Pengantar Ilmu Hukum*. Padang: Get Press Indonesia.

Magnis-Suseno, Franz. 2016. *Etika Politik: Prinsip-Prinsip Moral Dasar Kenegaraan Modern*. Jakarta: Gramedia Pustaka Utama.

Mangaluk, Efraim, Sepriano Sepriano, and Agus Nasrullah. 2025. *Buku Referensi Wawasan Pancasila*. Jambi: PT. Sonpedia Publishing Indonesia.

Marzuki, Peter Mahmud. 2021. *Penelitian Hukum*. Jakarta: Kencana

_____. 2008. *Pengantar Ilmu Hukum*. Jakarta: Kencana Jakarta.

Mulyadi, Lilik. 2018. *Hak Asasi Manusia dalam Perspektif Hukum dan Konstitusi Indonesia*. Bandung: Alumni.

Notonagoro. 1980. *Pancasila Secara Ilmiah Populer*. Jakarta: Pantjuran Tujuh.

Pratama, F. A. L., A. Trisiana, N. N. Anggraini, L. S. Kurniawati, A. S. Nugraha, and A. T. Nawangsih. 2023. *Implementasi Nilai Pancasila dalam Bhinneka Tunggal Ika Sebagai Alat Pemersatu Bangsa di Era Generasi Milenial*. Unisri Press.

Raharjo, A. 2021. *Perlindungan Hukum terhadap Privasi dan Data Pribadi di Indonesia.* Jakarta: Sinar Grafika.

Rahardjo, S. 2007. *Biarkan Hukum Mengalir: Catatan Kritis tentang Pergulatan Manusia dan Hukum*. Jakarta: Penerbit Buku Kompas.

Ramlan, Tengku Erwinsyahbana dan Surya Perdana. 2023. *Metode Penelitian Hukum dalam Pembuatan Karya Ilmiah*. Edited by Ismail Koto. Medan: UMSU Press.

Ratnaningtyas, Endah Marendah, Edi Saputra, Desi Suliwati, Bekty Taufiq Ari Nugroho, Muhammad Habibullah Aminy, Nanda Saputra, and Adi Susilo

Jahja. 2023. *Metodologi Penelitian Kualitatif*. Aceh: Yayasan Penerbit Muhammad Zaini.

Rifa'i, I. J. 2023. *Ruang Lingkup Metode Penelitian Hukum. Metodologi Penelitian Hukum.* PT. Sada Kurnia Pustaka

Rosadi, Sinta Dewi. 2023. *Pembahasan UU Pelindungan data pribadi yang bersifat spesifik (UU RI Nomor 27 Tahun 2022)*. Jakarta: Sinar Grafika.

Safitri, Indra. 2021. *Hukum Siber dan Pelindungan data pribadi yang bersifat spesifik di Indonesia*. Jakarta: Kencana.

Sari, Ratih Mega Puspa, and, Sivani Ardi Apritania. 2026. *Kewarganegaraan Dan Pranata Hukum Di Indonesia*. Yogyakarta: Penerbit KBM Indonesia.

Shihab, M. Quraish. 2005. *Tafsir al-Mishbah: Pesan, Kesan, dan Keserasian Al-Qur'an*. Jilid I. Cet. V. Jakarta: Lentera Hati.

_____. 2006. *Tafsir Al-Mishbah: Pesan, Kesan, dan Keserasian Al-Qur'an*. Jakarta: Lentera Hati.

Sholihah, H., L. Judijanto, R. M. Fajrina, I. N. S. Saleh, A. Apriyanto, D. Pujiningsih, and J. Milia. 2024. *HAK ASASI MANUSIA: Asal Usul, Penyusunan, dan Implementasi*. PT. Sonpedia Publishing Indonesia.

Sidharta, B. A. 2000. *Refleksi Tentang Struktur Ilmu Hukum*. II Bandung: Mandar Maju.

Soekarno. 1947. *Lahirnya Pancasila*. Jakarta: Departemen Penerangan Republik Indonesia.

Soekanto, S. 1983. *Faktor-faktor yang Mempengaruhi Penegakan Hukum di Indonesia*. Jakarta: Sinar Grafika.

_____. 2010. *Pokok-Pokok Sosiologi Hukum*. Jakarta: Rajawali Pers.

Soeprapto, M. F. I. 2018. *Ilmu Perundang-undangan 2: Proses dan Teknik Penyusunan*. Jakarta: PT Kanisius.

Sugiyono, P. D. 2017. *Metode Penelitian Bisnis: Pendekatan Kuantitatif, Kualitatif, Kombinasi, Dan R&D*. Bandung: Penerbit CV. Alfabeta.

Suteki dan Galang Taufani. 2020. *Metode Penelitian Hukum (Filsafat, Teori dan Praktik)*. Depok: Rajawali Pers.

Suwasta, A. D., and U. Juhana. 2024. *Pengantar Ilmu Hukum*. Tohar Media.

Tahir, R., I. G. P. Astawa, A. Widjajanto, M. L. Panggabean, M. M. Rohman, N. P. P. Dewi, N. A. Deliarnoor, M. Abas, R. F. Ayu, and N. P. S. Meinarni. 2023.

Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori dan Praktik. PT. Sonpedia Publishing Indonesia.

Tilaar, H. A. R. 2012. *Membenahi Pendidikan Nasional*. Jakarta: Rineka Cipta.

Wajdi, F., and D. Susanti. 2023. *Hukum Pelindungan Konsumen*. Setara Press.

Waty, Ervina, Annisa Fitri Anggraeni, Anita Apriani, Hasan Ibrahim, Afrina Sari, Henny A. Manafe, Galuh Juniarto, Tinjung Desy Nursanti, and Yayan Hadiya. 2023. *Metodologi Penelitian Bisnis: Teori & Panduan Praktis Dalam Penelitian Bisnis*. Jambi: PT. Sonpedia Publishing Indonesia.

Wawra, Daniela. 2023. "Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison." P. hlm. 169-194 in *De Gruyter eBooks*. Berlin

Westin, Allan F. 2003. *Privacy and Freedom*. Dalam Edmon Makarim. *Kompasi Hukum Telematika*. Jakarta: Raja Grafindo Persada.

Wibowo, Agus, and Sri Yulianingsih. 2023. *Hukum Teknologi Informasi*. Semarang: Yayasan Prima Agus Teknik.

Wiraguna, Sidi A., and Megawati Barthos. 2025. *Hukum Privasi Dan Pelindungan Data Pribadi Di Indonesia*. edited by N. Rismawati. Bandung: CV Widina Media Utama.

Yanto, A. 2021. *Mazhab-Mazhab Hukum: Suatu Pengantar Memahami Dimensi Pemikiran Hukum*. Jakarta: Penerbit Segap Pustaka.

Yasid, D. R. A. 2016. *Logika Hukum: Dari Mazhab Rasionalisme Hukum Islam hingga Positivisme Hukum Barat*. Yogyakarta: Saufa.

Zainuddin Ali. 2019. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Zahrah, Muhammad Abu. 2009. *Konsep Hak Asasi Manusia dalam Islam*. Jakarta: Pustaka Al-Kautsar.

B. Jurnal

Abdillah, Ibnu, Nur Asyarah Tanjung, Aprila Ayu Puspita, Anis Nur Aqilah, and Yusuf Khalifah. 2024. "Pancasila Sebagai Pedoman Dasar Dalam Perlindungan Hukum Terhadap Hak Asasi Manusia." *Jurnal Moralita: Jurnal Pendidikan Pancasila Dan Kewarganegaraan* 5(2): 57-63. https://doi.org/10.36985/k6v8ap16.

Adhyputra, Muhammad Fadel, Thoriq Ahmadi, and Mohammad Rifqi. 2024. "Analisis Komparatif Rancangan LPPDP Indonesia Dengan Otoritas Pelindungan Data Singapura Dalam Penegakan Hukum Pelanggaran Data Pribadi: The Notion Of Personal Data Protection By Indonesia's Lppdp: A

Comparative Study With The Singapore Personal Data Prot." *Jurnal Nomokrasi* 2(2): 56-74. http://journal.unhas.ac.id/index.php/jnomokrasi/article/view/41388.

Adlhiyati, Zakki, dan Achmad Achmad. 2020. "Melacak Keadilan Dalam Regulasi Poligami: Kajian Filsafat Keadilan Aristoteles, Thomas Aquinas, dan John Rawls." *Undang: Jurnal Hukum* 2(2):409–431. DOI: 10.22437/ujh.2.2.409-431. https://doi.org/10.22437/ujh.2.2.409-431.

Aguspriyani, Yani, Miko Polindi, Putri Diesy Fitriani, Trisna Taufik Darmansyah, and Rezky Mehta Setiadi. 2023. "Pengaruh Strategi Digital Marketing Terhadap Keputusan Pembelian Produk Asuransi Pada Generasi Milenial." *AT-TAWASSUTH: Jurnal Ekonomi Islam* 8(1): 35-48. https://jurnal.uinsu.ac.id/index.php/tawassuth/article/download/14937/6830.

Ahyani, Edi, and Elfridawati Mai Dhuhani. 2024. "Transformasi Digital Dalam Manajemen Perkantoran Pendidikan: Sebuah Kajian Literatur." *Jurnal Visionary: Penelitian Dan Pengembangan Dibidang Administrasi Pendidikan* 12(1): 205-215. https://doi.org/10.33394/vis.v12i1.10785.

Aida, Melly, Yunita Maya Putri, Ria Wierma Putri, dan Ria Silviana. 2023. "Kepentingan Indonesia Mengaksesi Konvensi Apostille dan Relevansinya di Bidang Kenotariatan." *Jurnal Ilmiah Hukum Kenotariatan* 12(1):85–98. DOI: 10.28946/rpt.v12i1.2908.

Aisyah, Ririn Nur, Hana Khalidah, Surya Putri Nazrina, Johan Silalahi, and Dhini Aulia. 2025. "Efektivitas UU No. 8 Tahun 1999 Dalam Melindungi Data Pribadi Konsumen Di Sektor E-Commerce." *Jurnal Moralita: Jurnal Pendidikan Pancasila Dan Kewarganegaraan* 6(1): 9-18. https://doi.org/10.36985/v7dfhf27.

Alexander, Nicholas, Bayu Angga Wijaya, and Rico Wijaya Dewantoro. 2025. "Penerapan Blockchain Untuk Keamanan Data Rekam Medis Elektronik: Literatur Review." *AT-TAKLIM: Jurnal Pendidikan Multidisiplin* 2(3): 191-201. https://doi.org/10.71282/at-taklim.v2i3.210.

Alfi, Muhammad, Ni Putu Yundari, and Ahnaf Tsaqif. 2023. "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 6(2): 5. DOI: 10.7454/jkskn.v6i2.10082.

Alfitri, Nur Alfiana, Rahmawati Rahmawati, and Firmansyah Firmansyah. 2024. "Perlindungan Terhadap Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4(2): 92-111. DOI:10.54065/jss.4.2.2024.511.

Al Ghozali, Falah, and Try Hardyanthi. 2024. "Perlindungan Konsumen Pada Platform E-Commerce: Regulasi Dan Peran Pemerintah." *Ethics and Law Journal: Business and Notary* 2(3): 136-141. https://doi.org/10.61292/eljbn.220.

Al Hadad, Alwi. 2023. "Keamanan Data Dalam Proses Pemilu 2024: Identifikasi Dan Mitigasi Ancaman Kebocoran Data Elektoral." *Jurnal Keadilan Pemilu* 4(2):hlm. 86-98. doi: https://doi.org/10.55108/jkp.v4i2.429.

Al Mahdi, Muhammad Putra Syawal, and Irwan Triadi. 2025. "Dari Rectsvaccum Menuju Kepastian Hukum: Pembentukan Lembaga Perlindungan Data Pribadi Sebagai Penemuan Hukum Di Era Digital." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 12(11):hlm. 4416-4430. doi: https://doi.org/10.31604/jips.v12i11.2025.4416-4430.

Al Mustaqim, Dede. 2023. "Strategi Pengembangan Pariwisata Halal Sebagai Pendorong Ekonomi Berkelanjutan Berbasis Maqashid Syariah." *AB-JOIEC: Al-Bahjah Journal of Islamic Economics* 1(1): 26-43. https://doi.org/10.61553/abjoiec.v1i1.20

Amboro, Florianus Yudhi Priyo, and Viona Puspita. 2021. "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)." *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* 1: 415-427. https://journal.uib.ac.id/index.php/combines/article/view/4466.

Aminin, Rista Izza. 2024. "Analisis Implementasi Teknologi Blockchain Dalam Meningkatkan Transparansi, Efisiensi, Dan Keamanan Transaksi Keuangan Perbankan Syariah Indonesia." *Jurnal Hukum Ekonomi Syariah: AICONOMIA* 3(2): 92-106. https://doi.org/10.32939/acm.v3i2.4575.

Amir, Budi Praptawismacaya. 2024. "Pengaruh Globalisasi Terhadap Perekonomian Ditinjau Dari Hukum Niaga." *Syntax Literate; Jurnal Ilmiah Indonesia* 9(5): 2967-2975. http://dx.doi.org/10.36418/syntax-literate.v9i5.

Amri, Ahmad Ihsan, and Y. A. Triana Ohoiwutun. 2024. "Analisis Pelindungan data pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana." *Opinia de Journal* 4(1):hlm. 13-26. doi: https://doi.org/10.35888/opiniadejournal.v4i1.58.

Ananta Fadli Sutarli, and Shelly Kurniawan. 2023. "Peranan Pemerintah Melalui Undang-Undang Pelindungan data pribadi Dalam Menanggulangi Phising Di Indonesia." *INNOVATIVE: Journal Of Social Science Research* 3(2): 1-14. https://j-innovative.org/index.php/Innovative/article/view/760.

Ananta, Klarisa Desi, Triyo Ambodo, and Agus Tohawi. 2024. "Pengaruh Media Sosial Terhadap Peningkatan Kejahatan Siber Di Indonesia." *Islamic Law: Jurnal Siyasah* 9(2): 113-118. https://doi.org/10.53429/iljs.v9i2.858.

Anggen Suari, Kadek Rima, and I. Made Sarjana. 2023. “Menjaga Privasi Di Era Digital: Pelindungan data pribadi Di Indonesia.” *Jurnal Analisis Hukum* Vol. 6(1):hlm. 132-142. doi: 10.38043/jah.v6i1.4484.

Angnesia, Khetrina Maria, and Sidi Ahyar Wiraguna. 2025. “Analisis Pertanggungjawaban Hukum Pemerintah Dalam Menegakkan Pelindungan data pribadi yang bersifat spesifik Di Era Digital.” *Perspektif Administrasi Publik Dan Hukum* 2(2): 176-187. https://doi.org/10.62383/perspektif.v2i2.249

Anisa, Siti, Musyfikah Ilyas, dan Nurfaika Ishak. 2022. "Analisis Normatif Terhadap Perceraian Karena Penggunaan Media Sosial." *Jurnal Qadauna* 4(1): 307-320. DOI: 10.24252/qadauna.v4i1.30903.

Antoine, Revalina Annisa, Najalya Siti Farizqa, Alifia Hafizha Hasna, and Masta Pasaribu. 2025. “Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia).” *Jurnal Multidisiplin Ilmu Akademik* 2(1): 316-327. https://doi.org/10.61722/jmia.v2i1.3147.

Ardhana, Valian Yoga Pudya. 2024. “Konsep Smart City Dalam Tata Kelola Pemerintahan Dan Pembangunan Berkelanjutan.” *Journal of Computer Science and Information Technology* 1(2): 69-74. https://doi.org/10.59407/jcsit.v1i2.492.

Ardhianty, Indryana Widi. 2025. “Tantangan Dan Strategi Perlindungan Konsumen Pada Layanan Perbankan Di Tengah Kemajuan Teknologi.” *Jurnal Multidisiplin Ilmu Akademik* 2(2):hlm. 151-162. doi: https://doi.org/10.61722/jmia.v2i2.4223.

Ardika, I. Wayan Cenik. 2025. “Tinjauan Hukum Terhadap Pelindungan data pribadi Di Era Digital: Kasus Kebocoran Data Pengguna Layanan.” *Indonesian Journal of Law and Justice* 2(3): 1-11. https://doi.org/10.47134/ijlj.v2i3.3601.

Arianto, Dwiky, and Wafda Vivid Izziyana. 2026. “Peran Strategis Dewan Pengawas Syariah (DPS) Dalam Struktur Kelembagaan Keuangan Syariah.” *Ghanimah: Journal of Sharia Economics and Business* 2(1):hlm. 26-39. doi: 10.61169/ghanimah.v2i1.376.

Aritonang, Lenny Maria, Zyetwill Zyetwill, and Rara Handayani. 2025. “Analisis Hukum Terhadap Kebocoran Data Pribadi Dan Penyalahgunaan Identitas Dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.” *Ranah Research: Journal of Multidisciplinary Research and Development* Vol. 7(5):hlm. 3146-3158. doi: https://doi.org/10.38035/rrj.v7i5.1665.

Arkansyah, M., Ida Nadirah, dan Cakra Arbas. 2023. "Pengawasan Dalam

Pengadaan Barang dan Jasa: Optimalisasi Peran Pejabat Pembuat Komitmen Kementerian Perhubungan." *Jurnal Bedah Hukum* 7(1):287–292. https://jurnal.umsu.ac.id/index.php/sanksi/article/view/19056.

Arrasuli, Beni Kharisma, and Khairul Fahmi. 2023. "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi." *UNES Journal of Swara Justisia* 7(2): 369-392. https://doi.org/10.31933/ujsj.v7i2.351.

Asa, Agam Ibnu, and M. Mukhtasar Syamsuddin. 2025. "Rekontruksi Makna Pancasila Dalam Konteks Sumber Tertib Hukum (Tinjauan Filsafat Hukum)." *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKN* 12(1):hlm. 59-77. doi: https://doi.org/10.36706/jbti.v12i1.193.

Ashari, Mahmud. 2022. "Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga Adalah Data Pribadi." *Djkn.Kemenkeu.Go.Id*. Retrieved April 23, 2025 (https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html).

Aslam, Muhammad Nur, Abu Hasan Al Anshori, and Maulana Izaki. 2025. "Cloud Computing: Solusi Efektif Untuk Pengelolaan Data Di Era Digital." *Jurnal Batirsi* 8(2): 34-36. https://e-journal.stmik-tegal.ac.id/index.php/batirsi/article/view/89.

Atara, Irvin, Sharron Syallomeita, and Raffi Aqil Baihaqi Haksoro. 2025. "Analisis Kriminologi Terhadap Pencurian Data Pribadi Di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023." *Jurnal Ilmiah Penelitian Mahasiswa* 3(2): 129-140. https://doi.org/10.61722/jipm.v3i2.787.

Aulia, Elza. 2024. "Analisis Pasal 56 Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik Dari Perspektif Kepastian Hukum." *UNES Law Review* 7(1): 220-227. https://doi.org/10.31933/unesrev.v7i1.2267.

Ayiliani, Fanisa Mayda, and Elfia Farida. 2024. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6(3): 431-455. https://doi.org/10.14710/jphi.v6i3.%p.

Azhari, Farhan, Sumarno Sumarno, Achmad Fauzi, Demas Rizky Pratama, Muhammad Adityn Musyafa, Muhammad Rifa Nawawi, and Naufal Shafly Abdul Ghaffar. 2024. "Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-Wallet." *Jurnal Kewirausahaan Dan Multi Talenta* 2(2): 138-147. https://doi.org/10.38035/jkmt.v2i2.163.

Azmi, Muhamad Naufal Aulia, Habib Saifudin, Cristine T. Purba, Asri Suryaningtyas, and Urfani Syamuria Situmorang. 2024. "Analisa Kasus

Kebocoran Data Pada Bank Indonesia Dalam Sistem Perbankan: Indonesia." *Jurnal Multidisiplin Ilmu Akademik* 1(6): 448-458. https://doi.org/10.61722/jmia.v1i6.3267.

Bahram, Muhammad. 2023. "Transformasi Masyarakat Di Era Digital: Menjaga Kaidah Hukum Sebagai Landasan Utama." *SENTRI: Jurnal Riset Ilmiah* 2(5): 1733-1746. https://doi.org/10.55681/sentri.v2i5.884.

Bahtiar, Naylawati. 2024. "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah." *Development Policy and Management Review (DPMR)* 2(1): 85-100. http://journal.unhas.ac.id/index.php/DPMR/article/download/32144/11326.

Barli Tomia. n.d. "Perlindungan Hukum Terhadap Data Pribadi Di Indonesia Tantangan Dan Solusi Dalam Era Digital." *Kompasiana.Com*. Retrieved May 12, 2025 (https://www.kompasiana.com/adityasaputra3664/67814681c925c459f631bfe2/perlindungan-hukum-terhadap-data-pribadi-di-indonesia-tantangan-dan-solusi-dalam-era-digital).

Bestari, Novina Putri. 2024. "Misterius, Begini Nasib Lembaga Pengawasan Pelindungan data Pribadi." *Cnbcindonesia.Com*. Retrieved May 6, 2025 (https://www.cnbcindonesia.com/tech/20241114193435-37-588354/misterius-begini-nasib-lembaga-pengawasan-perlindungan-data-pribadi).

Bukit, Abigail Natalia, and Rahmi Ayunda. 2022. "Urgensi Pengesahan RUU Pelindungan data pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat." *Reformasi Hukum* 26(1): 1-20. https://doi.org/10.46257/jrh.v26i1.376.

Busroh, Firman Freaddy, Fatria Khairo, and Putri Difa Zhafirah. 2024. "Harmonisasi Regulasi Di Indonesia: Simplikasi Dan Sinkronisasi Untuk Peningkatan Efektivitas Hukum." *Jurnal Interpretasi Hukum* 5(1): 699-711. https://doi.org/10.22225/juinhum.5.1.7997.699-711.

Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat. 2025. "Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia." *Dame Journal of Law* Vol. 1(1):hlm. 111-133. https://doi.org/10.64344/djl.v1i1.6.

Caseba, Farah Labibah, and Totok Dewayanto. 2024. "Penerapan Artificial Intelligence, Big Data, Dan Blockchain Dalam Fintech Payment Terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review." *Diponegoro Journal of Accounting* 13(3): 1-15. https://ejournal3.undip.ac.id/index.php/accounting/article/view/46058.

Caturjayanti, Vermonita Dwi. 2020. “The Concept of Privacy by Design as the Protection of Personal Data of Users of the Application" Peduli Lindungi".” *Jurnal Hukum Lex Generalis* 1(9): 70-87. https://doi.org/10.56370/jhlg.v1i9.251.

Chandra, Imelda Audry, Vieta Imelda Cornelis, and Noenik Soekorini. 2025. “Pelindungan data pribadi Dalam Mencegah Tindak Pidana Penyalahgunaan Hak Pasien.” *Jurnal Pendidikan Dan Pengajaran* 6(2): 32-45. https://ijurnal.com/1/index.php/jpp/article/view/557.

Chaturvedi, Ashish. 2023. “Controversies in the Personal Data Protection Bill, 2019: An Analysis of Government Exemptions, Data Localization, and The Right to Be Forgotten.” *International Journal of Law Management & Humanities* 6(3): 803. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlmhs23&section=73

Choirunnisa, Laili, Try Hajar Caesar Oktaviana, Ahmad Ainur Ridlo, and Elva Imeldatur Rohmah. 2023. “Peran Sistem Pemerintah Berbasis Elektronik (SPBE) Dalam Meningkatkan Aksesibilitas Pelayanan Publik Di Indonesia.” *Sosio Yustisia: Jurnal Hukum Dan Perubahan Sosial* 3(1): 71-95. https://doi.org/10.15642/sosyus.v3i1.401.

Christiana, Veronika, Didik Suahriyanto, and Ismail Ismail. 2025. “Pelindungan data Nasabah Perbankan Dengan Perjanjian Pembukaan Rekening.” *Mutiara: Multidiciplinary Scientifict Journal* 3(1): 1-16. https://mutiara.al-makkipublisher.com/index.php/al/article/view/329.

Cross, Cassandra, and Thomas J. Holt. 2025. “Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims.” *Journal of Crime and Justice* Vol. 1(1):hlm. 1-24. doi: 10.1080/0735648X.2025.2535007.

Daeng, Yusuf, Nasri Linra, Atan Darham, Derry Handrianto, Risky Risandy Sianturi, Denny Martin, Rendy Pratama Putra, and Hendi Saputra. 2023. “Perlindungan Data Pribadi Dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi.” *Innovative: Journal Of Social Science Research* 3(6):hlm. 2898-2905. doi: https://j-innovative.org/index.php/Innovative/article/view/6662.

Darmayanti, Elda Septi, and Sidi Ahyar Wiraguna. 2025. “Tanggung Jawab Hukum Pinjaman Online Terhadap Penyebaran Data Nasabah Secara Ilegal.” *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3(2): 233-251. https://doi.org/10.59246/aladalah.v3i2.1313

Delpiero, Maichle, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah. 2021. “Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Pelindungan data pribadi

Pengguna Pada Kasus Kebocoran Data." *Padjadjaran Law Review* 9(1): 1-22. https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509.

Dewi, Sinta, Robert Walters, Leon Trakman, and Bruno Zeller. 2019. "The Role of International Mediation in Data Protection and Privacy Law-Can It Be Effective?" *University of New South Wales Law Research Series* Vol. 1(1):hlm. 61-73. doi: https://dx.doi.org/10.2139/ssrn.3462113.

Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Arwa Meida Aninda. 2023. "Pelindungan data pribadi Di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1(2): 66-90. https://doi.org/10.37253/sasenal.v1i2.8579.

Dwisvimiar, Inge. 2011. "Keadilan Dalam Perspektif Filsafat Ilmu Hukum." *Jurnal Dinamika Hukum* 11(3):522–531. https://dinamikahukum.fh.unsoed.ac.id/index.php/JDH/article/viewFile/179/127.

Duo, W., M. Zhou, dan A. Abusorrah. 2022. "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges." *IEEE/CAA Journal of Automatica Sinica* 9(5):784–800. https://doi.org/10.1109/JAS.2022.105548.

Edo, Onome, Imokhai Tenebe, Egbe-Etu Etu, Atamgbo Ayuwu, Joshua Emakhu, and Shakiru Adebiyi. 2022. "Zero Trust Architecture: Trend and Impact on Information Security." *International Journal of Emerging Technology and Advanced Engineering* Vol. 12(7):hlm. 140-147. doi: 10.46338/ijetae0722_15.

Endiputra, Fadil Isam Yusuf, Adrian Pratama Nasution, and Akbar Dwi Febrian. 2025. "Blockchain: Inovasi Pembaruan Dalam Sektor Pengamanan E-Government Dalam Meningkatkan Sistem Akuntabilitas Pemerintahan Di Indonesia." *Journal of Legal Reform* 1(1): 1-14.

Erikha, Annisa, and Zainal Arifin Hoesein. 2025. "Strategi Pencegahan Kebocoran Data Pribadi Melalui Peran Kominfo Dan Gerakan Siberkreasi Dalam Edukasi Digital." *Jurnal Retentum* 7(1): 48-64. http://dx.doi.org/10.46930/retentum.v7i1.5272.

Fadhilah, Na'im, dan Deswalantri. 2022. "Nilai-Nilai Pendidikan Karakter dalam Al-Qur'an Surat Al-Hujurat Ayat 11-13: Kajian Tafsir Al-Azhar Karya Hamka." Jurnal Pendidikan Tambusai Vol. 6(3): hlm. 13525-13534. doi: 10.31004/jptam.v6i3.4468.

Fadillah, Nessya, Andini Diah Pitaloka, Nur Herfina, and Sri Handayani. 2025. "Kewajiban Transparansi Dan Pelindungan data Pengguna Dalam Layanan Paylater Pada Aplikasi Shopee." *Jurnal Riset Multidisiplin Edukasi* 2(5): 1-14. https://doi.org/10.71282/jurmie.v2i5.256.

Faraby, Ahmad Habib Al. 2024. “Perkembangan Teknologi Informasi Dan Transaksi Elektronika (ITE) Di Indonesia (Suatu Kajian Dari Peran Penyidik Kepolisian Dalam Menangani Penyalahgunaan Informasi Dan Transaksi Elektronika (Ite)).” *Faraby Meraja Journal* 7(1): 48-61. https://garuda.kemdiktisaintek.go.id/documents/detail/4372500.

Farhan, Shendy Rahmat, and Asep Suherman. 2024. “Perlindungan Hukum Terhadap Penyandang Disabilitas Dalam Perspektif Hak Asasi Manusia Di Indonesia.” *Jurnal Inovasi Hukum Dan Kebijakan* 5(4): 287-303. https://ejurnals.com/ojs/index.php/jihk/article/view/493.

Farid, Wajdi, dan Rahmat Ramadhani. 2022. "Legal Problems of Land Services Daring." *International Journal Reglement & Society* 3(1):19–29. https://jurnal.bundamediagrup.co.id/index.php/ijrs/article/download/201/191

Fatmawati, Yuli. 2024. “Penerapan Kebijakan Data Privacy Di Era Teknologi 5G Di Indonesia: The Implementation of Data Privacy Policies in the 5G Technology Era in Indonesia.” *Pencerah Publik* 11(1): 42-49. https://doi.org/10.33084/pencerah.v11i1.7851

Faustina, Yaffa Ivana, and Sidi Ahyar Wiraguna. 2025. “Pelindungan data Pengguna Oleh Marketplace Shopee Berdasarkan Undang-Undang Nomor 27 Tahun 2022.” *Jurnal Kajian Hukum Dan Kebijakan Publik* 2(2): 1037-1044. https://doi.org/10.62379/p1f2tr70.

Fauzi, Muhamad Rizal, Saimi Saimi, and Fathoni Fathoni. 2024. “Tantangan Dan Solusi Administrasi Kesehatan Di Era Digital (Tinjauan Literature Review Atas Implementasi Teknologi).” *AL-MIKRAJ Jurnal Studi Islam Dan Humaniora* (E-ISSN 2745-4584) 5(01): 1093-1103.

Fauziah, Yessy Andriani, Husin Alhadad, and Yudhistira Prawira Utama. 2024. “Etika Dan Tantangan Penggunaan Kecerdasan Buatan Dalam Kedokteran Gigi.” *Jurnal Hukum Dan Etika Kesehatan* 4(2): 1-14. https://doi.org/10.30649/jhek.v4i2.200.

Fikri, Khairul, dan Umi Wasilatul Firdausiyah. 2021. “Privasi dalam Dunia Digital: Analisis QS. An-Nur (24): 27 Menggunakan Pendekatan Ma’na-Cum-Maghza.” *Islamika Inside: Jurnal Keislaman dan Humaniora* 7(2):198–222. https://doi.org/10.35719/islamikainside.v7i2.135.

Firmansyah, Prado Dian, Achmad Fauzi, Riky Barja, Andrea Putra Mulyana, Theresia Naomi Putri, Adam Surachman, and Gilang Ramadhan. 2024. “Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Pelindungan data Dengan Teknologi Lanjutan.” *Jurnal Kewirausahaan Dan Multi Talenta* 2(2): 112-125. https://doi.org/10.38035/jkmt.v2i2.160

Fristanto, Kevin Bramantya, and Sultoni Fikri. 2025. "Perlindungan Hukum Terhadap Penggunaan Data Pribadi Oleh Partai Politik Tanpa Izin." *Journal Evidence Of Law* 4(1): 266-271. https://doi.org/10.59066/jel.v4i1.1030

Fuad, Fuad, Rio Rama Baskara, and Anas Urbaningrum. 2025. "Desain Perlindungan Hukum Bagi Konsumen Dan Data Pribadi Untuk Kegiatan Usaha Menggunakan Fintech Di Indonesia." *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana* 7(1): 176-187. http://dx.doi.org/10.46930/jurnalrectum.v7i1.5360

Garamba, Yafianus, and Aryanto Nur. 2024. "Analisis Kepuasan Pelanggan Pada E-Commerce." *Jurnal Ilmu Komputer Dan Informatika* 1(2): 27-37.). https://jurnal.globalscients.com/index.php/jiki/article/view/48.

Gatt, Lucilla, and Ilaria Amelia Caggiano. 2022. "Consumers and Digital Environments as a Structural Vulnerability Relationship." *European Journal of Privacy Law & Technologies* Vol. 1(2):hlm. 8-16. doi: https://doi.org/10.57230/EJPLT222LGIAC.

Gerasela, Elza Noveliani, Dapid Aryando, and Sani Safitri. 2025. "Perkembangan Ilmu Pengetahuan Dan Teknologi: Menyongsong Era Baru Dalam Prespektif Ilmu Sosial." *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 4(4):hlm. 5983-5989. doi: 10.56799/peshum.v4i4.9257.

Gustryan, Muhammad, and Zainal Arifin Hoesein. 2025. "Peran Undang-Undang ITE Dan Undang-Undang Pelindungan data pribadi Dalam Pelindungan data Dan Privasi Di Era Ekonomi Digital." *Jurnal Minfo Polgan* Vol. 14(2):hlm. 3333-3343. doi: https://doi.org/10.33395/jmp.v14i2.15746.

Gultom, Olisias, Auditya Firza Saputra, and Muhammad Faiz Aziz. 2021. "Pelindungan data pribadi Di Indonesia." *Asian Journal of Engineering, Social and Health* 5: 135. https://igj.or.id/wp-content/uploads/2022/08/Perlindungan-Data-Pribadi-Indonesia-APRN-Final-report.pdf

Gunawan, Imam. 2024. "Upaya Preventif Dan Represif Dalam Penanggulangan Kebocoran Data Pada Penyelenggaraan Pinjaman Online." *Officium Notarium* 4(1): 25-49. https://doi.org/10.20885/JON.vol4.iss1.art3.

Gutari, Revol. 2022. "Tinjauan Yuridis Pendekatan Komparatif Dalam Antropologi Hukum." *OSF Preprint* hlm. 1-14. doi: https://doi.org/10.31219/osf.io/kz5e8.

Hanafi, Fauzan, Abdul Balgis Hi Talib, and Musaddi Din. 2025. "Analisis Keadilan Substansial Pada Penerapan Undang-Undang Perlindungan Data Pribadi Terhadap Hak Pemilik Data Dalam Perspektif Hukum Positif Dan Hukum Islam." *Qadauna: Jurnal Ilmiah Mahasiswa Hukum Keluarga Islam* 6(3):hlm. 274-291. doi: https://doi.org/10.24252/qadauna.v6i3.52578.

Hansen Samin, Herol. 2023. “Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif.” *Jurnal Sains Student Research* 1(2): 1-15. https://doi.org/10.61722/jirs.v1i3.386.

Hapsari, Dwi Ratna Indri, and Kukuh Dwi Kurniawan. 2020. “Consumer Protection: Principle of Proportionality in Banking Credit Agreement under the Indonesian Law.” *Fiat Justisia: Jurnal Ilmu Hukum* Vol. 14(4): hlm. 337-352. https://scholar.archive.org/work/csc3bwa73bggveu3rz33sezla4/access/wayback/https://jurnal.fh.unila.ac.id/index.php/fiat/article/download/1884/1549.

Hapsari, Paramita. 2025. “Blockchain Untuk Perlindungan Hak Cipta: Solusi Inovatif Untuk Kasus Konten Viral.” *Pro Film Jurnal* 7(1): 38-63. https://doi.org/10.56849/jpf.v4i1.72.

Hariyanto, Pipit Aprilia Susanti, Michael Hadjaat, Muhammad Wasil, dan Agnes Dwita Susilawati. 2023. "Meningkatkan Literasi Teknologi di Masyarakat Pedesaan Melalui Pelatihan Digital." *Jurnal Abdimas Peradaban* 4(2):12–21. DOI:10.54783/ap.v4i2.24.

Hasibuan, Diva Viola Natasya, and Muhammad Irwan Padli Nasution. 2024. “Penerapan Big Data Dalam Pemasaran Digital: Studi Kasus Pada Industri E-Commerce Di Indonesia.” *Jurnal Ilmiah Nusantara* 1(4): 776-783. https://doi.org/10.61722/jinu.v1i4.1913.

Hartanto, Hartanto. 2024. “Antisipasi Dan Perkembangan Kejahatan Dunia Maya.” *Virtue Jurisprudence* Vol. 2(2):hlm. 162-173. doi: https://jurnal.usp.ac.id/index.php/virtue-jurispudence/article/download/158/126.

Herera, Dinda Aprilita, dan Muhamad Hasan Sebyar. 2023. "Pelindungan Hukum Terhadap Serangan Siber: Tinjauan atas Kebijakan dan Regulasi Terbaru." *Jurnal Hukum dan Kewarganegaraan* 1(5):1–16. DOI: 10.3783/causa.v1i1.571.

Hermanto, Bagus, Rengga Kusuma Putra, Lita Tyesta Addy Listya Wardhani, Ni Luh Gede Astariyani, Retno Eko Mardani, and Anatolijs Krivins. 2026. “Diskursus Epistemologis Dalam Pembentukan Hukum Digital: Quo Vadis Navigasi Perundang-Undangan Indonesia Kedepan.” *Jurnal Ilmu Perundang-Undangan* 2(1):hlm. 14-26. doi: https://asipper.or.id/index.php/asipper/article/view/6.

Hestianingsih, Unun, and Nurmadiah. 2024. “Analisis Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Elektronik Di Indonesia.” *Jurnal Pro Justice* 2(8): 234-235. https://www.jurnal.uts.ac.id/index.php/projustice/article/view/5222.

Hidayat, Noviani Arum Sari Nur, Ratih Novi Septian, and Yusuf Tri Herlambang.

2024. “Sosial Media Dalam Masyarakat Sebagai Konsep Nyata Determinisme Teknologi.” *UPGRADE: Jurnal Pendidikan Teknologi Informasi* 1(2): 73-80. https://doi.org/10.30812/upgrade.v1i2.3715.

Hidayat, W., & Sarono, A. (2022). Pelindungan hukum terhadap konsumen jasa umroh/haji dalam perbuatan melawan hukum. *Notarius*, 15(1), 283–295. https://ejournal.undip.ac.id/index.php/notarius/article/view/46041.

Hoofnagle, Chris Jay, Bart van der Sloot, dan Frederik Zuiderveen Borgesius. 2019. "The European Union *General Data Protection Regulation* : What It Is and What It Means." *Information and Communications Technology Law* 28(1):65–98. https://doi.org/10.1080/13600834.2019.1573501.

Ibna, Aulia Zaky, and Muhammad Irwan Padli Nasution. 2024. “Implikasi Penggunaan Basis Data Dalam Era Big Data.” *Journal Sains Student Research* 2(4): 255-265. https://doi.org/10.61722/jssr.v2i4.1995.

Ichsan, Matthew Tommy. 2024. “Peran Telematika Dalam Era Digital: Kemajuan Zaman, E-Commerce, Dan Tantangan Keamanan Data.” *Jurnal Telematika* 1(1): 1-9. https://www.academia.edu/download/120786932.

Ihsan, Muhammad, Fitri Yani, Fani Budi Kartika, Edi Kristanta Tarigan, and Rita Natalia Pangaribuan. 2024. “Penyuluhan Perlindungan Hukum Data Pribadi Dalam Penyelenggaraan Fintech Di Desa Percut Sei Tuan.” *JUDIMAS* 5(1): 19-26. https://www.ojs.stmikpontianak.ac.id/judimas/article/view/485.

Ikrom, Moh Bagas Fadhli Dzil, and Badrut Tamam. 2024. “Perlindungan Hukum Hak Privasi Warga Negara Terhadap Kebocoran Data Pribadi Di Indonesia.” *Constituion Journal* 3(2): 139-154. https://doi.org/10.35719/constitution.v3i2.105.

Ilham, Mahipal, Muhammad Ramadhani, Muhammad Said Ridho, Rifqi Hidayat, and Yusuf Afrenoldi Todi. 2025. “Komparasi Hukum Indonesia Dan Hukum Islam Terhadap Pelindungan data pribadi Dalam Transaksi Ekonomi Syariah Digital.” *Jurnal Media Akademik (JMA)* 3(4): 1-21. https://doi.org/10.62281/f9fnqv92.

Ilham, Muh. Arhanul, Haslindah, and Muh. Arafah. 2024. “Analisis Perlindungan Hak Konsumen Pada Transaksi Jual Beli Online Di Masa Kini Ditinjau Dalam Perspektif Islam (Studi Pada Pengguna Online Shop Di Kecamatan Tanete Riattang Kabupaten Bone).” *Jurnal Ilmiah Multidisiplin Terpadu* 8(9): 213-241. https://oaj.jurnalhst.com/index.php/jimt/article/view/4414/4520

Indriani, Masitoh, and Annida Aqiila Putri. 2023. “Persetujuan Dinamis Sebagai Sarana Optimalisasi Pelindungan data pribadi yang bersifat spesifik Dan Hak Atas Privasi (The Dynamic Consent for Optimizing Personal Data Protection

and The Right to Privacy).” *Jurnal HAM* 14(2): 105-122. http://dx.doi.org/10.30641/ham.2023.14.105-122

Irawan, Iwan. 2024. “Penerapan Etika Pancasila Dalam Pengembangan Kecerdasan Buatan Yang Bertanggung Jawab Di Indonesia.” *Journal Bit-Tech* Vol. 7(2):hlm. 263-271. https://doi.org/10.32877/bt.v7i2.1740.

Irsyahma, Ahmat Yasir, and Dwi Putri Lestarika. 2024. “Hak Asasi Manusia Di Era Globalisasi Pers.” *Indonesian Research Journal on Education* 4(4): 1870-1876. https://doi.org/10.31004/irje.v4i4.1568

Irvita, Misnah, Wijayono Hadi Sukrisno, Husni Thamrin, and Robi Rendra Tribuana. 2024. “Pengawasan Pemerintah Terhadap Pelanggaran Yang Dilakukan Oleh Lembaga Swadaya Masyarakat (Lsm): Meningkatkan Efektivitas Pengawasan Pemerintah Terhadap Pelanggaran Oleh Lembaga Swadaya Masyarakat (Lsm).” *Jurnal Legalitas (JLE)* 2(1): 1-13. https://doi.org/10.58819/jle.v2i1.113

Iskandar, Iskandar, Shinta Azzahra Sudrajat, Ryan Fachryan Lesmana Putra, Hamdan Purnama, Muhammad Rosyid Ridho, and Diah Nurafifah. 2025. “Analisis Kritis Terhadap Teori Hukum Murni Dalam Perkembangan Hukum Kontemporer.” *TERAJU* 7(01): 48-65. https://doi.org/10.35961/teraju.v7i01.1926.

Ismail Koto, Ida Hanifah, Surya Perdana, Tarmizi, dan Ida Nadirah. 2023. "Pelindungan Hukum Atas Kekayaan Intelektual Perspektif Hukum Islam." *Jurnal Yuridis* 10(2):66–73. https://doi.org/10.35586/jyur.v10i2.7142

Isnugraheny, Rizqika Farah, Zahra Ekasiwi Megawati, and Siti Susilawati. 2024. “Optimalisasi Prinsip Kerahasiaan Data Nasabah Dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi.” *Media Hukum Indonesia (Mhi)* 2(4). https://doi.org/10.5281/zenodo.14181761

Jaang, Syaharie. 2023. "Analisis Pelindungan Hukum Terhadap Konsumen Berdasarkan Prinsip Keadilan." *Jurnal Hukum dan HAM Wara Sains* 2(5):349–357. https://wnj.westscience-press.com/index.php/jhhws/article/download/303/241/1532.

Jamal, Rayyan, Achmad Alfarizal Ikhval, Nova Ainun Nisa, Salwa Hulyatul Qulbi, and Muhammad Usman Arifin. 2024. “Penggunaan Teknologi Informasi Dalam Mengoptimalisasi Supply Chain Management.” *Jurnal Inovasi Global* 2(7): 737-750. https://doi.org/10.58344/jig.v2i7.117

Jannah, Miftahul, Muhamad Faris Hidayat, Mutiara Agustiyyani, Pandu Wira Buana, and Fenny Purwani. 2024. “Implementasi Autentikasi Biometrik Untuk Meningkatkan Keamanan Dan Privasi Pengguna Dompet Digital.” *Journal of Scientech Research and Development* 6(2): 531-539. https://doi.org/10.56670/jsrd.v6i2.606.

Judijanto, Loso. 2025. "Aplikasi Artificial Intelligence (Ai) Dalam Proses Administratif Pemerintahan: Aspek Hukum Dan Regulasi." *ADMIN: Jurnal Administrasi Negara* 3(2): 8-15. https://injoqast.net/index.php/ADIMEN/article/view/71.

Judijanto, Loso, and Al-Amin. 2025. "Transformasi Digital Dalam Pelayanan Publik: Implikasi Dan Tantangan Hukum Administrasi Negara." *Jurnal Administrasi Negara* 3(2): 1-7. https://injoqast.net/index.php/ADIMEN/article/view/70

Julianti, Desi. 2024. "Strategi Kebijakan Penguatan Pelayanan Publik Dan Pengawasan Perizinan Berusaha Dengan Aplikasi Berbasis Teknologi Informasi." *Kybernology Jurnal Ilmu Pemerintahan Dan Administrasi Publik* 2(2): 324-363. https://doi.org/10.71128/kybernology.v2i2.131

Junaedi, Asep Mahbub. 2025. "Urgensi Pelindungan data pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan data Pribadi." *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan* 5(2):hlm. 247-257. https://doi.org/10.51878/knowledge.v5i2.5269.

Kadir, Zul Khadir. 2025. "Dari Privasi Ke Eksploitasi: Memetakan Jejak Kriminalisasi Revenge Porn Dalam Era Media Sosial." *Dewantara: Jurnal Pendidikan Sosial Humaniora* 4(1): 133-152. https://elibrary.ru/item.asp?id=81423535

Kanaya, Safira, Iffat Husna, and Fatma Ulfatun Najicha. 2023. "Pancasila Dan Hubungannya Dengan Hak Asasi Manusia Di Indonesia." *JCE: Jurnal Civic Education* 7(2): 104-112. https://ejurnal.unima.ac.id/index.php/civic-edu/article/view/7869

Karjalainen, Tuulia. 2022. "All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm." *European Data Protection Law Review* Vol. 8(1):hlm. 19-30. doi: https://doi.org/10.21552/edpl/2022/1/6.

Kartiko, Nafis Dwi, Samuel Putra Soegiono, Carissa Amanda Siswanto, and Rizky Pratama Putra Karo-Karo. 2023. "Konsekuensi Yuridis Pengaturan Pelindungan data pribadi Terhadap Data Wajib Pajak Dalam Perspektif Perpajakan." *National Conference on Law Studies (NCOLS)* 5: 355-365. https://conference.upnvj.ac.id/index.php/ncols/article/view/2698.

KK, Azizah Shodiqoh Rafidah, and Happy Novasila Maharani. 2024. "Inovasi Dan Pengembangan Produk Keuangan Syariah: Tantangan Dan Prospek Di Era Revolusi Industri 4.0." *Jurnal Ilmiah Edunomika* 8(1): 1-14. https://jurnal.stie-aas.ac.id/index.php/jie/article/view/11649.

Kriswandaru, Althea Serafim, Berliant Pratiwi, and Suwardi. 2024. "Efektivitas

Kebijakan Pelindungan data pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus." *Jurnal Ilmu Hukum Dan Sosial* 2(4): 740-755. doi: 10.51903/hakim.v2i04.2157.

Kriswandaru, Althea Serafim, Berliant Pratiwi, and Suwardi Suwardi. 2024. "Efektivitas Kebijakan Pelindungan data pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus." *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2(4): 740-756. https://doi.org/10.51903/hakim.v2i4.2157

Kurnianingrum, Trias Palupi. 2023. "Urgensi Pelindungan data pribadi yang bersifat spesifik Konsumen Di Era Ekonomi Digital." *Kajian* 25(3): 197-216. https://doi.org/10.22212/kajian.v25i3.3893.

Kurniawan, Ade Agung, and Muhlishatun Niswah. 2024. "Etika Profesional Pengembangan Teknologi Informasi Serta Tanggung Jawab Di PT Anugrah Bungo Lestari." *Jurnal Pengembangan Teknologi Informasi Dan Komunikasi (JUPTIK)* 2(2): 60-67. https://doi.org/10.52060/juptik.v2i2.2681

Laia, Fariaman. 2022. "Penerapan Hukum Pidana Pada Tindak Pidana Gratifikasi Yang Dilakukan Dalam Jabatan." *Jurnal Panah Keadilan* Vol. 1(2):hlm. 1-16. https://doi.org/10.57094/jpk.v1i2.448.

Laksana, Tri Ginanjar, and Sri Mulyani. 2024. "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan." *Jurnal Ilmiah Multidisiplin* 3(01): 109-122. https://doi.org/10.56127/jukim.v3i01.1143.

Lazuardi, Maulana, Annisabella Oktaviani, and Randi Setiawan Qodri. 2025. "Urgensi Pembentukan Kelembagaan Independen Sebagai Penguatan Pelindungan data pribadi Untuk Melindungi Hak Privasi Warga Negara." *Journal of Legal Reform* 1(1): 26-39. https://journal.unnes.ac.id/journals/jllr

Leski Rizkinaswara. n.d. "Empat Pihak Yang Harus Melindungi Data Pribadi Di Ruang Digital – Ditjen Aptika." *Aptika.Kominfo.Go.Id*. Retrieved May 9, 2025 (https://aptika.kominfo.go.id/2020/07/empat-pihak-yang-harus-melindungi-data-pribadi-di-ruang-digital/).

Lestari, Lusi, Naura Athira, Rintan Gitaria, and Sri Handayani. 2025. "Dampak Kebijakan Pelindungan data Pribadi: Implikasi Terhadap Praktik Pemasaran Digital Di Aplikasi Tokopedia Indonesia." *Integrative Perspectives of Social and Science Journal* 2(02): 1843-1852. https://ipssj.com/index.php/ojs/article/view/266

Lilik Mulyadi. 2009. "Teori Hukum Pembangunan Prof. Dr. Mochtar Kusumaatmadja, S.H., Ll.M." *Jurnal Hukum Indonesia* 8(2):1–29. https://badilum.mahkamahagung.go.id/upload_file/img/article/doc/kajian_deskriptif_analitis_teori_hukum_pembangunan.pdf.

Lum'ah, Diana Durrotul, Suqiyah Musafa'ah, dan Muhammad Ihsan Mahbub. 2025. "The Paradigm of Digital Privacy in Indonesian Tafsir: A Study of Tafsir Al-Azhar on QS. Al-Hujurāt (49): 12 in the Age of Information." *MUSHAF: Jurnal Tafsir Berwawasan Keindonesiaan* 5(2):235–249. https://doi.org/10.33650/mushaf.v5i2.11148.

Mahameru, Danil Erlangga, Aisyah Nurhalizah, Haikal Badjeber, Ahmad Wildan, and Haikal Rahmadia. 2023. "Implementasi UU Pelindungan data pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Jurnal Esensi Hukum* 5(2): 115-131. https://doi.org/10.35586/esensihukum.v5i2.240.

Mahanani, Anajeng Esri Edhi. 2024. "Urgensi Kewenangan Mahkamah Konstitusi Dalam Pengujian Dan Pengaduan Konstitusional Atas Undang-Undang Non-Meaningful Participation." *Journal of Indonesian Law* 5(2): 199-229. doi: 10.18326/jil.v5i2.

Maharani, Rista, and Andria Luhur Prakoso. 2024. "Pelindungan data pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7(1): 333-347. https://doi.org/10.26623/julr.v7i1.8705

Maheswari, Elvina Putri, and Sidi Ahyar Wiraguna. 2025. "Urgensi Persetujuan Pemilik Data Dalam Pengelolaan Data Pribadi Oleh Platform Digital." *Jurnal Ilmu Komunikasi Dan Sosial Politik* 2(4): 908-914. https://doi.org/10.62379/jiksp.v2i4.2498

Makkawaru, Zulkifli, and Almusawir Almusawir. 2024. "Perlindungan Hukum Data Pribadi Dalam Perspektif Hak Asasi Manusia." *Indonesian Journal of Legality of Law* 7(1): 46-51. https://doi.org/10.35965/ijlf.v7i1.5267

Manalu, Iwandi Agung, Usman Usman Lubis, and Yati Sharfina Desiandri. 2024. "Hak Asasi Manusia Dan Keadilan Sosial: Analisis Implementasi Nilai-Nilai Pancasila Dalam Sistem Peradilan." *Innovative: Journal of Social Science Research* 4(6):hlm. 5308-5316. doi: https://doi.org/10.31004/innovative.v4i6.17117.

Manan, Abdul. 2023. "Disrupsi Teknologi Hukum Terhadap Jasa Advokat Dalam Pandangan Hukum Pembangunan Mochtar Kusumaatmadja." *Reformasi Hukum* 27(2): 270-276. https://doi.org/10.46257/jrh.v27i2.622

Manurung, Jonathan, and Tom Finaldin. 2025. "Peran ASEAN Melalui Cybersecurity Cooperation Strategy (ACCS) Dalam Menangani Kejahatan Siber Di Indonesia." *Global Mind* 7(1): 31-38. https://doi.org/10.53675/jgm.v7i1.1217

Matheus, Juan, and Ariawan Gunadi. 2024. "Pembentukan Lembaga Pengawas Pelindungan data pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *Justisi* 10(1): 20-35.

https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Megawati, dan Rahmiati. 2019. "Efektivitas Pelayanan Terpadu dalam Perizinan Mendirikan Bangunan Guna Mewujudkan Kualitas Pelayanan Publik di Kabupaten Sinjai." *Siyasatuna: Jurnal Ilmiah Mahasiswa Siyasah Syar'iyyah* 1(1): 16-29. https://journal.uin-alauddin.ac.id/index.php/siyasatuna/article/view/10536.

Milafebina, Rachel, Idham Putra Lesmana, and Moody Rizqy Syailendra. 2023. "Pelindungan data pribadi Terhadap Kebocoran Data Pelanggan E-Commerence Di Indonesia." *Jurnal Tana Mana* 4(1): 157-169. https://doi.org/10.33648/jtm.v4i1.331

Miswanto, Agus. 2022. "Rekognisi Dan Redistribusi Dalam Pencapaian Keadilan Sosial: Analisis Komparatif Terhadap Unsur-unsur Teoritis Nancy Fraser Dan Axel Honneth." *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 11(2): 141-160. doi: 10.14421/sh.v11i2.2748.

Molitor, Dominik, Aditya Saharia, Viju Raghupathi, and Wullianallur Raghupathi. 2024. "Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study." *Journal of Information Security* Vol. 15(02):hlm. 168-195. doi: 10.4236/jis.2024.152011.

Mufrihah, Wilda Malika, and Nandang Najmudin. 2024. "Transformasi Hukum Dagang Internasional Di Era Teknologi Blockchain Dan Cryptocurrency." *Ikraith-Ekonomika* 7(3): 382-396. https://journals.upi-yai.ac.id/index.php/IKRAITH-EKONOMIKA/article/view/4455

Muin, Indriani. 2023. "Pelindungan data pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia." *Journal Law And Justice* 1(2): 81-91. https://jurnalilmiah.co.id/index.php/MJPJLJ/article/view/30

Munajat, Andi Ahmad, and Hudi Yusuf. 2024. "Peran Teknologi Informasi Dalam Pencegahan Dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital." *JIIC: Jurnal Intelek Insan Cendikia* 1(9): 4853-4865. https://jicnusantara.com/index.php/jiic/article/view/1385

Munthe, Anselinus Kevin, Achmad Fauzi, Alfath Nare Utama, Herlin Rahmasari, Lola Kambuno, Audri Angelia Ignesia, Dwi Nanda Oktaviany, and Agung Setiawan. 2024. "Peran Manajemen Sekuriti Terhadap Keamanan Data Dan Kepercayaan Konsumen Pada Pengguna Ojek Online." *IJESM Indonesian Journal of Economics and Strategic Management* 2(2): 1598-1611. https://doi.org/10.69718/ijesm.v2i2.221

Muslimah. 2025. "Integrasi Ilmu Hukum Dan Teknologi Etika Dan Regulasi Dalam

Era Digital." *Jurnal Hukum Dan Kolaborasi Keilmuan* 1(1):hlm. 27-34. doi: https://terranovajournal.com/Interlegal/article/view/109.

Muzairoh, Erni, Suharso Suharso, Dilli Trisna Noviasari, and Habib Muhsin Syafingi. 2024. "Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital Dalam Prespektif Hak Asasi Manusia." *Borobudur Law and Society Journal* 3(1): 31-36. https://doi.org/10.31603/11824

Nainggolan, Alfredo, Ivo E. Lumbantoruan, and Sahata Manalu. 2024. "Eksistensi Negara Hukum Dalam Era Digital." *MIMBAR KEADILAN: Jurnal Ilmu Hukum* 1(3):hlm. 62-70. doi: https://doi.org/10.5139.vol1iss3pp62.

Najwa, Fadhila Rahman. 2024. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia." *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum* 2(1): 8-16. https://doi.org/10.32520/albahts.v2i1.3044

Natamiharja, Rudi, dan Mindoria Stefany. 2019. "Pelindungan Hukum Atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Selular)." *Prodigy Jurnal Perundang-undangan* 7(2):115–137. http://repository.lppm.unila.ac.id/20585/

Naufal, Irfan, and Ali Rokhman. 2024. "Analisis Ketahanan Data Dan Keamanan Informasi Dalam Manajemen Publik Di Era Digital." *Jurnal Pemasaran Bisnis* 6(3): 259-277. https://journalversa.com/s/index.php/jpb/article/view/4005

Negarawati, Esa, and Siti Rohana. 2024. "Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital." *Jurnal Ekonomi, Bisnis Dan Manajemen* 3(4): 46-60. https://jurnal-stiepari.ac.id/index.php/gemilang/article/view/1573

Ngamal, Yohanes, dan Maximus Ali Perajaka. 2021. "Penerapan Unsur-unsur Manajemen Risiko Teknologi Digital di Lembaga Perbankan Berkaca pada Cetak Biru Transformasi Digital Perbankan Indonesia." *Jurnal Manajemen Risiko* 2(2):59–74. DOI: 10.33541/mr.v2iiv.4099.

Niffari, Hanifan. 2020. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7(1):hlm. 105-119. doi: https://doi.org/10.35814/selisik.v6i1.1699.

Nofita Rudiani Asbanu, Claudina Margarida Freitas Belo, and Yakobus Adi Saingo. 2025. "Analisis Peran DPR Dalam Menyuarakan Kepentingan Rakyat Berdasarkan Sila Keempat Pancasila." *MUTIARA: Jurnal Ilmiah Multidisiplin Indonesia* 3(1):hlm. 120-134. doi: 10.61404/jimi.v3i1.364.

Noveno, Bonggal. 2025. "Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of

Information Security Questionnaire (HAIS-Q) Di Universitas Telkom Bandung." *E-Proceeding of Engineering* 12(1): 2282-2293. https://doi.org/10.25124/logic.v3i2.9590

Novida, Diah Rachmawatie. 2025. "Evolusi Sistem Informasi Akuntansi Dalam Era Digital: Tinjauan Literatur Tentang Tren, Tantangan, Dan Peluang." *Jurnal Minfo Polgan* 14(1): 77-85. https://doi.org/10.33395/jmp.v14i1.14628

Nugroho, Inaz Indra, Reza Pratiwi, and Salsabila Rahma Az Zahro. 2021. "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia." *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal* 1(2): 115-129. https://doi.org/10.15294/ipmhi.v1i2.53698

Nuhi, Muhammad Hanan, Gathan Sbastyan, Achmad Hanif Avicenna Setiady, and Ridha Wahyuni. 2024. "Tinjauan Hak Asasi Manusia Terhadap Pelindungan data pribadi Dan Kepastian Hukumnya Di Indonesia." *National Conference on Law Studies (NCOLS)* 6: 433-447. https://conference.upnvj.ac.id/index.php/ncols/article/view/2952

Nurmalasari, Nurmalasari. 2021. "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum." *Syntax Idea* 3(8):hlm. 1947-1966. doi: https://doi.org/10.46799/syntax-idea.v3i8.1414

Nurmansyah, Gunsu, Rudi Natamiharja, and Ikhsan Setiawan. 2025. "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach." *Pancasila and Law Review* Vol. 6(1):hlm. 15-44. doi: https://doi.org/10.25041/plr.v6i1.4138.

Nurtresna, Robby, and Mabsuti Mabsuti. 2024. "Peran Hukum Dalam Mewujudkan Keadilan Sosial Di Masyarakat." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 4(2): 1581-1596. https://bureaucracy.gapenas-publisher.org/index.php/home

Nusantara, Abdul Hakim Satria, Irhan Kahirul Umam, and Muharman Lubis. 2024. "Jaminan Informasi Dan Keamanan Yang Lebih Baik: Studi Kasus BPJS Kesehatan." *Nuansa Informatika* 18(2): 120-127. https://doi.org/10.25134/ilkom.v18i2.202

Okditazeini, Vannyora, and Irwansyah Irwansyah. 2018. "Ancaman Privasi Dan Data Mining Di Era Digital: Analisis Meta-Sintesis Pada Social Networking Sites (SNS)." *Jurnal Studi Komunikasi Dan Media* 22(2): 109. doi: 10.31445/jskm.2018.220202.

Olivia, Denindah, Sinta Dewi Rosadi, and Rika Ratna Permata. 2020. "Pelindungan data pribadi Dalam Penyelenggaraan Aplikasi Surveilans Kesehatan Pedulilindungi Dan Covidsafe Di Indonesia Dan Australia." *DATIN Law*

Jurnal 1(2): 1-15. https://doi.org/10.36355/dlj.v1i2.453

Pakina, Ridho, and Mohammad Solekhan. 2024. “Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia.” *Journal of Scientech Research and Development* 6(1): 273-286. https://www.idm.or.id/JSCR/index.php/JSCR/article/view/376

Pemuli, Reihana, Abdul Halim Barkatullah, Program Studi, Magister Kenotariatan, Fakultas Hukum, and Universitas Lambung Mangkurat. 2024. “Liability of Business Actors for Breaches in Electronic Banking Systems.” *Jurnal Hukum Sehasen* 10(2): 535-550. https://doi.org/10.37676/jhs.v10i2.6839

Permadi, Ikhsan Bagus, and Ali Rokhman. 2023. “Implementasi Identitas Kependudukan Digital Dalam Upaya Pengamanan Data Pribadi.” *JOPPAS: Journal of Public Policy and Administration Silampari* 4(2): 80-88. https://journal.ipm2kpe.or.id/index.php/JOPPAS/article/view/6199

Prabowo, Wisnu, Satriya Wibawa, and Fuad Azmi. 2020. “Pelindungan data Personal Siber Di Indonesia.” *Padjadjaran Journal of International Relations* 1(3): 218. doi: 10.24198/padjir.v1i3.26194.

Pramana, Juliantio Dwi, Mikho Ardinata, Ahmad Dasan, and Rangga Jayanuarto. 2024. “Law Enforcement Of Criminal Acts Of Dissemination Of Population Document Data By Dinas Dukcapil Kab. Mukomuko.” *Jurnal Hukum Sehasen* 10(1): 329-338. https://doi.org/10.37676/jhs.v10i1.5995

Prasetyoningsih, N., N. Ismail Nawang, W. V. Putri, and M. N. R. Amirullah. 2024. "Legal Protection for the Personal Data in Indonesia and Malaysia." In International Conference on Human-Computer Interaction, pp. 161–169. https://link.springer.com/chapter/10.1007/978-3-031-61379-1_11.

Pratiwi, Friska Yulanda, and Fajar Rachmad Dwi Miarsa. 2025. “Urgensi Edukasi Publik Dalam Menangkal Penyalahgunaan Data Pribadi.” *RIGGS: Journal of Artificial Intelligence and Digital Business* 4(2):hlm. 1342-1349. doi: https://doi.org/10.31004/riggs.v4i2.672.

Prayuti, Yuyut. 2024. "Dinamika Pelindungan Hukum Konsumen di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce dan Pelindungan Data Konsumen di Indonesia." *Meraja Journal* 5(3):115–137. https://doi.org/10.55637/juinhum.5.1.8482.903-913.

Priliasari, Erna. 2023. "Pelindungan data pribadi yang bersifat spesifik Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia." *Jurnal Rechts Vinding* 12(2):261–279. https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/article/viewFile/1285/329.

Puanandini, Dewi Asri, Muhammad Syahid Syidiq, and Jihan Pasha Noevera. 2023. "Efektivitas Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang." *Public Sphere: Jurnal Sosial Politik, Pemerintahan Dan Hukum* 2(2): 39-49. https://jurnal.penerbitwidina.com/index.php/JPS/article/view/1048

Purnamasari, Teti Indrawati, and Rendra Khaldun. 2024. "Relevansi Al-Qur'an, Hak Asasi Manusia, Dan Gender Dalam Melindungi Hak Kehormatan Pribadi Di Era Digital: Tinjauan Literatur." *MODELING: Jurnal Program Studi PGMI* 11: 154-172. https://doi.org/10.69896/modeling.v11i4.2642

Putra, Nurshoim Ramadhan, Irwan Triadi, Wicipto Setiadi, Mustafid Milanto Achmad, and Mohammad Wangsit Supriyadi. 2024. "Politik Hukum Teknologi Blockchain Indonesia Menuju Kerangka Hukum Yang Implementasi Inovasi Dan Adaptasi." *Hukum Dinamika Ekselensia* 6(4): 209-222. https://journalversa.com/s/index.php/hde/article/view/3410

Putri, Adelia, Nilam Sari, Putri Fajrina, and Siti Aisyah. 2025. "Keamanan Online Dalam Media Sosial: Pentingnya Pelindungan data pribadi Di Era Digital (Studi Kasus Desa Pematang Jering)." *Jurnal Pengabdian Nasional (JPN) Indonesia* 6(1): 38-52. https://doi.org/10.35870/jpni.v6i1.1097

Putri, Anastasia Vienessa, Deby Naya Maskut, Rosdiana Meni Kwuta, and Baren Sipayung. 2025. "Tarakan Smart City: Meningkatkan Transparansi Dan Akuntabilitas Layanan Publik Melalui E-Government." *Tumoutou Social Science Journal* 2(1): 61-73. https://doi.org/10.61476/jcm2fw95

Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. 2021. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Pelindungan data Pribadi." *Borneo Law Review* 5(1): 46-68. https://doi.org/10.35334/bolrev.v5i1.2014

Putri, Dewi Fatmala, Widya Ratna Sari, and Faricha Lita Nabbila. 2023. "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking." *Jurnal Ilmiah Ekonomi Dan Manajemen* 1(4): 173-181. https://doi.org/10.61722/jiem.v1i4.331

Putri, Tiara Shafa, and Moody Rizqy Syailendra Putra. 2024. "Implementasi Undang-Undang Pelindungan data pribadi yang bersifat spesifik: Peran Manajemen Risiko Hukum Bagi Prosesor Data Pribadi." *Jurnal Hukum Lex Generalis* 5(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/730

Putri, Thiara Octaviani, and Muhamad Farudin. 2025. "Pelindungan data pribadi yang bersifat spesifik Konsumen Pada Perusahaan E-Commerce Yang Mengalami Kepailitan Di Indonesia Ditinjau Berdasarkan Hukum Positif Indonesia." *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora* 2(1):

260-279. https://doi.org/10.62383/progres.v2i1.1355

Putri, Wilga Secsio Ratsja, Nunung Nurwati, dan Meilanny Budiarti S. 2016. "Pengaruh Media Sosial Terhadap Perilaku Remaja." *Jurnal Prosiding Penelitian & Pengabdian Masyarakat* 3(1): 47-51. DOI: 10.35448/jmb.v11i2.6061.

Rahayu, Annisa. 2023. "Sektor Pemerintah Jadi Sasaran Empuk Serangan Siber." *Goodstats.Id*. Retrieved May 6, 2025 (https://goodstats.id/article/sektor-pemerintah-jadi-sasaran-empuk-serangan-siber-9EqE0).

Rahayu, Layla Intan, Tri Wahyudiono, and Dewi Ulfa Lailatul Fitria. 2023. "Efektivitas Kebijakan Hukum Dalam Penanganan Pandemi." *Jurnal Online Mahasiswa (Jom) Hukum Tata Negara* 1(2): 80-112. https://ejurnal.iaipd-nganjuk.ac.id/index.php/jom-htn/article/view/1266

Ramadhan, Aditya, and Kartika Novitasari. 2023. "Strategi Pengembangan Literasi Ekonomi Berbasis Digital Terhadap Regulasi Pemberdayaan Perilaku Sosial Dan Sumber Daya Manusia Di Era Industri 4.0." *AB-JOIEC: Al-Bahjah Journal of Islamic Economics* 1(1): 14-25. https://doi.org/10.61553/abjoiec.v1i1.10

Ramadhani, Wyanda Kinanti Syauqi, and Sidi Ahyar Wiraguna. 2025. "Implementasi Pelindungan data pribadi yang bersifat spesifik Dalam Sistem Informasi Pada Perusahaan Jasa Keuangan." *Perspektif Administrasi Publik Dan Hukum* 2(2): 158-175. https://doi.org/10.62383/perspektif.v2i2.248

Rahman, Irsan, Sahrul, Riezka Eka Mayasari, Tia Nurapriyanti, dan Yuliana. 2023. "Hukum Pelindungan Konsumen di Era E-Commerce: Menavigasi Tantangan Pelindungan Konsumen dalam Lingkungan Perdagangan Digital." *Jurnal Hukum dan HAM Wara Sains* 2(8):704–712. DOI: 10.58812/jhhws.v2i08.605.

Raymond, Richard, Fahrur Rozzi Nasution, Andrew Law, Philisya Salim, and Christin Christovany. 2024. "Pengaruh Teknologi Blockchain Terhadap Transformasi Sistem Pembayaran Digital: Tantangan Keamanan Dan Regulasi." *Jurnal Studi Multidisipliner* 8(11): 60-74. https://oaj.jurnalhst.com/index.php/jsm/article/view/5425

Riefky, Teuku, and Jahen F. Rezki. 2023. "Isu Keamanan Siber Perbankan Dan Potensi Bank Run." *LPEM FEB UI: Institute for Economic and Social Research* 1(1): 1-9. https://lpem.org/wp-content/uploads/2023/05/Special_Report_V1_No1.pdf

Rifa, Fauzi, and Maslihati Nur Hidayati. 2024a. "Kebijakan Penal Dalam Pelindungan data pribadi Nasabah Fintech Lending Di Indonesia." *Binamulia Hukum* 13(2): 461-481. doi: 10.37893/jbh.v13i2.964.

Rifa, Fauzi, and Maslihati Nur Hidayati. 2024b. “Kebijakan Penal Dalam Pelindungan data pribadi Nasabah Fintech Lending Di Indonesia.” *Binamulia Hukum* 13(2): 461-481. https://doi.org/10.37893/jbh.v13i2.964

Rinjani, Muhamad Adri, and Ricky Firmansyah. 2025. “Hambatan Implementasi UU 27/2022 Dan Strategi Penguatan Pelindungan data pribadi Di Indonesia.” *Jurnal Analisis Hukum* 8(1):hlm. 70-83. doi: https://doi.org/10.38043/jah.v8i1.6793.

Rizal, Muhamad, Sinta Dewi Rosadi, and Agus Taryana. 2024. “Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia.” *Journal of Law and Sustainable Development* Vol. 12(1):hlm. 1-30. doi: https://doi.org/10.55908/sdgs.v12i1.2809.

Rohmansyah, Duta Agung, Kevin Mandela Saputra, and Badrus Sholih. 2023. “Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi Di Era Digitilasasi Berdasarkan Prinsip Negara Hukum.” *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 5(2): 1099-1110. doi: 10.37680/almanhaj.v5i2.3054.

Rosadi, Sinta, and Garry Gumelar Pratama. 2018. “Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia.” *Veritas et Justitia* 4(1):hlm. 88-110. doi: 10.25123/vej.2916.

Saba, Savira Savira. 2024. “Implementasi Strategi Inovasi Dalam Peningkatan Daya Saing Usaha Kecil Dan Menengah Di Era Digital.” *JMEB Jurnal Manajemen Ekonomi & Bisnis* 2(02): 38-45. https://journal.sabajayapublisher.com/Index.Php/Jmeb/Article/View/362

Sadewa, Muhammad Tengku, Dedek Kurniadi, and Tata Sutabri. 2025. “Keamanan Dan Keselamatan Implementansi Internet Of Things (IOT): Tantangan Pada Sektor Industri Dan Rumah Tangga.” *Jurnal Sistem Dan Teknologi Informasi (JSTI)* 7(1): 115-130. https://www.researchgate.net/publication/382991155

Safalla, Nansya Janaika. 2024. “Perlindungan Hukum Konsumen Terhadap Tindak Pidana Pencurian Data Pribadi Dalam Transaksi E-Commerce Di Indonesia.” Doctoral dissertation, Universitas Islam Sultan Agung Semarang

Sahatatua, Richart, Yenrizka Gusmaria, I. Ketut Astawa, Ade Maman Suherman, Try Setiady, and Wahyu Donri Tinambunan. 2024. “Cyber Law Analysis of E-KTP Data Leakage: A Case Approach of 102 Million KTP Data Allegedly Leaked from the Ministry of Social Affairs to a Hacker Forum.” *Journal of Multidisciplinary Academic and Practice Studies* Vol. 2(3):hlm. 151-161. doi: 10.35912/jomaps.v2i3.2219.

Salsabila, Fara Anindita, and Andi Aina Ilmih. 2024. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2(4): 176-181. https://www.researchgate.net/publication/350385220

Salsabila, Shafa, and Sidi Ahyar Wiraguna. 2025. "Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan data pribadi yang bersifat spesifik Indonesia." *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 2(2):hlm. 145-157. doi: https://doi.org/10.62383/konsensus.v2i2.736.

Samin, Herol Hansen. 2024. "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif." *Jurnal Ilmiah Research Student* 1(3): 1-15. https://doi.org/10.61722/jirs.v1i3.386

Santi, Vidya Loka, and Zaenal Wafa. 2024. "Pengaruh Sistem Pengendalian Internal, Komite Audit, Dan Whistleblowing System Terhadap Pencegahan Fraud." *Value: Jurnal Manajemen Dan Akuntansi* 19(3): 919-936. https://www.researchgate.net/profile/Vidya-Santi/publication/387580257

Santos, Ricardo, and Ermania Widjajanti. 2025. "Penyelesaian Perkara Pidana Siber Kasus Kebocoran." *Quantum Juris: Jurnal Hukum Modern* 07(1): 128-137. https://journalversa.com/s/index.php/jhm/article/view/806

Santoso, Totok Imam. 2021. "Media Sosial Dalam Konteks Data Kependudukan Di Era Prosumsi Digital." *Komunikologi: Jurnal Ilmiah Ilmu Komunikasi* 18(2): 101-113. https://doi.org/10.47007/jkomu.v18i02.228

Saputra, Ricky, and Viola Damayanti. 2023. "Perlindungan Konsumen Dalam Transaksi E-Commerce Internasional." *Repertorium: Jurnal Ilmiah Hukum Kenotariatan* 12(2): 240-251. https://doi.org/10.28946/rpt.v12i2.3364

Saputra, Wawan Nova, Ipah Ema, Indah Nurmala Sari, and Qaulis Tsabit Ramadhani. 2024. "Trasformasi Birokrasi Digital Dalam Pelayanan Publik: Studi Kasus Penerapan E-Government." *Jurnal Sosial, Ekonomi Dan Humaniora* 3(2): 82-94. https://jurnal.unnur.ac.id/index.php/sosiera/article/download/868/799

Satria, Fajar, Anggi Ari Purnomo, Agung Maulana, and Abdurrozzaq Hasibuan. 2025. "Kecerdasan Buatan (AI) Dalam Dunia Industri." *Variable Research Journal* 2(01): 253-262. https://variablejournal.my.id/index.php/VRJ/article/view/183

Satria, Muhammad Kamarulzaman, and Hudi Yusuf. 2024. "Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Pelindungan data Pribadi." *JICN: Jurnal Intelek Dan Cendikiawan Nusantara* 1(2): 2442-2456. https://jicnusantara.com/index.php/jicn/article/view/266

Sepyah, Sepyah, Idul Adnan, Rahmatun Ulfa, and Elpipit Elpipit. 2022. "Implikasi Hukum Terhadap Pelindungan data pribadi Di Era Digital." *AL-BALAD: Jurnal Hukum Tata Negara Dan Politik Islam* 2(1): 26-36.

https://doi.org/10.59259/ab.v2i1.95

Setiawan, Andry, and Uswatun Khasanah. 2024. “Hukum Perdata Dan Keamanan Siber: Menanggapi Ancaman Dan Risiko Teknologi Terhadap Hak-Hak Individu.” *JPeHI (Jurnal Penelitian Hukum Indonesia)* 5(02): 101-118. https://doi.org/10.61689/jpehi.v5i02.675

Setiawan, Hezkiel Bram, and Fatma Ulfatun Najicha. 2022. “Pelindungan data pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data.” *Jurnal Kewarganegaraan* 6(1): 976-982. https://doi.org/10.31316/jk.v6i1.2657

Setiawan, Setiawan, Abdul Azis, and Eko Wahyudi. 2024. “Evaluasi Efektivitas Disaster Recovery Plan Dalam Pemulihan Layanan Teknologi Informasi Pasca Bencana Berbasis Iso 22301 (Studi Kasus PT. Jasa Raharja).” *P. Hlm.* 351-356 in *Prosiding Seminar SeNTIK*. Vol. 8. https://garuda.kemdiktisaintek.go.id/author/view/377121

Siagian, Riduan, Leonard Siahaan, and Ichwan Hamzah. 2023. “Human Rights in The Digital Era: Online Privacy, Freedom Of Speech, and Personal Data Protection.” *Journal Of Digital Learning And Distance Education* Vol. 2(4):hlm. 513-523. doi: 10.56778/jdlde.v2i4.149.

Sianturi, Cindy Gladys Pratiwi, Roida Nababan, and Ria Juliana Siregar. 2024. “Peran Hukum Dalam Melindungi Data Pribadi.” *Innovative: Journal Of Social Science Research* 4(5):hlm. 2607-2624. doi: https://doi.org/10.31004/innovative.v4i5.15192.

Sidik, Berto Purnomo, and Sidi Ahyar Wiraguna. 2025. “Tinjauan Hukum Terhadap Aplikasi Digital Sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi.” *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2(2): 219-232. https://doi.org/10.62383/humif.v2i2.1520

Sifa, Abdan. 2024. “Transformasi Digital E-Commerce Dalam Menguasai Kosentrasi Pasar Di Indonesia.” *Jurnal Ilmiah Ekonomi Dan Manajemen* 2(12): 405-413. https://doi.org/10.61722/jiem.v2i12.3239

Sijabat, Hotmaria Hertawaty, and Gunawan Widjaja. 2025. “Privasi Dan Keamanan Data Dalam Layanan Cloud: Perspektif Hukum Dan Regulasi.” *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4(4): 279-288. https://doi.org/10.54443/sibatik.v4i4.2649

Sinaga, Erlina Maria Christin, dan Mery Christian Putri. 2020. "Formulasi Legislasi Pelindungan data pribadi yang bersifat spesifik dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding* 9(2): 237-256. DOI: 10.33331/rechtsvinding.v9i2.428.

Sinaga, Zaky Asdhika, and Lokot Muda Harahap. 2025. “Transformasi Ekonomi

Indonesia Menuju Ekonomi Digital: Tantangan Dan Strategi." *Jurnal Rumpun Manajemen Dan Ekonomi* 2(3): 26-33. https://doi.org/10.61722/jrme.v2i3.4273

Siregar, Rospita, and Haposan Sinaga. 2025. "Aspek Hukum Perlindungan Data Pasien Dalam Penyelenggaraan Rekam Medis Elektronik Di Indonesia." *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 11(1):hlm. 106-116. doi: 10.55809/tora.v11i1.433.

Situmeang, Sahat Maruli Tua. 2021. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *Sasi* 27(1): 38. doi: 10.47268/sasi.v27i1.394.

Soeprapto, Sri. 2013. "Konsep Muhammad Hatta tentang Implementasi Pancasila dalam Perspektif Etika Pancasila." *Jurnal Filsafat* 23(2):99–116. doi:10.22146/jf.13194.

Soer, U. Darmanto, and Nining Yurista Prawitasari. 2025. "Perlindungan Hukum Data Pribadi Konsumen Dalam Transaksi E-Commerce Di Indonesia." *SABAJAYA Jurnal Pengabdian Kepada Masyarakat* 3(01): 49-55. https://doi.org/10.59561/sabajaya.v3i01.542

Soleh, Mohamad, and Zubakhrum Tjenreng. 2024. "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital." *Jurnal Kajian Pemerintah (JKP) Journal of Government, Social and Politics* 11(1): 1-10. https://doi.org/10.25299/jkp.2025.vol11(1).20524

Suari, Kadek Rima Anggen, and I. Made Sarjana. 2023. "Menjaga Privasi Di Era Digital: Pelindungan data pribadi Di Indonesia." *Jurnal Analisis Hukum* 6(1): 132-146. doi: 10.38043/jah.v6i1.4484.

Sudanto, Sudanto. 2025. "Transformasi Digital Dan Automasi Proses Bisnis Syariah Melalui Artificial Intelligence." *RIGGS: Journal of Artificial Intelligence and Digital Business* 4(2): 14-23. https://journal.ilmudata.co.id/index.php/RIGGS/article/view/444/191

Sudira, I. Wayan. 2025. "Keadilan Digital: Tantangan Hukum Dalam Era Disrupsi Teknologi." *Kertha Widya* 12(2): 35-59. https://doi.org/10.37637/kw.v12i2.2203

Suganda, Azhar, Andriansyah Hasibuan, Elsa Novri Regina, Mita Dewi Nasution, and Bonaraja Purba. 2024. "Tinjauan Hukum Komersial Terhadap Perlindungan Hukum Konsumen Dalam E-Commerce Di Indonesia." *Jurnal Sosial Humaniora Sigli* 7(2): 94-106. https://journal.unigha.ac.id/index.php/JSH/article/view/2482/2042

Sugiarto, Ramadhina Eka Putri, Nita Afriani, and Rendy Kurniawan. 2026. "Analisis Yuridis Normatif Efektivitas Konvensi Kecerdasan Buatan

Terhadap Perlindungan Hak Asasi Manusia." *Littera Legis: Journal of Law, Society, and Justice* 1(2):hlm. 15-31. doi: https://journal.geminilittera.com/littera-legis/article/view/43.

Suleiman, Ajisatria, Pingkan Audrine, and Thomas Dewaranu. 2022. "Menjelaskan Kesenjangan Regulasi: Mengapa Pengaturan Bersama Dalam." *Center for Indonesian Policy Studies* (May 2025).

_____. *Pengaturan Bersama Dalam Pelindungan data Pribadi: Potensi Peran Asosiasi Industri Sebagai Organisasi Regulator Mandiri.* Center for Indonesian Policy Studies.

Sumarna, Dadang, and Ayyub Kadriah. 2023. "Penelitian Kualitatif Terhadap Hukum Empiris." *Jurnal Penelitian Serambi Hukum* Vol. 16(02):hlm. 101-113. doi: 10.59582/sh.v16i02.730.

Supriadi, Iman. 2024. "Transformasi Sistem Perpajakan Menggunakan Teknologi Blockchain Untuk Meningkatkan Transparansi Dan Mengurangi Penyimpangan." *Journal of Tax Policy, Economics, and Accounting (TAXPEDIA)* 2(1): 29-44. https://doi.org/10.61261/muctj.v2i1.44

Suryadi, Suryadi, and Faizal Amir Parlindungan Nasution. 2023. "Revolusi Industri, Tren Pekerjaan Masa Depan, Dan Posisi Indonesia." *Jurnal Ketenagakerjaan* 18(2): 124-141. https://doi.org/10.47198/jnaker.v18i2.237

Suryawijaya, Tito Wira Eka. 2023. "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia." *Jurnal Studi Kebijakan Publik* 2(1): 55-68. https://doi.org/10.21787/jskp.2.2023.55-68

Sutarli, Ananta Fadli, and Shelly Kurniawan. 2023. "Peranan Pemerintah Melalui Undang-Undang Pelindungan data pribadi Dalam Menanggulangi Phising Di Indonesia." *Innovative: Journal Of Social Science Research* 3(2): 4208-4221. https://j-innovative.org/index.php/Innovative/article/view/760

Sutono, Agus, Fuad Noorzeha, dan Supriyono Purwosaputro. 2025. "Konsep Negara Integral Soepomo dan Relevansinya pada Penerapan Konstitusi di Indonesia Tahun 2024." *PACIVIC: Jurnal Pendidikan Pancasila dan Kewarganegaraan* 5(1):30–46. https://doi.org/10.36456/p.v5i1.9839

Sutrisna, Cecep. 2021. "Aspek Hukum Pelindungan data pribadi Dan Kondisi Darurat Kebocoran Atas Data Pribadi Di Indonesia." *Wacana Paramarta: Jurnal Ilmu Hukum* 20(5): 1-10. https://doi.org/10.32816/paramarta.v20i5.138

Suvil, Aulia Alayna, Firdaus, M. Arif Ramadhan, Wanda Darma Putra, and Dwi Putri Lestarika. 2024. "Implementasi Pelindungan data pribadi Berdasarkan

Undang-Undang Nomor 11 Tahun 2020." *Jurnal Hukum, Politik Dan Ilmu Sosial* 3(4): 70-80. https://elibrary.ru/item.asp?id=73928847

Syahriar, Irman, Jamil Bazarah, and Khairunnisah Khairunnisah. 2024. "Keadilan Sosial Di Dalam Negara Hukum Indonesia." *Journal of Knowledge and Collaboration* 1(2): 28-38. doi: 10.59613/wqx8hn76.

Syafi'i, Maulana, and Surya Sukti. 2025. "Transformasi Hukum Dalam Ruang Sosial: Relasi Antara Masyarakat, Nilai Keadilan, Dan Pembinaan Hukum." *AT-TAKLIM: Jurnal Pendidikan Multidisiplin* 2(6):hlm. 689-701. doi: https://doi.org/10.71282/at-taklim.v2i6.502.

Syarifuddin, Syarifuddin, Teresia Din, Tri Andriani, Antonius Rino Vanchapo, Hezron Sabar Rotua Tinambunan, and Dhiraj Kelly Sawlani. 2024. "Reformasi Hukum Di Era Digital: Tantangan Dan Peluang Di Indonesia." *Indonesian Research Journal on Education* 4(4): 3206-3215. https://doi.org/10.31004/irje.v4i4.1685

Syifa, Achmad Rufaiddin, and Richard C. Adam. 2024. "Pelindungan data pribadi Nasabah Peminjam Dalam Layanan Pinjaman Meminjam Berbasis Teknologi Informasi Berdasarkan Hukum Pelindungan data Pribadi." *UNES Law Review* 6(2): 6739-6752. https://doi.org/10.31933/unesrev.v7i2.2352

Tampubolon, Wahyu Simon. 2016. "Upaya Pelindungan Hukum Bagi Konsumen Ditinjau dari Undang-Undang Pelindungan Konsumen." *Jurnal Ilmiah Advokasi* 4(1):53–61. https://jurnal.ulb.ac.id/index.php/advokasi/article/viewFile/356/342.

Taufik, Muhammad, and Fatimah Zahara. 2024. "Pengaturan Perlindungan Data Pribadi Dalam E-Commerce Menurut Perspektif Maqashid Syariah (Studi Kasus Marketplace Facebook)." *Jurnal Ilmu Hukum, Humaniora Dan Politik* 4(6):hlm. 2378-2392. doi: 10.38035/jihhp.v4i6.2744.

Taufiq, Muchamad, and Ananda Salsabila Kenyo. 2025. "The Legal Protection of

Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR." *International Journal of Business, Law, and Education* Vol. 6(2):hlm. 1260-1268. doi: https://doi.org/10.56442/ijble.v6i2.1178.

Tolani, Chisomo, and Prof Pareek. 2024. "Introduction to Data Protection Frameworks: A Review." *International Journal of Advanced Research in Science, Communication and Technology* Volume 4: 251-255. doi: 10.48175/IJARSCT-18732. Doi: 10.48175/IJARSCT-18732

Tri Mahendra, Bovin, Taufik Yahya, Akbar Kurnia Putra, and Sukamto Satoto. 2025. "Kebijakan Hukum Pidana Terhadap Penyebaran Data Pribadi Oleh Jurnalis Dalam Rangka Pelindungan data pribadi Di Indonesia." (Doctoral dissertation, Universitas Jambi). https://doi.org/10.36355/rlj.v6i1.1653

Triadi, Muhammad, Sumiadi, and Yusrizal. 2023. "Perlindungan Terhadap Korban Pencurian Data Pribadi Melalui Media Digital." *REUSAM: Jurnal Ilmu Hukum* 11(1): 45. doi: 10.29103/reusam.v11i1.10178.

Triansyah, Abdurrazaq, Putri Nur Siti Julianti, Nadyva Fakhriyah, and Andi M. Afif. 2022. "Peran Otoritas Jasa Keuangan Dalam Perlindungan Hukum Bagi Pengguna Pinjaman Online Ilegal (Studi Kasus Pinjol Ilegal Di Yogyakarta)." *Cross-Border* 5(2): 1090-1104. https://ojs.kolaborasi.web.id/index.php/Cross-Border/article/view/1241

Trisno, Andhika, Marlien Lapian, and Sofia Pangemanan. 2017. "Penerapan Prinsip-Prinsip Good Governance Dalam Pelayanan Publik Di Kecamatan Wanea Kota Manado." *Jurnal Eksekutif* 1(1): 1-10. https://ejournal.unsrat.ac.id/index.php/jurnaleksekutif/article/view/16611

UNESCO. 2023. "Bridging the Digital Divide and Ensuring Online Protection." *UNESCO*. Retrieved May 6, 2025 (https://www.unesco.org/en/right-education/digitalization).

UNICEF. 2022. "UNICEF Annual Report 2022." *UNICEF*. Retrieved May 6, 2025 (https://www.unicef.org/reports/unicef-annual-report-2022).

Usman, Noval bin, and Satria Unggul Wicaksana Prakasa. 2024. "Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP Legal." *DOKTRINA Journal of Law* 7(27): 178-201. https://garuda.kemdiktisaintek.go.id/documents/detail/4753689

Utama, Mohammad Wira. 2024. "Rekonstruksi Regulasi Pelindungan data pribadi Bagi Nasabah Perbankan Yang Berbasis Nilai Keadilan." *Universitas Islam Sultan Agung (Indonesia), Semarang.*

Utiarahman, Nuraisah Masita. 2025. "Peraturan Hukum Perdata Nasional Di Era Digital Hambatan Dan Kesempatan Dalam Melindungi Data Pribadi." *Ganec Swara* 19(1): 147-154. https://doi.org/10.59896/gara.v19i1.194

Utomo, Muhammad Fikri. 2024. "Eksplorasi Peran Smartwatch Android Berbasis IoT Dalam Bidang Kesehatan." *Jurnal Sains Dan Teknologi 4.0* 1(2): 15-23. https://jurnal.komputasi.org/index.php/jst/article/view/23

Valentino, Muhammad Ryan. 2023. "Security Analysis Of AI-Based Mobile Application For Fraud." *Jurnal Komputer Indonesia* 2(1): 9-18. https://doi.org/10.37676/jki.v2i1.563

Vandercruysse, Laurens, Caroline Buts, and Michaël Dooms. 2020. "A Typology of Smart City Services: The Case of Data Protection Impact Assessment." *Cities* Vol. 104(1):hlm. 1-15. doi: https://doi.org/10.1016/j.cities.2020.102731.

Vania, Cindy, Markoni Markoni, Horadin Saragih, and Joko Widarto. 2023. "Tinjauan Yuridis Terhadap Pelindungan data pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber." *Jurnal Multidisiplin Indonesia* 2(3): 654-666. https://doi.org/10.58344/jmi.v2i3.157

Varany, Yacinta Tira, and Listyowati Sumanto. 2025. "Dinamika Sistem Hukum Pelindungan Data Pribadi: Analisis Interaksi Struktur, Substansi, Dan Kultur Hukum Di Era Big Data." *Jurnal Impresi Indonesia* 4(11):hlm. 5172-5185. doi: https://doi.org/10.58344/jii.v4i11.7182.

Veranda, Chessyca, and Muhammad Alwan Zain Nusantara. 2024. "Analisis Perbandingan Pelindungan data pribadi yang bersifat spesifik Antara Indonesia Dan Arab Saudi." *PUSKAPSI Law Review* 4(2): 236-256. https://elibrary.ru/item.asp?id=81184195

Verizon. 2025. "2025 Data Breach Investigations Report." *Verizon*. Retrieved May 6, 2025 (https://www.verizon.com/business/resources/reports/dbir/).

Wahyuliana, Ida, Lucky Dafira Nugroho, Aprilina Pawestri, and Kata Kunci. 2022. "Pendidikan Karakter Melalui Pendidikan Pancasila Sebagai Upaya Preventif Penyalahgunaan Data Pribadi Dalam Perkembangan Iptek." *Jurnal Pancasila* 3(1): 1-11. https://ejurnalpancasila.bpip.go.id/index.php/PJK

Wahyunanda Kusuma Pertiwi, and Oik Yusuf. n.d. "Data Tokopedia, Gojek, Dan Bukalapak Bocor Di Tengah Absennya RUU PDP." *Tekno.Kompas.Com*. Retrieved May 12, 2025 (https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp).

Wang, Claudia, Monique Zhang, Ali Sesunan, and Laurencia Yolanda. 2023. "Peran Teknologi Dalam Transformasi Pendidikan Di Indonesia." *Kemdikbud* 4(2): 1-7. https://repositori.kemendikdasmen.go.id/30537/1/Indonesias-K-12-Education-Quality-Improvement-Bahasa-05122023.pdf

Wardhono, R. Dwi Tjahja K., Wishnu Badrawani, Ayu Deviana, and Nadhia Shalehanti Melati Pramudyastuti. 2024. "Pelindungan data pribadi yang bersifat spesifik Di Bank Indonesia Dan Lembaga Jasa Keuangan: Rekomendasi Kebijakan Dan Teknis Pengaturan." *Bi.Go.Id*. Retrieved May 6, 2025 (https://www.bi.go.id/id/publikasi/kajian/Pages/Pelindungan-Data-Pribadi-Di-Bank-Indonesia-Dan-Lembaga-Jasa-Keuangan.aspx).

Wati, Dwi Sinta, Siti Nurhaliza, Mulia Wulan Sari, and Rizka Amallia. 2024. "Dampak Cyber Crime Terhadap Keamanan Nasional Dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum." *Jurnal Bevinding* 2(01): 44-55. https://www.journal.uniba.ac.id/index.php/JB/article/view/1167

Wibawa, Aurelia Elma Adriana Surya. 2024. "Etika Dan Hukum Penggunaan Ai Untuk Pemasaran Digital Dalam Perspektif Hukum Bisnis Di Indonesia." (Doctoral dissertation, Universitas Atma Jaya Yogyakarta). https://repository.uajy.ac.id/id/eprint/33099/4/190513467%202.pdf

Widjaja, Gunawan. 2025. "Pengaruh Perjanjian Perdagangan Internasional Terhadap Kebijakan Pelindungan data Pribadi." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 4(4): 345-354. https://doi.org/10.54443/sibatik.v4i4.2659

Wijaya, Alvian Dwiangga, and Teddy Prima Anggriawan. 2022. "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi Di Smartphone." *Inicio Legis* 3(1):hlm. 63-72. doi: https://doi.org/10.21107/il.v3i1.14873.

Wijaya, Catherine, Corrie Yemima Ilona, Cristin Rosa Gultom, and Sri Handayani. 2025. "Pelindungan data pribadi Konsumen Dalam Layanan Keuangan Digital: Tinjauan Dari UU PDP." *Birokrasi: JURNAL ILMU HUKUM DAN TATA NEGARA* 3(2): 30-42. https://www.researchgate.net/publication/391312973.

Wijaya, Johan, Aji Titin Roswitha Nursanthy, and Muhammad Arganata Thamrin. 2024. "Perlindungan Terhadap Data Pribadi Dalam Berselancar Di Dunia Maya." *The Juris* 8(2):hlm. 638-644. doi: https://doi.org/10.56301/juris.v8i2.1477.

Wijaya, Putra, Gusliana Hb, and Muhammad A. Rauf. 2024. "Relevansi Hak Privasi Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang -Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945." *Jurnal Ilmiah Wahana Pendidikan* 10(22): 662-672. https://doi.org/10.5281/zenodo.14574771

Wijayanto, Budi Tri. 2025. "Regulasi Konflik Kepentingan Di Era Disrupsi: Tantangan Dan Urgensi Pembaharuan Di Indonesia." *Jurnal Globalisasi Hukum* 2(1): 148-174. https://www.researchgate.net/publication/396144780.

Wildan, Muhammad, Daud Renata Candra Ramadhan, and Zulfa Rena Wijayanti. 2024. "Analisis Tanggung Jawab Bank Terhadap Kebocoran Data Nasabah: Ditinjau Dalam Perspektif Hukum Perbankan." *Media Hukum Indonesia (MHI)* 2(4). https://doi.org/10.5281/zenodo.14201758

Wiraguna, Sidi Ahyar. 2024. "Strategi Meningkatkan Kesadaran Hak Privasi Dalam Penggunaan Layanan Online Dalam Era Digital." *Jurnal Res Justitia: Jurnal Ilmu Hukum* 4(1): 266-278. https://resjustitia.lppmbinabangsa.id/index.php/home/article/view/118

Wiryanthi, Ni Putu Ega Maha. 2025. "Peran Hukum Dalam Meningkatkan Etika Bisnis Di Perusahaan Media Online." *Kertha Wicaksana* 19(1): 18-28.

https://doi.org/10.22225/kw.19.1.2025.18-28

Vanin, Fausto Neri da Silva, Lucas Micol Policarpo, Rodrigo da Rosa Righi, Sandra Marlene Heck, Valter Ferreira da Silva, José Goldim, dan Cristiano André da Costa. 2023. "A *Blockchain*-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach." *Sensors* 23(1):1–20. https://pubmed.ncbi.nlm.nih.gov/36616613/

Wu, H., H. Han, X. Wang, dan S. Sun. 2020. "Research on Artificial Intelligence Enhancing *Internet of Things* Security: A Survey." *IEEE Access* 8(10):153826–153848. https://ieeexplore.ieee.org/document/9172062/

Xanderina, Meilinda, Adam Aditya Nafil, and Faris Jatmiko. 2024. "Analisis Manajemen Sumber Daya Manusia Instansi Negeri Era Digitalisasi Dengan Kecerdasan Buatan." *JATI (Jurnal Mahasiswa Teknik Informatika)* 8(4): 4451-4456. https://doi.org/10.36040/jati.v8i4.9952

Yamani, Akhmad Zaki. 2025. "Analisis Tantangan Dalam Penyusunan Rancangan Undang-Undang Di Era Transformasi Digital: Antara Regulasi, Inovasi, Dan Perlindungan Hak." *Journal of Law and Nation (JOLN)* 4(2): 312-324. https://joln.my.id/index.php/joln/article/view/211

Yamin, Ahmad Fachri, Annisa Rachmawati, Rio Aditia Pratama, dan Jonathan Kevin Wijaya. 2022. "Pelindungan data pribadi yang bersifat spesifik Dalam Era Digital: Tantangan dan Solusi." *Meraja Journal* 5(3):115–137. https://doi.org/10.33080/mrj.v7i2.352.\

Yudistira, Muhammad, and Ramadani Ramadani. 2023. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh KOMINFO." *UNES Law Review* 5(4): 3917-3929. https://doi.org/10.31933/unesrev.v5i4.698

Yulianingrum, Aullia Vivi, and Muhammad Nurcholis. 2025. "Poltik Hukum Pengaturan Dan Pembangunan Hukum Transportasi Online Di Era Disrupsi Berbasis E-Governance Dan Dynamic Governance." *Jurnal Rectum* 7(1): 18-33. http://dx.doi.org/10.46930/jurnalrectum.v7i1.5199

Yunita, Marsya Indah, Ridha Artsani Ksvara, Divanny Aulia Hanif, Nurul Maharani, and Beny Dwi Lukitoaji. 2025. "Tantangan Etika Dan Privasi Terhadap Perspektif Global Pendidikan Teknologi Bagi Generasi Mendatang." *EDUCREATIVA: Jurnal Seputar Isu Dan Inovasi Pendidikan* 1(1): 64-74. https://journal.mahsya-educreativa.com/index.php/sosiolapedagogi/article/view/10

Yunita, Sri, Aina Mardiah, Dhea Amelia Manurung, Diska Qolbu Mutia, Melfa Romanna Elisabet, Sinta Wulida Mustasfa, and Siska Juliana Baringbing.

2024. “Peranan Hukum Dalam Penegakan Hak Asasi Manusia (Ham) Di Era Digital.” *Jurnal Review Pendidikan Dan Pengajaran* 7(4): 16726-16731. https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/38180

Yusuf, Susy Ariyanie, Christine Herlina, and Liston Sibarani. 2024. “Aspek Legal Dan Etika Penggunaan Data Pasien Dalam Teknologi Big Data Dan Kecerdasan Buatan Di Sektor Kesehatan.” *Proceeding Masyarakat Hukum Kesehatan Indonesia* 1(1): 381-393. https://rumah-jurnal.com/index.php/pmhki/article/view/223

Zaenudin, Imam, and Ade Bani Riyan. 2024. “Perkembangan Kecerdasan Buatan (AI) Dan Dampaknya Pada Dunia Teknologi.” *Jurnal Informatika Utama* 2(2): 128-153. https://doi.org/10.55903/jitu.v2i2.240

Zaky, Farhan A., and Andi Aina Ilmih. 2024. “Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Pelindungan data Pribadi.” *Media Hukum Indonesia (MHI)* 2(3). https://doi.org/10.5281/zenodo.12736637

Zebua, Della Yunika, and Alfan Pintalius Zebua. 2025. “Tantangan Etika Dalam Profesi Teknologi Informasi.” *Jurnal Ilmu Ekonomi, Pendidikan Dan Teknik* 2(1): 35-44. https://doi.org/10.70134/identik.v2i1.162

Zilda, M. Fachri, Darto Miradhia, and Ramadhan Pancasilawan. 2022. “Implementasi Program E-Samsat Di Jawa Barat.” *JANE-Jurnal Administrasi Negara* 13(2): 161-170. https://doi.org/10.24198/jane.v13i2.28691

C. Hasil Penelitian

Aditya, Tegar. 2024. *Kajian Keamanan Data Pribadi Dalam Layanan E-Government Di Indonesia: Analisis Hukum Privasi*. Tesis, Universitas Diponegoro.

Adli, Muhammad, dan Nadirah Ida. 2022. "Optimalisasi Mediasi dalam Penyelesaian Sengketa Bisnis Perspektif Keadilan Pancasila." Penelitian Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Afifah, Nabila. 2023. *Regulasi Pelindungan data pribadi Pada Platform E-Commerce Di Indonesia*. Tesis, Universitas Airlangga.

Aji, Dian. 2024. *Analisis Kebijakan Pelindungan data pribadi Dalam Era Transformasi Digital Di Indonesia*. Skripsi, Universitas Kristen Satya Wacana.

Alfiana, Dina. 2023. *Implementasi Kebijakan Pelindungan data pribadi Pada Sistem E-Government Di Indonesia*. Skripsi, Universitas Muhammadiyah Yogyakarta.

Alfian, Zulfi. 2025. *Regulasi Pelindungan data pribadi Di Indonesia Dalam Era Digital: Tinjauan Hukum Dan Kebijakan*. Disertasi, Universitas Indonesia.

Alfiana, Putri. 2024. *Pengelolaan Data Pribadi Dalam Era Digital Di Indonesia: Tinjauan Hukum Dan Implementasi*. Skripsi, Universitas Brawijaya.

Amira, Rani. 2025. *Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Layanan Digital Di Indonesia*. Disertasi, Universitas Indonesia.

Andika, Prawira. 2024. *Keamanan Data Pribadi Dalam Pengelolaan E-Commerce: Tinjauan Hukum Di Indonesia*. Skripsi, Universitas Islam Indonesia.

Andri, Irfan. 2023. *Pelindungan data pribadi Dalam Sektor Perbankan Digital Di Indonesia*. Skripsi, Universitas Indonesia.

Ariana, Dwi. 2023. *Strategi Pelindungan data pribadi Dalam Layanan E-Commerce: Perspektif Hukum Dan Kebijakan Di Indonesia*. Skripsi, Universitas Negeri Yogyakarta.

Ardianto, Rian. 2023. *Kajian Implementasi Regulasi Pelindungan data pribadi Di Indonesia Dalam Sektor Jasa Keuangan*. Tesis, Universitas Kristen Satya Wacana.

Arif, Radian. 2023. *Kajian Terhadap Kebijakan Pelindungan data pribadi Pada Aplikasi Digital Di Indonesia*. Skripsi, Universitas Diponegoro.

Aulia, Siti. 2023. *Pelindungan data pribadi Dalam Layanan Digital: Pengaruh Kebijakan Privasi Terhadap Keamanan Data Di Indonesia*. Tesis, Universitas Sebelas Maret.

Azhar, Ahmad. 2024. *Pelindungan data pribadi Dalam Industri Teknologi Informasi: Kasus Perusahaan E-Commerce Di Indonesia*. Skripsi, Universitas Sebelas Maret.

Azhar, Muhammad. 2025. *Pelindungan data pribadi Di Era Digital: Perspektif Hukum Indonesia Dan Internasional*. Disertasi, Universitas Hasanuddin.

Barkatullah, Abdul Halim. 2006. "Pelindungan Hukum Bagi Konsumen Dalam Transaksi E-Commerce Lintas Negara di Indonesia." Disertasi, Universitas Islam Indonesia.

Budi, Yani. 2024. *Penerapan Pelindungan data pribadi Dalam Sistem Keamanan Digital Pada Layanan E-Commerce Di Indonesia*. Skripsi, Universitas Sebelas Maret.

Cahya, Dwi. 2024. *Analisis Implementasi Kebijakan Pelindungan data pribadi Di Era Industri 4.0 Di Indonesia*. Tesis, Universitas Negeri Jakarta.

Dewi, Anisa. 2024. *Analisis Keamanan Data Pribadi Pada Sistem E-Government Di Indonesia*. Skripsi, Universitas Pendidikan Indonesia.

Diana, Fadhilah. 2024. *Pelindungan data pribadi Dalam Layanan Digital Di Indonesia: Sebuah Pendekatan Analisis Kebijakan*. Skripsi, Universitas Negeri Jakarta.

Fadil, Azzam. 2024. *Regulasi Pelindungan data pribadi Di Indonesia: Tinjauan Implementasi Undang-Undang Pelindungan data Pribadi*. Tesis, Universitas Padjadjaran.

Fajri, Rizal. 2024. *Pelindungan data pribadi Dalam Platform E-Commerce Di Indonesia: Kajian Regulasi Dan Praktik Keamanan Data*. Skripsi, Universitas Negeri Malang.

Farhan, Azzam. 2024. *Evaluasi Kebijakan Pelindungan data pribadi Dalam Sektor Pendidikan Tinggi Di Indonesia*. Tesis, Universitas Airlangga.

Farhan, Muhammad. 2024. *Strategi Pelindungan data pribadi Pada Platform Digital Di Indonesia*. Tesis, Universitas Sebelas Maret.

Fathi, Mursyid. 2024. *Pelindungan data pribadi Dalam Layanan E-Commerce Di Indonesia: Pendekatan Hukum Dan Teknologi*. Skripsi, Universitas Trunojoyo Madura.

Fitria, Citra. 2024. *Kebijakan Pelindungan data pribadi Di Indonesia: Pelaksanaan Dan Tantangan Di Era Teknologi Informasi*. Skripsi, Universitas Muhammadiyah Yogyakarta.

Fitria, Yuliana. 2024. *Pelindungan data pribadi Dalam E-Government: Tinjauan Regulasi Di Indonesia*. Tesis, Universitas Indonesia.

Fitriani, Nur. 2024. *Penerapan Sistem Manajemen Keamanan Data Untuk Pelindungan data pribadi Di Indonesia*. Tesis, Universitas Diponegoro.

Gandhi, Irfan. 2023. *Analisis Pelindungan data pribadi Melalui Pendekatan Hukum Internasional*. Skripsi, Universitas Diponegoro.

Guna, Heri. 2024. *Pelindungan data pribadi Pada Aplikasi Transaksi Digital: Analisis Keamanan Di Indonesia*. Skripsi, Universitas Brawijaya.

Haris, Rahmat. 2024. *Pelindungan data pribadi Dalam Sistem Pembayaran Digital Di Indonesia: Studi Kasus Pada Layanan E-Wallet*. Tesis, Universitas Sumatera Utara.

Haris, Yunita. 2025. *Pelindungan data pribadi Dalam Penggunaan Layanan Fintech Di Indonesia: Perspektif Hukum Dan Keamanan Siber*. Disertasi, Universitas Gadjah Mada.

Hidayat, Aulia. 2024. *Efektivitas Peraturan Pelindungan data pribadi Di Era Digital Di Indonesia: Pendekatan Hukum Kritis*. Tesis, Universitas Islam Negeri Jakarta.

Hummerson, Andi Widiatno.2023. "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Pengendali dan Prosesor Terhadap Kebocoran Data Pribadi di Indonesia." Disertasi, Program Studi Doktor Hukum Universitas Tarumanagara.

Ihsan, Ahmad. 2024. *Peran Pemerintah Dalam Pengaturan Pelindungan data pribadi Di Indonesia*. Disertasi, Universitas Gajah Mada.

Iqbal, Syahrul. 2024. *Tanggung Jawab Pelaku Usaha Dalam Pelindungan data pribadi Konsumen Di Indonesia*. Skripsi, Universitas Negeri Jakarta.

Ismanto, Endra. 2024. *Pelindungan data pribadi Dalam Layanan Keuangan Digital: Studi Kasus Di Indonesia*. Tesis, Universitas Kristen Satya Wacana.

Junaidi, Ahmad. 2024. *Pelindungan data pribadi Dalam Teknologi Informasi: Studi Kasus Di Layanan E-Government Di Indonesia*. Tesis, Universitas Gadjah Mada.

Junaidi, Ilham. 2024. *Pengawasan Dan Penegakan Hukum Dalam Pelindungan data pribadi Di Indonesia*. Tesis, Universitas Islam Indonesia.

Kusuma, Joko. 2025. *Implementasi Pelindungan data pribadi Dalam Sistem E-Government Di Indonesia: Studi Kasus Pada Layanan Publik Digital*. Disertasi, Universitas Padjadjaran.

Lestari, Amira. 2024. *Pelindungan data pribadi Dalam Layanan E-Government Di Indonesia*. Tesis, Universitas Gajah Mada.

Lestari, Nia. 2024. *Kebijakan Pelindungan data pribadi Pada Layanan Keuangan Digital Di Indonesia*. Tesis, Universitas Gajah Mada.

Mahendra, Dwi. 2024. *Transformasi Pelindungan data pribadi Pada Sistem Informasi Digital Di Indonesia*. Skripsi, Universitas Sebelas Maret.

Mansyur, Arif. 2024. *Efektivitas Implementasi Kebijakan Pelindungan data pribadi Di Indonesia Pada Era E-Government*. Tesis, Universitas Muhammadiyah Yogyakarta.

Meylina, Fitri. 2024. *Analisis Hukum Terhadap Pelindungan data pribadi Di Dunia Digital: Tinjauan Dari Perspektif Hukum Indonesia*. Tesis, Universitas Brawijaya.

Mufida, Alia. 2024. *Penerapan Blockchain Untuk Keamanan Data Pribadi Di Indonesia*. Skripsi, Universitas Negeri Surabaya.

Mukti, Shinta. 2025. *Perlindungan Hukum Terhadap Kebocoran Data Pribadi Dalam Sistem Perbankan Indonesia*. Disertasi, Universitas Gadjah Mada.

Mulia, Riza. 2023. *Pelindungan data pribadi Dalam Aplikasi Layanan Kesehatan Online Di Indonesia*. Skripsi, Universitas Hasanuddin.

Munthe, Surya, Triono Eddy, dan Ida Nadirah. 2023. "Wewenang Polri Menyelesaikan Pidana Penipuan dan Penggelapan Arisan Daring Melalui Keadilan Restoratif: Perspektif Hukum Islam." Seminar Nasional Hukum, Sosial, dan Ekonomi, Universitas Muhammadiyah Sumatera Utara.

Mutiara, Nadia. 2024. *Evaluasi Kebijakan Pelindungan data pribadi Dalam Layanan Keuangan Digital Di Indonesia*. Tesis, Universitas Gadjah Mada.

Nabil, Taufik. 2023. *Pelindungan data pribadi Dalam Platform Teknologi: Analisis Terkait Kepatuhan Regulasi Di Indonesia*. Skripsi, Universitas Sriwijaya.

Nabila, Putri. 2023. *Analisis Keamanan Data Pribadi Di Layanan E-Commerce Berdasarkan Undang-Undang Pelindungan data pribadi Di Indonesia*. Skripsi, Universitas Sumatera Utara.

Nadira, Zahra. 2024. *Kajian Pelindungan data pribadi Di Layanan Aplikasi Kesehatan Digital: Studi Hukum Di Indonesia*. Tesis, Universitas Gadjah Mada.

Natamiharja, Rudi, dan Mindoria Stefany. 2019. "Pelindungan Hukum Atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Selular)." *Prodigy Jurnal Perundang-undangan* 7(2):115–137.

Nazarudin, Rizal. 2024. *Pelindungan data pribadi Dalam Sistem Cloud Computing Di Indonesia: Studi Hukum Tentang Keamanan Data Pengguna*. Skripsi, Universitas Muhammadiyah Yogyakarta.

Novianti, Siti. 2025. *Pelindungan data pribadi Di Layanan E-Commerce: Tinjauan Hukum Di Indonesia*. Tesis, Universitas Padjadjaran.

Putra, Adi. 2025. *Pelindungan data pribadi Pada Platform E-Commerce Dalam Menanggulangi Kebocoran Data Di Indonesia*. Tesis, Universitas Kristen Satya Wacana.

Putra, Andi. 2024. *Analisis Keamanan Data Pribadi Dalam Sistem Digital Payment Di Indonesia: Tinjauan Regulasi Dan Kepatuhan*. Tesis, Universitas Airlangga.

Putra, Ardi. 2024. *Pelindungan data pribadi Di Platform E-Commerce: Kajian Hukum Di Indonesia*. Tesis, Universitas Padjadjaran.

Putra, Novi. 2024. *Pelindungan data pribadi Di Sektor Pendidikan Di Indonesia: Tantangan Dan Solusi Regulasi*. Tesis, Universitas Kristen Satya Wacana.

Putri, Syifa. 2024. *Analisis Keamanan Data Pribadi Dalam Sistem Keamanan Digital Di Indonesia*. Tesis, Universitas Kristen Satya Wacana.

Rahayu, Melina. 2025. *Strategi Pelindungan data pribadi Dalam Layanan Fintech Indonesia*. Disertasi, Universitas Gadjah Mada.

Rahma, Siti. 2023. *Pelindungan data pribadi Pada Aplikasi Keuangan Digital: Studi Kasus Di Indonesia*. Tesis, Universitas Airlangga.

Rahmad, Wulan. 2024. *Kajian Pelindungan data pribadi Pada Platform E-Commerce Indonesia: Analisis Dari Perspektif Hukum Positif*. Skripsi, Universitas Udayana.

Rama, Aditia. 2024. *Penerapan Kebijakan Pelindungan data pribadi Di Indonesia: Kasus Dan Tantangan*. Tesis, Universitas Bina Nusantara.

Ramadhan, Taufik. 2025. *Transformasi Pelindungan data pribadi Dalam Industri Perbankan Digital Di Indonesia*. Disertasi, Universitas Indonesia.

Ratna, Siti. 2024. *Pelindungan data pribadi Dalam Konteks Keamanan Siber Di Indonesia: Studi Kasus Keamanan Sistem Transaksi Digital*. Skripsi, Universitas Udayana.

Riana, Cindy. 2025. *Pelindungan data pribadi Dalam Sistem Keamanan Digital: Studi Kasus Di Layanan Keuangan Digital Indonesia*. Disertasi, Universitas Bina Nusantara.

Riani, Melati. 2024. *Penerapan Sistem Pengelolaan Data Pribadi Di Indonesia: Studi Kasus Keamanan Sistem Elektronik Di Layanan Keuangan Digital*. Skripsi, Universitas Airlangga.

Rifki, Reza. 2024. *Perlindungan Hukum Data Pribadi Melalui Pendekatan Teknologi Blockchain: Studi Kasus Di Indonesia*. Tesis, Universitas Padjadjaran.

Rifqi, Abdurrahman. 2024. *Penerapan Kebijakan Pelindungan data pribadi Pada Sistem Informasi Digital Pemerintah Di Indonesia*. Skripsi, Universitas Muhammadiyah Yogyakarta.

Rizal, Ahmad. 2024. *Evaluasi Pelindungan data pribadi Dalam Sektor Keuangan Digital Di Indonesia: Pendekatan Hukum Internasional*. Tesis, Universitas Pendidikan Indonesia.

Rizki, Muhammad. 2024. *Keamanan Data Pribadi Dalam Transaksi Digital Di Indonesia: Studi Kasus Pada Platform E-Commerce*. Skripsi, Universitas Brawijaya.

Rizky, Muhammad. 2025. *Strategi Pelindungan data pribadi Di Layanan Digital Di Indonesia: Pembentukan Regulasi Yang Efektif*. Tesis, Universitas Islam Indonesia.

Rosyid, Irfan. 2023. *Strategi Pelindungan data pribadi Dalam Sistem Pendidikan Digital Di Indonesia*. Tesis, Universitas Pendidikan Indonesia.

Sabilah, Violeta. 2025. *Kajian Terhadap Kebijakan Data Pribadi Di Era Digital: Perspektif Hukum Di Indonesia*. Disertasi, Universitas Udayana.

Santi, Rina. 2024. *Keamanan Data Pribadi Dalam Penggunaan Teknologi Cloud Computing Di Indonesia*. Skripsi, Universitas Pendidikan Indonesia.

Saptohutomo, Aryo Putranto. 2023. "Dugaan Kebocoran Data Pemilih Diperkirakan Bisa Membahayakan Pemilu." Kajian regulasi. Jakarta: Mahkamah Konstitusi RI.

Sari, Intan. 2024. *Pelindungan data pribadi Pada Aplikasi Kesehatan Digital Di Indonesia: Analisis Hukum Terhadap Kebijakan Privasi*. Tesis, Universitas Gadjah Mada.

Satyaputra, Febri Ardiansyah. 2025. *Pengaruh Transformasi Digital Pada Praktik Bisnis Syariah Di Indonesia.* Universitas Islam Sultan Agung, Semarang.

Sudirman, Firdaus. 2024. *Penerapan Blockchain Untuk Pengamanan Data Pribadi Dalam Sistem Perbankan Digital Di Indonesia*. Skripsi, Universitas Gadjah Mada.

Sukma, Dwi. 2024. *Pelindungan data pribadi yang bersifat spesifik Dalam Era Digital: Pengaruhnya Terhadap Kebijakan E-Government Di Indonesia*. Skripsi, Universitas Padjadjaran.

Syafira, Zahra. 2024. *Analisis Pelindungan data pribadi Dalam Sistem Keamanan Informasi Di Indonesia*. Skripsi, Universitas Kristen Satya Wacana.

Tama, Rina. 2024. *Evaluasi Pelindungan data pribadi Dalam Transaksi Digital Di Indonesia: Perspektif Hukum Dan Keamanan Siber*. Skripsi, Universitas Islam Negeri Jakarta.

Taufik, Arief. 2025. *Studi Komparatif Pelindungan data pribadi Antara Indonesia Dan Negara Eropa: Tantangan Dan Solusi*. Disertasi, Universitas Airlangga.

Taufik, Farhan. 2024. *Keamanan Data Pribadi Dalam Penggunaan Aplikasi Pembayaran Digital Di Indonesia*. Skripsi, Universitas Airlangga.

Taufik, Riska. 2025. *Penerapan Blockchain Untuk Pengelolaan Data Pribadi Di Indonesia: Solusi Keamanan Digital*. Tesis, Universitas Diponegoro.

Tirto, Samuel. 2024. *Evaluasi Kebijakan Pelindungan data pribadi Di Indonesia Dalam Layanan E-Government*. Tesis, Universitas Gadjah Mada.

Utama, Mohammad Wira. 2024. "Rekonstruksi Regulasi Pelindungan data pribadi yang bersifat spesifik Bagi Nasabah Perbankan yang Berbasis Nilai Keadilan." Disertasi, Universitas Islam Sultan Agung.

Wibowo, Ilham. 2025. *Penerapan Teknologi Blockchain Untuk Keamanan Data Pribadi Di Layanan Keuangan Digital*. Disertasi, Universitas Brawijaya.

Yulianto, Andi. 2024. *Pelindungan data pribadi Dalam Transaksi Digital: Perspektif Hukum Indonesia*. Skripsi, Universitas Negeri Malang.

Yusuf, Adi. 2024. *Pelindungan data pribadi Dalam Layanan Digital Banking Di Indonesia: Kajian Hukum Perdata*. Tesis, Universitas Airlangga.

Yusuf, Dian. 2024. *Pelindungan data pribadi Dalam Sistem Transaksi Digital: Studi Kasus Penggunaan Platform E-Commerce Di Indonesia*. Tesis, Universitas Sumatera Utara.

Zahidi, Fadhil. 2024. *Pemanfaatan Teknologi Cloud Computing Untuk Keamanan Data Perbankan Di Indonesia*. Disertasi, Universitas Indonesia.

Zahra, Dina. 2024. *Pelindungan data pribadi Dalam Layanan Pendidikan Online: Pendekatan Hukum Di Indonesia*. Skripsi, Universitas Muhammadiyah Jakarta.

Zuwandy, Iqbal. 2023. *Pelindungan data pribadi Dalam Perekonomian Digital: Pendekatan Hukum Di Indonesia*. Skripsi, Universitas Gadjah Mada.

D. Situs Internet

Akamai. 2024. "Keamanan Menjadi Prioritas Bisnis Generasi Era Digital Di Asia Untuk Mencapai Pertumbuhan Berkelanjutan 2024/25 Tech Insider." Akamai.Com. Diakses 6 Mei 2025. (https://www.akamai.com/site/en/dl/2024/asia-digital-native-businesses-report.pdf).

BBC Indonesia. 2025. "Bukalapak Diserang Peretas, Pengguna Diimbau Ganti Password." Diakses 10 April 2025. (https://www.bbc.com/indonesia).

Berita Satu. 2025. "Deretan Kasus Kebocoran Data yang Pernah Terjadi di Indonesia." Diakses 9 April 2025. (https://www.beritasatu.com).

CNN Indonesia. 2022. "10 Kasus Kebocoran Data 2022, Bjorka Dominan, Ramai-Ramai Bantah." Diakses 9 April 2024. (https://www.cnnindonesia.com/techno).

Center, Katadata Insight. 2020. "Digitalisasi, Strategi UMKM Selamat Dari Krisis - Analisis Data Katadata | Berita Ekonomi Bisnis Terbaru Dan Terkini Hari Ini." *Katadata.Co.Id*. Retrieved May 6, 2025 (https://katadata.co.id/analisisdata/5f03cf11e0198/digitalisasi-strategi-umkm-selamat-dari-krisis).

European Data Protection Board. 2023. "Dewan Pelindungan data Eropa – EDPB | Uni Eropa." Diakses 9 Mei 2025. (https://european--union-europa-eu.translate.goog/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_en?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sge).

GDPR-Info. 2020. "General Data Protection Regulation (GDPR) – Legal Text." Https://Gdpr-Info.Eu/. Diakses 9 Mei 2025. (https://gdpr-info.eu/).

Government of Canada. 2022. "CSIS Public Report 2022 - Canada.Ca." Canada.Ca. Diakses 6 Mei 2025. (https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2022.html).

Gartner. 2023. "Gartner Predicts Fines Related to Mismanagement of Data Subject Rights Will Exceed $1 Billion by 2026." Gartner.Com. Diakses 6 Mei 2025.

(https://www.gartner.com/en/newsroom/press-releases/2023-08-24-gartner-predicts-fines-related-to-mismanagement-of-data-subject-rights-will-exceed-1-billion-dollars-by-2026).

Halock. 2022. "Summarizing the Ponemon Cost of a Data Breach Report 2022." Halock.Com. Diakses 6 Mei 2025. (https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/).

Harmen, Ferry Andika. 2023. "Website DJKN." Https://Www.Djkn.Kemenkeu.Go.Id/. Retrieved April 1, 2026 (https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html).

IBM. 2024. "Cost of a Data Breach 2024 | IBM." Ibm.Com. Diakses 6 Mei 2025. (https://www.ibm.com/reports/data-breach).

Indonesia, Kementerian Komunikasi dan Informatika Republik, and Katadata Insight Center. 2023. "Status Literasi Digital di Indonesia 2023."

ITEBA. 2020. "Pelindungan data pribadi Di Era Digital - ITEBA." Iteba.Ac.Id. Diakses 9 Mei 2025. (https://iteba.ac.id/berita/perlindungan-data-pribadi-di-era-digital/).

Kominfo. 2023. "Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia." Diakses 27 April 2025. (https://www.kominfo.go.id/content/detail/50017/siaran-pers-no-132hmkominfo072023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia/0/siaran_pers).

Morgan, Steve. 2020. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damage-costs-10-5-trillion-annually-by-2025/.

Negara, Badan Siber dan Sandi. 2023. *Lanskap Keamanan Siber Indonesia Tahun 2022*. Jakarta: Direktorat Operasi Keamanan Siber BSSN. https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf

Privy. 2024. "Kebocoran Data Di Indonesia Dan Pencegahannya." Privy.Id. Diakses 6 Mei 2025. (https://privy.id/blog/kebocoran-data-di-indonesia-dan-pencegahannya/).

Security, I. B. M. 2023. *Cost of a Data Breach Report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach.

Siagian, Jefri Ronald Parulian. 2024. Meningkatkan Sumber Daya Manusia Yang Berdaya Saing Di Era Teknologi Digital Guna Mendukung Transformasi Digital Nasional. Diakses pada 1 Mei 2025 http://lib.lemhannas.go.id/public/media/catalog/0010-092400000000067/swf/7839/53 - Jefri Siagian.pdf.

Surfshark. 2024. "Global Data Breach Statistics: 2023 Recap." https://surfshark.com/research/study/data-breach-recap-2023.

Sutrisna, Cecep. 2021. "Aspek Hukum Pelindungan data pribadi Dan Kondisi Darurat Kebocoran Atas Data Pribadi Di Indonesia." Wacana Paramarta: Jurnal Ilmu Hukum 20(5): Hlm. 1-10. Diakses 6 Mei 2025. (https://www.wacana-paramarta.com).

Wahyunanda Kusuma Pertiwi, and Oik Yusuf. 2020. "Data Tokopedia, Gojek, Dan Bukalapak Bocor Di Tengah Absennya RUU PDP." Tekno.Kompas.Com. Diakses 12 Mei 2025. (https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp).

Yudha Pratomo, and Reza Wahyudi. 2020. "Kebocoran Data 15 Juta Pengguna, Pengakuan Tokopedia, Dan Analisis Ahli." Tekno.Kompas.Com. Diakses 12 Mei 2025. (https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli).

E. Peraturan Perundang-Undangan

Indonesia, Pemerintah Pusat. 2022. "Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik." Jakarta.

_____. *Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Pelindungan data pribadi yang bersifat spesifik Dalam Sistem Elektronik*. *Peraturan Menteri Republik Indonesia*. Kementerian Komunikasi dan Informatika Republik Indonesia, 2016.

_____. "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945." *Pasal 28G Ayat 1*. Pemerintah Republik Indonesia, 1945.

_____. *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. *Undang-Undang Republik Indonesia*. Pemerintah Republik Indonesia, 2008.

_____. "Undang-Undang Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan." *Undang-Undang Republik Indonesia*. Pemerintah Republik Indonesia, 2013.

_____. “Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik.” *Undang-Undang Republik Indonesia*. Pemerintah Republik Indonesia, 2022.

_____. *Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia*. *Undang-Undang Republik Indonesia*. Pemerintah Republik Indonesia, 1999.

_____. “Undang-Undang Nomor 43 Tahun 2007 Tentang Perpustakaan.” 2007

_____. Mahkamah Agung Republik. “Putusan Nomor 438/Pid.Sus/2020/PN Jkt.Utr,” 2020.

_____. “Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan data pribadi yang bersifat spesifik.” Jakarta, 2022.