DIKLAT PEMBENTUKAN JAKSA • TAHUN 2026

# PELINDUNGAN DATA PRIBADI

## *dalam Penegakan Hukum*

Membaca UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi bersama KUHAP dan KUHP Nasional — dari hak asasi manusia hingga penuntutan tindak pidana pelindungan data pribadi.

**Dr. Rudi Pradisetia Sudirdja, S.H., M.H.**

Jakarta, 19 September 2026





> *Jaksa, akademisi, dan penulis berfokus pada hukum pidana, kebijakan penegakan hukum, dan tata kelola kelembagaan*

## Profil

# Dr. Rudi Pradisetia Sudirdja

Jaksa Kejaksaan Republik Indonesia • Dosen Universitas Adhyaksa

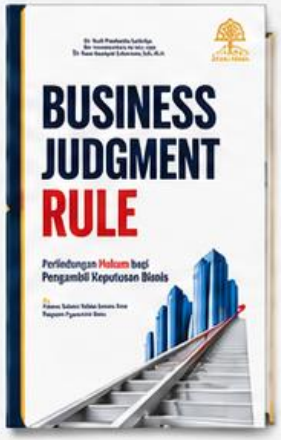
### Riwayat Pendidikan

- S1 Universitas Pasundan
- S2 Universitas Padjadjaran
- S3 Universitas Indonesia

### Riwayat Pekerjaan

- Calon Jaksa pada Kejari Tapaktuan
- Jaksa pada Kejari Kabupaten Bekasi
- Jaksa pada Asisten Khusus Jaksa Agung
- Staf Khusus Ketua Komisi Kejaksaan
- Kepala Sub Bagian Pengelolaan Data, Biro Perencanaan
- Kepala Sub Bagian Pemantauan dan Evaluasi II, Biro Perencanaan
- Kepala Sub Bagian Penyusunan Rencana Anggaran dan Program Kerja, Biro Perencanaan
- Dosen Universitas Adhyaksa

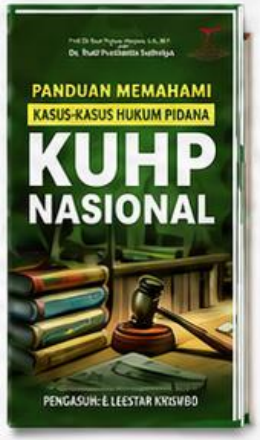
### Karya/Buku
















@rudipradisetia | rudipradisetia.com

PETA MATERI

# Pokok Materi

I Data pribadi sebagai hak fundamental

II Istilah dasar dalam UU PDP

III Dasar & prinsip pemrosesan

IV Hak subjek data & pengecualian

V Kejaksaan sebagai pengelola data

VI Tindak pidana data pribadi

VII Investigasi kebocoran data

VIII KUHAP & KUHP Nasional

IX Penuntutan perkara PDP

X Latihan

XI Penutup



BAGIAN I

# Data Pribadi sebagai Hak Fundamental

I

Yang dilindungi bukan semata-mata datanya, tetapi manusia yang berada di balik data tersebut.

BAGIAN I · KEDUDUKAN GANDA

# Jaksa: penegak hukum sekaligus pemegang data

Perkembangan teknologi menjadikan data identitas, komunikasi, transaksi keuangan, lokasi, biometrik, kesehatan, dan catatan kejahatan menjadi bagian penting dalam pembuktian tindak pidana. Pada saat yang sama, penggunaannya menyentuh hak fundamental seseorang atas pelindungan diri pribadi.

### Sebagai penegak hukum

Menangani tindak pidana yang berkaitan dengan data pribadi — dari perolehan yang melawan hukum hingga jual-beli data.

### Sebagai pemegang amanah data

Memperoleh, menggunakan, menyimpan, dan menguasai data pribadi dalam setiap penanganan perkara.

**MENGAPA PENTING**

Pemahaman UU PDP membuat Jaksa mampu menggunakan data secara sah untuk penegakan hukum, sekaligus mencegah penyalahgunaannya di dalam proses itu sendiri.

# Dua Kedudukan Jaksa

- Penegak hukum atas tindak pidana terkait Data Pribadi
- Pengelola Data Pribadi dalam penanganan perkara



BAGIAN I · ALASAN

# Mengapa data pribadi harus dilindungi?

Data pribadi bukan sekadar kumpulan informasi. Ia melekat pada seseorang dan dapat memengaruhi kehidupan, kebebasan, keamanan, kehormatan, hingga kepentingan ekonominya.

- **Pencurian identitas**
- **Penipuan & kerugian ekonomi**
- **Diskriminasi**
- **Rusaknya reputasi**
- **Ancaman keselamatan**
- **Kehilangan kendali**

CONTOH

Bocornya hasil pemeriksaan kesehatan seorang tersangka bukan sekadar "file yang tersebar", melainkan pengungkapan kondisi kesehatan seseorang kepada pihak yang tidak berhak.



**Bocornya hasil pemeriksaan kesehatan tersangka bukan sekadar “file yang tersebar” —**

melainkan pengungkapan kondisi seseorang kepada pihak yang tidak berhak.

# Mengapa Data Pribadi Harus Dilindungi?

Data melekat pada manusia dan memengaruhi kehidupan, kebebasan, dan keamanannya



BAGIAN I · DASAR HUKUM

# Pelindungan data pribadi adalah bagian dari HAM

**Dasar:** Konsiderans UU PDP & Pasal 1 angka 2

## Konsiderans UU PDP

Menyatakan tegas bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang menjadi bagian dari pelindungan diri pribadi.

## Pasal 1 angka 2

Pelindungan Data Pribadi adalah keseluruhan upaya melindungi data pribadi dalam rangkaian pemrosesannya, guna menjamin hak konstitusional Subjek Data Pribadi.

**PESAN UTAMA**

Penggunaan data pribadi oleh negara — termasuk dalam penegakan hukum — harus berada dalam kerangka penghormatan hak konstitusional warga negara. Yang dilindungi bukan semata-mata datanya, tetapi manusia di baliknya.

# Yang dilindungi bukan semata-mata datanya

— tetapi manusia yang berada di balik data tersebut.

BAGIAN I · KESEIMBANGAN

# Privasi bukan berarti semua data dirahasiakan

Hak atas privasi tidak berarti data pribadi sama sekali tidak boleh dikumpulkan atau digunakan. Negara, bank, rumah sakit, dan institusi lain boleh memproses data sepanjang memiliki dasar yang sah. Persoalannya adalah:

- **? Siapa yang memproses?**
- **? Untuk tujuan apa?**
- **? Atas dasar apa?**
- **? Kepada siapa diberikan?**
- **? Bagaimana digunakan?**
- **? Bagaimana diamankan?**

**CONTOH**

Nomor telepon diberikan ke perusahaan ekspedisi agar kurir dapat menghubungi penerima. Pegawai perusahaan tidak otomatis boleh memakainya untuk kepentingan pribadi.

**PERTANYAAN**

Apakah tersangka tetap punya hak atas pelindungan data pribadi? Ya. Status tersangka tidak menghapus kedudukannya sebagai Subjek Data — namun hak itu tidak mutlak.



# Nomor telepon untuk kurir
# ≠ izin pegawai
## menggunakannya untuk kepentingan pribadi

# Apakah Tersangka Tetap Punya Hak Data Pribadi?

## Ya — status tersangka tidak menghapus kedudukan sebagai Subjek Data



BAGIAN II

# Memahami Istilah Dasar dalam UU PDP

II

Subjek Data, Pengendali, Prosesor, dan Pemrosesan — kosakata yang menentukan seluruh analisis berikutnya.

# Apa itu Data Pribadi?

Pasal 1 angka 1: data yang dapat mengidentifikasi seseorang, secara langsung atau dikombinasikan



BAGIAN II · PASAL 1 ANGKA 1

# Apa yang dimaksud data pribadi?

Data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi:

**Teridentifikasi / dapat diidentifikasi**

**Tersendiri atau dikombinasikan**

**Langsung maupun tidak langsung**

**Elektronik maupun nonelektronik**

**BELUM TENTU IDENTITAS**

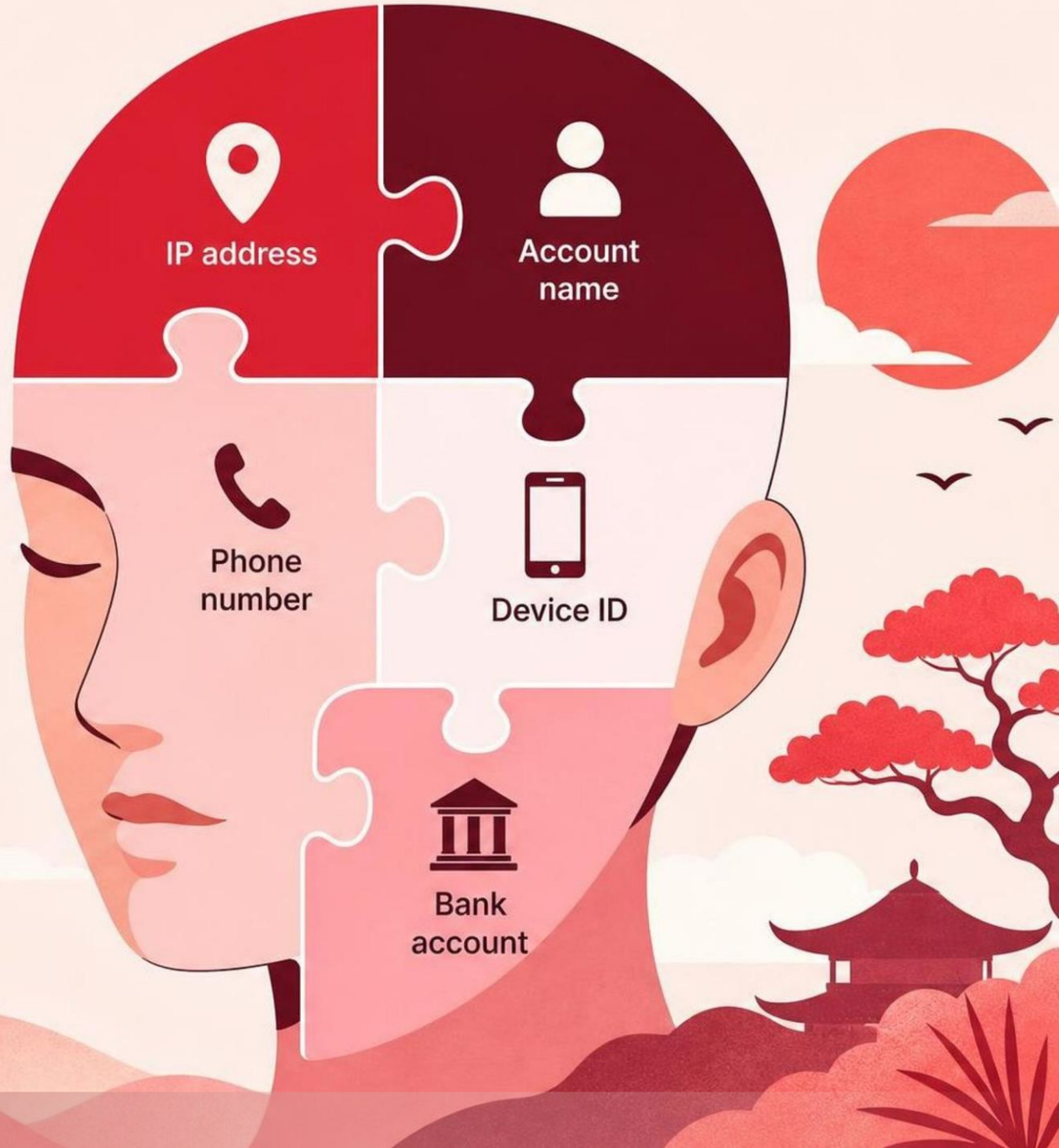
"Pria berusia 35 tahun" — informasi ini sendiri belum tentu mengidentifikasi seseorang.

**MENJADI IDENTITAS**

Nama + NIK + tanggal lahir + alamat + nomor telepon — kombinasi ini dapat mengidentifikasi seseorang secara spesifik.

# Data Pribadi Tidak Selalu Berupa Nama

Kombinasi jejak elektronik dapat mengidentifikasi seseorang secara spesifik



BAGIAN II · JEJAK DIGITAL

# Data pribadi tidak selalu berupa nama

Informasi tertentu mungkin tidak langsung menunjukkan identitas. Namun ketika digabungkan dengan informasi lain, orang tersebut dapat diidentifikasi. Dalam perkara digital, data pribadi kerap berupa kombinasi berbagai jejak elektronik.

## CONTOH — LIMA JEJAK YANG SALING MENGUNCI

**Alamat IP** › **Akun pengguna** › **Nomor telepon** › **Identitas perangkat** › **Rekening bank**

**IMPLIKASI**

Menilai apakah sekumpulan jejak elektronik merupakan data pribadi tidak cukup dengan mencari "nama". Jaksa harus melihat apakah kombinasi jejak itu — bila disatukan — cukup untuk menunjuk satu individu tertentu.

# Data Pribadi Umum vs. Spesifik

Pasal 4 UU PDP




VS.



- **Umum:** nama, jenis kelamin, agama, status perkawinan

- **Spesifik:** kesehatan, biometrik, genetika, catatan kejahatan, data anak, keuangan

BAGIAN II · PASAL 4

# Data pribadi yang bersifat umum dan spesifik

## BERSIFAT UMUM

- Nama lengkap
- Jenis kelamin
- Kewarganegaraan
- Agama
- Status perkawinan
- Data yang dikombinasikan untuk mengidentifikasi seseorang

## BERSIFAT SPESIFIK

- Data kesehatan
- Data biometrik
- Data genetika
- Catatan kejahatan
- Data anak
- Data keuangan pribadi
- Data lain sesuai peraturan perundang-undangan

# Catatan Kejahatan adalah Data Spesifik

Semakin sensitif data,
semakin tinggi kebutuhan
kehati-hatian



BAGIAN II · PASAL 4

# Catatan kejahatan adalah data yang bersifat spesifik

**Penting bagi Jaksa.** Pasal 4 secara eksplisit menempatkan catatan kejahatan sebagai data pribadi yang bersifat spesifik. Penjelasan UU memasukkan catatan tertulis mengenai seseorang yang melakukan perbuatan melawan hukum atau sedang dalam proses peradilan.

**SEMAKIN SENSITIF DATA → SEMAKIN TINGGI KEHATI-HATIAN**

Mengakses › Menggunakan › Menyimpan › Mengungkapkan

**CONTOH**

Data seseorang sebagai tersangka yang terdapat dalam sistem penanganan perkara tidak boleh disebarkan kepada pihak yang tidak berkepentingan — hanya karena data itu kebetulan berada dalam penguasaan aparat. Lembaga penegak hukum justru institusi yang sehari-hari mengelola data paling sensitif.

BAGIAN II · SUBJEK DATA

# Siapa Subjek Data Pribadi?

Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi. Dalam penanganan perkara, ia dapat berupa:

- **Korban**
- **Saksi**
- **Tersangka**
- **Terdakwa**
- **Terpidana**
- **Ahli**

**PRINSIP**

Status seseorang sebagai tersangka atau terdakwa tidak menghapus kedudukannya sebagai Subjek Data.

**CONTOH**

Penyidik memperoleh data rekening A untuk kepentingan penyidikan. A tetap merupakan Subjek Data Pribadi atas informasi rekening tersebut.

BAGIAN II · PASAL 19

# Pengendali dan Prosesor Data Pribadi

## Pengendali Data Pribadi

Pihak yang menentukan tujuan dan melakukan kendali pemrosesan — menentukan MENGAPA dan BAGAIMANA data diproses.

## Prosesor Data Pribadi

Pihak yang memroses data ATAS NAMA Pengendali — melaksanakan berdasarkan kepentingan dan instruksi Pengendali.

**Pasal 19** menegaskan Pengendali dan Prosesor dapat berupa Setiap Orang, Badan Publik, dan Organisasi Internasional.

**CONTOH**

Bank menentukan data apa yang diperlukan dari nasabah, mengapa dikumpulkan, dan bagaimana digunakan → Bank adalah Pengendali. Penyedia layanan penyimpanan data yang dipakai instansi dapat berkedudukan sebagai Prosesor sesuai hubungan dan kewenangannya.

BAGIAN II · PASAL 16

# Pemrosesan bukan sekadar "mengambil data"

Pemrosesan mencakup seluruh siklus hidup data — dan setiap tahapnya menimbulkan kewajiban:

Pemerolehan › Pengolahan › Penyimpanan › Pembaruan › Pengungkapan › Pemusnahan

## SIKLUS DATA DALAM PENANGANAN PERKARA

Perolehan › Analisis › Bukti › Penyimpanan › Pengarsipan › Penghapusan

### IMPLIKASI BAGI JAKSA

Membaca, menyimpan, menganalisis, memindahkan, menampilkan, dan mengungkapkan data dalam berkas perkara semuanya merupakan pemrosesan. Pelindungan data tidak berakhir ketika data berhasil diperoleh secara sah.



BAGIAN III

# Dasar & Prinsip Pemrosesan Data Pribadi

III

Tidak memerlukan persetujuan bukan berarti tidak memerlukan dasar hukum.

BAGIAN III · PASAL 20

# Setiap pemrosesan harus memiliki dasar

Pengendali Data Pribadi wajib memiliki dasar pemrosesan. Kesalahan yang sering terjadi adalah menyamakan "tidak ada persetujuan" dengan "pemrosesan ilegal".

## MITOS

*"Tidak ada persetujuan = pemrosesan ilegal."*

## FAKTA

Persetujuan hanya SALAH SATU dasar pemrosesan. Masih ada lima dasar lain yang sah.

**KUNCI**

Pertanyaannya bukan "apakah ada persetujuan", melainkan "apakah ada dasar pemrosesan yang sah".

BAGIAN III · PASAL 20

# Enam dasar pemrosesan data pribadi

1. Persetujuan yang sah secara eksplisit
2. Pemenuhan kewajiban perjanjian
3. Pemenuhan kewajiban hukum
4. Pelindungan kepentingan vital Subjek Data
5. Tugas untuk kepentingan umum / pelayanan publik / kewenangan menurut UU
6. Kepentingan sah lain dengan keseimbangan kepentingan para pihak

BAGIAN III · ILUSTRASI

# Memahami dasar pemrosesan lewat contoh

| | |
|---|---|
| **Persetujuan** | Pengguna menyetujui pemakaian alamat surel untuk menerima promosi. |
| **Perjanjian** | Alamat pembeli diberikan kepada kurir untuk mengirim barang. |
| **Kewajiban hukum** | Bank memproses identitas nasabah demi memenuhi kewajiban peraturan. |
| **Kepentingan vital** | Data kesehatan pasien tak sadar diproses untuk menyelamatkan nyawanya. |
| **Kewenangan publik** | Aparat memproses data berdasarkan kewenangan UU untuk penegakan hukum. |

# Contoh Dasar Pemrosesan

Persetujuan • Perjanjian • Kewajiban hukum • Kepentingan vital • Kewenangan publik




Email Opt-In



Parcel Delivery




Bank Compliance



Unconscious Patient



Law Enforcement

BAGIAN III · PASAL 18–19

# Penegakan hukum tak selalu perlu persetujuan tersangka

Dasar pemrosesan oleh aparat dapat berasal dari kewajiban hukum atau pelaksanaan kewenangan menurut UU. Karena itu pencabutan persetujuan oleh tersangka tidak otomatis membuat data yang sah diperoleh harus dihapus.

**TETAPI**
Tidak memerlukan persetujuan bukan berarti tidak memerlukan dasar hukum.

**Pemerolehan yang sah ≠ penggunaan tanpa batas ≠ pengungkapan tanpa batas**

**Data rekening yang diperoleh sah untuk membuktikan pidana TIDAK otomatis boleh:**

- Disebarkan ke pihak tak berkepentingan
- Dipakai untuk kepentingan pribadi
- Diunggah ke media sosial
- Dipakai untuk tujuan lain tanpa dasar

BAGIAN IV

# Hak Subjek Data & Pengecualian untuk Penegakan Hukum

IV

Pengecualian untuk penegakan hukum bukan berarti kekebalan dari pelindungan data pribadi.

BAGIAN IV · PASAL 5–13

# Hak Subjek Data Pribadi

- Memperoleh informasi
- Melengkapi, memperbarui & memperbaiki data
- Memperoleh akses & salinan
- Mengakhiri pemrosesan, menghapus / memusnahkan
- Menarik persetujuan
- Keberatan atas keputusan berbasis pemrosesan otomatis
- Membatasi pemrosesan
- Menggugat & memperoleh ganti rugi
- Memperoleh & menggunakan data sesuai UU

BAGIAN IV · PASAL 15

# Hak atas data pribadi tidak bersifat mutlak

Hak-hak tertentu dikecualikan untuk lima kepentingan:

- **Pertahanan & keamanan nasional**
- **Proses penegakan hukum**
- **Kepentingan umum penyelenggaraan negara**
- **Pengawasan jasa keuangan, moneter & stabilitas sistem keuangan**
- **Statistik & penelitian ilmiah**

**SYARAT**

Pengecualian tersebut hanya dapat dilaksanakan dalam rangka pelaksanaan ketentuan undang-undang.

BAGIAN IV · MAKNA

# Pengecualian penegakan hukum bukan kekebalan

**CONTOH**

Tersangka meminta seluruh data transaksinya yang telah diperoleh penyidik dihapus. Permintaan itu tidak otomatis harus dipenuhi bila data diperlukan secara sah dalam proses penegakan hukum — namun itu tidak berarti data bebas dipakai untuk tujuan apa pun.

**Pengecualian hanya berlaku terhadap hak/kewajiban tertentu yang tegas ditentukan UU. Aparat tetap terikat:**

- **Harus ada dasar kewenangan**
- **Penggunaan terkait tujuan yang sah**
- **Keamanan & kerahasiaan dijaga**

**KALIMAT UTAMA**

Pengecualian untuk penegakan hukum tidak mengecualikan aparat sepenuhnya dari pelindungan data pribadi.




# Contoh: Permintaan Hapus Data oleh Tersangka

Tidak otomatis harus dipenuhi jika data diperlukan secara sah dalam penegakan hukum

BAGIAN IV · PASAL 17 & 50

# Pemantauan visual dan dua pengecualian yang berbeda

PASAL 17 · PEMANTAUAN VISUAL

Penggunaan alat pengolah data visual di tempat umum pada prinsipnya harus memenuhi syarat tertentu. Namun kewajiban memberi informasi dan larangan mengidentifikasi seseorang dikecualikan untuk pencegahan tindak pidana & penegakan hukum sesuai peraturan.

## PASAL 15

Pengecualian terhadap HAK tertentu Subjek Data Pribadi.

## PASAL 50

Pengecualian terhadap KEWAJIBAN tertentu Pengendali Data Pribadi.

JANGAN KELIRU

Bukan "penegakan hukum dikecualikan dari UU PDP". Yang benar: UU PDP memberikan pengecualian tertentu dan terbatas untuk kepentingan penegakan hukum.

# Pemantauan Visual & Penegakan Hukum

Pasal 17: pengecualian kewajiban informasi untuk pencegahan tindak pidana — tetap butuh dasar kewenangan





BAGIAN V

# Kejaksaan sebagai Pengelola Data Pribadi

Jangan sampai penegak hukum justru menjadi sumber kebocoran data.

# Kejaksaan Menguasai Data Sangat Sensitif




Kejaksaan adalah pemegang amanah atas data yang paling sensitif

BAGIAN V · AMANAH

# Jaksa menguasai data pribadi yang sangat sensitif

- NIK & alamat
- Data rekening
- Data komunikasi
- Lokasi
- Data kesehatan
- Biometrik
- Data anak
- Foto & video pribadi
- Identitas korban
- Catatan kejahatan

**PESAN**

Kejaksaan bukan sekadar pengguna data pribadi, tetapi pemegang amanah atas data yang sangat sensitif.

# Jangan Sampai Penegak Hukum Jadi Sumber Kebocoran

Pemerolehan sah tidak otomatis membenarkan pengungkapan kepada pihak yang tidak berkepentingan



BAGIAN V · PERINGATAN

# Jangan penegak hukum menjadi sumber kebocoran

CONTOH KASUS

Dalam perkara kekerasan seksual terdapat identitas korban, alamat, rekam medis, dan foto. Seorang pegawai yang punya akses ke berkas memotret dokumen dan mengirimkannya ke grup percakapan yang tidak berkaitan dengan penanganan perkara.

***Karena data awalnya diperoleh secara sah, apakah pengungkapan tersebut juga sah?***

JAWABAN

Tidak otomatis. Kesahan cara memperoleh data tidak dengan sendirinya menyahihkan setiap pengungkapan atau penggunaan sesudahnya.

BAGIAN V · PASAL 39

# Kewajiban menjaga keamanan data

Pengendali wajib mencegah data pribadi diakses secara tidak sah dengan sistem keamanan yang andal, aman, dan bertanggung jawab. Dalam konteks Kejaksaan, pelindungan mencakup empat lapis:

## Fisik

Pengamanan ruang & arsip

## Teknologi

Kata sandi, enkripsi, kendali akses

## Organisasi

Pembatasan kewenangan mengakses data

## SDM

Disiplin & kesadaran pegawai

BAGIAN V · PASAL 46

# Kegagalan pelindungan data & kewajiban notifikasi

Penjelasan Pasal 46 mengaitkan kegagalan dengan hilangnya salah satu dari tiga hal:

**Kerahasiaan**

**Integritas**

**Ketersediaan**

*Kegagalan dapat disengaja maupun tidak — termasuk laptop berisi data perkara yang hilang, meski tanpa peretas.*

**KEWAJIBAN KETIKA TERJADI KEGAGALAN**

Pengendali wajib menyampaikan pemberitahuan tertulis paling lambat 3 × 24 jam. Minimal memuat: (1) data pribadi yang terungkap; (2) kapan dan bagaimana terungkap; (3) upaya penanganan & pemulihan. Ketentuan ini harus dibaca bersama pengecualian tertentu dalam Pasal 50.

# Pejabat Pelindungan Data Pribadi

Pasal 53: wajib ada saat pemrosesan skala besar atas data spesifik — sangat relevan bagi Kejaksaan



BAGIAN V · PASAL 53

# Pejabat atau petugas pelindungan data pribadi

## Kapan diperlukan

Pejabat/petugas fungsi PDP dibutuhkan dalam kondisi yang ditentukan UU — termasuk ketika kegiatan inti melibatkan pemrosesan skala besar terhadap data yang bersifat spesifik dan/atau data yang berkaitan dengan tindak pidana.

## Relevansi bagi Kejaksaan

Pengelolaan data penegakan hukum dalam skala besar menjadikan tata kelola fungsi pelindungan data pribadi sangat relevan bagi institusi Kejaksaan.

**IMPLIKASI KELEMBAGAAN**

Data spesifik + skala besar + kaitan tindak pidana adalah tepat gambaran kerja Kejaksaan. Tata kelola fungsi PDP karenanya bukan formalitas, melainkan kebutuhan.



BAGIAN VI

# Tindak Pidana yang Berkaitan dengan Data Pribadi

VI

Tidak setiap kebocoran data merupakan tindak pidana — unsur delik tetap harus dibuktikan.

BAGIAN VI · PRASYARAT

# Tidak setiap kebocoran data merupakan tindak pidana

Sebelum membaca Pasal 65, pahami bahwa satu kegagalan pelindungan data dapat menimbulkan tiga jenis pertanggungjawaban:

**Administratif** › **Perdata** › **Pidana (dalam keadaan tertentu)**

**KONSEKUENSI**

Kebocoran data tidak otomatis merupakan tindak pidana. Jaksa tetap harus membuktikan unsur delik — bukan menyimpulkan pidana dari fakta kebocoran semata.

**SIKAP JAKSA**

Mulai dari peristiwa dan alat bukti, lalu uji unsur delik. Jangan membalik urutan itu dengan menuju pasal pidana terlebih dahulu.

BAGIAN VI · PASAL 65–66

# Empat perbuatan utama yang dilarang

## 1 Memperoleh / mengumpulkan

Data pribadi secara melawan hukum

## 2 Mengungkapkan

Data pribadi secara melawan hukum

## 3 Menggunakan

Data pribadi secara melawan hukum

## 4 Membuat / memalsukan

Data pribadi palsu atau memalsukan data

*Keempatnya harus dibedakan karena bentuk perbuatannya berbeda.*

BAGIAN VI · PASAL 65(1) JO. 67(1)

# Memperoleh data secara melawan hukum

## UNSUR POKOK

- Setiap Orang
- Dengan sengaja dan melawan hukum
- Memperoleh / mengumpulkan data pribadi yang bukan miliknya
- Dengan maksud menguntungkan diri sendiri / orang lain
- Yang dapat mengakibatkan kerugian Subjek Data

**CONTOH**

Pegawai mengunduh satu juta data pelanggan untuk dijual.

**AKSES SAH DAPAT BERUBAH JADI MELAWAN HUKUM**

Administrator basis data punya akses resmi, lalu mengunduh database untuk dijual. Pertanyaannya bukan sekadar "apakah ia punya akses?", melainkan "apakah kewenangan akses itu mencakup pengambilan dan penggunaan data untuk tujuan tersebut?"

BAGIAN VI · PASAL 65(2) JO. 67(2)

# Mengungkapkan data pribadi secara melawan hukum

**CONTOH**

Seseorang menyebarkan foto KTP dan alamat orang lain melalui media sosial tanpa dasar hukum.

## FOKUS PEMBUKTIAN

- **Data pribadi milik siapa?**
- **Siapa yang mengungkapkan?**
- **Kepada siapa diungkapkan?**
- **Apakah dilakukan dengan sengaja?**
- **Adakah dasar hukum untuk pengungkapan?**

BAGIAN VI · PASAL 65(3), 66 JO. 67–68

# Menggunakan dan memalsukan data pribadi

**MENGGUNAKAN · PASAL 65(3)**

Pelaku memakai identitas orang lain untuk mengajukan pinjaman daring.

**MEMALSUKAN · PASAL 66**

Pelaku mengubah foto dan identitas dalam dokumen untuk membuka rekening penampungan.

## BEDAKAN TIGA BENTUK PERBUATAN

**Memperoleh**
*bagaimana data didapat*

**Mengungkapkan**
*data diberikan ke pihak lain*

**Menggunakan**
*data dimanfaatkan untuk suatu tindakan*

**TUGAS JAKSA**

Bedakan menggunakan data asli milik orang lain dari membuat atau memalsukan data pribadi.

BAGIAN VI · PASAL 70

# Pertanggungjawaban korporasi

Jika tindak pidana dilakukan oleh korporasi, pidana dapat dijatuhkan kepada:

- **Pengurus**
- **Pemegang kendali**
- **Pemberi perintah**
- **Pemilik manfaat**
- **Korporasi**

**Pertanyaan Jaksa jangan berhenti pada "siapa pegawai yang mengunduh data", tetapi juga:**

- **? Siapa memerintahkan?**
- **? Siapa mengendalikan?**
- **? Siapa memperoleh manfaat?**
- **? Untuk kepentingan korporasi?**

**PRINSIP**

Telusuri rantai kendali dan manfaat — bukan hanya tangan terakhir yang menyentuh data.



BAGIAN VII–IX

# Investigasi, KUHAP/KUHP Baru & Penuntutan

Dari insiden menuju konstruksi pembuktian: fakta → alat bukti → unsur delik → pertanggungjawaban.

BAGIAN VII · INVESTIGASI

# Dari peristiwa menuju investigasi

**JANGAN MULAI DARI KESIMPULAN**

"Data bocor, berarti ada peretas." Mulailah dari pertanyaan, bukan dari asumsi pelaku.

## PERTANYAAN PEMBUKA INVESTIGASI

- ? Data apa yang terdampak?
- ? Sistem mana yang terdampak?
- ? Siapa punya akses?
- ? Bagaimana data keluar?
- ? Ke mana data berpindah?
- ? Siapa memperoleh manfaat?

## TAHAPAN INVESTIGASI KEBOCORAN DATA

Deteksi › Preservasi bukti › Forensik digital › Identifikasi pelaku › Kualifikasi hukum

**Ingat:** *kesalahan mengamankan bukti di tahap awal memengaruhi pembuktian di persidangan.*

# Bukti Digital yang Dicari

Tujuan: membangun hubungan antara pelaku, sistem, data, perbuatan, dan akibatnya



BAGIAN VII · BUKTI DIGITAL

# Bukti digital yang perlu dicari

- Access log
- Catatan autentikasi
- Alamat IP
- Identitas akun
- Timestamp
- Riwayat unduhan
- Log komputasi awan
- Perangkat elektronik
- Percakapan / surel
- Database
- Transaksi pembayaran
- Forensic image

**TUJUAN**

Bukan mengumpulkan sebanyak mungkin data, melainkan membangun hubungan antara pelaku, sistem, data, perbuatan, dan akibatnya.

## DATA YANG BEREDAR BELUM MEMBUKTIKAN SUMBERNYA

| Provenance | Authenticity | Integrity | Kronologi | Atribusi |
|---|---|---|---|---|
| *dari mana asal data* | *apakah autentik* | *apakah berubah* | *kapan diperoleh* | *siapa pelakunya* |

BAGIAN VII · CHAIN OF CUSTODY

# Rantai penguasaan barang bukti

Rantai penguasaan barang bukti (ch*ain of custody*) menjelaskan perjalanan bukti sejak ditemukan sampai diajukan di persidangan:

1. **Identifikasi**
2. **Pemerolehan**
3. **Pengamanan**
4. **Pemeriksaan**
5. **Analisis**
6. **Penyajian di sidang**



**PERTANYAAN**

Bagaimana memastikan data yang diperiksa di persidangan sama persis dengan data yang diperoleh saat penyidikan?

# Rantai Penguasaan Barang Bukti




Memastikan data di persidangan identik dengan data yang diperoleh saat penyidikan

BAGIAN VIII · UU NO. 20/2025

# KUHAP baru & investigasi data elektronik

## Pasal 112

Memasukkan Informasi Elektronik dan Dokumen Elektronik sebagai objek yang dapat digeledah untuk kepentingan penyidikan.

## Pasal 113

Pemeriksaan/penyitaan dalam penggeledahan hanya terhadap barang bukti yang terkait dengan tindak pidana.

**IMPLIKASI**

- Pemerolehan bukti digital harus memiliki dasar hukum
- Tindakan atas data harus berkaitan dengan tindak pidana yang ditangani
- Legalitas cara memperoleh bukti menjadi bagian penting kesiapan penuntutan

**PERTANYAAN BAGI JAKSA**

Bukan hanya "apakah data ini membuktikan perkara?", tetapi juga "apakah data ini diperoleh melalui prosedur yang sah?"

BAGIAN VIII · KUHP NASIONAL

# UU PDP harus dibaca bersama KUHP Nasional

**Sejak 2 Januari 2026,** ketentuan pidana di luar KUHP harus dibaca bersama Buku Kesatu KUHP Nasional dan UU No. 1 Tahun 2026 tentang Penyesuaian Pidana — yang menyelaraskan ketentuan pidana di luar KUHP dengan Buku Kesatu.

## KARENA ITU JAKSA HARUS MEMPERHATIKAN

- **Pertanggungjawaban pidana**
- **Kesengajaan**
- **Penyertaan**
- **Pertanggungjawaban korporasi**
- **Sistem pemidanaan**
- **Hubungan dengan tindak pidana lain**

BAGIAN IX · ALUR PENUNTUTAN

# Dari peristiwa menuju pertanggungjawaban pidana

**Fakta** › **Alat bukti** › **Unsur delik** › **Kualifikasi** › **Pertanggungjawaban**

**JANGAN BERPIKIR PINTAS**

"Ada kebocoran data → ada tersangka → gunakan Pasal 67." Alur seperti ini melompati pembuktian.

## YANG BENAR — LIMA PERTANYAAN BERURUT

1. Apa fakta yang terjadi?
2. Apa alat bukti yang mendukungnya?
3. Unsur delik apa yang dapat dibuktikan?
4. Tindak pidana apa yang paling tepat menggambarkan perbuatan?
5. Siapa yang dapat dimintai pertanggungjawaban?

BAGIAN IX · PASAL 67(1)

# Menghubungkan unsur delik dengan alat bukti

| UNSUR YANG DIBUKTIKAN | ALAT BUKTI / FAKTA YANG DICARI |
|---|---|
| **Dengan sengaja** | Komunikasi, instruksi, pola tindakan |
| **Melawan hukum** | Kewenangan akses, SOP, kontrak, dasar hukum |
| **Memperoleh / mengumpulkan** | Access log, perangkat, salinan forensik |
| **Data bukan miliknya** | Database & identifikasi Subjek Data |
| **Maksud menguntungkan** | Penawaran penjualan, percakapan, transaksi |
| **Dapat menimbulkan kerugian** | Sifat data, cara penggunaan & dampaknya |

***Tugas Jaksa: mengubah peristiwa teknologi menjadi konstruksi pembuktian hukum.***

BAGIAN IX · PASAL 69

# Telusuri data — dan telusuri aliran keuntungan

Investigasi jangan berhenti pada "siapa yang mengambil database". Telusuri rantai orang di balik data:

Memperoleh › Menyimpan › Mengungkap › Menjual › Membeli › Memakai › Untung

**PASAL 69**

Memungkinkan pidana tambahan berupa perampasan keuntungan dan/atau harta hasil tindak pidana, serta pembayaran ganti kerugian.

**SATU PERISTIWA DAPAT MELIBATKAN BEBERAPA TINDAK PIDANA**

Akses sistem › Ambil data › Jual data › Pakai identitas › Penipuan › Hasil kejahatan

**PESAN**

Jangan melihat "kebocoran data" sebagai satu peristiwa tunggal — uraikan rantai perbuatannya.

# Kebocoran satu juta data

KRONOLOGI

- A adalah administrator sistem pada Instansi X, berwenang mengakses database penduduk untuk pekerjaannya.
- A mengunduh satu juta data: nama, NIK, alamat, nomor telepon, dan informasi rekening.
- A menawarkan database itu lewat aplikasi percakapan dan menerima pembayaran Rp100 juta.
- Pembeli memakai sebagian data untuk mengajukan pinjaman daring atas nama orang lain.



DATA TERDAMPAK

- Nama
- NIK
- Alamat
- Nomor telepon
- Informasi rekening

BAGIAN X · DISKUSI 10–15 MENIT

# Pertanyaan

1. Siapa Subjek Data & siapa Pengendali?
2. Pemrosesan data apa saja yang terjadi?
3. Pada titik mana tindakan A melawan hukum?
4. Apakah akses yang semula sah menghapus pidana?
5. Perbuatan Pasal 65 mana yang terpenuhi?
6. Alat bukti digital apa yang harus diamankan?
7. Bagaimana membuktikan data berasal dari Instansi X?
8. Bagaimana membuktikan kesengajaan & maksud untung?
9. Apakah pembeli data juga dapat dipidana?
10. Adakah tindak pidana lain? Apa yang harus dilakukan atas Rp100 juta?

# PENUTUP: PESAN UNTUK CALON JAKSA

1. PDP adalah bagian dari HAM — data mewakili hak dan kepentingan seseorang.
2. Penegakan hukum membutuhkan data; UU PDP tidak menghalanginya dan memberi pengecualian tertentu.
3. Pengecualian bukan kekebalan — kewenangan tak membenarkan penggunaan & pengungkapan tanpa batas.
4. Tidak setiap kebocoran adalah pidana — unsur delik tetap harus dibuktikan.
5. Jaksa adalah penegak hukum sekaligus penjaga data pribadi.

*Penegakan hukum dan pelindungan data pribadi bukan dua kepentingan yang harus dipertentangkan — keduanya bagian dari penegakan hukum yang berkeadilan, akuntabel, dan menghormati hak asasi manusia.*

# Terima Kasih

Apabila ingin berdiskusi lebih lanjut —
Instagram: @rudipradisetia • rudipradisetia.com

**Dr. Rudi Pradisetia Sudirdja, S.H., M.H.**
Dosen Fakultas Hukum Universitas Adhyaksa

*"Fiat Justitia Ruat Caelum · Ikatlah ilmu dengan menuliskannya"*

