SEKOLAH TINGGI HUKUM
INDONESIA JENTERA

PSHK
Pusat Studi Hukum & Kebijakan Indonesia

LeIP

KAJIAN HUKUM DAN KELEMBAGAAN

Implementasi Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia

KAJIAN HUKUM DAN KELEMBAGAAN

Implementasi Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia

April 2026
Sekolah Tinggi Hukum Indonesia Jentera

KAJIAN HUKUM DAN KELEMBAGAAN

Implementasi Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia

PENELITIAN KOLABORATIF OLEH

Sekolah Tinggi Hukum Indonesia Jentera (STHI Jentera)
Pusat Studi Hukum dan Kebijakan Indonesia (PSHK)
Lembaga Kajian dan Advokasi untuk Independensi Peradilan (LeIP)

PENELITI

Dian Rositawati
Asfinawati
Bugivia Maharani
Shevierra Danmadiyah
Raden Violla Reininda
Raynov Tumorang

DISUNTING OLEH:

Raditya Kosasih
Fajri Nursyamsi

DUKUNGAN PROYEK

Kajian ini dilaksanakan atas dukungan dari program *Safeguarding Personal Data in Indonesia's Criminal Justice System: Assessment and Capacity Building for Ethical Data Governance*, British Embassy Jakarta - UK Ministry of Justice.

Daftar Isi

Daftar Isi iii
Kata Pengantar vii
Ringkasan Eksekutif ix

1. Pendahuluan 1
   1.1. Latar Belakang 1
   1.2. Tujuan 6
   1.3. Ruang Lingkup dan Batasan Studi 6
   1.4. Metodologi 7
   1.5. Sistematika Kajian 7

2. Kerangka Hukum dan Kebijakan Pelindungan Data Pribadi 11
   2.1. Pelindungan Data Pribadi sebagai Bagian dari Pelindungan HAM 11
   2.2. Kerangka Hukum Pelindungan Data Pribadi di Indonesia 14
   2.3. Pengecualian dalam Penegakan Hukum pada UU PDP 18
   2.4. Kerangka Hukum Terkait Data Pribadi yang Relevan dalam Penegakan Hukum Pidana 20

3. Sistem Peradilan Pidana di Indonesia dan Kewajiban PDP 27
   3.1. Sistem Peradilan Pidana di Indonesia dan Kewajiban PDP 27
      a. Tahap Penyelidikan dan Penyidikan 28
      b. Tahap Penuntutan 29
      c. Tahap Persidangan di Pengadilan 30
      d. Tahap Pelaksanaan Putusan dan Lembaga Pemasyarakatan 30
   3.2. KUHP dan KUHAP Baru serta Implikasinya pada PDP 32

4. Pelindungan Data Pribadi pada Lembaga Pelaksana Peradilan Pidana 35
4.1. Kepolisian 35
4.2. Kejaksaan 44
4.3. Mahkamah Agung dan Badan Peradilan 53
4.4. Lembaga Perlindungan Saksi dan Korban (LPSK) 65
4.5. Lembaga Pemasyarakatan 79

5. Pengelolaan dan Pertukaran Data dalam Sistem Peradilan Pidana Terpadu 95
5.1. Mekanisme Pertukaran Data Antar Lembaga 96
5.2. Titik Risiko dalam Pengelolaan dan Pertukaran Data 97
5.3. Isu Akuntabilitas Lintas Sistem 98

6. Analisis Lintas Lembaga dan Problematika Pelindungan Data 103
6.1. Aspek Regulasi dan Kebijakan: Pelindungan Data Masih Terfragmentasi dan Belum Menjadi Titik Tolak Utama 103
6.2. Tata Kelola Data dan Akuntabilitas: Data Mengalir, tetapi Tanggung Jawab Tidak Selalu Jelas 105
6.3. Tantangan dan Risiko Sistemik: Menyeimbangkan Efisiensi dan Pelindungan 106
6.4. Dampak terhadap Kelompok Rentan: Tingkat Resiko yang Lebih Besar 108
6.5. Mekanisme Pengaduan: Belum Ada Mekanisme Khusus 109
6.6. Sintesis: Kesenjangan antara Norma, Desain Sistem, dan Praktik Kelembagaan 110

7. Rekomendasi Penguatan Tata Kelola Pelindungan Data Pribadi dalam Sistem Peradilan Pidana 113
1) Penetapan kerangka standar minimum lintas lembaga 113
2) Pergeseran paradigma dari keterbukaan menuju keseimbangan dengan pelindungan data 114
3) Penataan tata kelola pertukaran data dalam sistem peradilan pidana 114
4) Penguatan akuntabilitas kelembagaan dalam pengelolaan data 115
5) Pengembangan mekanisme penanganan insiden dan pengaduan 115

6) Prioritisasi pelindungan kelompok rentan 116
7) Penguatan praktik operasional dalam penggunaan dan pengamanan data 116
8) Penguatan kapasitas dan penataan peran SDM dalam pengelolaan data 117
9) Penguatan koordinasi dan kelembagaan pengawasan 117
10) Integrasi pelindungan data dalam agenda reformasi peradilan digital 118

8. Kesimpulan dan Penutup 119

Daftar Pustaka 121

Kata Pengantar

TRANSFORMASI DIGITAL dalam sistem peradilan pidana di Indonesia telah berkembang pesat, ditandai dengan meningkatnya penggunaan sistem elektronik dalam pengelolaan perkara dan pertukaran informasi antar lembaga penegak hukum. Perkembangan ini membawa peluang besar bagi efisiensi dan transparansi, namun sekaligus memperluas risiko terhadap pelindungan data pribadi, terutama mengingat skala, sensitivitas, dan kompleksitas data yang dikelola dalam proses peradilan pidana.

Dalam praktiknya, data pribadi yang diproses dalam sistem peradilan pidana mencakup informasi yang sangat sensitif—mulai dari identitas tersangka, korban, dan saksi, hingga data yang berkaitan dengan kondisi sosial, ekonomi, maupun kesehatan. Tanpa kerangka tata kelola yang memadai, pengelolaan data tersebut berpotensi menimbulkan dampak serius, termasuk pelanggaran privasi, reviktimisasi korban, serta penurunan kepercayaan publik terhadap sistem peradilan.

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi merupakan langkah penting dalam membangun kerangka hukum nasional. Namun, tantangan utama terletak pada implementasi. Hingga saat ini, masih terdapat kesenjangan antara norma hukum dan praktik kelembagaan, baik dalam hal standar operasional, mekanisme pengawasan, maupun kapasitas institusi dalam mengelola data secara aman dan akuntabel. Selain itu, karakter sistem peradilan pidana yang bersifat lintas lembaga menuntut adanya pendekatan yang terintegrasi, bukan sektoral.

Buku ini merupakan laporan riset disusun secara kolaboratif oleh Sekolah Tinggi Hukum Indonesia-Jentera (STH Indonesia Jentera), Lembaga Kajian dan Advokasi Independensi Peradilan

(LeIP) dan Pusat Studi Hukum & Kebijakan Indonesia (PSHK), yang didukung oleh Ministry of Justice United Kingdom melalui Kedutaan Besar Inggris di Jakarta, untuk memberikan dasar analisis yang komprehensif mengenai kondisi pelindungan data pribadi dalam sistem peradilan pidana di Indonesia. Kajian ini mengidentifikasi berbagai risiko utama, termasuk potensi *over-collection*, penggunaan data di luar tujuan, lemahnya kontrol akses, serta belum optimalnya mekanisme anonimisasi dan pengamanan data. Hal ini menjadi penting, mengingat inisiatif keterbukaan di lembaga penegak hukum diawali dari semangat keterbukaan, yang tidak sepenuhnya kompatibel dengan konsep PDP. Di sisi lain, kajian ini juga menyoroti peluang penguatan melalui pengembangan kerangka kebijakan, instrumen operasional, dan praktik kelembagaan yang selaras dengan prinsip-prinsip pelindungan data.

Secara khusus, temuan dalam buku ini diharapkan dapat menjadi rujukan bagi perumusan kebijakan yang lebih terarah, termasuk dalam: (i) penguatan regulasi turunan dan pedoman teknis implementasi UU PDP di sektor peradilan pidana; (ii) pembentukan dan penguatan fungsi pengawasan serta akuntabilitas lintas lembaga; (iii) pengembangan kapasitas sumber daya manusia dan infrastruktur teknologi; serta (iv) penerapan instrumen pelindungan data seperti data *protection impact assessment* dan *record of processing activities*.

Penguatan pelindungan data pribadi dalam sistem peradilan pidana tidak hanya merupakan kewajiban hukum, tetapi juga prasyarat bagi terwujudnya sistem peradilan yang adil, akuntabel, dan berorientasi pada perlindungan hak asasi manusia. Oleh karena itu, diperlukan komitmen bersama dari seluruh pemangku kepentingan untuk memastikan bahwa proses digitalisasi tidak mengorbankan hak fundamental warga negara.

Kami berharap buku ini dapat berkontribusi dalam mendorong reformasi kebijakan dan praktik kelembagaan yang lebih responsif terhadap tantangan pelindungan data pribadi di Indonesia.

Jakarta, Maret 2026

Ketua STH Indonesia Jentera
Dr. Aria Suyudi, SH., LLM

Ringkasan Eksekutif

Kajian Hukum dan Kelembagaan atas Implementasi Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia

1. Latar Belakang

Transformasi digital dalam sistem peradilan pidana Indonesia telah berkembang pesat dalam satu dekade terakhir, ditandai dengan penggunaan sistem elektronik dalam pengelolaan perkara dan pertukaran data antar lembaga penegak hukum. Inisiatif seperti integrasi Sistem Peradilan Pidana Terpadu berbasis Teknologi Informasi (SPPT-TI) memperlihatkan arah menuju efisiensi dan koordinasi yang lebih baik. Namun, perkembangan ini juga meningkatkan skala, kompleksitas, dan sensitivitas data pribadi yang diproses dalam seluruh tahapan peradilan pidana.

Data pribadi dalam sistem ini mencakup informasi yang sangat sensitif, termasuk identitas tersangka, korban, saksi, serta data sosial, ekonomi, dan kesehatan. Data tersebut tidak hanya dikumpulkan, tetapi juga mengalir lintas institusi, dari penyidikan hingga pemasyarakatan, sehingga membentuk ekosistem pengelolaan data berskala besar. Tanpa tata kelola yang memadai, kondisi ini berpotensi menimbulkan risiko serius, seperti kebocoran data, penyalahgunaan, *profiling* yang tidak proporsional, hingga pelanggaran hak atas privasi dan *fairtrial*.

Kehadiran Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam membangun kerangka hukum nasional. Namun, tantangan utama terletak pada implementasi, khususnya dalam konteks sistem peradilan pidana yang bersifat lintas lembaga dan kompleks.

Pelindungan data pribadi berakar pada jaminan konstitusional atas hak atas privasi, sebagaimana tercermin dalam UUD 1945 yang menjamin pelindungan diri pribadi, kehormatan, dan martabat. Kehadiran UU Pelindungan Data Pribadi mempertegas jaminan tersebut dengan mengkonsolidasikan prinsip, hak, dan kewajiban dalam satu rezim hukum yang komprehensif. Dengan demikian, pelindungan data pribadi tidak hanya merupakan isu administratif atau teknis, tetapi merupakan bagian dari pemenuhan kewajiban negara dalam melindungi hak asasi manusia.

Dalam konteks penegakan hukum, terdapat pengecualian untuk kepentingan penegakan hukum. Namun, pengecualian ini tidak bersifat tanpa batas dan tetap harus tunduk pada prinsip kebutuhan, proporsionalitas, pembatasan tujuan, dan akuntabilitas. Tanpa batasan yang jelas, pengecualian tersebut berisiko mendorong praktik pemrosesan data yang berlebihan dan tidak terkontrol, sehingga berpotensi mengganggu pelindungan hak asasi serta legitimasi sistem peradilan pidana.

2. Tujuan dan Pendekatan Kajian

Kajian ini bertujuan untuk memberikan pemetaan awal terhadap kondisi pengelolaan data pribadi dalam sistem peradilan pidana, mengidentifikasi risiko yang muncul dalam praktik kelembagaan, serta menyediakan dasar bagi pengembangan kebijakan dan penguatan kapasitas institusi. Dengan demikian, laporan ini tidak hanya bersifat deskriptif, tetapi juga diarahkan untuk mendukung perumusan intervensi kebijakan yang lebih terarah.

Pendekatan metodologis yang digunakan menggabungkan analisis doktrinal terhadap kerangka hukum dengan analisis institusional terhadap praktik yang berlangsung. Pengumpulan data dilakukan melalui studi dokumen, wawancara dengan pemangku kepentingan, serta diskusi kelompok terfokus. Pendekatan ini memungkinkan triangulasi antara norma hukum dan praktik, sehingga menghasilkan gambaran yang lebih komprehensif mengenai kondisi aktual pelindungan data pribadi.

3. Temuan Utama

3.1. Fragmentasi Regulasi dan Kesenjangan Implementasi

Kajian ini menunjukkan bahwa pelindungan data pribadi dalam sistem peradilan pidana masih berkembang dalam kerangka yang terfragmentasi. Sebelum hadirnya UU PDP, pengaturan mengenai data pribadi tersebar dalam berbagai regulasi sektoral yang lahir dari logika yang berbeda, seperti kebutuhan pembuktian, perlindungan saksi dan korban, maupun keterbukaan informasi. Akibatnya, pelindungan data tidak dibangun dalam satu kerangka konseptual yang utuh, melainkan berkembang secara insidental dan tidak seragam.

Meskipun UU PDP telah berlaku penuh sejak 2024, undang-undang ini belum sepenuhnya menjadi rujukan utama dalam praktik. Hal ini disebabkan oleh belum adanya regulasi turunan dan standar operasional teknis lintas lembaga, kecenderungan untuk menafsirkan pengecualian penegakan hukum secara luas, serta dominasi regulasi sektoral dalam praktik sehari-hari . Dalam situasi ini, UU PDP berisiko berfungsi sebagai kerangka normatif yang deklaratif, sementara praktik tetap ditentukan oleh logika kelembagaan yang lama.

3.2. Paradigma Keterbukaan Informasi dan Lemahnya Perspektif Pelindungan Data

Temuan penting lainnya adalah bahwa pelindungan data pribadi masih cenderung dipahami dalam kerangka keterbukaan informasi (KIP-centric), bukan sebagai hak substantif yang berdiri sendiri. Dalam praktik, fokus utama sering kali terletak pada apakah suatu informasi dapat dibuka atau dikecualikan dari akses publik, bukan pada pertanyaan yang lebih mendasar mengenai legitimasi pemrosesan data.

Dengan demikian, prinsip-prinsip utama dalam pelindungan data, seperti pembatasan tujuan, minimisasi data, dan akuntabilitas, belum sepenuhnya terinternalisasi dalam praktik kelembagaan. Pergeseran paradigma yang diharapkan oleh UU PDP, yaitu dari logika keterbukaan menuju tata kelola data berbasis hak, masih dalam tahap awal .

3.3. Tata Kelola Data dan Akuntabilitas Lintas Lembaga

Sistem peradilan pidana pada dasarnya merupakan ekosistem pertukaran data lintas lembaga, di mana data bergerak secara berkelanjutan dari satu tahap ke tahap berikutnya. Namun, aliran data yang luas ini tidak diikuti dengan kejelasan pembagian tanggung jawab antar institusi.

Dalam praktik, mekanisme kontrol akses masih terbatas, dan belum terdapat standar minimum lintas lembaga yang mengatur bagaimana data harus diproses dan dilindungi. Kondisi ini menciptakan ketidakseimbangan antara intensitas pemrosesan data dan tingkat akuntabilitas. Data dapat digunakan secara luas, tetapi tanggung jawab atas perlindungannya tidak selalu jelas atau terdefinisi dengan baik .

3.4. Keterbatasan Instrumen dan Kapasitas Kelembagaan

Kajian ini juga menemukan bahwa berbagai kewajiban dalam UU PDP belum diimplementasikan secara operasional dalam banyak institusi. Penunjukan Data Protection Officer (DPO) belum dilakukan, mekanisme pencatatan aktivitas pemrosesan data belum tersedia, dan penilaian dampak pelindungan data (DPIA) belum menjadi praktik umum.

Selain itu, pedoman teknis pelindungan data masih tersebar dalam berbagai regulasi internal dan belum terintegrasi dalam satu kerangka operasional yang konsisten. Fokus kelembagaan juga masih cenderung terbatas pada aspek keamanan teknologi, tanpa diimbangi dengan pendekatan tata kelola data yang lebih komprehensif .

3.5. Risiko dalam Praktik Pengelolaan Data

Dalam praktik, sejumlah risiko utama dalam pengelolaan data pribadi dapat diidentifikasi. Risiko tersebut mencakup pengumpulan data yang berlebihan, penggunaan data di luar tujuan awal, lemahnya kontrol akses, serta belum optimalnya mekanisme anonimisasi. Risiko ini menjadi semakin signifikan mengingat karakter data yang dikelola seringkali berkaitan dengan kelompok rentan, seperti korban tindak pidana, anak, dan saksi.

Temuan ini menunjukkan bahwa pelindungan data tidak hanya berkaitan dengan aspek teknis keamanan, tetapi juga dengan

bagaimana data digunakan, dibagikan, dan disimpan dalam siklus penegakan hukum .

3.6. Persoalan Struktural dalam Pelindungan Data

Lebih jauh, penelitian ini menegaskan bahwa persoalan pelindungan data pribadi bersifat struktural. Ia merupakan hasil dari interaksi antara digitalisasi sistem yang berkembang cepat, kebutuhan koordinasi lintas lembaga, kerangka regulasi yang belum harmonis, serta kultur kelembagaan yang belum menempatkan data sebagai objek yang harus dilindungi secara ketat.

Dalam kondisi ini, implementasi UU PDP masih berada pada tahap awal, sementara ketergantungan terhadap data justru berkembang lebih cepat daripada pembangunan sistem perlindungannya. Hal ini menciptakan kerentanan sistemik yang tidak dapat diatasi hanya melalui intervensi teknis semata .

4. Rekomendasi

Penguatan pelindungan data pribadi dalam sistem peradilan pidana memerlukan pendekatan yang sistemik dan lintas dimensi, mencakup aspek regulasi, tata kelola kelembagaan, instrumen operasional, kapasitas, serta pengawasan. Berdasarkan temuan kajian, rekomendasi berikut diusulkan sebagai langkah strategis:

1) **Penetapan kerangka standar minimum lintas lembaga**
   Pelindungan data masih berkembang secara sektoral dengan variasi standar dan ketidakjelasan tanggung jawab antar lembaga. Diperlukan kerangka standar minimum lintas institusi sebagai *baseline* bersama untuk memastikan konsistensi dalam prinsip pemrosesan data termasuk pembatasan tujuan, keamanan, retensi, dan akuntabilitas, serta menjembatani kesenjangan antara UU PDP dan praktik operasional.
2) **Pergeseran paradigma dari keterbukaan menuju keseimbangan dengan pelindungan data**
   Pendekatan yang masih berorientasi pada keterbukaan perlu bergeser menuju keseimbangan dengan pelindungan data sebagai prinsip yang setara. Pelindungan data harus

diintegrasikan dalam kebijakan internal, pedoman publikasi, dan praktik operasional, sehingga tidak lagi bersifat reaktif, melainkan menjadi bagian dari desain proses peradilan.

3) **Penataan tata kelola pertukaran data dalam sistem peradilan pidana**

   Risiko utama terletak pada pertukaran data lintas lembaga, khususnya dalam sistem terintegrasi. Diperlukan kejelasan peran pengendali data, pembatasan tujuan penggunaan, serta mekanisme akuntabilitas dalam setiap alur pertukaran, agar integrasi tidak memperbesar risiko pelanggaran.

4) **Penguatan akuntabilitas kelembagaan dalam pengelolaan data**

   Pengelolaan data masih minim dokumentasi dan belum berbasis pemetaan alur maupun penilaian risiko. Setiap institusi perlu membangun pendekatan yang lebih sistematis untuk memastikan bahwa pemrosesan data tidak hanya sah, tetapi juga dapat dipertanggungjawabkan.

5) **Pengembangan mekanisme penanganan insiden dan pengaduan**

   Ketiadaan mekanisme penanganan kebocoran dan akses pengaduan menjadi kesenjangan penting. Diperlukan prosedur yang jelas untuk pelaporan, penanganan, dan pemulihan insiden, serta kanal pengaduan yang dapat diakses oleh subjek data.

6) **Prioritisasi pelindungan kelompok rentan**

   Dampak pelanggaran data lebih besar bagi kelompok rentan. Oleh karena itu, pelindungan perlu dirancang secara diferensial dengan mempertimbangkan risiko spesifik seperti stigmatisasi, reviktimisasi, dan ancaman keselamatan.

7) **Penguatan praktik operasional dalam penggunaan dan pengamanan data**

   Risiko juga muncul dari praktik sehari-hari, seperti penggunaan kanal komunikasi tidak aman. Diperlukan standar operasional yang lebih konsisten untuk memastikan pelindungan data terimplementasi dalam praktik kerja.

8) **Penguatan kapasitas dan penataan peran SDM dalam pengelolaan data**

Pengelolaan data masih bergantung pada praktik individual. Diperlukan penetapan peran yang jelas, termasuk fungsi pengelola data, serta peningkatan kapasitas praktis agar prinsip pelindungan data terinternalisasi.

9) **Penguatan koordinasi dan kelembagaan pengawasan**
   Koordinasi lintas lembaga dan fungsi pengawasan masih terbatas. Diperlukan mekanisme yang lebih terstruktur untuk memastikan konsistensi kebijakan dan akuntabilitas implementasi.
10) **Integrasi pelindungan data dalam agenda reformasi peradilan digital**
    Digitalisasi berkembang lebih cepat daripada tata kelola pelindungan data. Oleh karena itu, pelindungan data perlu diintegrasikan sejak tahap desain sistem agar efisiensi berjalan seiring dengan akuntabilitas dan perlindungan hak.

5. Penutup

Laporan ini menegaskan bahwa pelindungan data pribadi merupakan prasyarat bagi terwujudnya sistem peradilan pidana yang adil, akuntabel, dan berorientasi pada hak asasi manusia. Reformasi sistem peradilan tidak dapat hanya berfokus pada efisiensi dan digitalisasi, tetapi harus memastikan bahwa penggunaan data berlangsung dalam kerangka tata kelola yang sah, proporsional, dan akuntabel.

Dengan demikian, agenda ke depan bukan hanya mempercepat integrasi sistem, tetapi juga membangun arsitektur pelindungan data yang mampu menjaga keseimbangan antara kepentingan penegakan hukum dan perlindungan hak individu.

1

Pendahuluan

1. 1. Latar Belakang

Dalam satu dekade terakhir, transformasi digital dalam sistem peradilan pidana di Indonesia berkembang secara signifikan. Berbagai institusi penegak hukum: kepolisian, kejaksaan, pengadilan, hingga lembaga pemasyarakatan, mulai mengandalkan sistem elektronik dalam pengumpulan, pengolahan, penyimpanan, dan pertukaran data. Inisiatif seperti integrasi Sistem Peradilan Pidana Terpadu berbasis Teknologi Informasi (SPPT-TI),[1] digitalisasi administrasi perkara, serta publikasi putusan secara daring menunjukkan arah reformasi menuju sistem penegakan hukum yang lebih efisien.

Namun, perkembangan ini sekaligus menghasilkan konsekuensi baru yang belum sepenuhnya diantisipasi secara normatif maupun institusional. Sebagai ilustrasi, Direktori Putusan Mahkamah Agung telah mempublikasikan lebih dari 10 juta putusan.[2] Setiap putusan tersebut berpotensi memuat berbagai bentuk data pribadi, mulai dari identitas pihak berperkara, saksi, korban, hingga informasi sensitif terkait kondisi sosial, ekonomi, atau kesehatan. Jika ditambahkan dengan praktik serupa pada tahapan penyidikan dan penuntutan,

1 Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi (SPPT-TI) adalah kebijakan Pemerintah untuk mengintegrasikan data perkara pidana secara elektronik antar penegak hukum (Polri, Kejaksaan, MA, Ditjen PAS, KPK, BNN) dengan tujuan meningkatkan efisiensi penanganan perkara pidana. SPPT-TI dikembangkan sebagai bagian dari pelaksanaan Perpres Nomor 54 Tahun 2018 tentang Strategi Nasional Pencegahan Korupsi.

2 Laman Direktori Putusan Mahkamah Agung memuat putusan badan peradilan pada tingkat pertama hingga MA, sebagaimana dapat dilihat melalui https://putusan3.mahkamahagung.go.id/ .

maka volume data pribadi yang dikelola oleh sistem peradilan pidana menjadi sangat besar dan terus meningkat.

Dalam praktiknya, data tersebut tidak berhenti pada satu titik, melainkan mengalir dan dipertukarkan lintas institusi penegak hukum. Kepolisian mengumpulkan data sejak tahap penyelidikan dan penyidikan, kejaksaan mengolahnya dalam proses penuntutan, pengadilan menggunakannya dalam pembuktian dan putusan, sementara lembaga lain seperti Lembaga Perlindungan Saksi dan Korban (LPSK) dan Lembaga Pemasyarakatan juga memiliki akses dan kewenangan atas data yang sama.

Pada saat yang sama, data tersebut tidak hanya berhenti pada satu institusi, melainkan dipertukarkan lintas institusi dalam kerangka koordinasi penegakan hukum. Perjalanan data ini terjadi sejalan dengan perjalanan manajemen perkara pidana dari penyelidikan hingga pelaksanaan putusan. Pertukaran ini mencakup data perkara, data tersangka/terdakwa, rekam jejak pidana, hingga informasi pendukung lainnya. Dengan demikian, sistem peradilan pidana pada dasarnya merupakan ekosistem pengelolaan data pribadi berskala besar. Tanpa kerangka pelindungan data pribadi yang memadai, praktik ini berpotensi menimbulkan berbagai risiko, seperti penyalahgunaan data, kebocoran data dan informasi, profiling yang tidak proporsional, hingga pelanggaran hak atas privasi dan fair trial.

Situasi ini menimbulkan implikasi yang tidak dapat diabaikan. Volume data yang besar, intensitas pertukaran antar lembaga, serta keberadaan sistem elektronik dapat meningkatkan eksposur terhadap risiko penyalahgunaan, kebocoran, maupun penggunaan data di luar tujuan yang sah. Dalam konteks ini, pelindungan data pribadi seharusnya tidak lagi dapat diposisikan sebagai isu tambahan, melainkan sebagai elemen integral dari tata kelola peradilan pidana yang berkeadilan dan akuntabel serta perlindungan hak fundamental warga negara.

Secara normatif, pelindungan data pribadi berakar pada hak atas privasi sebagai bagian dari hak asasi manusia. Konstitusi. UUD 1945 dalam Amandemen Kedua, melalui Pasal 28G ayat 1 UUD 1945[3]

3 Ketentuan Pasal 28G ayat (1) merupakan jaminan atas hak. Pasal tersebut akan lebih lengkap jika ditambahkan ketentuan: Pasal 28I ayat (4) yang menekankan pada kewajiban negara, termasuk Pemerintah, untuk melaksanakan pelindungan hak tersebut. Dalam

telah menjamin pelindungan diri pribadi, keluarga, kehormatan, dan martabat. Dalam perkembangan global, pelindungan data pribadi mulai mengalami pergeseran menjadi rezim hukum yang berdiri sendiri, yang berbasis HAM, sebagai jaminan pelindungan bagi warga negara untuk memastikan bahwa individu memiliki kontrol atas informasi yang berkaitan dengan dirinya.[4] Dengan demikian, penguatan pelindungan data pribadi dalam sistem peradilan pidana bukan semata isu teknis, melainkan juga bagian dari pemenuhan kewajiban negara dalam melindungi hak asasi manusia.

Indonesia telah memiliki kerangka hukum utama melalui Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang secara efektif mulai berlaku penuh sejak tahun 2024 setelah masa transisi.[5] Kehadiran undang-undang ini menandai perubahan penting: pelindungan data pribadi tidak lagi tersebar dalam berbagai regulasi sektoral, melainkan dikonsolidasikan sebagai rezim hukum tersendiri yang mengatur hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme pengawasan dan sanksi.

Secara konseptual, UU PDP menegaskan bahwa pelindungan data pribadi merupakan bagian dari hak dasar individu. Posisi ini sejalan dengan perkembangan hukum internasional yang menempatkan pelindungan data sebagai turunan langsung dari hak atas privasi, yakni hak individu untuk mengontrol informasi yang berkaitan dengan dirinya. Dengan demikian, pelanggaran terhadap data pribadi pada dasarnya merupakan pelanggaran terhadap hak asasi manusia.

Namun demikian, keberadaan kerangka hukum tidak secara otomatis menjamin perubahan praktik. Dibandingkan dengan negara-negara yang telah lebih dahulu mengembangkan rezim pelindungan data, seperti Inggris melalui General Data Protection Regulation (GDPR) dan Data Protection Act 2018 dan penguatan kelembagaan

riset ini, penting untuk menambahkan Pasal 28I ayat (4) karena tidak hanya membahas tentang jaminan pelindungan hak, tetapi mendorong adanya penguatan hukum dan kelembagaan yang merupakan kewajiban Pemerintah.

4 Di Eropa, pelindungan data pribadi berkembang dari Data Protection Directive 95/46/EC menjadi General Data Protection Regulation (GDPR) yang berlaku sejak 2018, yang menegaskan prinsip-prinsip seperti *lawfulness, purpose limitation, data minimisation*, dan *accountability*. Di Inggris, prinsip-prinsip tersebut diadopsi melalui Data Protection Act 2018 yang berjalan seiring dengan kerangka GDPR.

5 UU PDP resmi berlaku penuh sejak 17 Oktober 2024, mengakhiri masa transisi dua tahun, sebagaimana diatur dalam Pasal 74.

melalui otoritas independen,[6] pelindungan data pribadi telah menjadi bagian dari kehidupan sehari-hari masyarakat, baik dalam layanan publik, sektor privat, maupun interaksi digital. Prinsip-prinsip seperti pembatasan tujuan, minimisasi data, dan akuntabilitas telah terinternalisasi dalam praktik administratif dan bisnis. Sehingga memiliki tingkat pelembagaan pelindungan data yang lebih matang.

Sebaliknya, di Indonesia, pelindungan data pribadi belum sepenuhnya terlembagakan dalam praktik sosial maupun institusional. Meskipun berbagai lembaga publik telah berupaya menerapkan kepatuhan terhadap UU PDP, penyalahgunaan data pribadi masih berlangsung secara luas dalam kehidupan sehari-hari. Hal ini tercermin, misalnya, dalam sejumlah kasus kebocoran data berskala besar, seperti kebocoran data peserta BPJS Kesehatan yang diperjualbelikan di forum daring, yang melibatkan ratusan juta data individu.[7] Selain itu, praktik distribusi data tanpa persetujuan juga terjadi secara sistemik, misalnya melalui penggunaan data pribadi untuk penawaran pinjaman online atau produk keuangan lainnya, di mana individu menerima akses atau komunikasi tanpa pernah memberikan persetujuan eksplisit.

Dalam konteks penegakan hukum, keterbukaan informasi merupakan elemen penting penegakan hukum. Publikasi putusan di MA merupakan capaian penting praktik transparansi peradilan. Namun pada perkara anak dan perkara sensitif lainnya masih terdapat praktik publikasi putusan yang memuat identitas lengkap korban atau pihak terkait, termasuk dalam perkara kekerasan seksual atau anak, yang seharusnya mendapatkan pelindungan khusus. Hal itu tetap terjadi meski telah terdapat ketentuan untuk melakukan pengaburan atau anonimisasi informasi.[8] Mekanisme anonimisasi

6 Lihat lebih lanjut pada laman resmi Pemerintah Inggris berikut ini https://www.gov.uk/data-protection

7 Kebocoran data BPJS Kesehatan pada tahun 2021 melibatkan dugaan peretasan 279 juta data peserta, termasuk Nomor Induk Kepegawaian (NIK), nama, dan riwayat kesehatan, yang dijual di forum daring. Lihat Nafiatul Munawaroh, "Tanggung Jawab BPJS atas Kebocoran Data Pribadi Pesertanya", https://www.hukumonline.com/klinik/a/tanggung-jawab-bpjs-atas-kebocoran-data-pribadi-pesertanya-lt6389d13f91363/ dan BBC, "BPJS Kesehatan: Data ratuasan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar, https://www.bbc.com/indonesia/indonesia-57196905 .

8 Ketentuan melakukan anonimisasi putusan diatur dalam Surat Keputusan Ketua MA (SK KMA) tentang pelayanan Informasi yang terakhir kalinya diatur melalui SK KMA No. 2-144 tahun 2022 tentang Standar Pelayanan Informasi di Pengadilan.

atau pengaburan identitas pribadi dalam putusan pengadilan juga masih dilaksanakan secara manual.

Sistem peradilan pidana secara inheren memerlukan pengumpulan dan penggunaan data pribadi untuk tujuan pembuktian dalam koridor penegakan hukum. UU PDP sendiri mengakui adanya pengecualian dalam konteks penegakan hukum sebagaimana diatur dalam Pasal 15 Ayat (1) b,[9] termasuk untuk kepentingan penyidikan, penuntutan, dan peradilan. Namun, pengecualian tersebut tidak dapat ditafsirkan sebagai ruang tanpa batas. Sebaliknya, pengecualian tersebut tetap berada dalam kerangka prinsip-prinsip pelindungan data, termasuk kebutuhan, proporsionalitas, dan akuntabilitas. Dengan kata lain, penegakan hukum memang memiliki legitimasi untuk mengakses dan memproses data pribadi, tetapi legitimasi tersebut harus dibatasi secara ketat oleh hukum. Tanpa batasan yang jelas, pengecualian berpotensi berubah menjadi praktik yang eksesif, dimana data dikumpulkan secara berlebihan, disimpan tanpa batas waktu, atau digunakan di luar tujuan awalnya.

Urgensi ini semakin meningkat dengan berkembangnya penggunaan teknologi analitik dan sistem berbasis data dalam proses peradilan pidana, termasuk potensi penggunaan *risk assessment tools* dan algoritma dalam pengambilan keputusan. Studi komparatif menunjukkan bahwa penggunaan teknologi semacam ini membawa manfaat sekaligus risiko, terutama terkait bias, akuntabilitas, dan kepatuhan terhadap prinsip pelindungan data. Dalam konteks Indonesia, perkembangan tersebut menuntut kesiapan kerangka hukum dan kelembagaan yang mampu memastikan bahwa digitalisasi tidak mengorbankan hak-hak dasar individu. Dalam kerangka tersebut, studi ini disusun untuk memberikan pemetaan awal (*initial assessment*) mengenai kondisi pelindungan data pribadi dalam sistem peradilan pidana, mengidentifikasi risiko, serta

9 Pasal 15 ayat (1) b UU PDP ini pada intinya mengatur sebagian hak Subjek Data Pribadi yang dapat dikecualikan untuk kepentingan proses penegakan hukum, yaitu hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi (Pasal 8), menarik persetujuan pemrosesan data pribadi (Pasal 9), mengajukan keberatan atas pemrosesan data pribadi secara otomatis (Pasal 10 ayat (1)), menunda atau membatasi pemrosesan data pribadi (Pasal 11), dan mendapatkan dan/atau menggunakan data pribadi serta mengirimkan data pribadi kepada Pengendali Data Pribadi lainnya (Pasal 13 ayat (1) dan ayat (2)).

merumuskan rekomendasi kelembagaan bagi penguatan kapasitas institusi penegak hukum untuk pelindungan data pribadi.

1.2. Tujuan

Laporan ini memiliki 3 (tiga) tujuan utama.

Pertama, melakukan pemetaan awal (*initial assessment*) terhadap aturan dan praktik pengelolaan data pribadi dalam sistem peradilan pidana. *Assesment* ini mencakup identifikasi fungsi penegakan hukum yang terkait dengan pengumpulan dan pengelolaan data, jenis data yang dikumpulkan dan diproses dalam pengelolaan data di masing-masing institusi penegak hukum.

Kedua, mengidentifikasi risiko pelindungan data pribadi yang muncul dalam praktik. Risiko tersebut tidak hanya mencakup aspek keamanan data (*data breach*), tetapi juga aspek yang lebih luas seperti ketidaksesuaian tujuan pemrosesan, minimnya dasar hukum yang jelas, lemahnya mekanisme kontrol akses, serta potensi pelanggaran prinsip-prinsip pelindungan data seperti akuntabilitas dan pembatasan tujuan.

Ketiga, menyediakan dasar bagi pengembangan *capacity building* dan kebijakan kelembagaan. Hasil *assessment* ini diharapkan menjadi pijakan untuk merancang intervensi kebijakan, penguatan kapasitas sumber daya manusia, serta pengembangan instrumen operasional seperti *data protection impact assessment, record of processing activities* (ROPA), dan protokol pertukaran data antar lembaga.

Dengan demikian, laporan ini tidak hanya bersifat deskriptif, tetapi juga berorientasi pada penguatan tata kelola pelindungan data pribadi dalam sistem peradilan pidana.

1.3. Ruang Lingkup dan Batasan Studi

Studi ini berfokus pada praktik pengelolaan data pribadi dalam institusi penegak hukum di Indonesia yang menjadi bagian dari sistem peradilan pidana, yaitu kepolisian, kejaksaan, pengadilan, lembaga pelindungan saksi dan korban, serta lembaga pemasyarakatan.

Ruang lingkup analisis mencakup:

1. Pengumpulan dan perekaman data pribadi;
2. Penyimpanan dan pengamanan data;
3. Penggunaan dan pemrosesan data dalam proses peradilan;
4. Pertukaran data antar institusi; dan
5. Mekanisme pengawasan dan akuntabilitas.

Namun demikian, studi ini memiliki beberapa batasan. Pertama, studi ini tidak dimaksudkan sebagai audit kepatuhan terhadap UU PDP, melainkan sebagai assessment awal untuk mengidentifikasi isu dan risiko. Kedua, analisis tidak mencakup seluruh sektor publik, melainkan dibatasi pada sistem peradilan pidana. Selain itu tidak semua lembaga penegak hukum menjadi bagian dari studi ini, misalnya Komisi Pemberantasan Tindak Pidana Korupsi ataupun fungsi-fungsi Penyidik Pegawai Negeri Sipil (PPNS) lainnya di luar Kepolisian. Ketiga, studi ini tidak melakukan pengujian teknis terhadap sistem elektronik, melainkan berfokus pada aspek normatif dan institusional.

Pembatasan ruang lingkup ini disebabkan karena keterbatasan waktu dan sumber daya penelitian. Diharapkan di masa depan, cakupan penelitian ini dapat diperluas dan diperdalam sehingga hasil yang diperoleh lebih komprehensif. Kajian ini diharapkan akan menjadi titik tolak untuk memasuki tahapan berikutnya dari kajian yang lebih mendalam dan lebih lengkap.

1.4. Metodologi

Studi ini menggunakan pendekatan metodologis yang menggabungkan analisis doktrinal dan institusional.

1) **Pendekatan doktrinal**
   Pendekatan ini digunakan untuk menganalisis kerangka hukum yang relevan, termasuk Undang-Undang pelindungan Data Pribadi, peraturan sektoral, serta instrumen hukum lain yang mengatur pengelolaan data dalam sistem peradilan pidana. Analisis ini bertujuan untuk menilai kesesuaian antara norma hukum dengan praktik yang berlangsung.

2) **Pendekatan institusional**
   Pendekatan ini digunakan untuk memahami bagaimana praktik pengelolaan data dilakukan dalam konteks kelembagaan. Fokusnya mencakup struktur organisasi, pembagian kewenangan, prosedur operasional, serta kapasitas institusi dalam mengelola data pribadi.
3) **Teknik pengumpulan data**
   Pengumpulan data dilakukan melalui beberapa metode:
   - Studi dokumen, termasuk peraturan perundang-undangan, pedoman internal, dan dokumen kebijakan;
   - Wawancara semi-terstruktur dengan pemangku kepentingan di masing-masing institusi;
   - Diskusi kelompok terfokus (FGD) untuk mengidentifikasi praktik dan tantangan lintas lembaga;

Berbagai metode di atas diterapkan untuk memastikan validitas temuan dan merupakan upaya untuk menerapkan prinsip triangulasi, yaitu dengan membandingkan dan mengkonfirmasi informasi dari berbagai sumber (dokumen dan wawancara). Pendekatan ini penting mengingat praktik pengelolaan data sering kali tidak sepenuhnya terdokumentasi secara formal, sehingga memerlukan verifikasi lintas sumber.

Secara keseluruhan, pendekatan metodologis ini dirancang untuk menghasilkan gambaran yang lengkap mengenai kondisi aktual pelindungan data pribadi dalam sistem peradilan pidana. Temuan dari bagian ini akan menjadi dasar bagi analisis pada bab-bab berikutnya, khususnya dalam mengidentifikasi gap antara kerangka hukum, praktik institusional, dan standar pelindungan data yang seharusnya diterapkan.

1.5. Sistematika Kajian

Laporan ini disusun secara sistematis untuk menggambarkan secara utuh kerangka hukum, praktik kelembagaan, serta tantangan perlindungan data pribadi dalam sistem peradilan pidana. Bagian awal menguraikan latar belakang, tujuan, dan metodologi penelitian, diikuti dengan pembahasan kerangka regulasi, dalam perspektif hak

asasi manusia, serta penjelasan tentang regulasi nasional pelindungan data pribadi. Selanjutnya, laporan mengkaji sistem peradilan pidana dan implikasi pemrosesan data pada setiap tahap, sebelum beralih pada assessment kelembagaan di masing-masing institusi penegak hukum. Analisis kemudian diperdalam pada aspek pengelolaan dan pertukaran data dalam konteks sistem terintegrasi (SPPT-TI). Bagian selanjutnya merupakan sintesis temuan mengenai persoalan struktural lintas kelembagaan. Berdasarkan sintesis tersebut, laporan diakhiri dengan rekomendasi kebijakan dan operasional yang ditujukan untuk memperkuat tata kelola pelindungan data pribadi dalam sistem peradilan pidana Indonesia.

2

Kerangka Hukum dan Kebijakan Pelindungan Data Pribadi

BAGIAN INI BERTUJUAN untuk mengidentifikasi dan memetakan kerangka hukum yang mengatur pelindungan data pribadi dalam konteks penegakan hukum pidana. Melalui pemetaan ini, diharapkan dapat terlihat dasar normatif yang berlaku serta ruang-ruang kesenjangan dalam pengaturannya. Pembahasan mencakup kerangka hukum umum yang dimulai dengan penjelasan PDP sebagai bagian dari hak fundamental, kemudian diikuti elaborasi tentang Undang-Undang Pelindungan Data Pribadi, serta berbagai regulasi sektoral yang relevan dalam sistem peradilan pidana.

2.1. Pelindungan Data Pribadi sebagai Bagian dari Pelindungan HAM

Pasca reformasi, Indonesia melakukan pengarusutamaan HAM dalam dokumen-dokumen negara secara bertahap. UU No. 39/1999 tentang HAM menjadi penanda pertama langkah ini. UU 39/1999 setidaknya memuat tiga pasal terkait pelindungan data pribadi. Pasal 21 melindungi hak "atas keutuhan pribadi" dan oleh karena itu "tidak boleh menjadi obyek penelitian tanpa persetujuan darinya". Penjelasan Pasal 21 ini memberikan pemahaman bahwa "menjadi obyek penelitian" adalah "kegiatan menempatkan seseorang sebagai yang dimintai komentar, pendapat atau keterangan yang menyangkut kehidupan pribadi dan data-data pribadinya serta direkam gambar dan suaranya". Ketentuan berikutnya adalah Pasal 29 Ayat (1) yang memberikan hak "atas pelindungan diri pribadi, keluarga,

kehormatan, martabat, dan hak miliknya". Terakhir adalah Pasal 32 yang melindungi "kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik" kecuali "atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan".

Perubahan kedua UUD 1945 pada tahun 2000 memuat ketentuan yang dapat menjadi landasan terhadap hak atas pelindungan data pribadi. Pasal 28G Ayat (1) memberikan hak atas "pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya." Ketentuan ini tidak hanya menegaskan perlindungan terhadap integritas pribadi, tetapi juga dapat ditafsirkan mencakup kontrol individu atas informasi mengenai dirinya. Dalam konteks ini, hak atas pelindungan data pribadi memiliki keterkaitan erat dengan Pasal 28F UUD 1945 yang menjamin hak untuk memperoleh dan mengelola informasi. Kedua ketentuan tersebut membentuk keseimbangan konstitusional antara hak atas informasi dan hak atas privasi, di mana pemrosesan dan pemanfaatan informasi, termasuk oleh negara, harus tetap menghormati dan melindungi kepentingan individu sebagai subjek data.

Pada dasarnya, ketentuan-ketentuan nasional terkait pelindungan atas hak pribadi tersebut juga selaras dengan ketentuan dalam Deklarasi Universal Hak Asasi Manusia dimana Indonesia sebagai anggota PBB juga terikat kepada dokumen ini. Hal ini setidaknya terlihat dari ketentuan Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) yang menyatakan "Tidak seorang pun boleh menjadi sasaran campur tangan sewenang-wenang terhadap privasi, keluarga, rumah, atau korespondensinya, maupun serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas pelindungan hukum terhadap campur tangan atau serangan tersebut".

Ketentuan dalam UU HAM, Konstitusi, dan DUHAM tersebut mempertegas bahwa kontrol atas informasi, termasuk data pribadi, merupakan bagian dari kebebasan individu, sekaligus menempatkan negara pada posisi untuk memastikan bahwa pemrosesan data tidak mengganggu pelindungan atas diri pribadi. Ketentuan-ketentuan ini menunjukkan bahwa sejak awal, pelindungan data pribadi di Indonesia berakar pada konsep hak atas privasi sebagai bagian dari

hak asasi manusia. Dengan demikian, pelindungan data pribadi bukan sekedar isu administratif atau teknis, melainkan merupakan turunan langsung dari jaminan konstitusional atas integritas dan otonomi individu. Dalam konteks ini, setiap bentuk pengumpulan, penggunaan, dan penyebaran data pribadi oleh negara, termasuk dalam proses penegakan hukum, pada dasarnya merupakan bentuk pembatasan terhadap hak asasi yang hanya dapat dibenarkan (*justified*) apabila dilakukan berdasarkan hukum, untuk tujuan yang sah, serta diperlukan dan proporsional.

Dalam perkembangannya, Indonesia juga telah menjadikan Kovenan Internasional Hak-hak Sipil dan Politik (KIHSP) menjadi hukum domestik di Indonesia melalui UU 12/2005. Pasal 17 Ayat (1) KIHSP mengatur bahwa "tidak seorang pun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah pribadi, keluarga, rumah atau korespondensinya, atau secara tidak sah diserang kehormatan dan nama baiknya. Selanjutnya Pasal 17 ayat (2) mengatur "setiap orang berhak atas pelindungan hukum terhadap campur tangan atau serangan tersebut".

Komentar Umum (*General Comment*) No. 16 Pasal 17 (*The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*) memberikan rincian tentang hak ini sebagai berikut. 1) pengumpulan dan penyimpanan informasi pribadi pada komputer, bank data, dan perangkat lain, baik oleh otoritas publik maupun individu atau badan swasta, harus diatur oleh hukum. 2) Negara harus mengambil langkah-langkah efektif untuk memastikan bahwa informasi mengenai kehidupan pribadi seseorang tidak sampai ke tangan orang-orang yang tidak berwenang menurut hukum untuk menerima, memproses, dan menggunakannya, dan tidak pernah digunakan untuk tujuan yang tidak sesuai dengan Kovenan. 3) Demi mendapatkan pelindungan yang paling efektif atas kehidupan pribadinya, setiap individu harus memiliki hak untuk mengetahui secara mudah dipahami, apakah, dan jika demikian, data pribadi apa yang disimpan dalam *file* data otomatis, dan untuk tujuan apa. 4) Setiap individu juga harus dapat mengetahui otoritas publik atau individu atau badan swasta mana yang mengontrol atau dapat mengontrol *file* mereka. Jika *file* tersebut berisi data pribadi yang

salah atau telah dikumpulkan atau diproses bertentangan dengan ketentuan hukum, setiap individu harus memiliki hak untuk meminta perbaikan atau penghapusan.

Rangkaian instrumen nasional dan internasional tersebut menunjukkan bahwa pelindungan data pribadi merupakan manifestasi konkret dari hak atas privasi dalam konteks modern, khususnya dalam era digital dan pengelolaan data berbasis sistem. Oleh karena itu, dalam konteks penegakan hukum pidana, kewenangan negara untuk mengakses dan memproses data pribadi harus selalu ditempatkan dalam kerangka pembatasan hak asasi manusia yang ketat, dan tidak dapat dilepaskan dari kewajiban untuk menjamin pelindungan terhadap individu dari penyalahgunaan kekuasaan berbasis data.

2.2. Kerangka Hukum Pelindungan Data Pribadi di Indonesia

Di Indonesia, UU PDP merupakan peraturan perundang-undangan utama yang mengatur pelindungan data pribadi. Lahirnya UU PDP merupakan penegasan terhadap pelindungan terhadap diri pribadi–atau umumnya dikaitkan dengan hak atas privasi–sebagaimana telah dijamin dalam konstitusi.[1] UU PDP mengatur berbagai ketentuan, di antaranya adalah 1) jenis data pribadi; 2) hak subjek data pribadi; 3) kewajiban pengendali dan prosesor data pribadi; 4) sanksi administratif; 5) kelembagaan lembaga pelindungan data pribadi; 6) penyelesaian sengketa dan hukum acara; 7) larangan dalam penggunaan data pribadi; dan 8) ketentuan pidana.

Dalam ekosistem pelindungan data pribadi, terdapat 3 (tiga) aktor utama yang diatur, yakni subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi. Pembagian aktor ini menjadi penting dalam konteks sistem peradilan pidana, karena institusi penegak hukum pada dasarnya beroperasi sebagai pengendali data pribadi dalam setiap tahapan proses perkara. Hal ini dikarenakan kepolisian, kejaksaan, pengadilan, dan lembaga pemasyarakatan menentukan tujuan dan cara pemrosesan data, mulai dari tahap penyidikan

1 UUD NRI Tahun 1945, Pasal 28G ayat (1).

hingga pelaksanaan putusan. Dengan demikian, kewajiban yang melekat pada pengendali data dalam UU PDP secara langsung relevan terhadap praktik penegakan hukum.

Subjek data pribadi, orang perseorangan yang pada dirinya melekat data pribadi,[2] merupakan aktor sentral dalam pelindungan data pribadi. Seluruh pengaturan terkait pelindungan data pribadi pada dasarnya bermuara pada pelindungan data pribadi yang melekat pada diri subjek data. Subjek data pribadi memiliki berbagai hak yang telah diatur dalam Pasal 5 hingga Pasal 14 UU PDP, yakni 1) hak atas informasi; 2) hak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi; 3) hak akses dan memperoleh salinan data pribadi; 4) hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi; 5) hak menarik kembali persetujuan pemrosesan data pribadi; 6) hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis; 7) hak menunda atau membatasi pemrosesan data pribadi; 8) hak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi; serta 9) hak atas portabilitas data pribadi. Keberadaan beberapa hak tersebut tidaklah mutlak,[3] melainkan terdapat kondisi tertentu di mana hak-hak tersebut dapat dikesampingkan, misalnya ketika terdapat kepentingan proses penegakan hukum yang perlu diutamakan.

Aktor selanjutnya yang diatur dalam UU PDP adalah pengendali data pribadi. Dalam UU PDP, pengendali data pribadi dimaknai sebagai "*setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.*"[4] Mengacu pada Pasal 20 hingga Pasal 49 UU PDP, pengendali data memiliki berbagai kewajiban, meliputi:[5]

2 UU PDP, Pasal 1 angka 6.

3 Hak-hak yang tidak mutlak meliputi 1) hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi; 2) hak menarik kembali persetujuan pemrosesan data pribadi; 3) hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis; dan 4) hak atas portabilitas data pribadi dapat dikecualikan. Lihat Ibid., Pasal 15.

4 *Ibid.,* Pasal 1 angka 6.

5 *Ibid.*

1) kewajiban memiliki dasar pemrosesan,
2) kewajiban untuk melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan;
3) kewajiban melakukan pemrosesan data pribadi sesuai dengan tujuan pemrosesan data pribadi;
4) kewajiban memastikan akurasi, kelengkapan, dan konsistensi data pribadi;
5) kewajiban memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi;
6) kewajiban melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi;
7) kewajiban memberikan akses kepada subjek data pribadi terhadap data pribadi yang diproses beserta rekam jejak pemrosesan data pribadi;
8) kewajiban melakukan penilaian dampak pelindungan data pribadi (*Data Protection Impact Assesment*/ DPIA);
9) melindungi dan memastikan keamanan data pribadi yang diprosesnya;
10) kewajiban menjaga kerahasiaan data pribadi;
11) kewajiban melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi yang berada di bawah kendalinya;
12) kewajiban melindungi data pribadi dari proses yang tidak sah;
13) kewajiban mencegah data pribadi diakses secara tidak sah;
14) kewajiban mengakhiri pemrosesan data pribadi dalam hal-hal yang telah ditentukan oleh UU PDP;
15) kewajiban memusnahkan data pribadi dalam hal-hal yang telah ditentukan oleh UU PDP;
16) kewajiban memberitahukan penghapusan dan/atau pemusnahan data pribadi kepada subjek data;
17) kewajiban memberitahukan kegagalan pelindungan data pribadi kepada subjek data pribadi, lembaga pelindungan data pribadi, dan/atau masyarakat; dan
18) kewajiban menunjuk pejabat atau petugas pelindungan data pribadi (*Data Protection Officer*/DPO).

Beberapa kewajiban pengendali data pribadi,[6] dapat dikecualikan. Salah satu pengecualian tersebut adalah apabila terdapat kepentingan proses penegakan hukum yang harus diutamakan.

Selain subjek data pribadi dan pengendali data pribadi, prosesor data pribadi juga merupakan aktor yang dimuat dalam UU PDP. Mengacu definisi yang ada pada UU PDP, prosesor data pribadi merupakan "*setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi.*"[7] Prosesor data pribadi memiliki kewajiban utama berupa melakukan pemrosesan data pribadi berdasarkan perintah pengendali data pribadi.[8] Selebihnya, prosesor data pribadi memiliki kewajiban yang kurang-lebih sama dengan pengendali data pribadi, seperti halnya kewajiban untuk:[9]

1) memastikan akurasi, kelengkapan, dan konsistensi data pribadi;
2) melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi;
3) melindungi dan memastikan keamanan data pribadi yang diprosesnya;
4) menjaga kerahasiaan data pribadi yang diprosesnya; dan
5) menunjuk DPO.

Terhadap kewajiban-kewajiban yang dimiliki oleh prosesor data pribadi, tidak terdapat ketentuan pengecualian karena pada dasarnya kewajiban-kewajiban yang diemban oleh prosesor data pribadi sangat bergantung pada kewajiban-kewajiban pengendali data pribadi. Oleh

6 Kewajiban pengendali data pribadi yang dapat dikecualikan meliputi kewajiban untuk 1) memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi; 2) memberikan akses kepada subjek data pribadi terhadap data pribadi yang diproses beserta rekam jejak pemrosesan data pribadi; 3) menjaga kerahasiaan data pribadi; 4) mengakhiri pemrosesan data pribadi dalam hal-hal yang telah ditentukan oleh UU PDP; 5) memusnahkan data pribadi dalam hal terdapat permintaan dari subjek data pribadi; 6) memberitahukan penghapusan dan/atau pemusnahan data pribadi kepada subjek data; serta 7) memberitahukan kegagalan pelindungan data pribadi kepada subjek data pribadi. Lihat *Ibid.*, Pasal 50.

7 *Ibid.*, Pasal 1 angka 5.

8 *Ibid.*, Pasal 51 ayat (1).

9 *Ibid.*, Pasal 52.

karenanya, kewajiban prosesor data pribadi hanya akan dikecualikan apabila terdapat pengecualian yang diterapkan kepada kewajiban pengendali data pribadi.

Kewajiban-kewajiban dalam UU PDP membawa konsekuensi penting terhadap pelembagaan pelindungan data di lembaga penegak hukum. Ketika institusi seperti kepolisian, kejaksaan, pengadilan, dan pemasyarakatan berperan sebagai pengendali data, kewajiban normatif dalam UU PDP menuntut adanya penyesuaian pada struktur organisasi, prosedur operasional, dan mekanisme pengawasan internal. Hal ini mencakup kebutuhan untuk menetapkan fungsi pengelolaan data, memastikan akuntabilitas dalam setiap tahap pemrosesan, serta mengelola relasi dengan pihak lain, termasuk antar lembaga maupun pihak ketiga sebagai prosesor data. Dalam konteks sistem peradilan pidana yang terintegrasi, konsekuensi ini menjadi semakin signifikan, karena pelindungan data tidak lagi dapat dipahami sebagai tanggung jawab individual lembaga, melainkan sebagai bagian dari tata kelola lintas sistem yang menuntut konsistensi standar dan kejelasan akuntabilitas.

2.3. Pengecualian dalam Penegakan Hukum pada UU PDP

Perlu ditegaskan bahwa UU Nomor 27 Tahun 2022 tentang pelindungan Data Pribadi memberikan ruang pengecualian untuk kepentingan penegakan hukum, namun pengecualian tersebut dirumuskan secara terbatas dan bersyarat. Secara normatif, pengecualian dapat ditelusuri antara lain dalam Pasal 15 UU PDP, yang mengatur bahwa hak-hak subjek data, seperti hak akses, hak perbaikan, maupun hak penghapusan, dapat dibatasi dalam hal pemrosesan data dilakukan untuk kepentingan pertahanan dan keamanan nasional, serta proses penegakan hukum.[10] Pembatasan

10 Pasal 15 ayat (1) b menyatakan bahwa: Hak-hak Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk: a. kepentingan pertahanan dan keamanan nasional; b. kepentingan proses penegakan hukum; c. kepentingan umum dalam rangka penyelenggaraan negara; d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau e. kepentingan statistik dan penelitian ilmiah.

ini dimaksudkan untuk memastikan efektivitas proses penyidikan, penuntutan, dan peradilan, yang dalam banyak situasi memang tidak memungkinkan adanya pemberitahuan atau persetujuan dari subjek data.

Namun demikian, pembatasan terhadap hak subjek data tersebut tidak serta-merta menghapus kewajiban pengendali data. Selanjutnya Pasal 20 ayat (2) UU PDP menegaskan bahwa pemrosesan data pribadi tetap harus didasarkan pada dasar yang sah, termasuk pemenuhan kewajiban hukum atau pelaksanaan kewenangan berdasarkan peraturan perundang-undangan. Dalam konteks penegakan hukum, dasar ini menjadi landasan utama bagi aparat untuk memproses data tanpa persetujuan, tetapi tetap dalam batas kewenangan yang diberikan oleh hukum acara pidana. Meskipun terdapat pengecualian terhadap hak subjek data, aparat penegak hukum tetap terikat pada kewajiban untuk memastikan bahwa data yang diproses relevan, tidak berlebihan, dan digunakan hanya untuk tujuan yang sah.

Kewajiban untuk menjaga keamanan data ditegaskan dalam Pasal 35 UU PDP, yang mengharuskan pengendali data untuk melindungi data pribadi dari akses yang tidak sah, pengungkapan yang tidak sah, serta kehilangan atau kerusakan data. Dalam konteks sistem peradilan pidana, kewajiban ini menjadi krusial mengingat tingginya sensitivitas data yang dikelola, termasuk data korban, saksi, dan tersangka. Selain itu, dalam konteks perkembangan teknologi, Pasal 34 UU PDP mengatur kewajiban untuk melakukan penilaian dampak pelindungan data pribadi apabila pemrosesan data memiliki risiko tinggi terhadap subjek data. Ketentuan ini menjadi relevan apabila dalam praktik penegakan hukum mulai digunakan teknologi berbasis analitik atau pemrosesan otomatis, termasuk dalam bentuk *profiling* atau *predictive analytics*.

Dengan demikian, kerangka UU PDP menunjukkan bahwa pengecualian untuk kepentingan penegakan hukum bukanlah pengecualian yang bersifat absolut, melainkan pengecualian yang tetap berada dalam koridor prinsip-prinsip pelindungan data pribadi. Aparat penegak hukum tetap berkewajiban untuk:

1) Memastikan adanya dasar hukum yang sah dalam setiap pemrosesan data (Pasal 20);

2) Mematuhi prinsip-prinsip pemrosesan data yang terbatas dan proporsional (Pasal 16);
3) Menjamin keamanan dan kerahasiaan data (Pasal 35); dan
4) Melakukan penilaian dampak dalam hal pemrosesan berisiko tinggi (Pasal 34).

Dalam praktik, tantangan utama terletak pada operasionalisasi ketentuan-ketentuan tersebut. Tanpa pedoman teknis dan mekanisme pengawasan yang memadai, pengecualian yang diberikan oleh UU PDP berpotensi ditafsirkan secara luas oleh masing-masing institusi, sehingga membuka ruang bagi praktik pengumpulan dan penggunaan data yang tidak terkontrol. Oleh karena itu, penting untuk memastikan bahwa pengecualian dalam UU PDP diterjemahkan ke dalam standar operasional yang jelas, terukur, dan dapat diawasi dalam setiap tahapan sistem peradilan pidana. Selain itu terdapat ketidakjelasan sanksi bagi sektor publik termasuk dalam penegakan hukum padahal pelanggaran oleh penegak hukum akan menimbulkan dampak serius. Ketidakjelasan sanksi ini menjadi salah satu tantangan dalam memastikan kepatuhan di sektor publik.

2.4. Kerangka Hukum Terkait Data Pribadi yang Relevan dalam Penegakan Hukum Pidana

Selain kerangka umum yang dibentuk oleh UU PDP, pengaturan pelindungan data pribadi dalam sistem peradilan pidana di Indonesia pada dasarnya juga tersebar dalam berbagai undang-undang sektoral. Pengaturan ini tidak dirancang sebagai satu rezim terpadu, melainkan berkembang secara parsial sesuai dengan kebutuhan masing-masing sektor. Secara normatif, keberadaan berbagai undang-undang sektoral tersebut juga menunjukkan bahwa sistem hukum Indonesia sebenarnya telah mengakui pentingnya pelindungan data pribadi, bahkan sebelum lahirnya UU PDP. Namun, pengakuan tersebut belum dibangun dalam kerangka konseptual yang konsisten, melainkan tersebar dalam norma-norma yang berbeda dengan orientasi yang beragam. Berbagai regulasi yang memuat aspek pelindungan data dapat dilihat dalam beberapa undang-undang sebagai berikut ini.

Pertama, adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diatur terakhir kalinya dalam UU No. 1 Tahun 2024, yang memberikan dasar bagi permintaan dan pemanfaatan data elektronik dalam kondisi tertentu. Salah satu ketentuan penting dalam UU ITE yang berkaitan langsung dengan perlindungan data pribadi adalah Pasal 26, yang menegaskan bahwa penggunaan data pribadi melalui media elektronik harus dilakukan atas persetujuan subjek data. Persetujuan subyek data adalah dasar legalitas tahap selanjutnya yaitu pemrosesan data dan pelindungan warga negara terhadap praktik sewenang-wenang dalam pemanfaatan data. Ketentuan ini menjadi relevan dalam praktik penyidikan yang semakin bergantung pada data digital, termasuk data yang berada dalam penguasaan penyelenggara sistem elektronik. Namun, pengaturan dalam UU ITE lebih berfokus pada legitimasi akses dan pembuktian, dan belum secara komprehensif mengatur batasan pemrosesan data pribadi dari perspektif pelindungan hak individu.

Kedua, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP) memperkenalkan prinsip keterbukaan dalam penyelenggaraan negara dengan mewajibkan badan publik membuka akses atas informasi yang berada di bawah penguasaannya. Namun, keterbukaan tersebut sejak awal tidak bersifat absolut. Pasal 2 ayat (2) menegaskan bahwa informasi publik yang dikecualikan bersifat ketat dan terbatas, sedangkan Pasal 2 ayat (4) mensyaratkan bahwa pengecualian harus didasarkan pada uji konsekuensi, yaitu penilaian apakah membuka atau menutup informasi lebih melindungi kepentingan yang lebih besar. UU KIP sendiri yaitu dalam Pasal 17 a sebenarnya membuat pengecualian untuk informasi yang apabila dibuka “dapat menghambat proses penegakan hukum, yaitu informasi yang dapat 1) menghambat proses penyelidikan dan penyidikan suatu tindak pidana; 2) mengungkapkan identitas informan, pelapor, saksi, dan/atau korban yang mengetahui adanya tindak pidana; 3) mengungkapkan data intelijen kriminal dan rencana-rencana yang berhubungan dengan pencegahan dan penanganan segala bentuk kejahatan transnasional; 4) membahayakan keselamatan dan kehidupan penegak hukum dan/

atau keluarganya; dan/atau 5. membahayakan keamanan peralatan, sarana, dan/atau prasarana penegak hukum.

Pengecualian tersebut dalam UU KIP memang dapat disimpangi tetapi dengan syarat tertentu yaitu pertama untuk kepentingan pemeriksaan di pengadilan artinya tidak bisa dilakukan dalam tahap penyidikan dan penuntutan sebagaimana diatur Pasal 18 ayat (3). Syarat kedua, harus mengajukan permintaan izin kepada Presiden (Pasal 18 ayat 4). Presiden juga dapat menolak permintaan tersebut (Pasal 18 ayat 7). Artinya, hal yang utama dalam informasi terkait penegakan hukum bukanlah keterbukaan.

Meskipun demikian, pendekatan UU KIP tetap berangkat dari logika akses terhadap informasi publik, bukan dari logika pelindungan data pribadi sebagai hak yang berdiri sendiri. Di sinilah relevansi UU PDP menjadi penting. Jika UU KIP mengatur apakah suatu informasi dapat dibuka atau dikecualikan dari akses publik, maka UU PDP mengatur secara lebih mendasar apakah data pribadi boleh dikumpulkan, digunakan, disimpan, dibagikan, atau diungkapkan, oleh siapa, untuk tujuan apa, dan dengan batasan apa. Dalam konteks lembaga penegak hukum, hubungan keduanya menjadi krusial: data pribadi dalam dokumen perkara, putusan, atau sistem informasi pengadilan tidak cukup hanya dinilai dari sudut keterbukaan atau pengecualian menurut UU KIP, tetapi juga harus diuji berdasarkan prinsip pemrosesan data dalam UU PDP, termasuk pembatasan tujuan, proporsionalitas, keamanan, dan akuntabilitas.

Ketiga, dalam konteks peradilan pidana anak, kerangka hukum Indonesia menunjukkan pendekatan yang lebih protektif terhadap pelindungan data pribadi. Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak (UU SPPA) secara tegas mengatur kewajiban untuk merahasiakan identitas anak yang berhadapan dengan hukum, baik sebagai pelaku, korban, maupun saksi. Pasal 3 huruf i menegaskan bahwa anak berhak untuk tidak dipublikasikan identitasnya, sementara Pasal 19 mengatur bahwa identitas anak, termasuk nama, alamat, wajah, dan informasi lain yang dapat mengungkap jati diri, wajib dirahasiakan dalam pemberitaan media. Ketentuan ini mencerminkan prinsip kepentingan terbaik bagi anak (*the best interests of the child*), yang menempatkan pelindungan

terhadap harkat, martabat, dan masa depan anak sebagai pertimbangan utama dalam proses peradilan pidana.

Pendekatan serupa juga tercermin dalam Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak, khususnya Pasal 64 yang menegaskan bahwa anak yang berkonflik dengan hukum merupakan kelompok yang memerlukan perlindungan khusus, termasuk perlindungan dari publikasi identitas di media massa untuk mencegah labelisasi. Dalam konteks internasional, prinsip ini sejalan dengan Konvensi Hak Anak yang telah diratifikasi melalui Keputusan Presiden Nomor 36 Tahun 1990, yang menekankan perlindungan anak dari perlakuan yang dapat merugikan kehormatan dan reputasinya. Dengan demikian, berbeda dengan pendekatan umum dalam regulasi lain, pelindungan data pribadi dalam peradilan anak telah diatur secara lebih spesifik dan operasional, sekaligus menunjukkan bahwa dalam kondisi tertentu, sistem hukum Indonesia telah mengadopsi standar pelindungan data yang lebih tinggi. Hal ini menjadi relevan untuk melihat bagaimana prinsip serupa dapat diperluas atau diadaptasi dalam sistem peradilan pidana secara umum, khususnya dalam kaitannya dengan pelindungan kelompok rentan.

Keempat, Undang-Undang pelindungan Saksi dan Korban (UU LPSK) memberikan jaminan pelindungan terhadap saksi dan korban, termasuk pelindungan atas identitas dan data pribadi mereka. Dalam konteks ini, pelindungan data pribadi diposisikan sebagai bagian dari pelindungan keamanan dan keselamatan, yang bertujuan untuk mencegah intimidasi, ancaman, atau reviktimisasi. Namun, sebagaimana halnya regulasi sektoral lainnya, pengaturan ini terbatas pada konteks tertentu dan tidak membentuk standar umum yang berlaku lintas institusi.

Kelima, UU Tindak Pidana Penghapusan Kekerasan Seksual memberikan hak pelindungan atas kerahasiaan identitas bagi korban dan keluarganya. Jaminan atas hak ini tertuang dalam kewajiban penuntut umum, hakim dan pengadilan. Penuntut umum pada dasarnya Dalam menguraikan fakta dan perbuatan yang terkait dengan seksualitas, penuntut umum “sedapat mungkin menghindari uraian yang terlalu detail, vulgar, dan berlebihan” dalam menguraikan fakta dan perbuatan yang terkait dengan seksualitas

pada surat dakwaan. Dalam perkara tindak pidana terhadap Korban yang dieksploitasi dan mengalami kekerasan seksual melalui media elektronik atau yang terkait dengan seksualitas, penuntut umum juga diwajibkan menghindari pencantuman atau penyalin rekatan gambar, ilustrasi, dan/ atau foto Korban atau yang memuat data Korban atau yang menunjukkan organ reproduksi, aktivitas, dan/atau objek seksual pada surat dakwaan. Kewajiban menjaga kerahasiaan identitas korban dan/atau saksi bagi hakim melekat dalam pembacaan putusan. Pengadilan juga harus merahasiakan informasi yang memuat identitas Saksi dan/ atau Korban dalam putusan atau penetapan pengadilan.

Selain itu, berbagai peraturan internal institusi penegak hukum, seperti peraturan kepolisian, kejaksaan, maupun pedoman peradilan, juga memuat ketentuan terkait pelindungan privasi, meskipun dalam derajat yang berbeda. Misalnya, kewajiban menjaga privasi tersangka, saksi, dan korban dalam proses penyidikan, atau pembatasan pengungkapan informasi dalam proses persidangan. Namun, ketentuan tersebut umumnya belum terstandarisasi dan belum sepenuhnya terintegrasi dengan prinsip-prinsip pelindungan data pribadi modern.

Dari keseluruhan kerangka tersebut, dapat ditarik beberapa implikasi penting, yaitu:

- Pertama, pengaturan pelindungan data pribadi dalam sistem peradilan pidana di Indonesia bersifat terfragmentasi, dengan masing-masing undang-undang mengatur aspek tertentu tanpa adanya koordinasi konseptual yang kuat.
- Kedua, pendekatan yang digunakan cenderung sektoral dan berbasis fungsi, bukan berbasis pada prinsip pelindungan data pribadi sebagai hak dasar. Hal ini menyebabkan standar pelindungan menjadi tidak seragam antar konteks dan institusi.
- Ketiga, dalam praktik, kondisi ini berpotensi menimbulkan ketidakpastian hukum, baik bagi aparat penegak hukum maupun bagi subjek data, terutama dalam menentukan batasan yang sah dalam pengumpulan, penggunaan, dan pengungkapan data pribadi.

Dengan demikian, kehadiran UU PDP seharusnya berfungsi sebagai kerangka payung (*umbrella framework*) yang mengharmonisasikan berbagai pengaturan sektoral tersebut. Namun, efektivitasnya sangat bergantung pada sejauh mana prinsip-prinsip dalam UU PDP dapat diinternalisasikan ke dalam praktik dan regulasi operasional di masing-masing institusi penegak hukum. Tanpa upaya harmonisasi tersebut, fragmentasi regulasi akan tetap menjadi sumber utama risiko pelanggaran pelindungan data pribadi dalam sistem peradilan pidana.

3

Sistem Peradilan Pidana di Indonesia dan Kewajiban PDP

3.1. Sistem Peradilan Pidana di Indonesia dan Kewajiban PDP

Sistem peradilan pidana di Indonesia merupakan suatu rangkaian proses yang terintegrasi, yang melibatkan berbagai institusi penegak hukum sejak tahap awal penanganan perkara hingga pelaksanaan putusan. Secara umum, tahapan tersebut meliputi penyelidikan dan penyidikan oleh kepolisian, penuntutan oleh kejaksaan, pemeriksaan dan ajudikasi oleh pengadilan, serta pelaksanaan pidana oleh penuntut umum, lembaga pemasyarakatan, pembimbing kemasyarakatan. UU 20/2025 tentang KUHAP yang baru memperjelas pengawasan dan pengamatan putusan tidak hanya oleh hakim yang ditunjuk oleh Ketua pengadilan tetapi hakim tersebut harus melibatkan pula "kementerian yang urusan pemerintahan di bidang keuangan, sebagai bendahara negara, kuasa pelaksana penilai, dan pelelang, dalam hal Putusan Pengadilan menetapkan perampasan barang sitaan diserahkan pada negara".[1] Dalam praktiknya, sistem ini tidak hanya memproses peristiwa pidana, tetapi juga memproduksi, mengelola, dan mendistribusikan data pribadi dalam jumlah besar dan beragam. Dalam konteks ini, kewajiban pelindungan data pribadi (PDP) tidak dapat dipahami sebagai kewajiban tambahan di luar proses penegakan hukum, melainkan sebagai bagian inheren dari setiap tahapan dalam sistem peradilan pidana.

1 *Ibid.*

a. Tahap Penyelidikan dan Penyidikan

Tahap penyelidikan dan penyidikan merupakan titik awal pengumpulan data dalam sistem peradilan pidana. Pada tahap ini, aparat penegak hukum mengumpulkan berbagai jenis data pribadi, termasuk identitas terlapor, saksi, korban, serta data pendukung lainnya seperti rekaman komunikasi, data lokasi, atau informasi keuangan dalam rangka menemukan dan membuktikan terjadinya suatu tindak pidana. Data yang dikumpulkan juga mencakup kategori data pribadi spesifik (*sensitive data*), seperti kondisi kesehatan, riwayat sosial, atau informasi biometrik.

Masalah data pribadi bertambah karena penggunaan teknologi pengenalan wajah/*face recognition*. Penggunaan teknologi ini setidaknya tercatat dalam pengeroyokan Ade Armando yang terjadi pada 11 April 2022[2], KTT G20 di Bali pada tahun 2022[3], Pekan Olah Raga Nasional XXI Aceh-Sumatra Utara pada tahun 2024[4] dan tilang elektronik[5].

CCTV berteknologi *Face Recognition* ini terhubung langsung dengan sistem administrasi kependudukan (adminduk). Oleh karena itu, ketika wajah seseorang tertangkap kamera, identitas orang tersebut, termasuk Nama dan Nomor Induk Kependudukan (NIK), muncul di layar sistem. Keterangan Polda Sumut, teknologi ini bukan hanya untuk kepentingan pengamanan acara, melainkan juga untuk melacak orang yang masuk dalam Daftar Pencarian Orang (DPO).

Teknologi pemindai wajah ini tidak selalu akurat. Dalam kasus pengeroyokan Ade Armando, dua orang yang diumumkan sebagai tersangka ternyata tidak ikut dalam demonstrasi di depan DPR. Polisi kemudian mengakui adanya salah identifikasi dari *face recognition*. Padahal, wajah dan identitas mereka sudah terlebih dahulu beredar di media sosial, jauh sebelum diumumkan secara resmi oleh polisi

2 KumparanNEWS, "Pakar Hukum: Tak Bisa Polisi Tetapkan Tersangka Hanya Pakai Face Recognition", Pakar Hukum: Tak Bisa Polisi Tetapkan Tersangka Hanya Pakai Face Recognition | kumparan.com

3 Tribrata, "Polri Terapkan Teknologi Face Recognition Dalam Pengamanan KTT G20", Polri Terapkan Teknologi Face Recognition Dalam Pengamanan

4 Komdigi, Polri Gunakan Teknologi Face Recognition untuk Pengamanan di PON Aceh-Sumut, 10 September 2024. Kementerian Komunikasi dan Digital

5 Tempo, "Antisipasi Kendaraan Tanpa Pelat, Polri Terapkan Face Recognition untuk Tilang Elektronik", Antisipasi Kendaraan Tanpa Pelat, Polri Terapkan Face Recognition untuk Tilang Elektronik | tempo.co

Sistem ini ternyata juga telah digunakan oleh perusahaan sehingga membuat akses Kepolisian kepada data pribadi semakin luas. PT Angkasa Pura II telah menggunakan sistem face recognition untuk penumpang pesawat yang akan melakukan keberangkatan melalui Bandara Soekarno Hatta (Soetta). Sistem ini telah dipakai sejak bulan Januari 2022.

Implikasi terhadap pelindungan data pada tahap ini sangat signifikan. Pertama, terdapat risiko pengumpulan data secara berlebihan (*over-collection*), terutama ketika batasan antara data yang relevan dan tidak relevan tidak didefinisikan secara ketat. Kedua, terdapat potensi penggunaan data di luar tujuan awal, misalnya penggunaan data yang diperoleh dalam satu perkara untuk kepentingan lain tanpa dasar hukum yang jelas termasuk pertukaran data dengan instansi lain. Misal untuk kepentingan *profiling*, yang tidak selalu memiliki dasar hukum yang jelas dan memadai. Ketiga, aspek keamanan data menjadi krusial mengingat data pada tahap ini sering kali belum memiliki kontrol akses yang memadai dan rentan terhadap kebocoran. Dalam kerangka UU PDP, aparat penegak hukum sebagai pengendali data tetap memiliki kewajiban untuk memastikan bahwa pengumpulan dan pemrosesan data dilakukan secara sah, terbatas pada tujuan yang spesifik, serta dilindungi dengan langkah pengamanan.

b. Tahap Penuntutan

Pada tahap penuntutan, data yang telah dikumpulkan dalam proses penyidikan diolah dan disusun menjadi berkas perkara yang akan diajukan ke pengadilan. Jaksa penuntut umum berperan sebagai pihak yang mengonsolidasikan berbagai jenis data, termasuk keterangan saksi, alat bukti, dan dokumen pendukung lainnya. Pada tahap ini, risiko utama berkaitan dengan integritas dan akurasi data. Kesalahan atau ketidakakuratan data dapat berdampak langsung pada kualitas pembuktian dan pada akhirnya mempengaruhi hak-hak terdakwa maupun korban. Selain itu, distribusi berkas perkara kepada berbagai pihak (pengadilan, penasihat hukum, dan pihak terkait lainnya) meningkatkan risiko akses yang tidak terkendali terhadap data pribadi.

Kewajiban PDP pada tahap ini menuntut adanya mekanisme kontrol yang jelas terhadap siapa yang dapat mengakses data, untuk tujuan apa, serta dalam jangka waktu berapa lama. Prinsip akuntabilitas menjadi penting untuk memastikan bahwa setiap penggunaan data dapat ditelusuri dan dipertanggungjawabkan.

c. Tahap Persidangan di Pengadilan

Tahap persidangan merupakan fase di mana data pribadi digunakan secara intensif dalam proses pembuktian. Data tersebut disajikan dalam persidangan, diuji melalui pemeriksaan saksi dan ahli, serta pada akhirnya dituangkan dalam putusan pengadilan. Di satu sisi, prinsip keterbukaan peradilan (*open justice*) menghendaki transparansi dalam proses persidangan, termasuk akses publik terhadap putusan. Namun disisi lain, prinsip pelindungan data pribadi menuntut pembatasan terhadap pengungkapan informasi tertentu, terutama yang berkaitan dengan korban, anak, atau data sensitif lainnya.

Ketegangan antara keterbukaan dan pelindungan data ini menjadi salah satu isu kunci dalam praktik. Salah satu contoh adalah publikasi putusan yang masih memuat identitas lengkap pihak berperkara menunjukkan bahwa mekanisme anonimisasi belum diterapkan secara konsisten. Dalam kerangka UU PDP, pengadilan tetap memiliki kewajiban untuk memastikan bahwa pengungkapan data dalam putusan dilakukan secara proporsional, dengan mempertimbangkan kepentingan publik dan pelindungan hak individu.

d. Tahap Pelaksanaan Putusan dan Lembaga Pemasyarakatan

Tahap pelaksanaan putusan melalui lembaga pemasyarakatan (lapas) merupakan fase yang sering luput dalam pembahasan pelindungan data pribadi, padahal pada tahap ini pengelolaan data berlangsung dalam jangka waktu yang panjang dan berkelanjutan. Setidaknya terdapat tiga sub tahapan dalam fase ini. Pertama, pelaksanaan putusan oleh Penuntut Umum dengan bimbingan oleh pembimbing kemasyarakatan. Dalam hal putusan berisi pencabutan hak tertentu terhadap Terpidana, maka salinan putusan akan dikirim pula kepada lembaga terkait yang akan melaksanakan putusan tersebut.

Kedua, pelaksanaan pidana penjara yang dilakukan di lembaga pemasyarakatan (Lapas). Lapas mengelola berbagai jenis data pribadi narapidana, termasuk identitas, riwayat pidana, data kesehatan, perilaku selama menjalani pidana, hingga data sosial dan keluarga. Data ini tidak hanya digunakan untuk administrasi, tetapi juga untuk penilaian pembinaan, klasifikasi narapidana, pemberian hak-hak seperti remisi, asimilasi, atau pembebasan bersyarat.

Ketiga, pengawasan dan pengamatan (wasmat) pelaksanaan putusan pengadilan. KUHAP baru memberikan mandat kepada hakim wasmat untuk melibatkan pihak lain. Pihak tersebut tidak hanya pihak yang telah terlibat sejak penyidikan seperti penyidik, advokat, selaku yang mewakili kepentingan terpidana dan keluarga terpidana dan korban tindak pidana tetapi juga pembimbing kemasyarakatan serta kementerian yang urusan pemerintahan di bidang keuangan, sebagai bendahara negara, kuasa pelaksana penilai, dan pelelang, dalam hal Putusan Pengadilan menetapkan perampasan barang sitaan diserahkan pada negara.

Implikasi pelindungan data pada tahap ini mencakup beberapa isu kunci. Pertama, persoalan retensi data, yaitu berapa lama data disimpan dan apakah terdapat mekanisme penghapusan atau pembatasan akses setelah masa pidana berakhir. Kedua, penggunaan data untuk tujuan sekunder, misalnya untuk kepentingan profiling atau pertukaran dengan instansi lain, yang tidak selalu memiliki dasar hukum yang jelas. Ketiga, keamanan data dalam sistem pemasyarakatan yang seringkali belum terintegrasi dengan standar pelindungan data yang memadai.

Selain itu, terdapat risiko bahwa data narapidana terus digunakan atau diakses bahkan setelah individu kembali ke masyarakat, yang dapat berdampak pada hak atas reintegrasi sosial. Dalam konteks ini, prinsip pembatasan tujuan dan pembatasan penyimpanan menjadi sangat penting. Dalam kerangka UU PDP, lembaga pemasyarakatan sebagai pengendali data tetap memiliki kewajiban untuk memastikan bahwa data hanya digunakan untuk tujuan yang sah, disimpan dalam jangka waktu yang terbatas, serta dilindungi dari akses yang tidak sah.

Dari keseluruhan tahapan tersebut, terlihat bahwa sistem peradilan pidana pada dasarnya merupakan suatu siklus pengelolaan

data pribadi yang berkelanjutan. Setiap tahap tidak berdiri sendiri, melainkan saling terhubung melalui aliran data yang terus bergerak antar institusi. Implikasi utamanya adalah bahwa pelindungan data pribadi tidak dapat diatur secara parsial atau sektoral, melainkan memerlukan pendekatan sistemik yang mencakup seluruh tahapan proses. Tanpa kerangka yang terintegrasi, risiko pelanggaran akan terus berulang di setiap titik dalam siklus tersebut.

Dalam konteks ini, penerapan prinsip-prinsip pelindungan data, termasuk legalitas, pembatasan tujuan, minimalisasi data, akurasi, keamanan, dan akuntabilitas, harus menjadi bagian dari desain dan operasional sistem peradilan pidana itu sendiri. Pengecualian untuk kepentingan penegakan hukum tidak boleh dimaknai sebagai pembebasan dari kewajiban, melainkan sebagai pengaturan khusus yang tetap berada dalam koridor pelindungan hak asasi manusia.

3.2. KUHP dan KUHAP Baru serta Implikasinya pada PDP

Selain perkembangan kelembagaan dan digitalisasi sistem, perubahan kerangka hukum pidana nasional melalui Kitab Undang-Undang Hukum Pidana (KUHP)[6] yang baru serta pembaruan Kitab Undang-Undang Hukum Acara Pidana (KUHAP)[7] turut memperluas implikasi pelindungan data pribadi dalam sistem peradilan pidana. Kedua peraturan penting di bidang hukum pidana ini berlaku efektif serentak sejak 2 Januari 2026.

KUHP baru memperluas cakupan kriminalisasi, termasuk ke dalam ranah yang berkaitan dengan moralitas, perilaku privat seperti kohabitasi, serta aktivitas di ruang digital. Selain itu, KUHP baru juga meluaskan seluruh tindak pidana yang memiliki unsur "dimuka umum" menjadi termasuk melalui media elektronik. Perluasan ini secara langsung meningkatkan jenis dan volume data pribadi yang diproses oleh aparat penegak hukum, termasuk data yang bersifat

6 UU No. 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana (KUHP) berlaku efektif sejak 2 Januari 2026.

7 UU No. 20 Tahun 2025 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP) berlaku efektif sejak 2 Januari 2026.

sensitif, seperti relasi personal, aktivitas komunikasi, dan ekspresi individu di ruang digital.

Di sisi lain, pembaruan KUHAP memberikan dasar hukum yang lebih eksplisit terhadap penggunaan teknologi dalam proses pembuktian. Pengaturan mengenai alat bukti elektronik, penggeledahan digital, serta teknik pengawasan (*surveillance*) memperkuat legitimasi penggunaan data digital dalam proses peradilan pidana. KUHAP baru juga memberikan perluasan terhadap cara penyelidikan yang dapat menjadi apa saja dengan klausul "kegiatan lain yang tidak bertentangan dengan ketentuan peraturan perundang-undangan". Konsekuensinya, praktik penegakan hukum berpotensi melanggar hak atas privasi termasuk data dan informasi, serta tidak lagi hanya bergantung pada alat bukti konvensional, tetapi semakin bertumpu pada pengolahan data elektronik dalam berbagai bentuk.

Perkembangan ini membawa sejumlah implikasi struktural. Pertama, digital forensik menjadi komponen sentral dalam proses pembuktian, yang memerlukan pengumpulan, ekstraksi, dan analisis data dari perangkat elektronik. Kedua, aparat penegak hukum secara rutin memproses metadata dan konten komunikasi, yang dalam banyak kasus mengandung informasi yang sangat detail mengenai perilaku dan relasi individu. Ketiga, terdapat potensi penggunaan alat analitik berbasis teknologi, baik dalam bentuk sistem semi-otomatis maupun otomatis, untuk membantu analisis data dalam proses penegakan hukum.[8]

Meskipun Indonesia belum secara luas mengadopsi penggunaan alat-alat tersebut, arah reformasi digital dalam sistem peradilan pidana menunjukkan potensi ke depan untuk mengintegrasikan pendekatan berbasis data, termasuk *predictive analytics*. Dalam konteks ini, ketentuan dalam UU PDP menjadi sangat relevan, khususnya terkait dengan pemrosesan data secara otomatis dan kewajiban untuk melakukan penilaian dampak pelindungan data

8 Dalam konteks global, perkembangan ini telah memunculkan perdebatan mengenai penggunaan alat analitik dan algoritma dalam sistem peradilan pidana, khususnya terkait dengan profiling dan pengambilan keputusan berbasis otomatis. Penggunaan alat seperti risk assessment tools dapat menimbulkan persoalan serius terkait bias, transparansi, dan akuntabilitas, terutama ketika digunakan untuk mempengaruhi keputusan hukum.

(*data protection impact assessment*). Ketentuan ini memberikan kerangka pengaman awal untuk memastikan bahwa penggunaan teknologi tidak mengarah pada praktik pengambilan keputusan yang tidak transparan atau diskriminatif.

Dengan demikian, pembaruan KUHP dan KUHAP tidak hanya memperluas kewenangan penegakan hukum, tetapi juga secara simultan memperbesar eksposur terhadap risiko pelanggaran data pribadi. Hal ini menegaskan bahwa penguatan pelindungan data pribadi harus berjalan seiring dengan reformasi hukum pidana dan digitalisasi sistem peradilan, agar perluasan kewenangan tidak berujung pada pelemahan pelindungan hak individu.

4

Pelindungan Data Pribadi pada Lembaga Pelaksana Peradilan Pidana

URAIAN MENGENAI TAHAPAN sistem peradilan pidana di atas menunjukkan bahwa pengelolaan data pribadi berlangsung secara berkelanjutan dan lintas institusi, dengan karakteristik risiko yang berbeda pada setiap tahap. Namun, analisis pada tingkat sistem belum cukup untuk menangkap kompleksitas praktik yang terjadi di lapangan. Oleh karena itu, bagian berikut ini akan menguraikan secara lebih mendalam praktik pengelolaan dan pelindungan data pribadi pada masing-masing lembaga penegak hukum, guna mengidentifikasi secara lebih spesifik bentuk-bentuk risiko, tantangan implementasi, serta kesenjangan antara kerangka normatif dan praktik institusional.

4.1. Kepolisian

a. Fungsi dan kewenangan

Kepolisian Negara Republik Indonesia/ Kepolisian merupakan pintu terdepan dalam penegakan hukum pidana di Indonesia. Sebagaimana diatur pada Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Kepolisian dibekali dengan 2 (dua) fungsi utama yakni sebagai penyelidik[1] dan penyidik[2].

Kedua fungsi Kepolisian tersebut masing-masing memiliki tujuan yang berbeda. Penyidikan diartikan sebagai tindakan untuk

1 KUHAP, Pasal 1 angka (7)
2 *Ibid.*, Pasal 1 angka (1)

mencari dan mengumpulkan alat bukti serta menemukan tersangka.[3] Sementara penyelidikan sendiri merupakan serangkaian tindakan untuk mencari dan menemukan peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan.[4] Oleh karenanya dalam pengertian yang sederhana, pada tahap penyidikan telah ditemukan adanya unsur-unsur pidana dalam suatu peristiwa, sedangkan penyelidikan merupakan tahap untuk mencari tahu ada atau tidaknya unsur-unsur pidana itu.

Dalam menjalankan fungsinya tersebut, Kepolisian berdasarkan KUHAP pun dibekali sejumlah kewenangan. Pada tahap penyelidikan, kewenangan Kepolisian antara lain;[5] a) menerima laporan atau pengaduan mengenai adanya tindak pidana baik secara tertulis maupun melalui media telekomunikasi dan/atau media elektronik; b) mencari, mengumpulkan dan mengamankan keterangan dan barang bukti; c) menyuruh berhenti seseorang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri; d) melakukan asesmen dan mengupayakan fasilitas dan/ atau rujukan bagi kebutuhan khusus perempuan dan kelompok rentan; e) mengadakan tindakan lainnya menurut hukum yang bertanggung jawab. Kendati dalam tahap penyelidikan seharusnya tidak diperkenankan dilakukannya serangkaian Upaya Paksa, akan tetapi atas perintah penyidik, penyelidik dapat melakukan;[6] a) penangkapan, larangan meninggalkan tempat, penggeledahan, dan penahanan; b) pemeriksaan dan penyitaan surat; c) mengambil sidik jari, melakukan identifikasi, memotret seseorang, dan mengambil data forensik seseorang; d) membawa dan menghadapkan seseorang pada penyidik.

Di tahap penyidikan, Kepolisian dibekali kewenangan untuk melakukan berbagai tindakan seperti;[7] a) menerima laporan atau pengaduan dari seseorang mengenai adanya tindak pidana; b) mencari dan mengumpulkan serta mengamankan alat bukti; c) melakukan tindakan pertama di tempat kejadian; d) menyuruh berhenti seseorang dan memeriksa surat atau tanda pengenal diri;

3 *Ibid.*, Pasal 1 angka (5)
4 *Ibid.*, Pasal 1 angka (8)
5 *Ibid.*, Pasal 5 ayat (1)
6 *Ibid.*, Pasal 5 ayat (2)
7 *Ibid.*, Pasal 7 ayat (1)

e) mencari orang yang diduga melakukan tindak pidana untuk menetapkan tersangka; f) melakukan upaya paksa; g) mengambil sidik jari, identifikasi, memotret seseorang dan mengambil dan mengambil data forensik seseorang; h) mendatangi orang yang berhubungan dengan tindak pidana untuk diperiksa dan didengar keterangannya; i) memanggil orang untuk diperiksa dan didengar keterangannya sebagai saksi, ahli atau tersangka; j) melakukan penghentian penyidikan dengan memberitahukan kepada Penuntut Umum; k) melakukan penyelesaian perkara melalui keadilan restoratif; l) menetapkan tersangka sebagai saksi mahkota; m) menerima pengakuan bersalah; n) melakukan asesmen dan mengupayakan fasilitas dan/atau rujukan bagi kebutuhan khusus perempuan dan kelompok rentan; o) melakukan tindakan lain sesuai dengan ketentuan peraturan perundang-undangan.

Selain berperan dan memiliki kewenangan untuk melakukan sendiri tahap penyidikan, penyidik Polri juga berperan sebagai koordinator dan pengawas dari Penyidik Pegawai Negeri Sipil (PPNS) dan Penyidik Tertentu. Posisi ini membuat penyidik Polri memiliki wewenang untuk mengakses berkas perkara yang sedang disidik oleh PPNS. PPNS sendiri merupakan pejabat negeri sipil yang diberi kewenangan untuk melakukan penyidikan berdasarkan undang-undang khusus. Misalnya PPNS Bea Cukai berdasarkan UU No. 10 Tahun 1995 tentang Bea Cuka, yang memberi kewenangan untuk melakukan penyidikan atas impor ilegal, pemalsuan cukai dan penyelundupan. Lalu, juga terdapat PPNS Kehutanan berdasarkan UU No. 18 Tahun 2013 tentang Kehutanan, memberikan kewenangan penyidikan atas penebangan liar (*illegal logging)*, penggunaan kawasan hutan secara tidak sah dan perdagangan satwa yang dilindungi. Sementara Penyidik tertentu merupakan pejabat suatu lembaga yang diberi kewenangan untuk melakukan penyidikan berdasarkan undang-undang tertentu. Seperti halnya penyidik tertentu Badan Narkotika Nasional berdasarkan UU No. 35 Tahun 2009 tentang Narkotika. Dalam hal ini setiap PPNS dan Penyidik tertentu kecuali yang dikecualikan berdasarkan KUHAP yakni kejaksaan, KPK, TNI AL, wajib berkoordinasi dengan Penyidik Polri sampai dengan penyerahan berkas perkara kepada Penuntut Umum.

Kepolisian baik dalam melaksanakan fungsinya sebagai penyelidik dan penyidik, memiliki kewenangan yang berkaitan dengan data pribadi. Pertama, baik dalam tahap penyelidikan maupun penyidikan mengumpulkan identitas tersangka yang sudah dituangkan dalam Surat Pemberitahuan Dimulainya Penyidikan (SPDP).[8] Kedua, berdasarkan KUHAP penyidik dan penyelidik atas perintah penyidik juga dapat mengambil beberapa data krusial lainnya seperti sidik jari, identifikasi, memotret seseorang hingga mengambil data forensik seseorang.

b. Jenis dan proses pengumpulan data

Secara umum, Kepolisian Republik Indonesia belum memiliki aturan internal yang spesifik mengatur terkait dengan pelindungan data pribadi. Kendati demikian, ditemukan beberapa peraturan internal kepolisian yang berkaitan dengan pengelolaan data secara umum maupun dalam konteks sistem peradilan pidana , antara lain yaitu:

1) Peraturan Kepolisian Negara Republik Indonesia Nomor 4 Tahun 2022 tentang Satu Data Kepolisian Negara Republik Indonesia, yang mengatur tata kelola data kepolisian secara umum.
2) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 1 Tahun 2024 tentang Penyelenggaraan Pusat Informasi Kriminal Nasional, yang mengatur terkait tata kelola sistem informasi kriminal.
3) Peraturan Kepala Badan Reserse Kriminal Polri No. 1 Tahun 2022 tentang Standar Operasional Prosedur Pelaksanaan Penyidikan Tindak Pidana, yang mengatur terkait prosedur melaksanakan penyidikan, salah satunya pencatatan proses penyidikan baik secara manual dan/ atau melalui aplikasi berbasis website (e-mp) sebagai database perkara pidana oleh penyidik atau penyidik pembantu.

8 Peraturan Kepala Kepolisian Negara Republik Indonesia (Perkap) No. 6 Tahun 2019 tentang Penyidikan Tindak Pidana, Pasal 14 ayat (2) huruf (d)

Peraturan Kapolri No. 1 Tahun 2024 tentang Penyelenggaraan Pusat Informasi Kriminal Nasional membagi beberapa jenis data kriminal yang terkait dengan penegakan hukum pidana. Seperti halnya data mengenai laporan polisi, penyelidikan, penyidikan hingga penyelesaian perkara yang termasuk dalam kategori data kejahatan dan pelanggaran yang direkam dalam pangkalan data melalui sistem informasi yang terintegrasi.[9] Berkaitan dengan data profil pelaku kejahatan dan pelanggaran, setidaknya memuat beberapa hal;[10] a) nama lengkap; b) foto pelaku; c) nomor induk kependudukan; d) tempat dan tanggal lahir; e) pekerjaan; f) pendidikan; g) suku; h) alamat; i) nomor surat izin mengemudi; j) nomor pokok wajib pajak; k) nomor paspor; l) data perlintasan; m) data cegah dan tangkal; n) data kartu izin tinggal tetap; o) data kartu izin tinggal sementara; p) data sidik jari; q) data biometrik wajah; r) data Interpol notice; dan/ atau s) data DNA.

Proses pengumpulan data kriminal tersebut setidaknya dilakukan melalui 4 tahapan, yakni;[11] a) pengumpulan; b) pengolahan; c) pengamanan; d) penyajian informasi kriminal. Pertama, pengumpulan data yang dimaksud dilakukan dalam bentuk digital atau dokumen fisik. Tahapan ini dilakukan melalui integrasi sistem informasi yang dimiliki oleh satuan kerja di lingkungan Polri dan kerja sama dengan kementerian/ lembaga. Kedua, tahap pengolahan data diselenggarakan dengan setidaknya menetapkan standarisasi data, melakukan pengelompokan data, kodifikasi data, verifikasi data dan melakukan validasi data, dengan monitoring dari pejabat yang ditunjuk oleh Kepala Pusat Informasi Kriminal Nasional Bareskrim Polri. Ketiga, ruang lingkup pengaman data, tidak terbatas pada aplikasi dan data, tetapi juga sistem jaringan, pengamanan akses data dan informasi, enkripsi penyimpanan dan transmisi data, pencadangan data dan aplikasi hingga pengamanan pengguna akhir. Tahap terakhir yakni penyajian data salah satunya yakni catatan kriminal yang meliputi identitas dari tersangka, jenis tindak pidana,

9 Peraturan Kepala Kepolisian Negara Republik Indonesia (Perkap) No. 1 Tahun 2024 tentang Penyelenggaraan Pusat Informasi kriminal Nasional, Pasal 4 ayat (3).
10 *Ibid.*, Pasal 5 ayat (4).
11 *Ibid.*, Pasal 9 ayat (1)

pasal yang dilanggar, tempat hingga waktu kejadian hingga barang yang dibutuhkan dalam penanganan tindak pidana.

Tak hanya itu, Standar Operasional Prosedur dalam melaksanakan penyidikan sendiri, juga mengatur mengenai adanya administrasi penyidikan tindak pidana atau pencatatan proses penyidikan baik secara manual dan/ atau melalui aplikasi.[12] Aplikasi yang dimaksud disini yakni aplikasi berbasis website (e-mp) yang digunakan sebagai sarana pengendalian dan database perkara pidana oleh penyidik atau penyidik pembantu dalam sistem manajemen penyidikan. Secara substansi, administrasi penyidikan tindak pidana ini meliputi isi berkas perkara; dan yang bukan merupakan isi berkas perkara.[13]

c. Tantangan dan risiko

Setidaknya terdapat beberapa tantangan dan risiko *over collection* hingga kebocoran data, yang dihadapi atas kewenangan Kepolisian untuk mengumpulkan dan memproses data, yakni:

1) Proses pengumpulan dan penyimpanan data termasuk data-data pada tahap penyidikan dilakukan secara *hybrid*, yakni manual dan/ atau melalui aplikasi. Tantangannya adalah Peraturan Kepala Badan Reserse Kriminal Polri No. 1 Tahun 2022 tentang Standar Operasional Prosedur Pelaksanaan Penyidikan Tindak Pidana, tidak mengatur secara rinci mengenai teknis penyimpanan dan pencatatan data penyidikan melalui 2 cara ini. Apakah inventarisasi dan pemrosesan dilakukan secara bersama-sama atau tidak, mekanisme pembaharuan hingga retensi dan pemusnahan yang jelas. Terlebih jika merujuk pada Peraturan Polisi No. 4 Tahun 2022 tentang Satu Data Kepolisian, juga mengatur mengatur bahwa penyimpanan data dilakukan dengan menggunakan media penyimpanan elektronik dan/ atau cetak, tanpa mengatur secara spesifik mengenai teknis penyimpanan berkas fisik maupun digital;

12 Peraturan Kepala Badan Reserse Kriminal Polri No. 1 Tahun 2022 tentang Standar Operasional Prosedur Pelaksanaan Penyidikan Tindak Pidana, Pasal 1 angka (23).

13 *Ibid.*, Pasal 4 ayat (1).

2) Berdasarkan Peraturan Kepala Kepolisian Negara Republik Indonesia No. 1 Tahun 2024 tentang Penyelenggaraan Pusat Informasi Kriminal Nasional (Perkap No. 1/2024) dan Peraturan Polisi No. 4 Tahun 2022 tentang Satu Data Kepolisian diperbolehkan adanya kerjasama dalam hal integrasi sistem informasi hingga pertukaran data baik dengan Kementerian/ lembaga, perguruan tinggi, maupun pihak lainnya. Sementara itu, Perkap 1/ 2024 secara spesifik juga menyebutkan bahwa kerjasama dapat dilakukan dengan Kementerian/ Lembaga yang menyelenggarakan tugas, fungsi dan kewenangan terkait pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum dan pelindungan, pengayoman dan pelayanan masyarakat sesuai dengan ketentuan peraturan perundang-undangan. Permasalahannya yakni kedua peraturan internal kepolisian tidak mengatur lebih jauh mengenai mekanisme atau standar operasional dalam melakukan transfer data, jenis data, hingga pengawasan terhadap proses transfer data itu.

Sementara itu, Kepolisian khususnya Polda Metro Jaya diduga pernah mengalami kebocoran terhadap 341.000 data pribadi dari personel Polri pada 2025. Kebocoran data itu berisikan identitas anggota Polri seperti nama, pangkat, satuan tugas, hingga kontak pribadi yang tersebar pada laman pribadi milik *hacker* Bjorka. Maka dari itu, peristiwa ini seharusnya menjadi alarm penting bagi Kepolisian untuk dapat membenahi sistem pengamanan terlebih yang berkaitan dengan data pribadi khususnya yang menyangkut informasi mengenai penegakan hukum pidana.

d. Dampak terhadap kelompok rentan

Berdasarkan UU No. 20 Tahun 2025, baik Penyidik dan Penyelidik berdasarkan izin dari Penyidik memiliki kewenangan dalam melakukan tindakan upaya paksa, termasuk mengambil sidik jari, melakukan identifikasi, memotret, dan mengambil data forensik seseorang.[14] Tak hanya itu, Penyidik juga diberikan kewenangan

14 KUHAP, Pasal 5 ayat (2) huruf (c) dan Pasal 7 ayat (1) huruf dan (g)

untuk mengakses rekaman kamera pengawas yang berisikan rekaman proses pemeriksaan terhadap tersangka.[15] Berdasarkan hal ini menggambarkan luasnya kewenangan yang dimiliki oleh Kepolisian dalam mengumpulkan dan memproses data dalam sistem peradilan pidana.

Sementara itu, dalam konteks perkara kekerasan berbasis gender (KBG) dan perkara lainnya yang melibatkan kelompok rentan, kewenangan kepolisian tersebut sangat beririsan langsung dengan kebutuhan akan pelindungan data pribadi korban yang bersifat sangat sensitif. Pada tahap awal pelaporan saja, korban diminta korban diminta memberikan berbagai informasi sangat detail terkait dengan peristiwa yang menimpanya. Akan tetapi, minimnya penjelasan mengenai tujuan penggunaan data dan *informed consent* sangat dimungkinkan terjadinya pengumpulan data berlebihan (*over collection*). Kerentanan data-data korban tidak berhenti pada tahap penyidikan saja, melainkan terus berlanjut ketika perkara dilimpahkan ke kejaksaan dan pengadilan. Dalam tahap ini, dokumen seperti Berita Acara Pemeriksaan (BAP) dan rekaman pemeriksaan menjadi bagian integral dari berkas perkara yang dilimpahkan kepada pihak lainnya dalam sistem peradilan pidana.

BAP dan rekaman tersebut umumnya memuat informasi yang sangat sensitif, termasuk identitas korban, anggota keluarga, dan detail kronologi serta pengalaman traumatis yang dialami korban, khususnya dalam kasus KBG. Proses pelimpahan dokumen-dokumen ini yang dapat diakses oleh jaksa, penasehat hukum, hakim, serta pihak lainnya seperti panitera, tentu saja akan meningkatkan risiko kebocoran dan penyalahgunaan data. Terlebih apabila dalam pelimpahan dokumen tersebut dilakukan tanpa anonimisasi korban. Korban tidak hanya kehilangan kontrol atas data pribadinya, tetapi juga harus menghadapi konsekuensi sosial seperti stigmatisasi hingga viktimisasi.

e. Kepatuhan terhadap UU PDP

Kendati telah terdapat pengaturan terkait pengumpulan dan pemrosesan hingga pengamanan data, akan tetapi baik KUHAP

15 *Ibid.*, Pasal 30

maupun pengaturan internal kepolisian belum dapat dikatakan sejalan dengan prinsip-prinsip utama Pelindungan Data Pribadi sebagaimana diatur dalam UU PDP. Bahkan baik pada beberapa pengaturan internal Kepolisian yang berkaitan erat dengan teknis pengumpulan, pemrosesan dan pengamanan data tidak ditemukan adanya klausa data pribadi dalam pengaturan pasalnya. Ada empat hal yang menjadi catatan utama atas kepatuhan Kepolisian terhadap UU PDP.

Pertama, selain tidak ada kebijakan atau SOP internal yang mengatur spesifik terkait Pelindungan Data Pribadi, dalam susunan organisasi Bareskrim Polri berdasarkan Perkap Nomor 4 Tahun 2025 tentang Perubahan Keenam atas Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2017 tentang Susunan Organisasi dan Tata Kerja Satuan Organisasi Pada Tingkat Markas Besar Kepolisian Negara Republik Indonesia pun tidak ditemukan adanya Pejabat Pelindungan Data Pribadi (DPO). Akan tetapi terdapat beberapa fungsi tertentu yang diberikan kewenangan dan tugas untuk melakukan pengolahan data. Berdasarkan Perpol 4/2022 tentang Satu Data Kepolisian Negara Republik Indonesia mengatur tiga pihak dalam pengolahan satu data Polri yakni ; 1) Pengarah Data yang diisi oleh Kapolri dan dibantu oleh tim Ahli bidang TIK melalui Keputusan Kapolri; 2) Walidata satuan kerja yang melaksanakan kegiatan pengumpulan dan pemeriksaan serta menyebarluaskan data; 3) Produsen Data yakni satker yang menghasilkan data berdasarkan kewenangannya dalam UU.

Kedua, meskipun Kepolisian memiliki daftar jenis data yang dikategorikan tidak berdasarkan UU PDP, akan tetapi didasarkan pada kategori; 1) data kejahatan (termasuk penyelidikan, penyidikan, penyelesaian perkara); 2) data lalu lintas; 3) data gangguan Kamtibmas. 4) data profil pelaku kejahatan (nama, foto, NIK, tempat, tanggal lahir, pekerjaan, alamat, sidik jari, biometrik wajah, DNA, dll), dan 5) data barang bukti). Sementara, berdasarkan kategori itu ditemukan beberapa jenis data yang termasuk dalam data spesifik dalam UU PDP. Seperti halnya data spesifik data pelaku kejahatan dan pelaku pelanggaran dalam kategori data kejahatan dan pelanggaran yakni antara lain data penyelidikan, penyidikan, penyelesaian perkara, data pelaku kejahatan serta pelanggaran. Adapun data

spesifik yang masuk dalam kategori profil kejahatan dan pelanggaran yakni data biometrik wajah dan data DNA.

Ketiga, inventarisasi data kejahatan dan pelanggaran yang dikumpulkan dan diolah termasuk data mengenai Laporan Polisi/ Kejadian, Penyelidikan, Penyidikan hingga penyelesaian perkara. Khusus terhadap proses pencatatan pada tahap penyidikan, dilakukan secara manual maupun aplikasi berbasis website yang disebut e-mp, sebagai sistem manajemen penyidikan. Akan tetapi, tidak jelas bagaimana mekanisme pengumpulan, pengamanan, masa retensi hingga pemusnahan data-data tersebut.

Keempat, pengaturan internal Kepolisian yang berkaitan dengan data belum mencakup hal-hal krusial berkaitan dengan penanganan insiden, seperti kebocoran data. Ketiadaan pengaturan mekanisme ini membuat sistem pengolahan data yang setidaknya sudah ada pada internal Polri menjadi rentan terhadap serangan hacker maupun cyber lainnya.

4.2. Kejaksaan

a. Fungsi dan kewenangan

Kejaksaan memiliki peran dalam bidang pidana, perdata dan tata usaha negara. Dalam bidang perdata dan tata usaha negara sesuai Pasal 30 ayat (2) UU Kejaksaan, kejaksaan dengan kuasa khusus dapat bertindak di dalam maupun di luar pengadilan untuk dan atas nama negara atau Pemerintah jika terjadi gugatan perdata terkait kebocoran data pada sistem milik pemerintah. Hal ini diatur lebih lanjut dalam Peraturan Jaksa Agung No. PER-025/A/JA/11/2015 tentang Petunjuk Pelaksanaan Penegakan Hukum, Bantuan Hukum, Pertimbangan Hukum, Tindakan Hukum Lain dan Pelayanan Hukum Di Bidang Perdata dan Tata Usaha Negara. Sesuai dengan Peraturan Kejaksaan ini, Kejaksaan dapat memberikan pertimbangan hukum dan pendampingan bagi instansi Pemerintah yang mengelola data publik agar sesuai dengan regulasi serta bertindak di dalam maupun di luar pengadilan untuk dan atas nama negara atau Pemerintah di bidang perdata dan tata usaha negara.

Kejaksaan juga memiliki wewenang dalam bidang intelijen penegakan hukum yaitu melaksanakan pengawasan multimedia sebagaimana diatur dalam Pasal 30B huruf e. Peran Kejaksaan dalam sistem acara pidana tergambar dalam Pasal 65 UU 20/2025. Ketentuan ini mengatur bahwa Penuntut Umum mempunyai wewenang berikut; Pertama adalah pra penuntutan yaitu menerima dan memeriksa berkas perkara Penyidikan dari Penyidik serta melakukan koordinasi antara Penyidik dan Penuntut Umum untuk kepentingan melengkapi hasil Penyidikan. Wewenang ini artinya Penuntut akan memiliki data setidaknya tentang identitas dan nomor alat komunikasi.

Kedua wewenang dalam masa penuntutan. Wewenang secara garis besar dalam bidang penuntutan sendiri terdiri dari 1) membuat dan melimpahkan surat dakwaan, 2) tidak melanjutkan Penuntutan 3) menerima pengakuan bersalah, 4) membuat perjanjian penundaan penuntutan, 4) melakukan penyelesaian perkara melalui mekanisme Keadilan Restoratif dan 5) menutup perkara demi kepentingan hukum.

Terkait wewenang penuntutan tersebut Penuntut Umum memiliki banyak wewenang. Salah satunya memberikan wewenang kepada Penuntut Umum untuk mengakses rekaman kamera pengawas yang memuat rekaman pemeriksaan terhadap tersangka (Pasal 30 UU 20/2025). Selain hal tersebut, wewenang penuntut yang bersifat teknis dalam tahapan ini adalah a) memberikan perpanjangan Penahanan, melakukan Penahanan atau Penahanan lanjutan, dan/atau mengubah status tahanan setelah perkaranya dilimpahkan oleh Penyidik; b) menyampaikan pemberitahuan kepada Terdakwa mengenai surat panggilan sidang kepada Terdakwa dan Saksi; c) menerima pengakuan bersalah. Wewenang ketiga Jaksa adalah melakukan eksekusi putusan yaitu melaksanakan penetapan dan/atau putusan Hakim pengadilan negeri, Hakim pengadilan tinggi, atau Hakim Mahkamah Agung.

Pengelolaan data, statistik kriminal serta penerapan dan pengembangan teknologi informasi di Kejaksaan merupakan tugas Pusat Data Statistik Kriminal dan Teknologi Informasi (Pusdakrimti) berdasarkan Pasal 714 Peraturan Kejaksaan Nomor 3 Tahun 2024 tentang Perubahan Keempat Atas Peraturan Jaksa Agung Nomor Per-006/A/Ja/07/2017 tentang Organisasi dan Tata Kerja.

Berdasarkan tugas tersebut, fungsi Pusdakrimti menurut Pasal 715 Peraturan Kejaksaan Nomor 3 Tahun 2024 adalah menyusun kebijakan teknis, rencana, program dan strategi, pelaksanaan pengelolaan, penerapan dan pengembangan dan pemantauan dan evaluasi pelaksanaan pengelolaan data, statistik kriminal serta penerapan dan pengembangan teknologi informasi.

Koordinasi lintas lembaga oleh Kejaksaan terdiri dari dua hal yaitu dalam hal peradilan pidana serta keamanan dan ketertiban. Koordinasi dalam peradilan pidana terdiri dari penuntutan tindak pidana yang masuk dalam peradilan umum dan peradilan militer. Koordinasi dalam hal peradilan umum dilakukan dengan penyidik serta oditurat untuk perkara koneksitas. Khusus peradilan militer, penyelenggaraan koordinasi teknis penuntutan dilakukan dengan oditurat.

Adapun koordinasi lintas lembaga dalam bidang ketertiban umum terkait dengan fungsi intelijen adalah Tim Koordinasi Pengawasan Aliran Kepercayaan dan Aliran Keagamaan dalam Masyarakat yang diatur melalui Peraturan Kejaksaan Nomor 5 Tahun 2019 tentang Perubahan Atas Peraturan Jaksa Agung Nomor Per-019/A/Ja/09/2015. Kementerian dan badan yang terlibat adalah Kementerian Dalam Negeri, Kementerian Agama, Kementerian Pendidikan dan Kebudayaan, Markas Besar Tentara Nasional Indonesia, Markas Besar Kepolisian Negara Republik Indonesia, Badan Intelijen Negara dan Perwakilan Forum Kerukunan Umat Beragama.

b. Jenis dan proses pengelolaan data

Wewenang penuntutan memberikan wewenang kepada Kejaksaan untuk memiliki berbagai dokumen dan data milik pelapor/korban maupun terlapor/tersangka dan terdakwa. Pasal 235 (1) f UU 20/2005 tentang Kitab UU Hukum Acara Pidana (KUHAP) mengatur alat bukti juga terdiri atas: bukti elektronik. Selanjutnya Pasal 242 mengatur bukti elektronik tersebut mencakup segala bentuk informasi elektronik, dokumen elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana. Bukti elektronik tersebut termasuk yang akan dilimpahkan ke pengadilan dalam proses penuntutan. Terkait putusan, berdasarkan Pasal 342 KUHAP, salinan putusan

akan dikirim panitera kepada Penuntut Umum baik secara elektronik maupun secara langsung.

Data identitas diri hanyalah salah satu informasi terkait korban yang dimiliki Kejaksaan sebagai penuntut umum. Informasi lain yang akan dimiliki oleh Penuntut umum antara lain peristiwa yang dialami korban, kerugian, tanda tangan, nomor rekening dan informasi di dalam rekeningnya untuk perkara yang melibatkan uang. Terkait perkara siber, Kejaksaan mengumpulkan bukti digital sesuai dengan jenis perkaranya. Berdasarkan hasil wawancara dalam penanganan perkara siber, jenis perkara yang banyak ditangani antara lain kasus judi online yaitu menggunakan identitas (KTP) orang lain untuk dijadikan anggota dalam situs judi *online*.[16] Selain dalam penanganan perkara tindak pidana ekonomi jaksa juga mengumpulkan dan memiliki data transfer rekening. Data penanganan perkara dikelola melalui berbagai sistem teknologi informasi yaitu SIPEDE, CMS, PUSDASKRIMTI, dan Data Intelijen untuk bidang Intelijen.

Sebagai organisasi, Kejaksaan juga memiliki data pribadi pegawai. Jenis data pegawai adalah kartu BPJS (Badan Penyelenggaran Jaminan Sosial), KTP (Kartu Tanda Penduduk) dengan muatan data pribadi, Foto, NPWP (Nomer Pokok Wajib Pajak), serta nomor rekening Perbankan. Data kepegawaian menggunakan sistem bernama SIMKARI. Data yang dapat dibagikan kepada pihak lain ada pada Pusdakrimti. Data tersebut adalah nomor rekening, foto wajah, KTP, NPWP dan curriculum vitae (Isian ROPA Kejaksaan).

Kejaksaan memiliki sistem data penanganan perkara yang disebut Case Management System (CMS), yang terdiri dari CMS publik dan privat. CMS publik menyediakan informasi seputar berapa banyak surat pemberitahuan dimulainya penyidikan (SPDP), apa saja perkara yang masuk dll. Adapun CMS privat antara lain berisi informasi sudah sampai manakah proses penanganan perkara (keterangan Kejaksaan, FGD). Selain Kejaksaan juga memiliki mekanisme pemusnahan data untuk perkara yang sudah in kracht. Barang bukti akan dimusnahkan setelah perkara selesai dan dilakukan di pengadilan, dalam beberapa

16 Hal ini disampaikan oleh perwakilan kejaksaan dalam *Focus Group Discussion* (FGD) pada tanggal 23 Januari 2026.

perkara proses pemusnahan barang bukti dilakukan dengan mengundang Muspida untuk menyaksikannya.[17]

Selain data penanganan perkara, Kejaksaan juga mengumpulkan data intelijen yustisial dengan tujuan mendukung penegakan hukum. Meski demikian, terdapat kecenderungan bahawa data intelijen yang dikumpulkan oleh Kejaksaan juga beragam dan memiliki potensi eksesif. Pada tahun 2025, Kejaksaan Agung membuat Mou atau nota kesepahaman dengan PT Telekomunikasi Indonesia Tbk, PT Telekomunikasi Selular, PT Indosat Tbk, dan PT Xl Smart Telecom Sejahtera Tbk dalam rangka penguatan pertukaran dan pemanfaatan informasi untuk kebutuhan intelijen.[18] Jaksa Agung Muda Intelijen dalam rilis Kejaksaan Agung menyampaikan bahwa "data atau informasi dengan kualifikasi A1 tersebut tentunya memiliki berbagai manfaat, diantaranya dalam tataran praktis seperti pencarian buronan atau daftar pencarian orang, pengumpulan data dalam rangka mendukung penegakan hukum"[19] MoU ini menuai kritik dari Koalisi Masyarakat Sipil yang terdiri atas Raksha Initiatives, Dejure, Centra Initiative, Imparsial, HRWG, ELSAM, ICJR karena kerja sama ini dinilai dapat mengancam hak privasi warga negara.[20]

c. Tantangan dan risiko

Saat ini belum ada lembaga pengawas independen yang mengawasi arus perpindahan data khususnya dalam sistem peradilan pidana. Sementara itu dalam praktik, terdapat tantangan koordinasi antar penegak hukum, serta belum komprehensifnya ketentuan yang mengatur alur informasi dan keamanan data anak. Sebagai contoh, rekaman sidang elektronik bisa saja tersimpan dalam sistem kejaksaan tanpa pelindungan metadata yang baik atau dipertukarkan melalui email yang tidak terenkripsi kepada panitera pengadilan.[21]

17 Keterangan Kejaksaan dalam FGD pada 23 Januari 2026, Loc. Cit.

18 Shela Octavia dan Danu Damarjati, "MoU Penyadapan dengan 4 Provider Disoal, Kejagung Jamin Tak Sembarangan",https://nasional.kompas.com/read/2025/06/26/20514751/mou-penyadapan-dengan-4-provider-disoal-kejagung-jamin-tak-sembarangan.

19 Tempo.co, Kejaksaan Agung Teken MoU Soal Penyadapan dengan Empat Operator Telekomunikasi, 2025. Kejaksaan Agung Teken MoU Soal Penyadapan dengan Empat Operator Telekomunikasi | tempo.co).

20 *Ibid.*

21 Saut Erwin Hartono A. Munthe, *Rekonstruksi Regulasi Perlindungan Hukum terhadap Kerahasiaan Keterangan Anak yang Berkonflik dengan Hukum Secara Elektronik*

Kejaksaan juga pernah mengalami pembobolan data pada tahun 2021. Pelakunya, MWF yang berusia 16 tahun, membobol sejumlah data Kejaksaan RI dan menjualnya lewat forum online. Setidaknya, ada 3.086.224 data yang dibobol dan diperjualbelikan dengan harga sekitar Rp400.000.[22]

d. Dampak terhadap kelompok rentan

Dalam proses penuntutan, Kejaksaan memproses berbagai jenis data sensitif, termasuk identitas korban, saksi, anak, serta informasi terkait kondisi kesehatan, psikologis, dan kekerasan berbasis gender. Data tersebut umumnya tercantum dalam berkas perkara dan dokumen persidangan, namun belum selalu dikelola dengan prinsip *data minimisation* dan pembatasan akses yang memadai. Penuntut Umum juga memiliki wewenang untuk mengakses rekaman kamera pengawas yang memuat rekaman pemeriksaan terhadap tersangka (Pasal 30 UU 20/2025). Terkait tindak pidana kekerasan seksual, rekaman pemeriksaan ini akan menjadi hal sensitif terkait data pribadi korban dan keluarganya apalagi terdapat pelimpahan perkara dari penyidik ke kejaksaan dan pengadilan. Perekaman data elektronik ini sudah dilakukan di beberapa daerah khususnya kasus anak dan isi serta statusnya sama dengan BAP.[23] Kondisi ini menimbulkan risiko viktimisasi, khususnya bagi kelompok rentan, ketika identitas atau informasi sensitif masih dapat dikenali baik secara langsung maupun tidak langsung. Risiko tersebut semakin meningkat dalam konteks pertukaran data antar-lembaga, di mana Kejaksaan berperan sebagai titik sentral dalam alur data antara kepolisian, pengadilan, LPSK, dan pemasyarakatan.

Koordinasi lintas lembaga juga ada dalam bidang ketertiban umum terkait dengan fungsi intelijen penegakan hukum. Dasar hukum terakhir yang mengatur hal ini adalah Peraturan Kejaksaan No. 5 Tahun 2019 tentang Perubahan Atas Peraturan Jaksa Agung

Berbasis Nilai Keadilan, Disertasi, (Semarang: Universitas Islam Sultan Agung, 2025), hal. 187.

22 CNBC Indonesia, "Hacker 16 Tahun Bobol Database Kejagung, Motifnya Iseng!", 19 Februari 2021. https://www.cnbcindonesia.com/tech/20210219202546-37-224785/hacker-16-tahun-bobol-database-kejagung-motifnya-iseng .

23 Keterangan Kejaksaan dalam FGD pada 23 Januari 2026, *Loc. Cit.*

Nomor Per-019/A/Ja/09/2015 membentuk Tim Koordinasi Pengawasan Aliran Kepercayaan dan Aliran Keagamaan dalam Masyarakat dengan melibatkan 7 lembaga. Kementrian dan badan yang terlibat adalah Kementerian Dalam Negeri, Kementerian Agama, Kementerian Pendidikan dan Kebudayaan, Markas Besar Tentara Nasional Indonesia, Markas Besar Kepolisian Negara Republik Indonesia, Badan Intelijen Negara dan Perwakilan Forum Kerukunan Umat Beragama (FKUB).

Fungsi Tim tersebut, yang diatur dalam Pasal 3 Peraturan Jaksa Agung 019/2015 adalah mengawasi aliran kepercayaan dan aliran keagamaan dalam masyarakat terhadap ajaran atau faham aliran kepercayaan masyarakat/keagamaan yang meresahkan masyarakat karena diindikasikan menyimpang atau sesat dan/atau menodai, menghina atau merendahkan satu aliran kepercayaan masyarakat atau suatu agama, dapat menimbulkan rasa kebencian/permusuhan dalam Masyarakat serta dapat merusak/mengganggu kerukunan umat beragama.

Tugas tim Pakem yang diatur dalam Pasal 6 Peraturan Jaksa Agung No. 019/2015, yaitu a) menerima dan menganalisis laporan dan atau informasi tentang aliran kepercayaan masyarakat atau aliran keagamaan, b) meneliti dan menilai secara cermat perkembangan suatu aliran kepercayaan atau aliran keagamaan untuk mengetahui dampak-dampaknya bagi ketertiban dan ketentraman umum, c) mengajukan laporan dan saran sesuai dengan jenjang wewenang dan tanggung jawab.[24] Ketentuan tersebut menimbulkan kerentanan kepada kelompok minoritas keagamaan atau kepercayaan. Tim Pakem baik di Kejaksaan Agung maupun kejaksaan tinggi dan negeri memiliki data komunitas yang dikategori sebagai menyimpang. Data ini tidak hanya diketahui oleh Kejaksaan tapi tersebar ke 7 lembaga.

24 Pengawasan aliran kepercayaan bersumber dari UU No. 1/PNPS/1965 yang melarang penafsiran atau kegiatan keagamaan yang menyimpang (Pasal 1), dengan sanksi berupa peringatan hingga pembubaran organisasi dan pidana (Pasal 2–3). Ketentuan ini juga ditegaskan dalam Keputusan Bersama Menteri Agama, Jaksa Agung, dan Menteri Dalam Negeri No. 3 Tahun 2008, KEP-033/A/JA/6/2008, dan No. 199 Tahun 2008. Meskipun Pasal 4 UU tersebut telah dicabut melalui Pasal 622 KUHP (berlaku 2 Januari 2026), ketentuan lainnya tetap berlaku dan isu penodaan agama masih diatur dalam regulasi lain.

Penyebaran ini bahkan lebih dari 7 lembaga tersebut karena FKUB terdiri dari perwakilan agama-agama yang ada di suatu wilayah.

FKUB diatur dalam Peraturan Bersama Menteri Agama dan Menteri Dalam Negeri Nomor: 9 dan 8 tahun 2006 tentang Pedoman Pelaksanaan Tugas Kepala Daerah/Wakil Kepala Daerah Dalam Pemeliharaan Kerukunan Umat Beragama, Pemberdayaan Forum Kerukunan Umat Beragama, dan Pendirian Rumah Ibadat. Keanggotaan FKUB terdiri atas pemuka-pemuka agama setempat dengan jumlah paling banyak 21 orang di Provinsi dan kabupaten/kota paling banyak 17 orang. Komposisi keanggotaan FKUB tersebut ditetapkan berdasarkan perbandingan jumlah pemeluk agama setempat dengan keterwakilan minimal 1 (satu) orang dari setiap agama yang ada di propinsi dan kabupaten/kota.

Gambaran tentang informasi yang disebarkan oleh Tim Pakem dapat tergambar dalam kasus Jemaat Ahmadiyah Kuningan. Tim Pakem Kabupaten Kuningan mengeluarkan surat No.B-461/0.2.22/Dsp.5/12/2002 ditujukan kepada Kepala Kantor Departemen Agama Kabupaten Kuningan perihal pihak Kantor Depag Kabupaten Kuningan e.q KUA untuk menolak mencatat perkawinan terhadap penganut JAI cabang Manis Lor.[25] Akibatnya, terdapat lebih dari 150 pasangan yang tidak bisa dicatat pernikahannya di KUA Manis Lor.[26] Meskipun kejadian berlangsung sebelum adanya UU PDP, bukan tidak mungkin hal yang sama terulang.

e. Kepatuhan terhadap UU PDP

Pada saat ini Kejaksaan Agung belum menunjuk Pejabat Pelindungan Data Pribadi (DPO) meskipun telah melakukan pelatihan serta sertifikasi *data protection officer* yang diikuti oleh perwakilan dari Kejaksaan Tinggi seluruh daerah.[27] Belum ada pula peraturan internal yang khusus mengatur mengenai pelindungan data. Sementara ini

25 Uli Parulian Sihombing, dkk, *Menggugat Bakor Pakem Kajian Hukum Terhadap Pengawasan Agama dan Kepercayaan di Indonesia* (Jakarta: The Indonesian Legal Resource Center, Jakarta, 2008), hal. 39-40.

26 *Ibid.*

27 Kejaksaan.go.id, Tingkatkan pelindungan Data Pribadi, JAM DATUN Adakan Pelatihan dan Sertifikasi Data Protection Officer, https://www.kejaksaan.go.id/conference/news/1839/read

peraturan tersebut tersebar dalam Peraturan Jaksa Agung tentang Kode Prilaku Jaksa dan Tata Cara Pemeriksaan Atas Pelanggaran Kode Perilaku Jaksa, Peraturan Jaksa Agung No. 3/2020 tentang *whistle blowing system* dan Peraturan Jaksa Agung No. 5/2021 tentang Sistem Pengelolaan Data dan Informasi Intelijen. Kode Prilaku Jaksa mengatur profesionalitas yang salah satunya memastikan saksi, korban, tersangka, dan/atau terdakwa mendapatkan informasi dan jaminan atas haknya sesuai dengan ketentuan peraturan perundang-undangan dan hak asasi manusia (Pasal 8h). Oleh karenanya UU pelindungan Data Pribadi termasuk yang harus diikuti oleh Jaksa.

Pengaturan pelindungan data pribadi juga diatur untuk pegawai yang melaporkan adanya dugaan pelanggaran hukum oleh pegawai lain di Kejaksaan. Pelindungan terkait informasi diberikan dalam bentuk: merahasiakan dan menyamarkan identitas pelapor, pelindungan atas catatan yang merugikan dalam arsip data kepegawaian dan/ atau merahasiakan isi Laporan, laporan hasil telaah Unit Penanganan Pelaporan dan tindak lanjut bidang pengawasan.

Khusus untuk informasi intelijen, ketentuannya relatif lebih lengkap misalnya dengan adanya aturan mengenai retensi, yaitu jangka waktu pelindungan dan penyimpanan, untuk data intelijen dan informasi intelijen meskipun pengaturannya hanya menyatakan ditentukan sesuai perundang-undangan. Secara umum unsur kerahasiaan dilakukan melalui pemberian otorisasi, akses, dan/ atau izin secara terbatas bagi pejabat sesuai dengan tugas dan kewenangannya dalam pengelolaan data dan informasi serta kewajiban menjaga data dan informasi sesuai dengan sifat atau tingkat kerahasiaannya (Pasal 20 ayat 2). Pengaturan mencakup pula tata cara mengakses data terbatas dan data tertutup yang bersifat rahasia yaitu "hanya dapat diakses atau dibagipakaikan kepada pengguna Data Eksternal setelah mendapat persetujuan dari Jaksa Agung Muda Intelijen atau pejabat berwenang yang ditunjuk" (Pasal 17). Selain itu, penyebarluasan data intelijen dan informasi intelijen yang termasuk dalam kategori rahasia intelijen yang dilakukan secara melawan hukum, dikenai sanksi sesuai dengan ketentuan peraturan perundang-undangan.

4.3. Mahkamah Agung dan Badan Peradilan

a. Fungsi dan kewenangan

Mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP), badan peradilan memiliki dua fungsi utama dalam sistem peradilan pidana, sebagai berikut:

Pertama, melakukan pengawasan terhadap pelaksanaan kewenangan negara. Dalam menjalankan fungsi ini, badan peradilan memiliki wewenang untuk memeriksa izin/permohonan yang diajukan oleh aparat penegak hukum, sebelum dilakukannya suatu upaya paksa atau wewenang lain yang membutuhkan izin/persetujuan dari pengadilan. Sebagai contoh, dalam hal penyidik melakukan penggeledahan, penyidik terlebih dahulu mengajukan permohonan izin kepada ketua pengadilan negeri tempat dilakukannya penggeledahan, sebelum akhirnya penyidik melakukan penggeledahan.[28] Permohonan izin tersebut berisikan beberapa data, termasuk data pribadi, yang di antaranya adalah data tersangka (dalam hal tersangka telah ditetapkan).[29] Permohonan izin ini diajukan oleh penyidik melalui Sistem Informasi Pengadilan (SIP), untuk selanjutnya diperiksa oleh pengadilan.

Selain menjalankan wewenang dalam bentuk memeriksa izin/permohonan sebagaimana diuraikan di atas, badan peradilan juga menjalankan wewenang praperadilan sebagai wujud pengawasan terhadap pelaksanaan kewenangan negara. Praperadilan ini dilakukan oleh badan peradilan apabila terdapat keberatan yang diajukan tersangka atau keluarga tersangka, korban atau keluarga korban, pelapor, atau advokat atau pemberi bantuan hukum yang diberi kuasa untuk mewakili kepentingan hukum tersangka atau korban, atas tindakan penyidik dalam melakukan penyidikan atau tindakan penuntut umum dalam melakukan penuntutan.[30] Permohonan praperadilan ini tentu memuat berbagai data pribadi, seperti halnya data pribadi pemohon.

28 Dalam keadaan mendesak, penyidik dapat langsung melakukan penggeledahan tanpa izin dari ketua pengadilan negeri. Lihat KUHAP, Pasal 113 ayat (4).

29 Surat Keputusan Ketua Mahkamah Agung (SK KMA) No. 239/KMA/SK/VIII/2022 tentang Petunjuk Teknis Administrasi Perkara Pidana Terpadu Secara Elektronik, Lampiran huruf C angka 2 (b).

30 KUHAP, Pasal 1 angka 15.

Kedua, kewenangan dalam mengadili perkara. Mengadili perkara merupakan serangkaian tindakan yang dilakukan oleh hakim untuk menerima, memeriksa, dan memutus perkara pidana.[31] Proses mengadili dimulai ketika penuntut umum melakukan pelimpahan perkara pidana ke pengadilan. Berkas pelimpahan perkara ini memuat berbagai data pribadi, seperti nama, umur, alamat, serta foto, baik milik tersangka, saksi, maupun korban. Berdasarkan berkas pelimpahan perkara tersebut, selanjutnya pengadilan memeriksa dan memutus sesuai dengan fakta dan isu hukum yang muncul selama persidangan. Pada tahap akhir mengadili perkara, yakni memutus, produk dokumen yang dikeluarkan oleh pengadilan adalah putusan. Dalam putusan ini, hakim mencantumkan data pribadi yang telah diperoleh dari penuntut umum sebelumnya dan data pribadi yang diperoleh selama proses persidangan.

b. Jenis dan proses pengelolaan data

UU PDP mengkategorikan data pribadi menjadi dua jenis, yakni data pribadi umum dan data pribadi spesifik.[32] Terhadap dua jenis data tersebut, UU PDP tidak memberikan definisi, melainkan mendaftar data-data apa saja yang masuk dalam masing-masing jenis. Dalam konteks data pribadi umum, yang termasuk di dalamnya adalah nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Adapun, yang termasuk dalam data pribadi spesifik adalah data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

Di internal instansi pengadilan, belum terdapat klasifikasi data sebagaimana diatur dalam UU PDP. Hanya terdapat informasi umum mengenai data-data apa saja yang dikumpulkan oleh pengadilan. Dalam kerangka Administrasi Perkara Pidana Terpadu secara elektronik,[33] pengadilan mengumpulkan berbagai jenis data

31 *Ibid*., Pasal 1 angka 13.
32 UU PDP, Pasal 4 ayat (1).
33 Administrasi Perkara Pidana Terpadu adalah layanan administrasi perkara pidana secara terintegrasi antara penyidik, penuntut umum, pengadilan, dan lembaga pemasyarakatan. Lihat SK KMA No. 239/KMA/SK/VIII/2022..., *Op. Cit.*, Lampiran huruf A angka 2.

Tabel 4.1. Data Pribadi dalam SIP

Dokumen	Data Pribadi yang Dikumpulkan dalam SIP dan Pihak yang Menginput/Mengunggah[a]
Pelimpahan berkas perkara pidana secara elektronik[b]	Penuntut Umum menginput data berikut dalam SIP: 1. nomor laporan penyidik; 2. nomor berkas perkara; 3. tanggal berkas perkara; dan 4. data penyidik. Penyidik menambahkan: 1. data penyidik (jika ada); 2. melengkapi data tersangka; 3. data penahanan tingkat penyidikan (apabila ditahan); dan 4. mengunggah dokumen berkas perkara tingkat penyidikan. Dokumen berkas perkara yang dimaksud, antara lain: 1. sampul berkas perkara; 2. daftar isi berkas perkara; 3. resume; 4. laporan polisi; 5. surat perintah penyidikan; 6. surat pemberitahuan dimulainya penyidikan; 7. berita acara pemeriksaan saksi; 8. berita acara pengambilan sumpah saksi; 9. berita acara pemeriksaan tersangka; 10. surat penunjukan penasihat hukum; 11. surat perintah penangkapan; 12. berita acara penangkapan; 13. surat perintah penahanan; 14. berita acara penahanan; 15. surat pemberitahuan penahanan; 16. surat permintaan perpanjangan penahanan; 17. perpanjangan penahanan; 18. surat perintah penyitaan; 19. berita acara penyitaan; 20. laporan penyitaan; 21. permohonan penyitaan; 22. penetapan penyitaan; 23. daftar saksi; 24. daftar barang bukti; 25. daftar pencarian barang bukti; 26. daftar tersangka; 27. foto / dokumen barang bukti; 28. foto tersangka; 29. identitas tersangka; 30. berita acara pemeriksaan ahli; dan 31. dokumen lain yang diperlukan.

Catatan kaki Tabel 4.1. a. Data pribadi yang dikumpulkan dalam konteks ini adalah data-data yang diunggah ke SIP. Data-data yang dikumpulkan dalam SIP ini bisa jadi bukan data pribadi apabila terpisah dengan data lainnya, tetapi apabila suatu data tersebut digabungkan dengan data-data lainnya, yang kemudian dapat mengidentifikasi orang perseorangan, maka data tersebut tetap masuk sebagai kualifikasi data pribadi. Lihat UU PDP, Pasal 1 angka 1.
b. SK KMA No. 239/KMA/SK/VIII/2022..., Op.Cit., Lampiran huruf C angka 1 (b, f, g).

Dokumen	Data Pribadi yang Dikumpulkan dalam SIP dan Pihak yang Menginput/Mengunggah[a]
Izin/persetujuan penggeledahan secara elektronik[c]	Penyidik menginput data penggeledahan, data tersangka (jika ada), dan mengunggah dokumen permohonan Izin/Persetujuan Penggeledahan ke dalam SIP.
Izin/persetujuan penyitaan secara elektronik[d]	Penyidik menginput data penyitaan, data tersangka (jika ada), dan mengunggah dokumen permohonan Izin/Persetujuan Penyitaan ke dalam SIP.
Permohonan perpanjangan penahanan secara elektronik[e]	Penyidik/Penuntut menginput data tersangka, data perkara, data penahanan dan mengunggah dokumen permohonan Perpanjangan Penahanan ke dalam SIP.
Izin besuk tahanan secara elektronik[f]	Pemohon mengunggah dokumen identitas pemohon ke dalam SIP.
Izin pinjam pakai barang bukti secara elektronik[g]	Pemohon mengunggah dokumen identitas pemohon dan bukti kepemilikan barang bukti ke dalam SIP.
Penetapan diversi secara elektronik[h]	Penyidik/Penuntut Umum mengunggah dokumen permohonan penetapan diversi dengan disertai surat kesepakatan diversi ke dalam SIP.
Permohonan pembantaran penahanan secara elektronik[i]	Pemohon mengunggah dokumen permohonan pembantaran penahanan ke dalam SIP.

Catatan kaki Tabel 4.1. c. *Ibid.*, Lampiran huruf C angka 2 (b); d. *Ibid.*, Lampiran huruf C angka 3 (b); e. *Ibid.*, Lampiran huruf C angka 4 (b); f. *Ibid.*, Lampiran huruf C angka 5 (b); g. *Ibid.*, Lampiran huruf C angka 6 (b); h. *Ibid.*, Lampiran huruf C angka 7 (b); i. *Ibid.*, Lampiran huruf C angka 8 (c).

pribadi yang termuat dalam dokumen pelimpahan berkas perkara pidana secara elektronik, izin/persetujuan penggeledahan secara elektronik, izin/persetujuan penyitaan secara elektronik, permohonan perpanjangan penahanan secara elektronik, izin besuk tahanan secara elektronik, izin pinjam pakai barang bukti secara elektronik, penetapan diversi secara elektronik, serta permohonan pembantaran penahanan secara elektronik melalui Sistem Informasi Pengadilan (SIP).[34] Data pribadi yang termuat tersebut dapat dilihat dalam Tabel 4.1.

Terhadap data-data yang diinput/diunggah ke SIP tersebut, panitera bertanggung jawab mengelolanya, termasuk melakukan verifikasi/pengecekan terhadap data-data tersebut serta mengarsipkannya.[35] Dalam mengelola, panitera tidak membedakan

34 SIP adalah seluruh sistem informasi yang disediakan oleh Mahkamah Agung untuk memberi pelayanan terhadap pencari keadilan yang meliputi administrasi, pelayanan perkara, dan persidangan secara elektronik. Lihat *Ibid.*, Lampiran huruf A angka 1.

35 *Ibid.*, Lampiran huruf C angka 1 (t, u), 2 (f), 3 (f), 4 (f), huruf D angka 1.

Tabel 4.2. Data Pribadi yang Dikumpulkan oleh MA

Dokumen	Data Pribadi yang Dikumpulkan oleh MA[a]
Penetapan penahanan	1. Kode jenis dokumen 2. Identitas dokumen: nomor penetapan penahanan, tanggal penetapan 3. Konten dokumen: nomor perkara, tingkat pengadilan, daftar terdakwa, daftar pasal dan undang-undang, kode jenis penahanan, kode satker tempat penahanan, lama penahanan, tanggal mulai penahanan, tanggal berakhir penahanan 4. Pejabat penandatanganan
Petikan putusan pengadilan	1. Kode jenis dokumen 2. Identitas dokumen: tingkat pengadilan, kode jenis upaya hukum, nomor putusan, tanggal putusan, nomor P-29, nomor surat pelimpahan 3. Konten dokumen: daftar terdakwa, amar, daftar pasal dan undang-undang 4. Pejabat penandatangan
Salinan putusan pengadilan	1. Kode jenis dokumen 2. Identitas dokumen: tingkat pengadilan, nomor putusan, tanggal putusan, nomor P-29 (tambah nomor berkas perkara), nomor surat pelimpahan, kode jenis upaya hukum 3. Konten dokumen: berkas digital, salinan putusan
Pemberitahuan permohonan banding	1. Kode jenis dokumen 2. Identitas dokumen: nomor, tanggal, nomor putusan 3. Konten dokumen: daftar terdakwa, daftar nama alias, daftar pasal dan undang-undang, pihak pemohon 4. Pejabat penandatangan
Pemberitahuan pencabutan banding	1. Kode jenis dokumen 2. Identitas dokumen: nomor akta pencabutan banding, tanggal akta permohonan banding, nomor akta permohonan banding, tanggal akta permohonan banding 3. Konten dokumen: daftar terdakwa, pihak pemohon 4. Pejabat penandatangan
Penetapan diversi tingkat penyidikan	1. Kode jenis dokumen 2. Identifikasi dokumen: nomor penetapan, tanggal penetapan, nomor surat permohonan, nomor berita acara diversi, tanggal berita acara diversi, tanggal kesepakatan diversi 3. Konten dokumen: identitas anak, kode jenis kesepakatan diversi 4. Pejabat penandatangan
Penetapan izin penggeledahan	1. Kode jenis dokumen 2. Identitas dokumen: nomor penetapan, tanggal penetapan, nomor surat permintaan izin penggeledahan, tanggal surat permintaan izin penggeledahan, nomor SPDP, tanggal SPDP 3. Konten dokumen: nama tersangka, lokasi penggeledahan (jenis lokasi, alamat), jenis tindak pidana, daftar pasal dan undang-undang 4. Pejabat penandatangan

Catatan kaki Tabel 4.2. a. Data-data yang dikumpulkan dalam dokumen-dokumen ini bisa jadi bukan data pribadi apabila terpisah dengan data lainnya, tetapi apabila suatu data tersebut digabungkan dengan data-data lainnya, yang kemudian dapat mengidentifikasi orang perseorangan, maka data tersebut tetap masuk sebagai kualifikasi data pribadi. Lihat UU PDP, Pasal 1 angka 1.

pengelolaan data pribadi umum dan data pribadi spesifik, melainkan memperlakukan dan mengelolanya secara sama.

Dalam perkembangannya, SIP diintegrasikan dengan berbagai sistem perkara milik aparat penegak hukum lainnya melalui Sistem Peradilan Pidana Terpadu berbasis Teknologi Informasi (SPPT-TI). Dalam SPPT-TI tersebut, MA memiliki tanggung jawab terhadap 33 (tiga puluh tiga) dokumen yang didalamnya berisikan pula data-data pribadi. Data-data pribadi tersebut hanya disebutkan saja, tanpa dibedakan jenis datanya menjadi umum dan spesifik. Data-data tersebut, di antaranya dapat dilihat dalam Tabel 4.2:[36]

Dokumen-dokumen beserta elemen-elemen data di dalamnya tersebut diproses oleh pengadilan, untuk selanjutnya dipertukarkan dalam kerangka SPPT-TI.

c. Tantangan dan risiko

Tantangan dalam pelindungan data pribadi di lingkungan peradilan tidak hanya bersumber dari aspek teknis, tetapi juga mencerminkan keterbatasan pada level kebijakan dan kapasitas kelembagaan. Dalam konteks sistem peradilan yang semakin terdigitalisasi, kelemahan pada satu aspek dapat berdampak sistemik terhadap keamanan dan akuntabilitas pengelolaan data. Oleh karena itu, identifikasi terhadap berbagai risiko ini menjadi penting untuk memahami sejauh mana kesiapan institusi peradilan dalam mengimplementasikan prinsip-prinsip pelindungan data pribadi secara efektif. Tantangan dan resiko pada badan peradilan adalah sebagai berikut.

1) Pengadilan belum memiliki peraturan internal yang secara khusus mengatur pelindungan data pribadi. Pengaturan terkait pelindungan data pribadi ditemukan secara tersebar dalam SK KMA No. 269/KMA/SK/XII/2018 tentang Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Mahkamah Agung dan Badan Peradilan yang Berada di

36 Kementerian Koordinator Bidang Politik dan Keamanan RI, *Buku Pedoman Pertukaran dalam Rangka Pelaksanaan Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi Versi 2024*, (Jakarta: Kementerian Koordinator Bidang Politik dan Keamanan RI, 2025), hal. 119.

Bawahnya (SK KMA 269/2018), SK KMA No. 2-144/KMA/SK/VIII/2022 tentang Standar Pelayanan Informasi Publik di Pengadilan (SK KMA 2-144/2022), SK KMA No. 239/KMA/SK/VIII/2022 tentang Petunjuk Teknis Administrasi Perkara Pidana Terpadu Secara Elektronik (SK KMA 239/2022), dan SK Bawas No. 63/BP/SK/PW1/XI/2024 tentang Pedoman Audit Teknologi Informasi dan Komunikasi atas Sistem Pemerintahan Berbasis Elektronik di Lingkungan Mahkamah Agung dan Badan Peradilan yang Berada di Bawahnya (SK Bawas 63/2024). Ketiadaan kebijakan internal yang secara khusus mengatur pelindungan data pribadi ini akan menjadi tantangan bagi personil badan peradilan untuk mengimplementasikan dan mengoperasionalisasikan UU PDP.

2) Bagi badan publik secara umum, pelindungan data pribadi merupakan isu yang relatif baru, mengingat kewajiban-kewajiban terkait pelindungan data pribadi baru muncul pasca disahkannya UU PDP pada tahun 2022. Hal ini tentu berdampak pada belum adanya sumber daya manusia khusus yang memiliki keahlian mengenai pelindungan data pribadi. Di Mahkamah Agung, pelindungan data pribadi, setidaknya, menjadi ruang lingkup pekerjaan dua unit, yakni Kepaniteraan serta Biro Hukum dan Humas. Kepaniteraan memiliki ruang lingkup terkait pelindungan data pribadi dalam hal memproduksi putusan dan mempublikasikannya melalui Direktori Putusan. Adapun, Biro Hukum dan Humas memiliki ruang lingkup terkait pelindungan data pribadi dalam hal mengelola informasi perkara yang ada dalam Sistem Informasi Penelusuran Perkara (SIPP). Berbeda dengan praktik di Mahkamah Agung, di pengadilan negeri dan tinggi, tanggung jawab mengenai pelindungan data pribadi hanya terdapat pada unit kepaniteraan.
3) Sistem yang aman dan andal adalah infrastruktur penting untuk melindungi data pribadi. Tanpa adanya sistem yang aman dan andal, data pribadi akan rentan mengalami kebocoran. Beberapa badan publik di Indonesia, termasuk Komisi Pemilihan Umum dan Kementerian Kesehatan, telah

mengalami peretasan yang berujung pada kebocoran data pribadi.[37] Tanpa adanya kebijakan pelindungan data pribadi yang matang, kapasitas sumber daya manusia yang mumpuni, serta sistem teknologi yang aman dan andal, kebocoran data pribadi bukan tidak mungkin terjadi di lingkungan badan peradilan.

d. Dampak terhadap kelompok rentan

Kebocoran data pribadi memiliki dampak berbeda terhadap kelompok rentan, seperti halnya perempuan korban kekerasan berbasis gender dan anak. Dalam kerangka kekerasan berbasis gender online (KBGO) misalnya–yang mana perempuan dan anak perempuan rentan menjadi korban–data pribadi seringkali dijadikan sebagai senjata untuk mengancam dan/atau memeras (khususnya berupa *sextortion*) korban. Apabila terdapat kebocoran data pribadi yang mengungkap data pribadi perempuan dan anak perempuan, bukan tidak mungkin bahwa pelaku akan menggunakan data tersebut untuk menghubungi, lalu menggunakan data-data yang telah dimilikinya (data nama, alamat, juga catatan fakta terkait bentuk kekerasan berbasis gender yang pernah dialami) untuk mengancam dan/atau memeras. Data-data yang bocor tersebut pada gilirannya akan tersebar kembali apabila pelaku melakukan *doxxing* (penyebarluasan data pribadi korban tanpa persetujuan) atau impersonasi (penggunaan data pribadi korban untuk membangun sebuah profil tiruan).

Selanjutnya, kebocoran data pribadi tentu berdampak serius terhadap anak. Data-data anak yang bocor dapat digunakan oleh pihak-pihak yang tidak bertanggung jawab untuk hal-hal seperti mempermalukan anak, memanipulasi anak, hingga penculikan dan perdagangan anak.

37 CNN Indonesia, "KPU Buka Suara Soal Dugaan 105 Juta Data Warga Indonesia Bocor", *CNN Indonesia,* 6 September 2022, https://www.cnnindonesia.com/nasional/20220906223223-20-844262/kpu-buka-suara-soal-dugaan-105-juta-data-warga-indonesia-bocor; M. Nurhadi, "Soroti Dugaan Kebocoran Data Kemenkes, Pakar Singgung Ancaman Foto Medis Pasien", *Suara.com*, 7 Januari 2022, https://www.suara.com/bisnis/2022/01/07/112835/soroti-dugaan-kebocoran-data-kemenkes-pakar-singgung-ancaman-foto-medis-pasien .

e. Kepatuhan terhadap UU PDP

Melihat pemaknaan pengendali[38] dan prosesor[39] data dalam UU PDP, Mahkamah Agung dan lingkungan peradilan di bawahnya merupakan badan publik yang masuk dalam kualifikasi aktor-aktor tersebut. Mengingat, Mahkamah Agung dan lingkungan peradilan di bawahnya melakukan pengumpulan data pribadi, pemrosesan data pribadi, serta penentuan tujuan pengumpulan dan pemrosesan data pribadi tersebut. Oleh karenanya, muncul berbagai kewajiban pada Mahkamah Agung dan lingkungan peradilan di bawahnya sebagai pengendali dan prosesor data pribadi,[40] yang bahkan diikuti pula oleh sanksi administratif dan sanksi pidana.[41]

Berikut merupakan penjelasan kepatuhan badan peradilan terhadap beberapa kewajiban yang ada dalam UU PDP:[42]

1) **Kewajiban memiliki dasar pemrosesan data pribadi**
   Pasal 20 ayat (1) mewajibkan setiap pengendali data pribadi untuk memiliki dan menentukan dasar pemrosesan data pribadi. Badan peradilan merupakan lembaga negara yang, setidaknya, memiliki wewenang untuk 1) melakukan pengawasan terhadap pelaksanaan kewenangan negara (misalnya, melalui pemberian izin/persetujuan atas upaya paksa yang dilakukan aparat penegak hukum) dan 2) mengadili perkara. Berkenaan dengan dua wewenang tersebut, badan peradilan membutuhkan berbagai data pribadi untuk menjalankan wewenangnya. Dalam konteks UU PDP, khususnya Pasal 20 ayat (1) dan ayat (2), badan peradilan telah memiliki dasar pemrosesan yang tepat, yakni "*pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan*."

38 UU PDP. Pasal 1 angka 4.
39 *Ibid.*, Pasal 1 angka 5.
40 *Ibid.*, Pasal 20 - Pasal 50.
41 *Ibid.*, Pasal 57.
42 Penilaian kepatuhan tidak dilakukan terhadap seluruh kewajiban badan peradilan yang ada dalam UU PDP karena terdapat keterbatasan sumber. Selain itu, semua penilaian yang ada dalam bagian ini, secara mayoritas, berdasar pada kajian terhadap peraturan-peraturan internal badan peradilan.

2) **Kewajiban memastikan akurasi, kelengkapan, dan konsistensi data pribadi**

   UU PDP memberi kewajiban bagi pengendali data pribadi untuk memastikan akurasi, kelengkapan, dan konsistensi data pribadi.[43] Dalam kerangka SIP, terdapat peran Panitera Muda untuk melakukan verifikasi/pengecekan terhadap dokumen-dokumen yang masuk dalam SIP.[44] Selain itu, dalam kerangka tata kelola teknologi informasi dan komunikasi di lingkungan badan peradilan, secara umum, terdapat proses penjagaan akurasi, kehandalan, dan pengkinian data agar data tetap handal, akurat, terpadu, terkini, dan aman, yang dilakukan oleh Pemilik Data—orang atau unit yang berwenang mengakses atau menolak akses terhadap data tertentu.[45]

3) **Kewajiban melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi**

   Pasal 31 UU PDP memberikan kewajiban kepada pengendali data pribadi untuk merekam seluruh kegiatan pemrosesan data pribadi. Saat ini, badan peradilan belum memiliki mekanisme khusus dalam merekam setiap kegiatan pemrosesan data pribadi.

4) **Kewajiban melakukan dampak pelindungan data pribadi (*Data Protection Impact Assessment*/DPIA)**

   Pasal 34 UU PDP mewajibkan pengendali data untuk melakukan DPIA apabila pemrosesan data pribadi yang dilakukannya memiliki potensi risiko tinggi terhadap subjek data pribadi. Potensi risiko tinggi tersebut meliputi: a) pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap subjek data pribadi; b) pemrosesan atas data pribadi yang bersifat spesifik; c) pemrosesan data pribadi dalam skala besar; d) pemrosesan data pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap subjek data pribadi;

43 UU PDP, Pasal 29.

44 SK KMA No. 239/KMA/SK/VIII/2022..., *Op.Cit*., Lampiran huruf C angka 1 (t, u), 2 (f), 3 (f), 4 (f).

45 SK KMA No. 269/KMA/SK/XII/2018..., *Op.Cit*., Lampiran I romawi I huruf K dan Lampiran I romawi III huruf D.

e) pemrosesan data pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data; f) penggunaan teknologi baru dalam pemrosesan data pribadi; dan/atau g) pemrosesan data pribadi yang membatasi pelaksanaan hak subjek data pribadi.

Pemrosesan data pribadi oleh badan peradilan, setidaknya, memenuhi dua unsur potensi risiko tinggi, yakni:

a. memroses data pribadi bersifat spesifik: data-data yang diproses oleh badan peradilan merupakan data pribadi spesifik, yang setidaknya dapat meliputi data biometrik, genetika, catatan kejahatan, anak, dan keuangan pribadi.
b. memroses data pribadi dalam skala besar: data-data yang diproses oleh badan peradilan merupakan data berskala besar yang jumlahnya mencapai jutaan data.

Oleh karenanya, badan peradilan memiliki kewajiban untuk melakukan DPIA sebagai langkah krusial untuk mengidentifikasi risiko dan menentukan langkah mitigasi atas risiko tersebut.

5) Kewajiban melindungi dan memastikan keamanan data pribadi

Pasal 35 UU PDP mewajibkan pengendali data untuk melindungi dan memastikan keamanan data pribadi melalui dua hal, yakni 1) penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi, dan 2) penentuan tingkat keamanan data pribadi. Terkait dengan poin pertama, badan peradilan belum memiliki pedoman teknis terkait pelindungan data pribadi. Meskipun demikian, terdapat beberapa regulasi internal badan peradilan yang berkaitan dengan pelindungan data pribadi, yakni SK KMA 269/2018, SK KMA 2-144/2022, SK KMA 239/2022, dan SK Bawas 63/2024. Dalam SK KMA 2-144/2022 misalnya, terdapat langkah teknis yang harus dilakukan oleh pengadilan untuk melindungi data pribadi, yakni dengan cara melakukan pengaburan identitas pihak-pihak tertentu dalam putusan perkara tertentu.[46] Lalu,

46 Identitas tersebut meliputi nama dan nama alias; nomor induk kependudukan (NIK)/ paspor; pekerjaan, tempat bekerja dan identitas kepegawaian yang bersangkutan; dan sekolah atau lembaga pendidikan yang diikuti. Lihat: SK KMA 2-144/2022, Lampiran I,

terkait dengan poin ke-dua, belum terdapat penentuan tingkat keamanan data pribadi. Badan peradilan baru berfokus pada penentuan keamanan dalam skala yang lebih luas, yakni keamanan teknologi.

6) **Kewajiban menunjuk pejabat atau petugas pelindungan data pribadi (*data protection officer*/DPO)**

UU PDP memberi kewajiban menunjuk DPO kepada pengendali dan prosesor data pribadi yang melaksanakan fungsi pelindungan data pribadi dalam kondisi-kondisi tertentu.[47] Namun, DPO belum dikenal di lingkungan pengadilan. Saat ini, hanya terdapat jabatan-jabatan yang memiliki fungsi terkait pelindungan data pribadi, di antaranya:

a. Panitera
b. Mengacu pada SK KMA 239/2022, Panitera Pengadilan bertanggung jawab mengelola informasi elektronik/ dokumen elektronik pada SIP.[48]
c. Petugas Keamanan Informasi
d. Mengacu pada SK KMA 269/2018, Petugas Keamanan Informasi adalah Pejabat yang menyelenggarakan urusan TIK dan memiliki tanggung jawab untuk menjamin pelaksanaan pelindungan kerahasiaan sesuai dengan tingkatannya dan berhak melakukan pemeriksaan dalam bentuk apapun untuk menguji ketertiban pelaksanaannya oleh pemilik dan pengguna data.[49]
e. Pemilik Data
f. Mengacu pada SK KMA 269/2018, Pemilik Data adalah orang atau unit yang berwenang untuk mengakses atau menolak akses terhadap data tertentu dan oleh karenanya bertanggung jawab terhadap akurasi, kehandalan dan

Romawi VIII, huruf G.

47 UU PDP, Pasal 53. Penunjukkan DPO diwajibkan bagi pengendali dan prosesor data pribadi dalam hal: a) pemrosesan data pribadi untuk kepentingan pelayanan publik; b) kegiatan inti pengendali data pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan c) kegiatan inti pengendali data pribadi terdiri dari pemrosesan data pribadi dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana.

48 SK KMA No. 239/KMA/SK/VIII/2022..., *Op.Cit.*, Lampiran huruf D angka 1.

49 SK KMA No. 269/KMA/SK/XII/2018..., *Op. Cit.*, Lampiran I romawi I huruf F dan Lampiran I romawi III huruf D angka 2.

pengkinian data.[50]

g. Pejabat Pengelola Informasi dan Dokumentasi (PPID) Mengacu pada SK KMA 2-144/2022 tentang, PPID adalah pejabat yang bertanggung jawab di bidang koordinasi penyimpanan, pendokumentasian, penyediaan, dan/atau pelayanan informasi di badan publik.[51]
h. Kewajiban melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi dan penilaian dampak pelindungan data/DPIA. Pasal 31 UU PDP memberikan kewajiban kepada pengendali data pribadi untuk merekam seluruh kegiatan pemrosesan data pribadi. Saat ini, badan peradilan belum memiliki mekanisme khusus dalam merekam setiap kegiatan pemrosesan data pribadi

4.4. Lembaga Perlindungan Saksi dan Korban (LPSK)

a. Fungsi dan kewenangan

Berdasarkan Undang-Undang No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban sebagaimana telah diubah dengan Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU Perlindungan Saksi dan Korban), Lembaga Perlindungan Saksi dan Korban (LPSK) adalah lembaga yang bertugas dan berwenang untuk memberikan perlindungan dan hak-hak lain kepada saksi, korban, saksi pelaku, pelapor, dan ahli. Perlindungan kepada para pihak tersebut pada hakikatnya bertujuan untuk memberikan rasa aman dalam memberikan keterangan pada setiap proses peradilan pidana. Selanjutnya, UU Perlindungan Saksi dan Korban juga menjabarkan hak-hak saksi, korban, saksi pelaku, pelapor, dan ahli yang menjadi tanggung jawab LPSK dalam pemenuhannya. Beberapa di antara hak-hak tersebut adalah: hak untuk memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya, serta bebas dari ancaman yang berkaitan dengan kesaksian yang akan, sedang, atau

50 *Ibid.*, Lampiran I romawi I huruf k dan Lampiran I romawi III huruf D.
51 SK KMA No. 2-144/KMA/SK/VIII/2022 tentang Standar Pelayanan Informasi Publik di Pengadilan, Lampiran I Romawi I angka 4.

telah diberikannya; dan hak untuk dirahasiakan identitasnya.

Dalam memberikan perlindungan serta menjamin pemenuhan hak-hak saksi, korban, saksi pelaku, pelapor, dan ahli, LPSK memiliki berbagai wewenang, yaitu[52]:

a. Meminta keterangan secara lisan dan/atau tertulis dari pemohon dan pihak lain yang terkait dengan permohonan;
b. Menelaah keterangan, surat, dan/atau dokumen yang terkait untuk mendapatkan kebenaran atas permohonan;
c. Meminta salinan atau fotokopi surat dan/atau dokumen terkait yang diperlukan dari instansi manapun untuk memeriksa laporan pemohon sesuai dengan ketentuan peraturan perundang-undangan;
d. Meminta informasi perkembangan kasus dari penegak hukum;
e. Mengubah identitas terlindung sesuai dengan ketentuan peraturan perundang-undangan;
f. Mengelola rumah aman;
g. Memindahkan atau merelokasi terlindung ke tempat yang lebih aman;
h. Melakukan pengamanan dan pengawalan;
i. Melakukan pendampingan saksi dan/atau korban dalam proses peradilan; dan
j. Melakukan penilaian ganti rugi dalam pemberian restitusi dan kompensasi.

Dari berbagai jenis kewenangan di atas, dapat dilihat bahwa dalam pelaksanaan tanggung jawabnya LPSK acapkali bersentuhan dengan data pribadi individu. Hal tersebut terjadi utamanya ketika meminta dan menelaah keterangan dari pemohon perlindungan dan pihak-pihak lain yang terkait, mengubah identitas terlindung, serta dalam hal melakukan komunikasi dan koordinasi dengan instansi lain, yaitu ketika meminta salinan surat atau dokumen yang diperlukan dari instansi lain untuk memeriksa laporan pemohon dan meminta

52 Disadur dari situs web Lembaga pelindungan Saksi dan Korban, https://www.lpsk.go.id/profile/about, diakses pada 3 Februari 2026. Lihat juga Undang-Undang Nomor Nomor 13 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 31 Tahun 2014 tentang Pelindungan Saksi dan Korban.

informasi perkembangan kasus dari penegak hukum. Sebagai contoh, dalam konteks meminta dan menelaah keterangan dari pemohon, LPSK mensyaratkan pemohon untuk melampirkan setidak-tidaknya salinan kartu identitas atau kartu keluarga serta informasi domisili pemohon[53] di mana di dalamnya tentu saja terkandung data-data pribadi. Selain itu, dalam konteks komunikasi dan koordinasi dengan instansi penegak hukum, LPSK dalam kondisi tertentu juga perlu berbagi informasi yang sifatnya rahasia, termasuk data pribadi pihak yang dilindungi[54].

Perlu juga ditekankan bahwa perlindungan terhadap saksi, korban, saksi pelaku, pelapor, dan ahli diberikan sejak tahap penyelidikan dimulai dan berakhir sesuai ketentuan yang diatur UU Perlindungan Saksi dan Korban. Oleh karena itu, LPSK memiliki peran di seluruh tahapan proses peradilan pidana karena perlindungan terhadap saksi, korban, saksi pelaku, pelapor, dan ahli sangat mungkin sudah mulai dibutuhkan sejak tahap penyelidikan dan sampai dengan setelah perkara diputus oleh pengadilan.

b. Jenis dan proses pengelolaan data

Tugas dan fungsi LPSK di bidang perlindungan saksi, korban, saksi pelaku, pelapor, dan ahli diwujudnyatakan lewat penyediaan berbagai pelayanan untuk publik. Berdasarkan Peraturan LPSK Nomor 1 Tahun 2024 tentang Standar Pelayanan di Lingkungan Lembaga Perlindungan Saksi dan Korban (PerLPSK No. 1/2024), terdapat 5 bentuk pelayanan yang disediakan, yaitu pelayanan:[55]

a. penerimaan permohonan;
b. tindakan proaktif;
c. pemberian pelindungan darurat;
d. pemberian pelindungan; dan
e. informasi publik

53 Disadur dari situs web Lembaga pelindungan Saksi dan Korban, https://www.lpsk.go.id/informasi-pelayanan/penerimaan-permohonan, diakses pada 3 Februari 2026.

54 Hasil wawancara dengan Sriyana, Sekretaris Jenderal Lembaga Perlindungan Saksi dan Korban, pada hari Senin, 12 Januari 2026.

55 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2024 tentang Standar Pelayanan di Lingkungan Lembaga Perlindungan Saksi dan Korban,* Pasal 4.

Dari kelima jenis pelayanan bagi publik tersebut, diketahui bahwa LPSK melakukan pemrosesan data pribadi setidaknya dalam hal pelayanan penerimaan permohonan, pelayanan pemberian perlindungan, dan pelayanan informasi publik.

Dalam hal pelayanan penerimaan permohonan, berdasarkan PerLPSK No. 1/2024, LPSK mensyaratkan pemohon perlindungan untuk menyertakan beberapa dokumen sebagai persyaratan formil, yaitu:[56]

a. surat permohonan tertulis;
b. fotokopi identitas atau kartu keluarga (dalam hal alamat tempat tinggal berbeda dengan domisili pemohon, persyaratan fotokopi identitas atau kartu keluarga dapat dilengkapi dengan surat keterangan atau informasi tentang domisili pemohon);
c. asli surat kuasa, jika permohonan diajukan melalui kuasa hukum atau pendamping;
d. surat izin dari orang tua atau wali, jika permohonan terkait perlindungan untuk anak dan permohonan yang tidak diajukan oleh orang tua/wali;
e. surat keterangan atau dokumen dari instansi terkait yang berwenang sesuai ketentuan peraturan perundang-undangan, yang menerangkan status saksi, korban, pelapor, saksi pelaku, atau ahli dalam kasus tindak pidana;
f. surat resmi dari pejabat yang berwenang jika permohonan diajukan oleh aparat penegak hukum dan/atau instansi yang berwenang; dan
g. kronologi uraian peristiwa tindak pidana.

Selain persyaratan formil, pemohon juga perlu memenuhi persyaratan materiel, yaitu[57]:

a. sifat pentingnya keterangan pemohon;
b. tingkat ancaman yang dialami pemohon, apabila permohonan diajukan untuk layanan perlindungan fisik;

56 Lembaga pelindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Pelindungan Saksi dan Korban Nomor 1 Tahun 2024 tentang Standar Pelayanan di Lingkungan Lembaga pelindungan Saksi dan Korban*, hal. 7.
57 *Ibid.*, hal. 8.

c. hasil analisis tim medis atau psikolog terhadap pemohon; dan
d. rekam jejak tindak pidana yang pernah dilakukan oleh pemohon.

Dari berbagai persyaratan tersebut, dapat disimpulkan bahwa dalam memberikan pelayanan penerimaan permohonan LPSK mengendalikan dan memproses data pribadi yang bersifat umum dan bersifat spesifik. Data pribadi yang bersifat umum tersebut berasal dari fotokopi kartu identitas atau kartu keluarga pemohon perlindungan serta surat keterangan domisili apabila diperlukan. Kartu identitas atau kartu keluarga setidaknya mencakup data pribadi berisi nama, jenis kelamin, kewarganegaraan, agama, status perkawinan serta alamat. Tetapi, tidak menutup kemungkinan juga dokumen-dokumen lainnya, seperti surat permohonan tertulis[58] atau surat keterangan dari instansi terkait yang berwenang juga mengandung data pribadi yang bersifat umum. Sementara itu, data pribadi bersifat spesifik yang dikumpulkan LPSK adalah hasil analisis tim medis atau psikolog terhadap pemohon dan rekam jejak tindak pidana yang pernah dilakukan oleh pemohon yang menjadi bagian dari persyaratan pengajuan permohonan perlindungan kepada LPSK.

Data-data yang menjadi bagian dari persyaratan tersebut akan menjalani proses penilaian oleh LPSK, khususnya Biro Penelaahan Permohonan[59]. Ketika syarat formil dan materiil dinyatakan lengkap, permohonan akan disampaikan ke Sidang Mahkamah Pimpinan LPSK untuk diputuskan akan berlanjut dengan penelaahan atau ditolak. Selanjutnya, apabila diputuskan bahwa permohonan memenuhi syarat untuk dilanjutkan dengan penelaahan, maka LPSK akan melakukan penelaahan tersebut dan hasilnya akan diserahkan kepada Sidang Mahkamah Pimpinan LPSK (SMPL) yang bersifat tertutup dan terbatas[60]. SMPL kemudian akan memutuskan apakah

58 Sebagai contoh, dalam surat permohonan tertulis, pemohon diminta untuk mencantumkan setidaknya: nama lengkap pemohon, nomor telepon dan/atau alamat surat elektronik, dan alamat domisili. Lihat Pasal 6 Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 2 Tahun 2020 tentang Permohonan Perlindungan Saksi dan/atau Korban Tindak Pidana.

59 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Sekretaris Jenderal Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Sekretariat Jenderal Lembaga Perlindungan Saksi Dan Korban*, Pasal 15.

60 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga pelindungan Saksi dan Korban Nomor 1 Tahun 2026 tentang Sidang Mahkamah Pimpinan Lembaga*

perlindungan dapat diberikan kepada pemohon. SMPL berisi berbagai elemen LPSK, antara lain pimpinan LPSK, pimpinan unit kerja paling rendah setingkat eselon II, tenaga ahli, dan kepala perwakilan LPSK di daerah[61].

Selanjutnya, LPSK juga akan mengendalikan dan memproses data pribadi dalam hal pelayanan pemberian perlindungan terhadap saksi, korban, saksi pelaku, pelapor, dan ahli. Dalam hal setelah penelaahan LPSK memutuskan untuk memberikan program perlindungan kepada pemohon, maka LPSK akan menyampaikan keputusan tersebut melalui surat kepada terlindung dan kepada aparat penegak hukum dan/atau instansi yang berwenang terkait perlindungan[62]. Di samping itu, agar program perlindungan dapat dilaksanakan, LPSK dan terlindung akan membuat surat perjanjian dan secara khusus terlindung akan membuat surat pernyataan kesediaan untuk mengikuti syarat-syarat perlindungan[63]. LPSK juga akan melakukan penginputan data terlindung ke dalam Sistem Informasi perlindungan Saksi dan Korban (SIMPUSAKA)[64]. Keseluruhan kegiatan tersebut memperlihatkan adanya pemrosesan data pribadi oleh LPSK dalam hal pemberian perlindungan kepada terlindung.

Dalam hal dibutuhkan program perlindungan terhadap terlindung berupa perlindungan fisik, maka LPSK juga akan melakukan pemrosesan data pribadi. Sebagai contoh, penempatan terlindung di rumah aman, LPSK setidaknya melakukan koordinasi dengan pemerintah setempat dan/atau instansi terkait lainnya di lingkungan tempat rumah aman tersebut dan melakukan pengurusan dokumen administrasi yang diperlukan[65], di mana kegiatan-kegiatan tersebut berpotensi melibatkan data pribadi terlindung. Contoh lainnya adalah dalam hal fasilitasi penyediaan identitas baru

Perlindungan Saksi dan Korban, Pasal 16. Tertutup artinya dihadiri hanya oleh peserta SMPL. Terbatas artinya SMPL dilakukan hanya untuk membahas agenda dan bahan tertentu.

61 *Ibid.*, Pasal 4.

62 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2022 tentang Pemberian Perlindungan kepada Saksi dan/atau Korban*, Pasal 16.

63 *Ibid.*

64 Hasil wawancara dengan Sriyana..., *Loc. Cit.*

65 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2022..., Op. Cit.*, Pasal 22.

terlindung. Dalam konteks ini LPSK akan mengajukan permohonan pengurusan mendapatkan identitas baru kepada Pengadilan Negeri dan dinas kependudukan dan catatan sipil sesuai dengan ketentuan peraturan perundang-undangan[66], sehingga kegiatan-kegiatan terkait penyediaan identitas baru bagi terlindung juga akan melibatkan pemrosesan data pribadi.

Terlepas dari contoh-contoh spesifik tersebut, secara umum, LPSK menyimpan dan memproses seluruh data pribadi terlindung dalam SIMPUSAKA dengan akses yang terbatas, dalam arti bahwa tidak semua pegawai maupun pimpinan LPSK dapat mengakses data dan informasi mengenai terlindung yang tersimpan dalam SIMPUSAKA[67]. Lebih lanjut lagi, pegawai yang bertanggung jawab untuk memberikan perlindungan memiliki akses hanya terhadap terlindung yang mereka dampingi sehingga pegawai LPSK pun tidak bisa mengetahui data semua terlindung yang didampingi LPSK[68]. Namun, di luar hal tersebut, LPSK juga melakukan koordinasi dengan pihak atau instansi di luar LPSK melalui berbagai metode, salah satunya surat-menyurat[69], yang berarti terjadi pemrosesan data pribadi juga di luar SIMPUSAKA.

Selain itu, LPSK juga mengumpulkan data pribadi dalam konteks pelayanan informasi publik. Salah satu syarat yang perlu dipenuhi oleh pihak yang mengajukan permintaan informasi publik kepada LPSK adalah salinan kartu tanda penduduk atau surat izin mengemudi atau paspor[70] di mana ketiga varian dokumen tersebut mengandung data pribadi yang setidaknya berisi nama, tanggal lahir, jenis kelamin, alamat, dan informasi lain yang apabila dikombinasikan dapat mengidentifikasi seseorang. Kemudian, permohonan informasi yang dianggap memenuhi syarat akan dicatat dalam buku register oleh petugas informasi[71]. Permohonan tersebut akan diteruskan kepada Pejabat Pengelola Informasi dan Dokumentasi (PPID) LPSK dan selanjutnya didistribusikan kepada unit kerja terkait agar unit

66 *Ibid.*, Pasal 23
67 Hasil wawancara dengan Sriyana..., *Loc. Cit.*
68 *Ibid.*
69 *Ibid.*
70 Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2024..., Op. Cit.*, hal. 21.
71 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 2 Tahun 2011 tentang Standar Operasional Prosedur Pelayanan Informasi Publik di Lingkungan Lembaga Perlindungan Saksi dan Korban*, Pasal 20 ayat (4).

kerja tersebut dapat mempersiapkan jawaban terhadap permohonan informasi tersebut[72]. Selain itu, apabila permohonan informasi publik tersebut ditolak oleh LPSK, maka pemohon dapat mengajukan keberatan. Dalam pengajuan keberatan ini, pemohon juga diwajibkan mencantumkan identitas lengkap pemohon dan kuasa pemohon (apabila ada) dalam formulir keberatan yang disediakan LPSK[73]. Identitas pemohon dan kuasanya tersebut akan dicatat dalam buku register keberatan[74]. Dari prosedur pengajuan permohonan informasi publik serta pengajuan keberatan tersebut dapat diketahui bahwa dalam konteks pelayanan informasi publik LPSK melakukan pemrosesan data pribadi, khususnya data pribadi yang bersifat umum.

Terkait penyimpanan atau retensi dokumen secara umum (termasuk dokumen yang mengandung data pribadi), LPSK memiliki kebijakan internal yang dituangkan dalam Peraturan LPSK Nomor 5 Tahun 2020 tentang Jadwal Retensi Arsip di Lingkungan LPSK (PerLPSK No. 5/2020). Dalam peraturan tersebut, LPSK menentukan masa retensi arsip dan rekomendasi perlakuan terhadap suatu arsip saat masa retensinya habis yang dapat berupa status "musnah", "permanen", atau "dinilai kembali".[75]

Penentuan masa retensi dan rekomendasi perlakuan ditetapkan berdasarkan masing-masing jenis arsip.

Berdasarkan PerLPSK No. 5/2020, arsip berkaitan dengan penerimaan dan penelaahan permohonan perlindungan diberikan status permanen, yang artinya dokumen-dokumen terkait penerimaan dan penelaahan permohonan perlindungan tersebut tidak dimusnahkan melainkan diserahkan kepada lembaga

72 *Ibid.*, Pasal 20 ayat (5).
73 *Ibid.*, Pasal 25 ayat (3).
74 *Ibid.*, Pasal 26 ayat (2).
75 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 5 Tahun 2020 tentang Jadwal Retensi Arsip di Lingkungan Lembaga Perlindungan Saksi dan Korban*, Pasal 1 angka 11, angka 12, dan angka 13. Status "musnah" artinya suatu jenis arsip dapat dimusnahkan karena jangka waktu penyimpanan telah habis dan tidak memiliki nilai guna, tidak ada peraturan perundang-undangan yang melarang dan tidak berkaitan dengan penyelesaian suatu kasus yang masih dalam proses hukum. Status "permanen" artinya suatu jenis arsip memiliki nilai guna sekunder atau nilai guna permanen, wajib diserahkan kepada lembaga kearsipan, sebagai bukti pertanggungjawaban sesuai dengan lingkup fungsi dan tugas LPSK. Status "dinilai kembali" artinya suatu jenis arsip belum dapat ditentukan rekomendasi akhirnya apakah dimusnahkan atau dipermanenkan, sehingga perlu dilakukan penilaian dan pengkajian kembali.

kearsipan sebagai pertanggungjawaban pelaksanaan tugas dan fungsi LPSK. Padahal, dokumen-dokumen tersebut sangat mungkin berisi data pribadi pemohon perlindungan. Selain itu, terdapat pula pengaturan terhadap arsip terkait persiapan dan administrasi putusan rapat paripurna pimpinan LPSK[76] yang memeriksa permohonan perlindungan dari pemohon. Dalam hal ini, terdapat perbedaan perlakuan: untuk dokumen-dokumen terkait persiapan rapat paripurna, LPSK menetapkan status permanen; sementara itu, untuk arsip terkait administrasi putusan rapat paripurna (baik yang menyatakan menerima atau menolak permohonan perlindungan), LPSK menetapkan status musnah (kecuali dalam perkara yang berskala nasional, maka statusnya ditetapkan permanen). Perlu juga menjadi catatan bahwa arsip-arsip terkait persiapan dan administrasi putusan rapat paripurna sangat mungkin berisi data-data pribadi pemohon perlindungan. [77]

Peraturan tersebut juga mengatur jadwal retensi arsip terhadap arsip terkait pemenuhan hak saksi dan korban, yang artinya dokumen-dokumen terkait program perlindungan oleh LPSK kepada terlindung dari tahap persiapan, pelaksanaan, dan pasca-pelaksanaan perlindungan. Dokumen-dokumen ini dapat dipastikan berisi data-data pribadi terlindung dan bersifat sangat rahasia karena terkait pelaksanaan program perlindungan LPSK. Berdasarkan PerLPSK No. 5/2020, LPSK menetapkan bahwa seluruh arsip terkait pemenuhan hak saksi dan korban wajib dimusnahkan; kecuali dalam perkara yang berskala nasional, maka ditetapkan status permanen.[78] Selain itu, terhadap arsip terkait pelayanan informasi publik, LPSK menentukan bahwa seluruh arsip tersebut wajib dimusnahkan tanpa ada pengecualian tertentu seperti yang berlaku terhadap arsip pemenuhan hak saksi dan korban.[79]

76 Dalam Peraturan LPSK Nomor 5 Tahun 2020 tentang Jadwal Retensi Arsip di Lingkungan LPSK, istilah yang digunakan untuk menerangkan Sidang Mahkamah Pimpinan LPSK (SMPL) adalah Rapat Paripurna Pimpinan LPSK.

77 Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 5 Tahun 2020 tentang Jadwal Retensi Arsip di Lingkungan Lembaga Perlindungan Saksi dan Korban*, hal. 11-14.

78 *Ibid.*, hal. 14-17.

79 *Ibid.*, hal. 82.

c. Tantangan dan risiko

Pada dasarnya, kerahasiaan data pribadi dan informasi terkait saksi, korban, saksi pelaku, pelapor, dan ahli sebagai terlindung di bawah program perlindungan LPSK adalah esensi dari tugas dan fungsi LPSK. Namun demikian, tidak berarti LPSK tidak menghadapi risiko atau tantangan dalam memenuhi tanggung jawab tersebut. Dari tinjauan terhadap regulasi LPSK yang diuraikan di atas, terdapat risiko yang dapat diidentifikasi dari pemberian layanan oleh LPSK dalam bidang perlindungan saksi dan korban serta pemenuhan hak atas informasi publik, di antaranya sebagai berikut:

1) Dalam beberapa prosedur yang LPSK implementasikan, termasuk dalam hal menerima permohonan perlindungan dari pemohon, masih mensyaratkan dokumen yang bersifat fisik. Sementara itu, tidak diketahui adanya mekanisme penyimpanan dokumen fisik yang menjamin perlindungan data pribadi yang ada di dalamnya. Penggunaan dokumen fisik (selain penggunaan sistem elektronik melalui SIMPUSAKA) membuka risiko terbukanya data pribadi. Apabila LPSK tidak menyimpan dan menangani dokumen terkait dengan sangat hati-hati, dokumen fisik yang berisi data pribadi dapat dilihat oleh pihak yang tidak berwenang atau tidak berhak. Kehati-hatian yang sama sebenarnya berlaku juga terhadap data yang tersimpan secara digital dalam SIMPUSAKA yang dimiliki oleh LPSK. Namun, setidaknya akses terhadap SIMPUSAKA terbatas untuk pegawai tertentu saja sehingga dalam hal ini ada batas pengaman agar tidak semua orang dapat mengakses data pribadi yang ada di dalam sistem tersebut.
2) Sebagaimana dijelaskan di atas, LPSK dalam pelaksanaan tugas dan fungsinya melakukan koordinasi dengan pihak atau instansi di luar LPSK. Namun, LPSK tidak memiliki mekanisme pertukaran data yang jelas dan yang menjamin perlindungan data pribadi ketika data atau informasi dipertukarkan antar-lembaga. Bahkan, terkadang karena kebutuhan mendesak yang menuntut waktu yang cepat, pegawai LPSK terpaksa membagikan dokumen melalui aplikasi percakapan yang

mana memunculkan potensi kebocoran data pribadi.[80]

3) LPSK belum memiliki mekanisme komplain bagi masyarakat dalam hal terjadi kebocoran data pribadi. Mekanisme komplain tersebut penting agar publik bisa segera merespon dan mencari solusi atas kebocoran data yang terjadi, termasuk dalam hal kejadian seperti ini terjadi di LPSK. Namun, ketika hal tersebut tidak ada, maka publik akan berpotensi menghadapi hambatan untuk memulihkan hak atas privasinya.

d. Dampak terhadap kelompok rentan

Sebagaimana diketahui umum, kemunculan LPSK berangkat dari upaya untuk melindungi saksi dan korban dari ancaman pihak lain sehingga mereka tidak lagi merasa takut untuk memberikan kesaksian kepada aparat penegak hukum dalam rangka mengungkap tindak pidana yang diduga terjadi.[81] Berkaca dari latar belakang tersebut, maka pada hakikatnya kesuksesan LPSK dalam melindungi saksi, korban, saksi pelaku, pelapor, dan ahli sangat bergantung kepada perlindungan terhadap identitas serta data pribadi lainnya dari terlindung. Selain itu, kerja-kerja LPSK juga banyak berhadapan dengan kelompok rentan (di antaranya perempuan dan anak), khususnya ketika melaksanakan perlindungan bagi terlindung dalam perkara-perkara tindak pidana perdagangan orang dan tindak pidana kekerasan seksual.

Oleh karena itu, ketika LPSK gagal menjamin kerahasiaan data pribadi para terlindung maka dampak negatif terhadap kelompok rentan tersebut menjadi berlipat ganda. Selain bahwa kelompok tersebut secara umum rentan menghadapi stigma dari masyarakat (terlepas dari ada atau tidaknya keterkaitan mereka dengan tindak pidana), ketika terungkap bahwa mereka memiliki kontribusi terhadap pengungkapan suatu tindak pidana maka mereka pun berpotensi mendapat ancaman dari pihak lain yang terlibat dalam tindak pidana tersebut, yang munkgin saja bisa membahayakan nyawa. Dengan demikian, aspek pelindungan data pribadi dalam

80 Hasil wawancara dengan Sriyana..., *Loc. Cit.*

81 Lihat Penjelasan bagian Umum pada Undang-Undang No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

pelaksanaan tugas dan fungsi LPSK menjadi semakin penting ketika pihak terlindung tergolong sebagai kelompok rentan.

e. Kepatuhan terhadap UU PDP

Secara umum, LPSK belum memiliki peraturan spesifik terkait pelindungan data pribadi. Dalam standar pelayanan LPSK yang diatur oleh PerLPSK No. 1/2024, kerahasiaan informasi menjadi salah satu syarat jaminan keamanan dan keselamatan dalam setiap jenis layanan yang LPSK sediakan. LPSK juga berupaya meningkatkan jaminan pelindungan data pribadi melalui penggunaan SIMPUSAKA dengan akses yang terbatas. Tetapi, di luar itu, kerahasiaan masih bergantung kepada kedisiplinan pegawai LPSK untuk tidak melakukan hal-hal yang bisa membuat pihak luar mengetahui terlindung yang menjadi tanggung jawab LPSK[82].

Sebagai pengendali sekaligus prosesor data pribadi, LPSK memiliki kewajiban sebagaimana diatur oleh UU Pelindungan Data Pribadi. Namun, beberapa di antaranya belum LPSK laksanakan. Salah satu kewajiban pengendali data pribadi adalah melakukan perekaman terhadap kegiatan pemrosesan data pribadi. Tetapi, LPSK belum memiliki mekanisme yang ajeg untuk perekaman tersebut, terutama apabila berhubungan dengan dokumen fisik.

Selain itu, terdapat kewajiban pengendali data pribadi untuk melakukan penilaian dampak pelindungan data pribadi dalam hal pemrosesan data pribadi memiliki potensi risiko tinggi terhadap subjek data pribadi. Pemrosesan data pribadi yang memiliki potensi risiko tinggi, salah satunya, dalam hal pengendali data pribadi melakukan pemrosesan atas data pribadi yang bersifat spesifik (di antaranya yaitu data dan informasi kesehatan dan catatan kejahatan). Hal ini relevan bagi LPSK karena dalam situasi tertentu LPSK akan berhadapan dengan permohonan bantuan medis atau rehabilitasi psikososial dan psikologis. Salah satu syarat yang ditetapkan LPSK bagi pemohon bantuan tersebut adalah hasil pemeriksaan tim medis atau psikolog terhadap pemohon[83]. Selain itu, LPSK

82 Hal ini disampaikan oleh Kepala Biro Hukum, Kerja Sama dan Hubungan Masyarakat Lembaga Perlindungan Saksi dan Korban, Arief Suryadi, dalam *Focus Group Discussion* pada tanggal 23 Januari 2026.

83 Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan*

juga mensyaratkan adanya dokumen rekam jejak tindak pidana yang pernah dilakukan oleh pemohon sebagai syarat mengajukan permohonan perlindungan[84]. Lebih khusus lagi, terdapat situasi juga di mana pemohon perlindungan adalah saksi pelaku[85]. Dalam hal ini, LPSK mensyaratkan adanya surat keterangan mengenai peran pelaku dalam tindak pidana yang diungkapkannya[86]. Dengan demikian, sebenarnya LPSK dalam konteks tertentu melakukan pemrosesan data pribadi yang memiliki potensi risiko tinggi. Tetapi, LPSK belum memiliki mekanisme penilaian dampak pelindungan data pribadi yang diwajibkan oleh UU Pelindungan Data Pribadi.

Kewajiban lain yang diatur oleh UU Pelindungan Data Pribadi adalah bahwa pengendali data pribadi dan prosesor data pribadi wajib menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dalam hal, salah satunya, pemrosesan data pribadi dilakukan untuk kepentingan pelayanan publik. LPSK adalah lembaga yang melakukan pelayanan publik dalam hal perlindungan saksi, korban, saksi pelaku, pelapor, dan ahli sehingga LPSK juga terikat dengan kewajiban tersebut. Tetapi, LPSK belum memiliki pejabat atau petugas pelindungan data pribadi.

Kewajiban penting lainnya yang wajib dipatuhi LPSK adalah terkait pemusnahan data pribadi. Aspek pemusnahan sangat penting karena hal ini terkait juga dengan kerahasiaan informasi dan data pribadi terlindung sebagai esensi tugas dan fungsi LPSK. Namun, terdapat catatan terhadap kebijakan internal LPSK terkait retensi arsip, yaitu PerLPSK No. 5/2020 yang telah dijelaskan dalam paragraf-paragraf sebelumnya. Mengacu kepada peraturan tersebut, ketika masa retensi habis, terdapat jenis-jenis arsip yang statusnya ditetapkan sebagai "permanen" (tidak dimusnahkan) atau "musnah" tetapi dengan pengecualian. Padahal, arsip-arsip tersebut berpotensi mengandung data pribadi pemohon perlindungan ataupun

Saksi dan Korban Nomor 1 Tahun 2024..., Op. Cit., hal. 8.

84 *Ibid.*

85 Saksi pelaku adalah tersangka, terdakwa, atau terpidana yang bekerja sama dengan penegak hukum untuk mengungkap suatu tindak pidana dalam kasus yang sama. Lihat Undang-Undang No. 31 Tahun 2014 *jo*. Undang-Undang No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, Pasal 1 angka 2.

86 Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2024..., Loc. Cit.*

terlindung. Sebagai contoh, LPSK menetapkan status "permanen" terhadap arsip yang berkaitan dengan penerimaan dan penelaahan permohonan perlindungan, padahal jenis arsip ini sangat berpotensi mengandung data pribadi pemohon. Contoh lainnya: arsip terkait administrasi putusan rapat paripurna pimpinan LPSK (baik yang menyatakan menerima atau menolak permohonan perlindungan), ditetapkan berstatus "musnah" kecuali dalam perkara yang berskala nasional, yang mana statusnya ditetapkan menjadi "permanen". Lebih lanjut lagi, terhadap arsip mengenai program perlindungan kepada terlindung (dari tahap persiapan, pelaksanaan, sampai pasca-pelaksanaan perlindungan) juga ditetapkan berstatus "musnah" kecuali dalam perkara yang berskala nasional, yang mana statusnya menjadi "permanen".

Idealnya, setiap jenis arsip LPSK yang mengandung data pribadi harus ditetapkan berstatus "musnah", tanpa ada pengecualian tertentu, ketika masa retensinya habis. Penentuan status "permanen" terhadap jenis arsip yang berisi data pribadi akan membahayakan pemohon perlindungan dan terlindung LPSK. Sebagaimana dijelaskan sebelumnya, penentuan status suatu arsip sebagai "permanen" bukan hanya berarti tidak dimusnahkan, tetapi juga wajib diserahkan kepada lembaga kearsipan. Hal ini berpotensi membuat data pribadi terkait pemohon perlindungan dan terlindung LPSK menjadi terbuka dan diketahui publik apabila mekanisme penyerahan data kepada lembaga kearsipan serta penyimpanannya tidak cukup andal dalam merahasiakan data pribadi.

Pemusnahan data pribadi yang berada di bawah pengendalian LPSK menjadi semakin relevan ketika suatu arsip tergolong sebagai arsip inaktif yang berarti frekuensi penggunaannya telah menurun disebabkan karena program perlindungan telah selesai.[87] Menurut UU Pelindungan Data Pribadi, pengendali data pribadi wajib memusnahkan data pribadi di antaranya ketika data

87 Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 5 Tahun 2020..., Op.Cit.,* Pasal 1 angka 4 dan angka 5. Arsip aktif adalah arsip yang frekuensi penggunaannya tinggi dan/atau terus menerus. Arsip inaktif adalah arsip yang frekuensi penggunaannya telah menurun. Dalam wawancara dengan Sriyana, Sekretaris Jenderal Lembaga Perlindungan Saksi dan Korban, pada hari Senin, 12 Januari 2026, juga dijelaskan lebih lanjut bahwa suatu jenis arsip menjadi inaktif karena perkara terlindung atau program perlindungan bagi terlindung sudah selesai.

tersebut tidak berkaitan dengan penyelesaian proses hukum suatu perkara, selain karena masa retensinya habis. Di sisi lain, LPSK juga perlu memperhatikan mekanisme pemusnahan arsip agar penuh kecermatan dan kehati-hatian sehingga pemusnahan arsip tidak menjadi pintu bagi terbukanya data pribadi dalam arsip tersebut.

4.5. Lembaga Pemasyarakatan

a. Fungsi dan kewenangan

Lembaga Pemasyarakatan (Lapas) merupakan salah satu bagian dari sistem peradilan pidana yang melaksanakan fungsi pemasyarakatan. Lapas adalah lembaga atau tempat yang menjalankan fungsi pembinaan terhadap narapidana berdasarkan Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan ("UU Pemasyarakatan"), yaitu kegiatan yang diselenggarakan untuk meningkatkan kualitas kepribadian dan kemandirian narapidana dan anak binaan. Lapas dibentuk di level kabupaten/kota.[88] Dalam UU Pemasyarakatan, selain Lapas, penyelenggaraan sistem dan fungsi pemasyarakatan juga dilakukan oleh Rumah Tahanan Negara (Rutan), Lembaga Penempatan Anak Sementara (LPAS), Lapas, Lembaga Pembinaan Khusus Anak (LPKA), Balai Pemasyarakatan (Bapas), atau tempat lain yang ditentukan. Penyelenggaraan pembinaan yang dilakukan oleh Lapas seharusnya diatur lebih lanjut dengan peraturan pemerintah. Namun demikian, peraturan turunan untuk melaksanakan teknis UU Pemasyarakatan belum dibentuk, sehingga fungsi tersebut masih merujuk pada aturan turunan Peraturan Pemerintah Nomor 31 Tahun 1999 tentang Pembinaan dan Pembimbingan Warga Binaan Pemasyarakatan.

Pada periode pemerintahan tahun 2024-2029, penyelenggaraan Lapas dilakukan di bawah Direktorat Jenderal Pemasyarakatan Kementerian Imigrasi dan Pemasyarakatan (Ditjen PAS). Kedudukan ini berpindah setelah sebelumnya Ditjen PAS berada di bawah naungan Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham) pada periode pemerintahan sebelumnya. Peralihan ini terjadi karena

88 UU Pemasyarakatan, Pasal 35 ayat (2).

pada pemerintahan tahun 2024-2029, terdapat pemecahan urusan kementerian yang sebelumnya diselenggarakan oleh Kemenkumham, yaitu menjadi Kementerian Hukum, Kementerian Hak Asasi Manusia, dan Kementerian Imigrasi dan Pemasyarakatan berdasarkan Peraturan Presiden Nomor 139 Tahun 2024 tentang Penataan Tugas dan Fungsi Kementerian Negara Kabinet Merah Putih Periode Tahun 2024-2029. Ketiga kementerian tersebut saat ini berada di bawah koordinasi Kementerian Koordinasi Bidang Hukum, HAM, Imigrasi, dan Pemasyarakatan. Oleh karena itu, saat ini ketiga kementerian tersebut, beserta direktorat di bawahnya, tidak terkecuali Ditjen PAS, sedang mengalami proses penyesuaian tata kelola lembaga, sumber daya manusia, dan hukum.

Untuk menilik bagaimana Lapas melakukan pelindungan data pribadi, berikut merupakan peraturan perundang-undangan yang menjadi objek analisis:

1) Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan;
2) Peraturan Pemerintah Nomor 58 Tahun 1999 tentang Syarat-Syarat dan Tata Cara Pelaksanaan Wewenang, Tugas dan Tanggung Jawab Perawatan Tahanan;
3) Peraturan Pemerintah Nomor 57 Tahun 1999 tentang Kerjasama Penyelenggaraan Pembinaan dan Pembimbingan Warga Binaan Pemasyarakatan;
4) Peraturan Pemerintah Nomor 32 Tahun 1999 tentang Syarat dan Tata Cara Pelaksanaan Hak Warga Binaan Pemasyarakatan;
5) Peraturan Pemerintah Nomor 31 Tahun 1999 tentang Pembinaan dan Pembimbingan Warga Binaan Pemasyarakatan;
6) Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 11 Tahun 2025 tentang Rencana Strategis Kementerian Imigrasi dan Pemasyarakatan Tahun 2025-2029;
7) Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 1 Tahun 2025 tentang Pedoman Penyelenggaraan Makanan di Unit Pelaksana Teknis Pemasyarakatan;

8) Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 4 Tahun 2024 tentang Organisasi dan Tata Kerja Kantor Wilayah Direktorat Jenderal Pemasyarakatan;
9) Peraturan Menteri Imigrasi dan Pemasyarakatan Nomor 5 Tahun 2024 tentang Pola Klasifikasi Kantor Wilayah Direktorat Jenderal Pemasyarakatan;
10) Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 8 Tahun 2024 tentang Penyelenggaraan Keamanan dan Ketertiban pada Satuan Kerja Pemasyarakatan;
11) Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 39 Tahun 2016 tentang Sistem *Database* Pemasyarakatan, sebagaimana diubah dengan Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 28 Tahun 2017;
12) Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 35 Tahun 2018 tentang Revitalisasi Penyelenggaraan Pemasyarakatan;
13) Panduan Sistem Database Pemasyarakatan.

Penyelenggaraan pembinaan yang dilakukan oleh Lapas meliputi: (a) penerimaan narapidana; (b) penempatan narapidana; (c) pelaksanaan pembinaan narapidana; (d) pengeluaran narapidana; dan (e) pembebasan narapidana.[89] Pembinaan dilakukan oleh Kepala Lapas yang dapat dibantu oleh Wali Pemasyarakatan.[90] Dalam penerimaan narapidana, Lapas melakukan pemeriksaan keabsahan dokumen dan kondisi kesehatan narapidana. Dokumen yang diperiksa merupakan dokumen terkait penjatuhan hukuman dan masa pembinaan di Lapas, seperti salinan atau petikan putusan pengadilan yang telah berkekuatan hukum tetap, berita acara pelaksanaan putusan, dan berita acara serah terima narapidana.[91] Setelah melakukan proses penerimaan narapidana, Lapas melakukan penempatan narapidana yang dikelompokkan berdasarkan usia dan jenis kelamin, atau alasan lain yang sesuai dengan asesmen risiko dan kebutuhan yang dilakukan oleh asesor pemasyarakatan.[92] Kemudian, narapidana

89 *Ibid.*, Pasal 36 ayat (1).
90 *Ibid.*, Pasal 40.
91 *Ibid.*, Pasal 36 ayat (3).
92 *Ibid.*, Pasal 36 ayat (4).

masuk ke tahapan pembinaan, yang dilakukan berdasarkan hasil penelitian kemasyarakatan[93] yang dilakukan oleh pembimbing kemasyarakatan, yaitu kegiatan pengumpulan, pengolahan, analisis, dan penyajian data yang dilakukan secara sistematis dan objektif, salah satunya untuk kepentingan pembinaan narapidana.

Dalam menjalani masa pembinaan, narapidana diberikan hak untuk keluar dari lapas dan petugas Lapas mendampingi proses pengeluaran narapidana. Alasan-alasan normatif yang memperbolehkan narapidana keluar dalam waktu tertentu, yaitu:

1. perawatan kesehatan;
2. masih ada perkara lain, misalnya menjadi saksi, tersangka, atau terdakwa dalam proses penuntutan dan pemeriksaan di sidang pengadilan;
3. pelaksanaan pembinaan, antara lain asimilasi, cuti mengunjungi keluarga, dan izin keluar dalam rangka pembinaan;
4. terdapat alasan penting lainnya antara lain menjadi wali pernikahan dan/atau menghadiri pernikahan anak yang sah menurut hukum, pembagian warisan, menjenguk keluarga yang sakit keras atau meninggal dunia; dan
5. kondisi darurat antara lain sakit keras, melahirkan, kebakaran, kerusuhan, huru-hara, bencana alam, dan kondisi darurat lainnya yang ditentukan berdasarkan penilaian kepala Lapas.

Selain menyelenggarakan fungsi pembinaan, Lapas juga memberikan perawatan terhadap narapidana, yaitu pemeliharaan kesehatan, rehabilitasi, dan pemenuhan kebutuhan dasar bagi narapidana.[94] Terhadap narapidana yang tergolong sebagai kelompok berkebutuhan khusus, Lapas memberikan perlakuan khusus. Kelompok tersebut terdiri atas anak, anak binaan, perempuan dalam fungsi reproduksi, pengidap penyakit kronis, penyandang disabilitas, dan manusia lanjut usia.[95] Lapas juga melakukan penyelenggaraan pengamanan yang berupa tindakan pencegahan, penindakan, dan pemulihan.

93 *Ibid.*, Pasal 36 ayat (5) dan (6).
94 *Ibid.*, Pasal 60 ayat (1) dan (2).
95 *Ibid.*, Pasal 61 ayat (1) dan ayat (2).

Tindakan pencegahan merupakan upaya untuk mengurangi atau menghilangkan potensi dan ancaman gangguan keamanan dan ketertiban. Petugas Lapas berwenang melakukan pemeriksaan, pengawasan komunikasi, dan tindakan pencegahan lainnya untuk memastikan keamanan dan ketertiban di Lapas.[96] Sementara itu, penindakan merupakan upaya untuk menghentikan, mengurangi, dan melokalisasi gangguan keamanan dan ketertiban, yang mana petugas pemasyarakatan diberikan kewenangan untuk: (a) mengamankan barang terlarang, yaitu barang yang terlarang yang dibawa oleh setiap orang ke dalam Lapas, seperti alat komunikasi, senjata tajam, dan barang terlarang lainnya; (b) menggunakan kekuatan dalam arti mengerahkan daya, potensi, atau kemampuan internal atau eksternal beserta perlengkapan pengamanannya dalam melakukan upaya paksa untuk mencegah, menghambat, menghentikan gangguan keamanan, atau melakukan penilaian terhadap eskalasi gangguan keamanan dan ketertiban sebagai dasar untuk permintaan bantuan; (c) menjatuhkan sanksi; dan (d) menjatuhkan tindakan pembatasan.[97]

Untuk mendukung penyelenggaraan keamanan, petugas pemasyarakatan di pasal Lapas juga berwenang melakukan kegiatan intelijen, berupa pengumpulan informasi intelijen, pengelolaan dan analisis informasi intelijen, penyajian data dan informasi intelijen, dan pertukaran informasi intelijen.[98] Kegiatan intelijen ini dilakukan untuk mendeteksi, mengidentifikasi, dan memberi peringatan dini terhadap ancaman keamanan di lingkungan pemasyarakatan sebagai bahan pertimbangan pengambilan kebijakan.

Dalam melaksanakan fungsi pembinaan, perawatan, dan penyelenggaraan keamanan Lapas, Ditjen PAS berperan sebagai pengendali data pribadi dan Lapas berperan sebagai prosesor data pribadi. Ditjen PAS menentukan tujuan dan kendali pemrosesan data pribadi narapidana untuk tujuan penyelenggaraan fungsi pembinaan, perawatan, dan penyelenggara keamanan di Lapas. Selain itu, Ditjen PAS juga bertanggung jawab atas penyelenggaraan Sistem *Database* Pemasyarakatan (SDP) berdasarkan Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 39 Tahun 2016 tentang Sistem

96 *Ibid.*, Pasal 65.
97 *Ibid.*, Pasal 66.
98 *Ibid.*, Pasal 81.

Database Pemasyarakatan, sebagaimana diubah dengan Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 28 Tahun 2017 ("Permenkumham SDP"), yang meliputi perumusan dan pelaksanaan kebijakan SDP, pengembangan SPD, pengelolaan SDP, pemanfaatan SDP, dan pemeliharaan SDP. Pengelola SDP terdiri atas direktur yang melaksanakan tugas dan fungsi di bidang pengelolaan data dan informasi di bidang pemasyarakatan pada Ditjen Pemasyarakatan, kepala divisi pemasyarakatan pada kantor wilayah, dan kepala unit pelaksana teknis (UPT).[99] Sementara itu, Lapas melakukan kegiatan pemrosesan data pribadi, yang meliputi: (a) pemerolehan dan pengumpulan; (b) pengolahan dan penganalisisan; (c) penyimpanan; (d) perbaikan dan pembaruan; (e) penampilan, pengumuman, transfer, penyebarluasan, atau pengangkatan; dan/atau (f) penghapusan atau pemusnahan data pada tiap fungsi pembinaan, perawatan, dan penyelenggaraan keamanan.

b. Jenis dan proses pengelolaan data

Jenis data yang dikelola Lapas berkaitan dengan penyelenggaraan fungsi pembinaan, fungsi perawatan, dan fungsi pengamanan yang diemban Lapas. Tidak seluruh informasi tentang jenis dan proses pengelolaan data dapat dilitik melalui peraturan perundang-undangan terkait, sebab konteks hukum pelindungan data pribadi di Lapas belum diakomodasikan dalam peraturan perundang-undangan secara khusus. Peraturan turunan untuk melaksanakan teknis UU Pemasyarakatan pun belum dibentuk, sehingga masih merujuk pada aturan turunan Peraturan Pemerintah Nomor 31 Tahun 1999 tentang Pembinaan dan Pembimbingan Warga Binaan Pemasyarakatan; Peraturan Pemerintah Nomor 58 Tahun 1999 tentang Syarat-Syarat dan Tata Cara Pelaksanaan Wewenang, Tugas dan Tanggung Jawab Perawatan Tahanan; Peraturan Pemerintah Nomor 57 Tahun 1999 tentang Kerjasama Penyelenggaraan Pembinaan dan Pembimbingan Warga Binaan Pemasyarakatan; Peraturan Pemerintah Nomor 32 Tahun 1999 tentang Syarat dan Tata Cara Pelaksanaan Hak Warga Binaan Pemasyarakatan, yang disahkan sebelum UU Pemasyarakatan terbaru berlaku. Oleh karena itu, beberapa informasi yang dituliskan

99 Permenkumham SDP, Pasal 9A ayat (1).

di dalam kajian ini berdasarkan pada wawancara ahli dan hasil *focus group discussion* yang dilakukan dengan melibatkan Dirjen PAS, khususnya Direktorat Teknologi Informasi dan Kerja Sama.

Fungsi pembinaan yang dilakukan Lapas, yaitu (a) penerimaan narapidana; (b) penempatan narapidana; (c) pelaksanaan pembinaan narapidana; (d) pengeluaran narapidana; dan (e) pembebasan narapidana. Jenis data tersebut tercantum dalam Tabel 4.3. Pada fungsi perawatan, Lapas mengelola jenis data dalam Tabel 4.4.

Sementara itu, pada fungsi pengamanan, dokumen/informasi yang dikelola dan substansi data pribadi yang terkandung di dalamnya tidak teridentifikasi, baik di dalam peraturan perundang-undangan, panduan Panduan Sistem *Database* Pemasyarakatan, dan aplikasi SDP. Data yang tercantum pada tabel di atas tidak termasuk informasi intelijen yang dikumpulkan, dianalisis, disajikan, dan dipertukarkan oleh petugas Lapas sebagai bentuk kegiatan pendukung untuk penyelenggaraan pengamanan.

Lapas mengelola informasi narapidana dengan tindak pidana yang beragam. Beragamnya jenis tindak pidana tidak menyebabkan perbedaan perlakuan terhadap pengelolaan informasi. Pemberian perlakuan khusus ditujukan pada informasi yang terkait dengan data narapidana anak dan data anak narapidana perempuan. Kedua informasi tersebut menjadi perhatian dan memperoleh perlakuan khusus oleh Ditjen PAS dan Lapas, yaitu data sangat tertutup dan aksesnya ketat.

Pengelolaan data di Lapas mengacu pada UU Keterbukaan Informasi Publik ketimbang berorientasi pada UU Pelindungan Data Pribadi. Pengelolaan data yang dilakukan ditujukan untuk mengelola dan menyediakan informasi terkait narapidana untuk kepentingan publik. Lapas mengelola sistem teknologi informasi pemasyarakatan, yang mencakup pengaturan mengenai kelembagaan, proses bisnis, sumber daya manusia, data, layanan dan aplikasi, infrastruktur, keamanan, audit teknologi informasi, dan pusat data. Informasi pembinaan narapidana disajikan pada sistem teknologi informasi tersebut dan diselenggarakan secara elektronik, melalui Sistem Database Pemasyarakatan (SDP) berdasarkan Permenkumham SDP. SDP dikelola oleh Pusat Data, Informasi, dan Komunikasi Publik Ditjen PAS.

Tabel 4.3. Jenis Data Pembinaan Lapas

No.	Tahap Pembinaan	Dokumen / Informasi yang Dikelola	Substansi Data Pribadi
1.	Penerimaan narapidana	• Salinan atau petikan putusan pengadilan yang telah berkekuatan hukum tetap. • Berita acara pelaksanaan putusan • Berita acara serah terima narapidana • Kondisi kesehatan narapidana yang dibuktikan dengan surat medis dari dokter pemerintah yang menyatakan narapidana dalam kondisi sehat	• Nama lengkap • Alamat • Jenis kelamin • Agama • Status perkawinan dan keluarga • Data dan informasi kesehatan • Data biometrik • Jenis pidana, lama penahanan, dan catatan residivis • Remisi • Data anak
2.	Penempatan narapidana	• Usia dan jenis kelamin • Asesmen risiko dan kebutuhan atau alasan lain sesuai dengan asesmen risiko dan kebutuhan yang dilakukan oleh asesor pemasyarakatan, antara lain meliputi kebutuhan pembinaan narapidana, risiko melarikan diri, risiko berbahaya terhadap orang lain dan kesehatan mental, fisik, dan psikologis narapidana	• Nama lengkap • Jenis kelamin • Data dan informasi kesehatan • Data biometrik
3.	Pelaksanaan pembinaan	• Hasil penelitian kemasyarakatan (litmas) yang disusun oleh pembimbing kemasyarakatan	(tidak teridentifikasi)
4.	Pengeluaran narapidana	• Informasi perawatan kesehatan • Informasi terkait keberadaan perkara lain, misalnya menjadi saksi atau terdakwa dalam proses penuntutan dan pemeriksaan di sidang pengadilan • Informasi pelaksanaan pembinaan, antara lain terkait asimilasi, cuti mengunjungi keluarga, dan izin keluar dalam rangka pembinaan • Informasi terkait alasan penting lainnya, misalnya seperti menjadi wali pernikahan dan/atau menghadiri pernikahan anak yang sah menurut hukum, pembagian warisan, menengok keluarga yang sakit keras atau meninggal dunia • Informasi terkait kondisi darurat, antara lain sakit keras, melahirkan, kebakaran, kerusuhan, huru-hara, bencana alam, dan kondisi darurat lainnya yang ditentukan berdasarkan penilaian kepala Lapas	• Nama lengkap • Alamat • Jenis kelamin • Data dan informasi kesehatan • Data biometrik

No.	Tahap Pembinaan	Dokumen / Informasi yang Dikelola	Substansi Data Pribadi
5.	Pembebasan narapidana	Informasi terkait masa penahanan	• Jenis pidana, lama penahanan, dan catatan residivis • Informasi pembebasan • Informasi pembebasan bersyarat • Remisi

Tabel 4.4. Jenis Data pada Fungsi Perawatan Lapas

No.	Kegiatan Perawatan	Dokumen / Informasi yang Dikelola	Substansi Data Pribadi
1.	Pemeliharaan kesehatan, rehabilitasi, dan pemenuhan kebutuhan dasar bagi narapidana	Informasi yang dikelola dari fungsi pembinaan	• Nama lengkap • Alamat • Jenis kelamin • Data dan informasi kesehatan • Data biometrik • Jenis pidana, lama penahanan, dan catatan residivis

Pada tahap penerimaan narapidana, petugas Lapas melakukan registrasi warga binaan pemasyarakatan (WBP) dengan menginput data pada SDP. Pada sistem tersebut, informasi yang diisi, yaitu:

1. Tanggal penerimaan;
2. Asal instansi;
3. Nomor surat;
4. Tanggal surat;
5. Deskripsi;
6. Identitas pribadi WBP yang meliputi nama, umur, tempat lahir, jenis kelamin;
7. Informasi pelengkap identitas pribadi WBP yang meliputi alamat tempat tinggal, agama, pekerjaan;
8. Informasi pemidanaan yang meliputi perkara/pasal, dasar penahanan/pidana, lama penahanan/pidana;
9. Informasi penahanan/pidana sebelumnya jika WBP adalah residivis, yang meliputi tempat penahanan/pidana sebelumnya,

dasar penahanan/pidana sebelumnya, dan lama penahanan/pidana sebelumnya;
10. Hasil pemeriksaan kesehatan; dan
11. Keterangan.

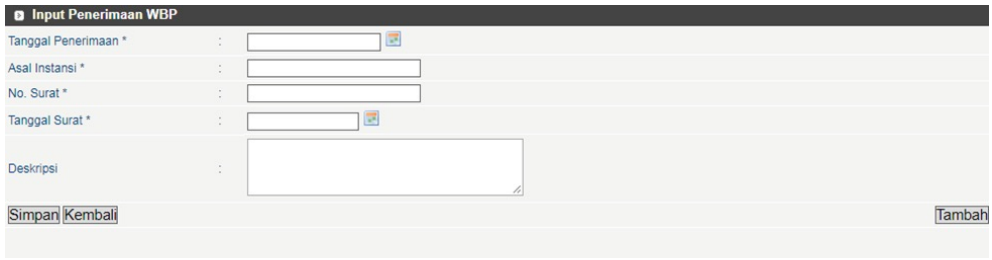
Formulir tersebut dapat dilihat pada Gambar 4.1-4.3.[100]

Pada SDP, dilakukan penyediaan dan pertukaran data yang bersifat terbatas, yaitu memerlukan permohonan akses data dan persetujuan dari pejabat terkait untuk memberikan akses data kepada masyarakat. Data yang dipublikasikan bersifat data agregat, sehingga data pribadi yang menyasar pada informasi identitas tidak dipublikasikan. Namun pada pengelolaan SPD, peraturan perundang-undangan dan panduan pengelolaan SDP tidak memiliki aturan yang memadai tentang pencatatan data yang akurat, penghapusan, dan pemantauan data secara berkala.[101] Tidak terdapat pula pengaturan spesifik mengenai masa retensi informasi pemasyarakatan.

Selain itu, pertukaran data yang dilakukan pada umumnya kepada aparat penegak hukum dan aparat keamanan. Pada wawancara yang dilakukan dengan Peneliti Center for Detention Studies Gatot Goei,[102] pertukaran data tersebut tidak berbasiskan *memorandum of understanding* (MoU) atau perjanjian kerja sama tertentu, meskipun menjadi mandat bahwa pertukaran data dan informasi dapat dilakukan setelah Menteri dengan pimpinan kementerian/lembaga pemerintahan atau lembaga lain menandatangani nota kesepahaman.[103] Namun demikian, mengonfirmasi ke Ditjen PAS, terdapat MoU yang mengikatkan Ditjen PAS dengan aparat penegak hukum dan aparat keamanan, tetapi peneliti tidak mengakses dokumen tersebut. Menurut Ditjen PAS, pada MoU, dicantumkan data-data yang dapat dimanfaatkan kedua belah pihak, klausul untuk saling menjaga kerahasiaan data, dan digitalisasi pertukaran data.

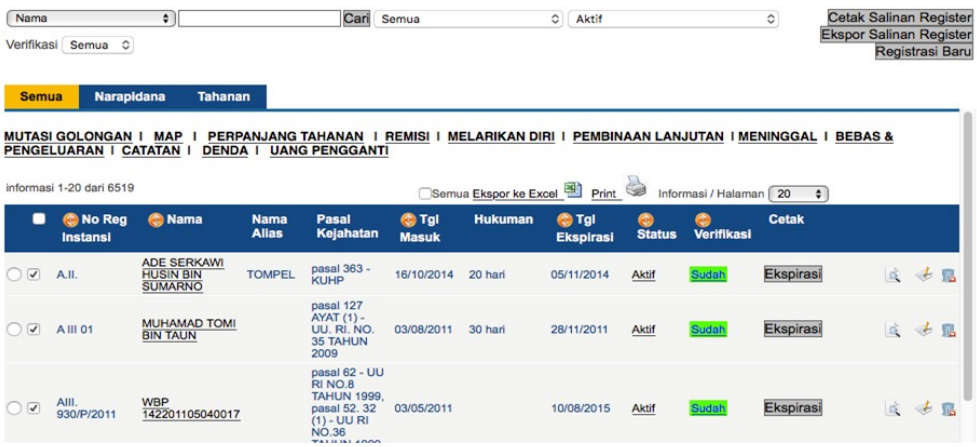
100 Ditjen PAS. (tanpa tahun). *Modul Penggunaan SDP,* diakses melalui https://sdp.ditjenpas.go.id/panduan/Penerimaan2.html , pada 30 Maret 2026.
101 Elisatris Gultom dan Buala Jefry,"Analisis Yuridis Pengelolaan Data Kesehatan: Telaah Aturan SOP Sistem dan Pelayanan Warga Binaan Pemasyarakatan dalam Rangka Pemenuhan UU 27 Tahun 2022", dalam *Jurnal Pendidikan Indonesia,* Vol. 6, No. 5, Mei 2025, hal. 2774.
102 Hasil wawancara dengan Gatot Goei, Peneliti Center for Detention Studies (CDS), pada 19 Januari 2026.
103 Permenkumham SDP, Pasal 12 ayat (2) dan ayat (3).

Gambar 4.1. Formulir Cara Penambahan Data WBP



Gambar 4.2. Formulir Data WBP yang Harus Diinput

Gambar 4.3. Contoh Hasil Penginputan Data



Lembaga penegak hukum yang selama ini bekerja sama melakukan pertukaran data dengan Lapas, di antaranya dan tidak terbatas pada Kepolisian, Kejaksaan, Badan Nasional Penanggulangan Terorisme (BNPT), Detasemen Khusus, Badan Intelijen Negara (BIN), lembaga peradilan, dan Lembaga Perlindungan Saksi dan Korban (LPSK). Pada dasarnya terdapat pula informasi mengenai pembinaan di Lapas yang

diperlukan untuk aktivitas kewargaan, seperti status narapidana untuk kebutuhan kepemiluan, perbankan, pelayanan kesehatan, dan sebagainya. Dirjen PAS melakukan pengintegrasian data tersebut dengan Dirjen Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri, yaitu dengan mempertukarkan informasi nomor induk kependudukan (NIK) dan status narapidana.

c. Tantangan dan Risiko

Tantangan dan risiko yang dihadapi dalam pelindungan data pribadi di Lapas pada dasarnya dapat ditilik melalui aspek *legal structure* (struktur hukum), *legal substance* (substansi hukum), dan *legal culture* (kultur hukum). Pada aspek *legal structure*, tantangan dan risiko yang dihadapi antara lain:

1. secara institusional, terdapat perubahan tata kelola kementerian, yaitu Ditjen PAS saat ini berada di bawah Kementerian Imigrasi dan Pemasyarakatan, yang menyebabkan perlunya dilakukan penyesuaian tata kelola dan sumber daya lembaga, sehingga pengarusutamaan dan pengadopsian UU PDP di internal lembaga tidak menjadi prioritas saat ini. Berdasarkan Peraturan Presiden Nomor 139 Tahun 2024 tentang Penataan Tugas dan Fungsi Kementerian Negara Kabinet Merah Putih Periode Tahun 2024-2029, terjadi pemecahan Kementerian Hukum dan HAM, yaitu menjadi Kementerian Hukum, Kementerian Hak Asasi Manusia, dan Kementerian Imigrasi dan Pemasyarakatan. Momentum ini seyogianya dimanfaatkan sebagai waktu untuk mengarusutamakan dan meningkatkan perspektif pelindungan data pribadi menurut UU PDP yang diinternalisasikan dalam lembaga dan tata kerja Ditjen PAS;
2. secara infrastruktur, Ditjen PAS telah memiliki aplikasi SDP untuk mengintegrasikan informasi pemasyarakatan dari seluruh Lapas di Indonesia. Namun perlu dilakukan peningkatan keamanan dan peningkatan kapasitas aplikasi agar sistem informasi dapat diakses petugas pemasyarakatan dan masyarakat dengan optimal dan menghindari sistem yang *down* atau *inaccessible*.

3. Jumlah lapas/rutan per 2024 adalah 531[104] dan tersebar di seluruh Indonesia termasuk di wilayah yang infrastrukturnya kurang. Jaringan internet oleh karenanya menjadi kendala. Misal yang dialami Lapas Wahai di Maluku Tengah sebelum meningkatkan koneksi internetnya dari terestrial ke satelit. Kepala Urusan Tata Usaha Lapas Wahai mengatakan gangguan jaringan internet belakangan ini cukup menghambat proses pelayanan, baik internal maupun kepada masyarakat. Pelaporan SDP sering terputus, layanan informasi terganggu, bahkan komunikasi administratif menjadi tidak maksimal.[105]
4. Kondisi kelebihan kapasitas atau over capacity di lapas dan rutan yang mencapai 93 persen juga berpengaruh terhadap kinerja. Kapasitas ideal sejumlah 146.260 orang, dipenuhi 281.762 orang.[106] Artinya pekerjaan meningkat dan pengawasan terhadap kerja menjadi lebih banyak. Hal ini tidak saja berpengaruh terhadap kondisi fisik tetapi juga berbagai kerja petugas termasuk terkait pengelolaan dan pengawasan data.

Pada aspek *legal substance*, tantangan dan risiko yang dihadapi, yaitu: terdapat pendekatan *cherry picking* dalam menafsirkan penyediaan data untuk kepentingan publik, dengan membenturkan UU Keterbukaan Informasi Publik dengan UU Pelindungan Data Pribadi. Misal dalam konteks pendaftaran peserta pemilu, informasi tentang status pemidanaan dan status eks-narapidana seringkali tidak dipublikasikan dengan mengedepankan semangat pelindungan data pribadi. Padahal, terdapat kepentingan umum yang dituju untuk memastikan bahwa syarat untuk menjadi peserta pemilu terpenuhi sesuai dengan peraturan perundang-undangan dan konstituen juga terinformasikan secara terbuka dengan status individu peserta pemilu yang hendak berkontestasi pada pemilu tersebut.

104 Kompas, "Lapas di Indonesia "Overcrowded", Kapasitas 140.000, Penghuninya 265.000 Orang", https://nasional.kompas.com/read/2024/06/13/07562511/lapas-di-indonesia-overcrowded-kapasitas-140000-penghuninya-265000-orang.

105 Direktorat Jenderal Pemasyarakatan, "Tantangan Wilayah Terpencil, Lapas Wahai Upgrade Koneksi Internet dari Terestrial ke Satelit",

106 Audrey Santoso, "Kondisi Overcapacity Lapas hingga Rutan di Indonesia Capai 93 Persen", https://news.detik.com/berita/d-8056099/kondisi-overcapacity-lapas-hingga-rutan-di-indonesia-capai-93-persen .

Pada aspek *legal culture*, belum terjadi pembiasaan untuk meningkatkan keamanan dan pelindungan data pribadi narapidana secara institusional, baik di Ditjen PAS maupun di Lapas. Misal transfer data dan informasi tentang data narapidana masih dilakukan melalui medium *WhatsApp* personal petugas pemasyarakatan kepada kementerian/lembaga lain yang membutuhkan data tersebut, mengingat kecepatan dan fleksibilitas transfer data. Selain terdapat pula kasus di mana pemrosesan dan peralihan data dilakukan menggunakan perangkat milik pribadi, bukan perangkat resmi yang disediakan secara khusus oleh Ditjen PAS dan Lapas.

d. Dampak terhadap kelompok rentan

Kelompok rentan yang terpetakan dan perlu diberikan perlakuan khusus di Lapas berdasarkan UU Pemasyarakatan, yaitu anak, anak binaan, perempuan dalam fungsi reproduksi, pengidap penyakit kronis, penyandang disabilitas, dan manusia lanjut usia.[107] Anak dalam hal ini adalah anak dari narapidana perempuan yang dibawa ke dalam Lapas atau yang lahir di Lapas. Anak ini dapat tinggal bersama ibunya dan ditempatkan secara khusus bersama dengan narapidana perempuan tersebut paling lama sampai berusia tiga tahun. Jika anak dari narapidana perempuan merupakan anak yang berkebutuhan khusus, anak dapat ditempatkan pada unit layanan disabilitas. Selain itu, anak narapidana perempuan dapat diberi makanan tambahan atas petunjuk dokter atau ahli gizi.[108] Berdasarkan Sistem Database Pemasyarakatan per tanggal 1 April 2024, jumlah tahanan, Anak, Narapidana, dan Anak Binaan seluruh Indonesia adalah 270.207 orang dengan rincian Tahanan 51.171 orang, Anak 458 orang, Narapidana 216.938 orang, dan Anak Binaan 1.640 orang.[109]

Data narapidana anak dan data anak narapidana perempuan menjadi perhatian khusus dari Ditjen PAS dan Lapas. Akses terhadap

107 UU Pemasyarakatan, Pasal 61 ayat (1) dan ayat (2).

108 *Ibid.*, Pasal 62.

109 *Direktorat Jenderal Pemasyarakatan, "159.557 Narapidana dan Anak Binaan Muslim Terima Remisi dan Pengurangan Masa Pidana Khusus Idulfitri 1445 Hijriah", https://www.ditjenpas.go.id/159557-narapidana-dan-anak-binaan-muslim-terima-remisi-dan-pengurangan-masa-pidana-khusus-idulfitri-1445-hijriah#:~:text=Berdasarkan%20Sistem%20Database%20Pemasyarakatan%20per,dan%20Anak%20Binaan%201.640%20orang.*

data tersebut bersifat tertutup dan ketat. Secara khusus, tantangan dan risiko pelindungan data pribadi yang terpetakan pada bab sebelumnya memiliki dampak pada kelompok rentan tersebut di atas, terutama dalam hal kebocoran dan penyalahgunaan data. Kebocoran dan penyalahgunaan data pribadi tersebut akan memberikan dampak yang lebih berat. Data dan informasi korban kekerasan seksual yang tersebar kemungkinan besar berakibat kepada stigma sosial atau diskriminasi dalam berbagai hal.

e. Kepatuhan terhadap UU PDP

Belum terdapat kepatuhan secara utuh terhadap UU PDP. Secara sumber daya, tidak terdapat jabatan *data privacy officer* (DPO) yang secara khusus melakukan fungsi pelindungan data pribadi. Fungsi ini dilekatkan pada Direktorat Teknologi Informasi dan Kerja Sama pada Ditjen PAS, yang mana memegang kedudukan sebagai pengendali data pribadi. Selain itu, masih di lingkup sumber daya, berdasarkan wawancara bersama Peneliti Center for Detention Studies Gatot Goei, pemrosesan data narapidana dan operator sistem dilakukan oleh tenaga tahanan atau narapidana, bukan petugas pemasyarakatan. Sebab terdapat problem kurangnya sumber daya manusia pada Divisi Registrasi, sehingga Lapas mengkaryakan narapidana. Narapidana diberikan akses terhadap data-data pribadi tahanan lainnya untuk diinput ke sistem, sehingga rawan terjadi kebocoran dan penyalahgunaan data pribadi.[110] Namun demikian, berdasarkan klarifikasi Ditjen PAS, Lapas tidak lagi memanfaatkan narapidana sebagai petugas pemroses data, hal tersebut telah dilakukan sepenuhnya oleh petugas pemasyarakatan. Akan tetapi, penelitian ini belum dapat mengonfirmasi praktik di lapangan secara langsung;

Pada aspek *legal substance*, rangkaian peraturan perundang-undangan dan panduan SDP belum mengakomodasikan orientasi pelindungan data pribadi sejalan dengan UU Pelindungan Data Pribadi. Secara khusus, panduan SDP yang dimiliki Ditjen PAS bersifat pedoman yang menggambarkan alur teknis administratif dan serangkaian formulir untuk penginputan informasi;

Juga belum ada peninjauan rutin terhadap pemrosesan data,

110 Hasil wawancara dengan Gatot Goei..., *Loc. Cit.*

peningkatan keamanan transfer informasi menggunakan kanal resmi dan bukan perangkat personal, dan tidak terdapat kejelasan pengaturan mengenai masa retensi dan penghapusan data.

5

Pengelolaan dan Pertukaran Data dalam Sistem Peradilan Pidana Terpadu

TRANSFORMASI DIGITAL dalam sistem peradilan pidana di Indonesia tidak hanya berlangsung pada tingkat masing-masing institusi, tetapi juga berkembang menuju integrasi lintas lembaga melalui Sistem Peradilan Pidana Terpadu berbasis Teknologi Informasi (SPPT-TI). Sistem ini dirancang untuk meningkatkan koordinasi, efisiensi, dan konsistensi penanganan perkara melalui pertukaran data antar institusi penegak hukum, mulai dari kepolisian, kejaksaan, pengadilan, hingga lembaga pemasyarakatan.

SPPT-TI pada dasarnya lahir sebagai respons atas persoalan klasik dalam sistem peradilan pidana Indonesia, yaitu fragmentasi proses, duplikasi administrasi, serta lambannya alur penanganan perkara akibat tidak terintegrasinya sistem antar lembaga. Dalam konteks tersebut, integrasi data diposisikan sebagai solusi untuk mempercepat proses penegakan hukum, meningkatkan efisiensi birokrasi, serta mengurangi ketergantungan pada dokumen fisik.

Namun demikian, integrasi ini juga membawa konsekuensi mendasar: pengelolaan data pribadi tidak lagi menjadi isu sektoral pada masing-masing lembaga, melainkan menjadi isu sistemik lintas institusi. Dalam konteks ini, risiko pelindungan data tidak hanya muncul dari praktik internal lembaga, tetapi juga dari mekanisme pertukaran, interoperabilitas sistem, dan absennya standar bersama yang mengikat seluruh aktor dalam sistem peradilan pidana.

5.1. Mekanisme Pertukaran Data Antar Lembaga

Secara konseptual, SPPT-TI memfasilitasi pertukaran data perkara secara berkelanjutan sepanjang siklus peradilan pidana. Data yang dikumpulkan pada tahap penyidikan menjadi input bagi proses penuntutan, kemudian digunakan dalam persidangan, dan selanjutnya diteruskan ke tahap pelaksanaan putusan. Alur ini menunjukkan bahwa satu set data pribadi dapat digunakan berulang kali oleh berbagai institusi dengan fungsi yang berbeda.

Dalam praktiknya, mekanisme pertukaran data ini mencakup beberapa karakteristik utama.

Pertama, pertukaran data bersifat berjenjang, mengikuti tahapan proses perkara. Data dari kepolisian menjadi dasar bagi kejaksaan, dan seterusnya. Dalam model ini, kualitas dan kelengkapan data pada tahap awal akan menentukan kualitas data pada tahap berikutnya.

Kedua, terdapat kecenderungan menuju integrasi sistem (*interoperability*), di mana sistem informasi masing-masing lembaga diupayakan untuk saling terhubung. Namun, tingkat integrasi ini belum sepenuhnya seragam. Dalam banyak kasus, pertukaran data masih dilakukan secara semi-digital atau bahkan manual, yang meningkatkan risiko inkonsistensi dan duplikasi data.

Ketiga, pertukaran data tidak selalu terjadi dalam kerangka sistem yang terstandarisasi. Selain melalui SPPT-TI, data juga dapat dipertukarkan melalui mekanisme informal atau ad hoc, seperti permintaan langsung antar institusi atau melalui media komunikasi tertentu. Kondisi ini menunjukkan bahwa SPPT-TI belum sepenuhnya menjadi satu-satunya kanal pertukaran data.

Dari perspektif pelindungan data pribadi, karakteristik tersebut menimbulkan sejumlah implikasi. Tidak adanya standar yang seragam dalam format data, klasifikasi data, maupun protokol pertukaran menyebabkan sulitnya memastikan bahwa data yang dipertukarkan tetap memenuhi prinsip pembatasan tujuan dan minimalisasi data. Selain itu, ketidakterpaduan sistem juga menyulitkan pelacakan (*traceability*) terhadap penggunaan data oleh masing-masing institusi.

Di sisi lain, dorongan untuk efisiensi dan percepatan proses melalui SPPT-TI menciptakan ketegangan dengan prinsip akuntabilitas dalam pengelolaan data pribadi. Semakin cepat dan mudah data dipertukarkan, semakin besar pula potensi hilangnya kontrol terhadap

data tersebut. Dalam konteks ini, efisiensi administratif berpotensi dicapai dengan mengorbankan prinsip-prinsip kehati-hatian dalam pemrosesan data, seperti pembatasan tujuan dan kontrol akses.

Ketegangan ini terlihat, misalnya, dalam praktik kebutuhan "real-time data sharing" antar lembaga, yang sering kali tidak diikuti dengan kejelasan mengenai batasan penggunaan data, mekanisme logging akses, maupun penentuan tanggung jawab apabila terjadi penyalahgunaan. Dengan kata lain, logika integrasi sistem mendorong percepatan, sementara logika pelindungan data menuntut pembatasan dan pengendalian—dua hal yang tidak selalu berjalan seiring.

5.2. Titik Risiko dalam Pengelolaan dan Pertukaran Data

Pengelolaan data dalam SPPT-TI menghadirkan risiko yang bersifat kumulatif, yang muncul di setiap titik dalam alur pertukaran data. Risiko tersebut tidak hanya terkait dengan keamanan teknis, tetapi juga dengan aspek hukum dan tata kelola. Identifikasi risiko tersebut adalah sebagai berikut:

1) Risiko *over-collection* dan *over-sharing*. Dalam praktik, tidak selalu terdapat batasan yang jelas mengenai jenis data yang perlu dibagikan antar lembaga. Akibatnya, data yang dipertukarkan sering kali melampaui kebutuhan spesifik suatu tahap proses. Hal ini bertentangan dengan prinsip minimalisasi data, di mana hanya data yang relevan dan diperlukan yang seharusnya diproses.
2) Risiko penggunaan data di luar tujuan awal pengumpulannya. Data yang dikumpulkan untuk kepentingan penyidikan, misalnya, dapat digunakan kembali untuk tujuan lain tanpa dasar hukum yang jelas. Dalam sistem yang terintegrasi, risiko ini semakin besar karena data tersedia bagi lebih banyak aktor.
3) Risiko inkonsistensi dan inakurasi data. Ketika data dipindahkan dari satu sistem ke sistem lain tanpa mekanisme verifikasi yang memadai, potensi kesalahan meningkat.

Kesalahan ini tidak hanya berdampak administratif, tetapi juga dapat mempengaruhi proses pembuktian dan hak-hak individu yang terlibat dalam perkara.

4) Risiko keamanan dan kebocoran data. Pertukaran data antar sistem memperluas potensi serangan, terutama jika standar keamanan antar lembaga tidak seragam. Kebocoran data dalam satu titik dapat berdampak pada keseluruhan sistem.
5) Risiko akses yang tidak terkendali (*unauthorized access*). Dalam sistem lintas lembaga, penentuan hak akses menjadi lebih kompleks. Tanpa pengaturan yang jelas mengenai siapa yang berhak mengakses data tertentu, terdapat potensi penyalahgunaan oleh pihak internal maupun eksternal.

Selain risiko yang telah diidentifikasi, terdapat risiko tambahan yang bersumber dari desain kelembagaan SPPT-TI itu sendiri. Integrasi sistem mendorong normalisasi pertukaran data secara luas (default sharing), di mana data dianggap sebagai sumber daya bersama antar lembaga. Dalam kondisi ini, batas antara *"need to know"* dan *"nice to know"* menjadi kabur, sehingga membuka ruang bagi praktik akses data yang tidak proporsional.

5.3. Isu Akuntabilitas Lintas Sistem

Salah satu tantangan utama dalam SPPT-TI adalah memastikan akuntabilitas dalam pengelolaan data lintas institusi. Dalam model tradisional, tanggung jawab atas data relatif jelas karena berada dalam satu institusi. Namun, dalam sistem terintegrasi, tanggung jawab menjadi terdistribusi. Beberapa permasalahan akuntabilitas dalam SPPT-TI meliputi hal-hal sebagai berikut:

1) Ketidakjelasan peran sebagai pengendali dan pemroses data. Dalam banyak kasus, setiap institusi dapat bertindak sebagai pengendali sekaligus penerima data. Hal ini menimbulkan pertanyaan mengenai siapa yang bertanggung jawab atas keabsahan, keamanan, dan penggunaan data setelah data tersebut dipertukarkan.
2) Keterbatasan mekanisme audit dan pengawasan. Sistem lintas

lembaga memerlukan mekanisme audit yang mampu melacak aliran data secara *end-to-end*. Namun, dalam praktik, sistem audit seringkali masih bersifat sektoral dan tidak terintegrasi. Akibatnya, sulit untuk menelusuri penggunaan data secara menyeluruh.

3) Ketiadaan standar operasional bersama. Meskipun terdapat kerangka umum melalui SPPT-TI, belum terdapat standar operasional yang mengikat seluruh institusi terkait pengelolaan data pribadi. Perbedaan prosedur internal antar lembaga menciptakan kesenjangan dalam tingkat pelindungan data.
4) Keterbatasan mekanisme pengaduan. Dalam hal terjadi pelanggaran atau kebocoran data, belum terdapat mekanisme yang jelas untuk menentukan tanggung jawab dan memberikan pemulihan kepada subjek data. Hal ini menjadi problematik karena pelanggaran dalam satu titik dapat melibatkan banyak institusi.

Dalam konteks SPPT-TI, isu akuntabilitas menjadi semakin kompleks karena melibatkan banyak aktor dengan kewenangan yang saling bersinggungan. Salah satu aktor kunci dalam koordinasi sistem ini adalah Kementerian Hukum dan HAM, yang selama ini berperan dalam mendorong integrasi sistem, termasuk melalui kebijakan pemasyarakatan dan koordinasi lintas lembaga. Namun, peran koordinatif ini belum selalu diikuti dengan mandat yang jelas dalam pengaturan tata kelola data pribadi lintas sistem.

Ketiadaan satu otoritas yang secara eksplisit bertanggung jawab atas tata kelola data dalam SPPT-TI menimbulkan apa yang dapat disebut sebagai "*diffused accountability*", di mana tanggung jawab tersebar, tetapi tidak ada satu institusi yang secara penuh dapat dimintai pertanggungjawaban. Dalam konteks UU PDP, kondisi ini menjadi problematik karena prinsip akuntabilitas mensyaratkan adanya penanggung jawab yang jelas sebagai pengendali data.

Selain itu, isu penting lain adalah ketiadaan atau keterbatasan pengaturan mengenai perjanjian pertukaran data (data sharing agreements) antar lembaga penegak hukum. Meskipun dalam praktik telah terdapat berbagai bentuk kerja sama dan pertukaran data,

pengaturan tersebut umumnya belum secara eksplisit mengacu pada prinsip-prinsip dalam UU PDP, seperti pembatasan tujuan, jangka waktu penyimpanan, klasifikasi data, serta kewajiban pengamanan. Akibatnya, pertukaran data berlangsung tanpa kerangka kontraktual atau normatif yang cukup untuk menjamin pelindungan data pribadi.

Dalam praktik internasional, pertukaran data lintas otoritas penegak hukum umumnya didasarkan pada instrumen formal yang secara rinci mengatur jenis data yang dipertukarkan, tujuan penggunaan, mekanisme pengamanan, serta tanggung jawab masing-masing pihak. Ketiadaan instrumen semacam ini dalam konteks SPPT-TI menunjukkan adanya kesenjangan antara desain sistem dan standar pelindungan data modern.

Dari analisis di atas, dapat disimpulkan bahwa pengelolaan dan pertukaran data dalam SPPT-TI tidak dapat dipahami semata sebagai persoalan teknis integrasi sistem, melainkan sebagai persoalan tata kelola (governance). Dalam konteks UU PDP, SPPT-TI harus diposisikan sebagai ekosistem pemrosesan data berisiko tinggi, yang memerlukan pendekatan kehati-hatian yang lebih tinggi, termasuk penerapan penilaian dampak pelindungan data dan penguatan prinsip akuntabilitas. SPPT-TI mencerminkan pergeseran mendasar dalam sistem peradilan pidana: dari sistem berbasis dokumen dan institusi menjadi sistem berbasis data dan jaringan. Pergeseran ini membawa potensi peningkatan efisiensi, namun sekaligus memperbesar risiko terhadap pelindungan data pribadi. Tanpa kerangka tata kelola yang jelas dan terintegrasi, sistem yang dirancang untuk memperkuat koordinasi justru berpotensi menciptakan kerentanan baru dalam pelindungan hak individu.

Dengan mempertimbangkan ketegangan antara efisiensi dan akuntabilitas, serta kompleksitas aktor dan mekanisme pertukaran data dalam SPPT-TI, maka penguatan tata kelola pelindungan data tidak dapat dilakukan secara parsial. Diperlukan pendekatan yang secara eksplisit menempatkan pelindungan data pribadi sebagai bagian dari desain sistem, bukan sekadar sebagai aspek kepatuhan tambahan.

Dalam konteks ini, pelaksanaan SPPT-TI memerlukan standar yang lebih ketat, termasuk kejelasan peran pengendali data lintas lembaga, kewajiban perjanjian pertukaran data, serta mekanisme

pengawasan yang independen. Tanpa intervensi tersebut, integrasi sistem berpotensi memperkuat efisiensi administratif, tetapi sekaligus memperbesar risiko pelanggaran hak atas privasi.

6

Analisis Lintas Lembaga dan Problematika Pelindungan Data

TEMUAN DALAM KAJIAN INI menunjukkan bahwa persoalan pelindungan data pribadi dalam sistem peradilan pidana Indonesia tidak dapat dipahami semata-mata sebagai persoalan kepatuhan administratif di tingkat masing-masing lembaga. Persoalan yang muncul justru bersifat struktural: ia terbentuk dari pertemuan antara desain sistem peradilan yang semakin terdigitalisasi, kebutuhan koordinasi lintas lembaga, kerangka regulasi yang belum sepenuhnya harmonis, serta kultur kelembagaan yang masih menempatkan data sebagai instrumen kelancaran proses, bukan sebagai objek tata kelola yang harus dilindungi secara ketat. Temuan ini juga memperlihatkan bahwa implementasi UU PDP dalam sistem peradilan pidana masih berada pada tahap awal, sementara ketergantungan pada data dan integrasi sistem berkembang jauh lebih cepat daripada pembangunan arsitektur pelindungannya.

6.1. Aspek Regulasi dan Kebijakan: Pelindungan Data Masih Terfragmentasi dan Belum Menjadi Titik Tolak Utama

Secara normatif, sistem peradilan pidana Indonesia tidak berangkat dari ruang hampa. Sebelum lahirnya UU PDP, pelindungan atas informasi pribadi telah tersebar di berbagai regulasi sektoral: KUHAP, UU Kepolisian, UU Kejaksaan, UU SPPA, UU LPSK, UU KIP, hingga aturan internal masing-masing lembaga. Namun, pengaturan tersebut lahir dari logika sektoral yang berbeda-beda. Ada yang berangkat dari

pelindungan saksi dan korban, ada yang berangkat dari keterbukaan informasi, ada pula yang berangkat dari kebutuhan pembuktian dan administrasi perkara. Akibatnya, pelindungan data pribadi di sektor peradilan pidana berkembang secara insidental, tidak seragam, dan tidak dibangun dalam satu kerangka konseptual yang utuh.

Temuan paling menonjol dalam assessment ini adalah bahwa orientasi sebagian lembaga masih cenderung KIP-centric, walaupun dalam pelaksanaannya tidak semua lembaga melaksanakan komitmen ini. pelindungan data pribadi lebih sering dipahami sebagai bagian dari pengecualian keterbukaan informasi, bukan sebagai hak substantif yang berdiri sendiri. Dalam kerangka seperti ini, pertanyaan utamanya menjadi: "apakah informasi ini boleh dibuka atau dikecualikan?", bukan "apakah data ini boleh diproses, untuk tujuan apa, oleh siapa, dalam jangka waktu berapa lama, dan dengan pelindungan apa?". Pergeseran cara pandang ini sangat penting, karena UU PDP menuntut agar pelindungan data tidak diposisikan semata-mata sebagai residu dari keterbukaan informasi, melainkan sebagai rezim hukum yang memiliki prinsip dan kewajiban tersendiri.

Meskipun UU PDP telah berlaku penuh sejak 2024, ia belum sepenuhnya menjadi rujukan utama dalam praktik. Hal ini terjadi setidaknya karena tiga sebab. Pertama, belum adanya regulasi turunan dan standar operasional teknis lintas lembaga yang menjembatani prinsip umum dalam UU PDP dengan kebutuhan penegakan hukum yang spesifik. Kedua, adanya kecenderungan untuk menafsirkan pengecualian bagi kepentingan penegakan hukum secara luas, tanpa diikuti dengan perumusan batasan yang rinci. Ketiga, lembaga-lembaga penegak hukum masih lebih familiar bekerja dengan rezim hukum sektoral masing-masing daripada dengan logika baru UU PDP.

Dengan demikian, kesenjangan regulasi yang muncul bukan semata-mata karena tidak adanya aturan, melainkan karena adanya ketidakselarasan antara kerangka normatif umum UU PDP dan regulasi sektoral yang mengatur fungsi-fungsi penegakan hukum secara spesifik. Dalam situasi seperti ini, UU PDP berisiko hanya berfungsi sebagai kerangka deklaratif, sementara praktik sehari-hari tetap ditentukan oleh logika lama kelembagaan.

6.2. Tata Kelola Data dan Akuntabilitas: Data Mengalir, tetapi Tanggung Jawab Tidak Selalu Jelas

Temuan dari kajian kelembagaan menunjukkan bahwa seluruh institusi dalam sistem peradilan pidana yakni kepolisian, kejaksaan, pengadilan, LPSK, dan pemasyarakatan, melakukan pengumpulan, penyimpanan, penggunaan, dan transfer data pribadi dalam skala yang besar. Data tidak berhenti pada satu lembaga, melainkan terus bergerak dari tahap ke tahap: dari penyelidikan dan penyidikan, ke penuntutan, persidangan, pelaksanaan putusan, hingga pemasyarakatan. Dalam konteks SPPT-TI, aliran ini semakin dipercepat melalui integrasi sistem, sinkronisasi dokumen, dan pertukaran elektronik antar institusi. Flowchart SPPT-TI sendiri menunjukkan betapa detail dan berlapisnya data yang dipertukarkan, termasuk identitas lengkap tersangka atau terdakwa, riwayat penahanan, informasi saksi, barang bukti, status penahanan, penetapan pengadilan, hingga data pelaksanaan tahanan dan pemindahan tahanan.

Namun, yang justru belum berkembang sepadan adalah tata kelola atas aliran data tersebut. Dalam banyak kasus, data flow lebih maju daripada data governance. Integrasi dipahami terutama sebagai persoalan konektivitas teknis dan efisiensi alur perkara, bukan sebagai tata kelola yang mensyaratkan kejelasan legal ground, penetapan tujuan, pembatasan akses, pencatatan aktivitas pemrosesan, masa retensi, penghapusan, dan penanganan insiden. Temuan dalam FGD dan workshop mengonfirmasi bahwa pertanyaan-pertanyaan kunci ini kerap tertinggal di belakang kebutuhan untuk memastikan data dapat segera dikirim, dibaca, dan digunakan oleh lembaga lain.[1]

Masalah sentralnya terletak pada akuntabilitas lintas sistem. Dalam sistem yang terintegrasi, menjadi semakin sulit untuk menjawab pertanyaan mendasar: siapa sesungguhnya pengendali data? Apakah lembaga asal yang pertama kali mengumpulkan data? Apakah lembaga yang kemudian memproses dan memanfaatkannya

1 Hal ini disampaikan dalam *Focus Group Discussion* pada tanggal 23 Januari 2026 dan Kegiatan Pengembangan Kapasitas Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia, pada 11-12 Februari 2026, dilaksanakan oleh STHI Jentera dan dihadiri oleh perwakilan lembaga penegak hukum dari Kepolisian, Kejaksaan, Mahkamah Agung, LPSK dan Lembaga Pemasyarakatan.

untuk fungsi yang berbeda? Apakah beberapa lembaga sekaligus bertindak sebagai joint controllers? Hasil diskusi dalam workshop bersama penegak hukum, menunjukkan bahwa bahkan dalam diskusi teknis mengenai ROPA, data sharing, dan transfer, pertanyaan mengenai relasi controller–processor–joint controller masih dipandang sebagai wilayah yang belum jelas dan sangat bergantung pada konteks pemrosesan.[2]

Ketidakjelasan ini bukan masalah teoritis belaka. Ia berimplikasi langsung pada penetapan tanggung jawab apabila terjadi pelanggaran. Ketika data bocor, digunakan untuk tujuan sekunder, atau diakses oleh pihak yang tidak berwenang, sangat mungkin masing-masing lembaga menganggap dirinya hanya menerima, meneruskan, atau memproses dalam rangka tugasnya. Akibatnya, yang muncul adalah pertanggungjawaban yang tersebar (*diffused accountability*): data terus bergerak, tetapi tanggung jawab tersebar dan menjadi kabur.

Situasi ini diperparah oleh ketiadaan instrumen formal yang seharusnya menjadi standar dalam pertukaran data lintas lembaga. Dari diskusi capacity building maupun assessment awal, terlihat bahwa belum terdapat standar minimum lintas lembaga mengenai ROPA, DPIA, data-sharing agreement, retensi, penghapusan data, maupun mekanisme penanganan insiden. Padahal, dalam praktik yang lebih matang, pertukaran data lintas pengendali atau antara pengendali dan prosesor selalu mensyaratkan kejelasan mengenai tujuan, kategori data, standar keamanan, hak audit, retensi, serta kewajiban pemberitahuan jika terjadi insiden. Hasil diskusi dalam workshop bersama penegak hukum, secara eksplisit menekankan pentingnya klausul kontraktual dan hak audit atas vendor atau pihak ketiga, serta menyebut bahwa praktik tersebut bahkan telah menjadi standar di sektor publik seperti Bank Indonesia.[3]

6.3. Tantangan dan Risiko Sistemik: Menyeimbangkan Efisiensi dan Pelindungan

SPPT-TI pada awalnya dikembangkan sebagai solusi atas problem

2 Kegiatan Pengembangan Kapasitas Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia..., *Loc. Cit.*

3 *Ibid.*

klasik sistem peradilan pidana Indonesia: proses yang terfragmentasi, lambat, duplikasi administrasi, ketergantungan pada dokumen fisik, dan lemahnya koordinasi antar lembaga. Dalam logika reformasi administrasi, integrasi data dan interoperabilitas sistem memang menjanjikan efisiensi, konsistensi, dan percepatan. Tidak mengherankan apabila kebijakan pengembangan SPPT-TI lebih dahulu bertumpu pada kebutuhan agar data dapat mengalir dan proses dapat dipercepat.

Akan tetapi, dari perspektif pelindungan data pribadi, desain seperti ini mengandung ketegangan yang inheren. Semakin besar orientasi pada percepatan pertukaran data, semakin besar pula risiko bahwa pembatasan, verifikasi, dan pengendalian dianggap sebagai hambatan administratif. Akibatnya, aspek-aspek seperti pembatasan tujuan, *need-to-know* basis, pengurangan data, klasifikasi sensitivitas, atau logging akses, belum dipertimbangkan dibanding kebutuhan untuk membuat sistem yang mengalir lancar.

Risiko yang timbul bersifat sistemik dan kumulatif. Pertama, terdapat risiko *over-collection* dan *over-sharing*: data yang dikumpulkan dan diteruskan antar lembaga berpotensi melampaui apa yang benar-benar diperlukan pada setiap tahap. Kedua, terdapat risiko penggunaan ulang data untuk tujuan selain tujuan awal pengumpulannya. Ketiga, terdapat risiko *security fragmentation*: standar pengamanan tidak seragam antar lembaga, sehingga titik terlemah dalam sistem dapat menjadi pintu masuk kebocoran. Keempat, dalam hal adanya keterlibatan vendor atau pihak ketiga, maka akan menambah layer risiko baru yang belum selalu diantisipasi oleh lembaga penegak hukum.

Temuan dalam workshop bersama perwakilan penegak hukum, menunjukkan dengan cukup jelas bahwa dalam praktik sehari-hari, pertukaran data masih dapat berlangsung melalui media yang secara prinsip rawan, termasuk pengiriman dokumen melalui aplikasi WhatsApp atau email biasa (bukan email lembaga) dengan alasan kecepatan dan kedaruratan.[4] Praktik-praktik semacam ini memperlihatkan bahwa risiko bukan hanya berada pada desain sistem makro, tetapi juga pada kebiasaan operasional yang berkembang di

4 *Ibid.*

bawah tekanan kebutuhan kerja. Justru di titik-titik "praktis" inilah kebocoran dan penyalahgunaan sering bermula.

Selain itu, perkembangan hukum acara pidana dan pembuktian elektronik memperbesar eksposur risiko ini. Dengan perluasan penggunaan bukti elektronik, digital forensics, metadata, CCTV, rekaman pemeriksaan, hingga potensi penggunaan analitik dan profiling di masa depan, sistem peradilan pidana semakin bergantung pada pemrosesan data yang bersifat sensitif dan berisiko tinggi. Dalam situasi seperti ini, absennya data governance yang kuat bukan sekadar problem administrasi; ia dapat mempengaruhi due process, fairness, dan legitimasi penegakan hukum itu sendiri.

6.4. Dampak terhadap Kelompok Rentan: Tingkat Resiko yang Lebih Besar

Kajian ini juga menunjukkan bahwa dampak kelemahan pelindungan data pribadi tidak dialami secara merata oleh semua subjek data. Anak, korban kekerasan berbasis gender, kelompok minoritas keagamaan, saksi terlindungi, korban tindak pidana seksual, dan warga binaan menanggung risiko yang jauh lebih besar karena sifat data mereka lebih sensitif dan konsekuensi kebocorannya lebih serius.

Dalam konteks korban kekerasan berbasis gender dan anak, pengungkapan identitas bukan hanya melanggar privasi, tetapi dapat menghasilkan stigma sosial, reviktimisasi, tekanan psikologis, dan bahkan ancaman fisik. Di sini, data pribadi tidak lagi hanya sebagai bagian dari "informasi", melainkan menjadi bagian dari struktur kerentanan. Karena itu, kebocoran atau pengungkapan dapat memiliki dampak ganda: merugikan hak atas privasi sekaligus memperburuk posisi korban dalam relasi sosial dan hukum.

Temuan pada LPSK memperlihatkan sensitivitas ini dengan sangat jelas. LPSK pada dasarnya dibangun di atas logika pelindungan kerahasiaan identitas dan keamanan subjek yang dilindungi. Namun, bahkan di lembaga yang secara institusional paling sadar akan pentingnya kerahasiaan ini, masih terdapat tantangan dalam hal pengelolaan dokumen fisik, transfer data ke lembaga lain, absennya mekanisme komplain khusus jika terjadi kebocoran, serta belum

adanya DPIA dan DPO. Ketiadaan DPIA menyebabkan lemahnya identifikasi risiko dan akibatnya kurangnya penerapan mitigasi risiko. Hal ini menunjukkan bahwa jika lembaga yang memiliki orientasi pelindungan kuat saja masih menghadapi kendala, maka risiko di lembaga lain bisa lebih besar.

Hal yang sama berlaku bagi warga binaan. Data tentang identitas, riwayat pidana, kesehatan, pembinaan, hingga status hukum mereka dapat mempengaruhi hak atas reintegrasi sosial setelah menjalani pidana. Jika data tersebut terus beredar tanpa batas retensi yang jelas, maka pemrosesan data tidak lagi berfungsi hanya untuk tujuan pemasyarakatan, tetapi dapat menghambat kesempatan seseorang untuk kembali ke masyarakat.

Dengan demikian, persoalan kelompok rentan tidak dapat diletakkan hanya di bagian "pelindungan khusus" yang terpisah dari isu data. pelindungan data pribadi justru merupakan bagian integral dari pelindungan HAM bagi kelompok rentan. Ketika data bocor, yang terlanggar bukan hanya prinsip keamanan informasi, tetapi juga hak untuk bebas dari diskriminasi, stigma, ancaman, dan kekerasan lanjutan.

6.5. Mekanisme Pengaduan: Belum Ada Mekanisme Khusus

Salah satu temuan penting lainnya adalah lemahnya mekanisme pengaduan dan pemulihan jika terjadi pelanggaran PDP dalam sistem peradilan pidana. Secara umum, lembaga-lembaga penegak hukum belum memiliki prosedur yang jelas dan mudah diakses oleh subjek data untuk:

1) mengetahui bahwa pelanggaran telah terjadi,
2) mengajukan pengaduan,
3) meminta penghentian atau pembatasan pemrosesan,
4) memperoleh perbaikan, penghapusan, atau pemulihan.

Dalam banyak kasus, mekanisme yang tersedia masih bertumpu pada jalur internal kelembagaan, kode etik, atau disiplin pegawai, bukan pada kerangka khusus penanganan pelanggaran data pribadi. Hal

ini menimbulkan dua persoalan. Pertama, subjek data tidak selalu mengetahui ke mana harus mengadu. Kedua, bahkan jika pengaduan diajukan, hasilnya belum tentu memadai untuk memulihkan kerugian yang timbul.

Padahal, dari perspektif HAM, mekanisme pemulihan yang efektif merupakan bagian penting dari pelindungan hak. Literatur yang dirujuk dalam kajian ini menekankan bahwa negara berkewajiban memastikan adanya otoritas dan prosedur yang dapat diakses, cepat, tidak memihak, dan mampu menghentikan pelanggaran yang sedang berlangsung. Dalam konteks sistem peradilan pidana Indonesia, mekanisme seperti itu belum terlihat terbentuk secara spesifik untuk pelanggaran PDP.

Ketiadaan lembaga pengawas PDP yang operasional semakin memperlemah situasi ini. Tanpa otoritas yang memiliki mandat jelas untuk mengawasi, menerima pengaduan, dan memerintahkan tindakan korektif lintas lembaga, maka penanganan pelanggaran cenderung terpecah-pecah menurut yurisdiksi institusi masing-masing. Akibatnya, pelanggaran dalam sistem terintegrasi justru tidak memiliki mekanisme pemulihan yang juga terintegrasi.

6.6. Sintesis: Kesenjangan antara Norma, Desain Sistem, dan Praktik Kelembagaan

Jika seluruh temuan di atas dibaca secara bersama, maka persoalan utama pelindungan data pribadi dalam sistem peradilan pidana Indonesia terletak pada kesenjangan antara norma, desain sistem, dan praktik kelembagaan.

Pada tingkat norma, Indonesia sudah memiliki UU PDP sebagai kerangka hukum umum. Pada tingkat desain sistem, negara telah mendorong digitalisasi dan integrasi data melalui berbagai platform dan mekanisme koordinasi lintas lembaga. Namun, pada tingkat praktik kelembagaan, penerapan prinsip-prinsip PDP masih sangat awal, parsial, dan belum terlembagakan secara kuat. Inilah sebabnya mengapa sistem peradilan pidana Indonesia saat ini dapat dikatakan telah menjadi *data-intensive,* tetapi belum memiliki *data governance architecture* yang sepadan.

Oleh karena itu, inti problematikanya bukan sekadar bahwa terdapat risiko kebocoran atau bahwa beberapa lembaga belum sepenuhnya patuh terhadap UU PDP. Persoalan yang lebih mendasar adalah bahwa reformasi penegakan hukum digital selama ini lebih banyak bergerak dalam logika integrasi dan efisiensi, sementara pelindungan data pribadi, akuntabilitas, dan due process belum dijadikan elemen desain yang setara. Selama kondisi ini belum berubah, maka setiap penguatan integrasi data, betapapun diperlukan untuk efisiensi, akan selalu membawa risiko sistemik terhadap hak atas privasi.

Dalam arti itu, persoalan pelindungan data pribadi dalam sistem peradilan pidana bukan lagi soal teknis semata, melainkan soal bagaimana negara mendefinisikan batas-batas penggunaan kekuasaan dalam era penegakan hukum berbasis data.

7

Rekomendasi Penguatan Tata Kelola Pelindungan Data Pribadi dalam Sistem Peradilan Pidana

BAGIAN INI MENYUSUN REKOMENDASI berdasarkan temuan komprehensif terkait kerangka regulasi, praktik kelembagaan, serta pengelolaan dan pertukaran data dalam sistem peradilan pidana. Analisis sebelumnya menunjukkan bahwa persoalan pelindungan data pribadi tidak berdiri sendiri, melainkan merupakan hasil dari kesenjangan antara norma hukum, desain sistem yang semakin terintegrasi, dan praktik operasional yang belum sepenuhnya menginternalisasi prinsip-prinsip pelindungan data.

Dalam konteks tersebut, rekomendasi ini tidak diarahkan semata pada pemenuhan kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi, tetapi pada penguatan tata kelola secara menyeluruh yang mampu menjawab kompleksitas sistem peradilan pidana berbasis data. Rekomendasi difokuskan pada aspek kebijakan, kelembagaan, dan praktik operasional, dengan mempertimbangkan kebutuhan implementasi yang realistis dan bertahap.

Dengan demikian, bagian ini diharapkan dapat menjadi rujukan awal bagi pengembangan kebijakan dan langkah tindak lanjut, sekaligus menjadi dasar untuk penguatan kapasitas dan koordinasi lintas lembaga dalam membangun sistem peradilan pidana yang tidak hanya efisien, tetapi juga akuntabel dan berorientasi pada pelindungan hak asasi manusia.

1) **Penetapan kerangka standar minimum lintas lembaga**
   Temuan menunjukkan bahwa pelindungan data pribadi dalam sistem peradilan pidana masih berkembang secara

sektoral dan belum memiliki standar minimum yang berlaku lintas institusi. Dalam praktik, masing-masing lembaga mengembangkan pendekatan sendiri, sehingga menghasilkan variasi tingkat pelindungan, ketidakjelasan tanggung jawab, dan risiko inkonsistensi dalam pertukaran data.

Dalam konteks ini, diperlukan penetapan kerangka standar minimum yang bersifat lintas lembaga sebagai baseline tata kelola. Standar ini tidak dimaksudkan untuk menggantikan pengaturan sektoral, melainkan sebagai rujukan bersama yang memastikan bahwa seluruh institusi dalam sistem peradilan pidana beroperasi dalam prinsip yang sama, khususnya terkait dasar pemrosesan data, pembatasan tujuan, retensi, keamanan, dan akuntabilitas. Keberadaan standar minimum ini juga penting untuk menjembatani kesenjangan antara kerangka normatif UU PDP dan praktik operasional yang saat ini masih terfragmentasi.

2) **Pergeseran paradigma dari keterbukaan menuju keseimbangan dengan pelindungan data**

Assessment menunjukkan bahwa orientasi kelembagaan masih didominasi oleh pendekatan keterbukaan informasi (KIP-centric), dimana pelindungan data pribadi cenderung diposisikan sebagai pengecualian, bukan sebagai prinsip dasar yang setara.

Ke depan, diperlukan pergeseran paradigma menuju pendekatan yang menempatkan pelindungan data pribadi sebagai bagian integral dari tata kelola peradilan yang adil dan berbasis hak asasi manusia. Pergeseran ini tidak berarti mengurangi prinsip keterbukaan peradilan, tetapi menuntut adanya keseimbangan yang lebih proporsional antara transparansi dan pelindungan individu. Dalam praktiknya, hal ini perlu diterjemahkan ke dalam kebijakan internal, pedoman publikasi informasi, serta praktik sehari-hari aparat penegak hukum, sehingga pelindungan data tidak lagi bersifat reaktif, melainkan terintegrasi sejak awal dalam desain proses.

3) **Penataan tata kelola pertukaran data dalam sistem peradilan pidana**

Risiko paling signifikan teridentifikasi pada titik pertukaran dan integrasi data antar lembaga, terutama dalam konteks sistem seperti SPPT-TI. Ketidakjelasan mengenai siapa yang bertindak sebagai pengendali data, serta tidak adanya mekanisme formal dalam pertukaran data, membuka ruang bagi praktik yang tidak terkontrol.

Oleh karena itu, penguatan tata kelola pertukaran data menjadi prioritas. Yang dibutuhkan bukan sekadar peningkatan aspek teknis integrasi sistem, melainkan kejelasan kerangka tata kelola yang mengatur hubungan antar lembaga dalam pemrosesan data. Hal ini mencakup penegasan peran dan tanggung jawab masing-masing institusi, pembatasan tujuan penggunaan data, serta mekanisme akuntabilitas dalam setiap alur pertukaran data. Tanpa penataan ini, efisiensi integrasi justru berpotensi memperbesar risiko pelanggaran.

4) **Penguatan akuntabilitas kelembagaan dalam pengelolaan data**

Temuan menunjukkan bahwa praktik pengelolaan data masih minim dokumentasi, belum berbasis pada pemetaan alur data yang jelas, serta belum didukung oleh mekanisme penilaian risiko yang sistematis.

Dalam konteks ini, penguatan akuntabilitas kelembagaan menjadi kunci. Setiap institusi perlu mulai membangun pemahaman yang lebih sistematis mengenai bagaimana data dikumpulkan, digunakan, disimpan, dan dibagikan dalam siklus peradilan pidana. Pendekatan ini penting untuk memastikan bahwa pemrosesan data tidak hanya sah secara hukum, tetapi juga dapat dipertanggungjawabkan secara administratif dan operasional. Penguatan akuntabilitas ini juga menjadi prasyarat bagi pengawasan yang efektif, baik internal maupun eksternal.

5) **Pengembangan mekanisme penanganan insiden dan pengaduan**

Salah satu kesenjangan penting yang teridentifikasi adalah ketiadaan mekanisme yang jelas untuk menangani insiden kebocoran data serta terbatasnya akses masyarakat terhadap mekanisme pengaduan.

Dalam sistem yang semakin berbasis data, insiden kebocoran bukan lagi kemungkinan yang bersifat hipotetis, melainkan risiko nyata yang harus diantisipasi. Oleh karena itu, setiap lembaga perlu memiliki mekanisme yang jelas untuk merespons insiden, termasuk prosedur pelaporan, penanganan, dan pemulihan. Di sisi lain, keberadaan mekanisme pengaduan juga penting untuk memastikan bahwa subjek data memiliki akses terhadap pelindungan dan pemulihan haknya. Tanpa mekanisme ini, prinsip akuntabilitas dalam UU PDP sulit diwujudkan dalam praktik.

6) **Prioritisasi pelindungan kelompok rentan**

Assessment menunjukkan bahwa dampak pelanggaran data tidak terdistribusi secara merata, melainkan cenderung lebih berat bagi kelompok rentan, seperti anak, korban tindak pidana yang berasal dari kelompok rentan, kelompok minoritas keagamaan, saksi, dan warga binaan.

Dalam konteks ini, pelindungan data pribadi perlu dirancang secara diferensial, dengan memberikan perhatian khusus pada kelompok-kelompok tersebut. pelindungan tidak cukup hanya bersifat umum, tetapi harus mempertimbangkan kerentanan spesifik yang dapat memperbesar risiko stigmatisasi, reviktimisasi, atau bahkan ancaman terhadap keselamatan. Pendekatan ini sejalan dengan kerangka hak asasi manusia yang menempatkan pelindungan kelompok rentan sebagai prioritas dalam kebijakan publik.

7) **Penguatan praktik operasional dalam penggunaan dan pengamanan data**

Temuan empiris menunjukkan bahwa sebagian risiko tidak hanya berasal dari desain sistem, tetapi juga dari praktik operasional sehari-hari, seperti penggunaan kanal komunikasi yang tidak aman atau pengelolaan dokumen fisik yang belum terstandarisasi.

Hal ini menunjukkan bahwa penguatan pelindungan data tidak dapat hanya bergantung pada regulasi atau sistem teknologi, tetapi juga memerlukan perubahan praktik kerja. Dengan demikian, diperlukan upaya untuk membangun

standar praktik operasional yang lebih aman dan konsisten, yang dapat diterapkan dalam kegiatan sehari-hari aparat penegak hukum. Perubahan pada level ini sering kali menjadi faktor penentu dalam efektivitas implementasi kebijakan.

8) **Penguatan kapasitas dan penataan peran SDM dalam pengelolaan data**

Temuan menunjukkan bahwa pengelolaan data dalam sistem peradilan pidana masih bergantung pada praktik individual tanpa didukung oleh penetapan peran yang jelas maupun kapasitas yang memadai.

Ke depan, setiap lembaga perlu menetapkan secara eksplisit fungsi atau petugas yang bertanggung jawab atas pengelolaan dan pemrosesan data pribadi, disertai mandat dan tanggung jawab yang jelas dalam struktur organisasi termasuk penunjukan PPDP/DPO. Dalam konteks pertukaran data lintas lembaga, juga diperlukan titik kontak yang terdefinisi untuk memastikan koordinasi dan akuntabilitas dalam alur data, terutama dalam sistem seperti SPPT-TI.

Di sisi lain, peningkatan kapasitas SDM menjadi prasyarat penting. Penguatan tidak hanya bersifat konseptual, tetapi perlu diarahkan pada pemahaman praktis yang relevan dengan tugas sehari-hari, sehingga prinsip pelindungan data dapat terinternalisasi dalam praktik operasional. Dengan demikian, penguatan SDM menjadi bagian integral dari upaya membangun tata kelola pelindungan data yang efektif dan berkelanjutan.

9) **Penguatan koordinasi dan kelembagaan pengawasan**

Ketiadaan mekanisme koordinasi lintas lembaga yang terstruktur serta belum optimalnya fungsi pengawasan menjadi salah satu hambatan dalam penguatan tata kelola PDP.

Dalam konteks ini, diperlukan penguatan koordinasi kelembagaan, baik melalui forum lintas lembaga maupun melalui peran otoritas pengawas pelindungan data. Koordinasi ini penting untuk memastikan konsistensi kebijakan, pertukaran praktik baik, serta penyelesaian isu yang bersifat

lintas institusi. Tanpa mekanisme koordinasi yang memadai, upaya penguatan akan cenderung berjalan parsial dan tidak berkelanjutan.

10) **Integrasi pelindungan data dalam agenda reformasi peradilan digital**

Digitalisasi sistem peradilan pidana berkembang lebih cepat dibandingkan dengan penguatan tata kelola pelindungan data.

Dalam situasi ini, terdapat risiko bahwa efisiensi dan inovasi teknologi justru tidak diimbangi dengan pelindungan yang memadai terhadap hak individu. Oleh karena itu, pelindungan data pribadi perlu diintegrasikan sebagai bagian dari agenda reformasi peradilan digital. Integrasi ini menuntut agar setiap pengembangan sistem tidak hanya mempertimbangkan aspek fungsional dan efisiensi, tetapi juga implikasi terhadap pelindungan data. Dengan demikian, digitalisasi dapat berjalan seiring dengan penguatan akuntabilitas dan pelindungan hak asasi manusia.

Secara keseluruhan, rekomendasi ini menunjukkan bahwa tantangan utama dalam pelindungan data pribadi dalam sistem peradilan pidana bukan terletak pada ketiadaan kerangka hukum, melainkan pada kesenjangan antara norma dan praktik. Sistem peradilan pidana Indonesia telah menjadi sistem yang sangat bergantung pada data, namun belum sepenuhnya didukung oleh tata kelola yang sepadan.

Dengan demikian, arah penguatan ke depan perlu difokuskan pada pembangunan kerangka lintas lembaga, internalisasi prinsip pelindungan data dalam praktik operasional, serta penguatan akuntabilitas kelembagaan. Pendekatan ini diharapkan dapat mendorong transformasi menuju sistem peradilan pidana yang tidak hanya efisien, tetapi juga menjunjung tinggi pelindungan hak asasi manusia dalam era digit

8

Kesimpulan dan Penutup

TRANSFORMASI DIGITAL dalam sistem peradilan pidana Indonesia telah menghasilkan perubahan mendasar dalam cara data dikumpulkan, diproses, dan dipertukarkan. Sistem ini kini berkembang menjadi ekosistem yang sangat bergantung pada data (data-intensive), dengan aliran informasi yang melibatkan berbagai institusi penegak hukum secara simultan. Namun demikian, temuan penelitian ini menunjukkan bahwa perkembangan tersebut belum diimbangi dengan arsitektur tata kelola pelindungan data yang memadai.

Secara konseptual, Indonesia telah memiliki kerangka hukum melalui Undang-Undang Pelindungan Data Pribadi. Selain itu, berbagai inisiatif integrasi sistem, seperti SPPT-TI, menunjukkan komitmen negara untuk meningkatkan efisiensi dan koordinasi lintas lembaga. Akan tetapi, pada tingkat implementasi, pelindungan data pribadi masih bersifat parsial, sektoral, dan belum terlembagakan secara sistematis. Kesenjangan antara norma, desain sistem, dan praktik kelembagaan menjadi persoalan utama yang menghambat terwujudnya tata kelola data yang akuntabel.

Dalam praktiknya, pendekatan reformasi penegakan hukum masih didominasi oleh logika efisiensi dan integrasi data, sementara aspek pelindungan data pribadi, akuntabilitas, dan jaminan due process belum menjadi bagian integral dari desain sistem. Akibatnya, integrasi data yang semakin luas berpotensi memperbesar risiko pelanggaran hak atas privasi secara sistemik, terutama dalam konteks pertukaran data lintas lembaga dan pemrosesan data berisiko tinggi.

Lebih jauh, penelitian ini juga menunjukkan bahwa persoalan pelindungan data tidak semata-mata bersifat teknis, melainkan berkaitan erat dengan cara negara mendefinisikan dan membatasi penggunaan kekuasaan dalam era digital. Tanpa adanya standar minimum lintas lembaga, kejelasan peran dan tanggung jawab, serta mekanisme pengawasan yang efektif, sistem yang ada berpotensi menghasilkan ketidakpastian hukum, inkonsistensi pelindungan, dan kerentanan bagi kelompok rentan.

Oleh karena itu, penguatan pelindungan data pribadi dalam sistem peradilan pidana memerlukan pergeseran paradigma. pelindungan data tidak dapat lagi diposisikan sebagai aspek tambahan, tetapi harus menjadi bagian inheren dari desain dan operasional sistem penegakan hukum. Hal ini mencakup pembentukan standar bersama lintas institusi, penguatan kapasitas kelembagaan, serta pengembangan mekanisme akuntabilitas yang mampu menjawab kompleksitas pertukaran data di era digital.

Sebagai penutup, penelitian ini menegaskan bahwa keberhasilan reformasi sistem peradilan pidana berbasis teknologi tidak hanya diukur dari peningkatan efisiensi, tetapi juga dari sejauh mana sistem tersebut mampu menjaga keseimbangan antara kepentingan penegakan hukum dan pelindungan hak atas privasi. Dengan demikian, agenda ke depan bukan hanya mempercepat digitalisasi, melainkan memastikan bahwa transformasi tersebut berlangsung dalam kerangka tata kelola yang adil, akuntabel, dan berorientasi pada pelindungan hak asasi manusia.

Daftar Pustaka

Buku, Jurnal, dan Hasil/Laporan Penelitian

Gultom, Elisatris dan Buala Jefry. (2025). *Analisis Yuridis Pengelolaan Data Kesehatan: Telaah Aturan SOP Sistem dan Pelayanan Warga Binaan Pemasyarakatan dalam Rangka Pemenuhan UU 27 Tahun 2022*. Jurnal Pendidikan Indonesia, Vol. 6, No. 5

Kementerian Koordinator Bidang Politik dan Keamanan RI. (2025). *Buku Pedoman Pertukaran dalam Rangka Pelaksanaan Sistem Peradilan Pidana Terpadu Berbasis Teknologi Informasi Versi 2024*. Jakarta: Kementerian Koordinator Bidang Politik dan Keamanan RI

Munthe, Saut Erwin Hartono A. (2025). *Rekonstruksi Regulasi Perlindungan Hukum terhadap Kerahasiaan Keterangan Anak yang Berkonflik dengan Hukum Secara Elektronik Berbasis Nilai Keadilan. Disertasi. Semarang: Universitas Islam Sultan Agung*

Sihombing, Uli Parulian Sihombing, dkk. (2008). *Menggugat Bakor Pakem Kajian Hukum Terhadap Pengawasan Agama dan Kepercayaan di Indonesia. Jakarta: The Indonesian Legal Resource Center*

Peraturan Perundang-undangan

Indonesia, *Undang-Undang Dasar Negara Republik Indonesia 1945*

Indonesia, *Undang-Undang No. 13 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang No. 31 Tahun 2014 tentang Pelindungan Saksi dan Korban*

Indonesia, *Undang-Undang No. 22 tahun 2022 tentang Pemasyarakatan*

Indonesia, *Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi*

Indonesia, *Undang-Undang No. 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana (KUHP*)

Indonesia, *Undang-Undang No. 20 Tahun 2025 tentang Kitab Undang-undang Hukum Acara Pidana (KUHAP)*

Mahkamah Agung, *Surat Keputusan Ketua MA (SK KMA) No. 144/KMA/SK/VIII/2007 yang terakhir kalinya diubah dengan SK KMA No. 2-144/KMA/SK/VIII/2022 tentang Standar Pelayanan Informasi Publik di Pengadilan*

Mahkamah Agung, *Surat Keputusan Ketua Mahkamah Agung No. 269/KMA/SK/XII/2018 tentang Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Mahkamah Agung dan Badan Peradilan yang Berada di Bawahnya*

Mahkamah Agung, *Surat Keputusan Ketua Mahkamah Agung No. 239/KMA/SK/VIII/2022 tentang Petunjuk Teknis Administrasi Perkara Pidana Terpadu Secara Elektronik*

Kementerian Hukum dan HAM, *Peraturan Menteri Hukum dan Hak Asasi Manusia No. 39 Tahun 2016 sebagaimana diubah dengan Peraturan Menteri Hukum dan Hak Asasi Manusia No. 28 Tahun 2017 tentang Sistem Database Pemasyarakatan*

Kepolisian Republik Indonesia, *Peraturan Kepala Kepolisian Negara Republik Indonesia No. 6 Tahun 2019 tentang Penyidikan Tindak Pidana*

Kepolisian Republik Indonesia, *Peraturan Kepala Kepolisian Negara Republik Indonesia No. 1 Tahun 2024 tentang Penyelenggaraan Pusat Informasi kriminal Nasional*

Kepolisian Republik Indonesia, *Peraturan Kepala Badan Reserse Kriminal Polri No. 1 Tahun 2022 tentang Standar Operasional Prosedur Pelaksanaan Penyidikan Tindak Pidana*

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 2 Tahun 2011 tentang Standar Operasional Prosedur Pelayanan Informasi Publik di Lingkungan Lembaga Perlindungan Saksi dan Korban*

Lembaga Perlindungan Saksi dan Korban, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 2 Tahun 2020 tentang Permohonan Perlindungan Saksi dan/atau Korban Tindak Pidana*

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 5 Tahun 2020 tentang Jadwal Retensi Arsip di Lingkungan Lembaga Perlindungan Saksi dan Korban*

Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 5 Tahun 2020*

tentang Jadwal Retensi Arsip di Lingkungan Lembaga Perlindungan Saksi dan Korban

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Sekretaris Jenderal Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2021 tentang Organisasi dan Tata Kerja Sekretariat Jenderal Lembaga Perlindungan Saksi Dan Korban*

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2022 tentang Pemberian Perlindungan kepada Saksi dan/atau Korban*

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban No. 1 Tahun 2024 tentang Standar Pelayanan di Lingkungan Lembaga Perlindungan Saksi dan Korban*

Lembaga Perlindungan Saksi dan Korban RI, *Lampiran Peraturan Lembaga Perlindungan Saksi dan Korban No. 1 Tahun 2024 tentang Standar Pelayanan di Lingkungan Lembaga Perlindungan Saksi dan Korban*

Lembaga Perlindungan Saksi dan Korban RI, *Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 1 Tahun 2026 tentang Sidang Mahkamah Pimpinan Lembaga Perlindungan Saksi dan Korban*

The European Parliament and the Council of the European Union. (2016). *the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (EU GDPR). Regulation (EU) 2016/679

Internet

_____. https://www.gov.uk/data-protection

_____. https://www.lpsk.go.id/profile/about

_____. https://www.lpsk.go.id/informasi-pelayanan/penerimaan-permohonan

_____.https://putusan3.mahkamahagung.go.id/

_____. https://sdp.ditjenpas.go.id/panduan/Penerimaan2.html

BBC. *BPJS Kesehatan: Data ratuasan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar.* Diakses dari https://www.bbc.com/indonesia/indonesia-57196905

CNBC Indonesia. *Hacker 16 Tahun Bobol Database Kejagung, Motifnya Iseng!*. Diakses dari https://www.

cnbcindonesia.com/tech/20210219202546-37-224785/hacker-16-tahun-bobol-database-kejagung-motifnya-iseng

Direktorat Jenderal Pemasyarakatan. *Tantangan Wilayah Terpencil, Lapas Wahai Upgrade Koneksi Internet dari Terestrial ke Satelit.* Diakses dari https://www.ditjenpas.go.id/tantangan-wilayah-terpencil-lapas-wahai-upgrade-koneksi-internet-dari-terestrial-ke-satelit

Direktorat Jenderal Pemasyarakatan. *159.557 Narapidana dan Anak Binaan Muslim Terima Remisi dan Pengurangan Masa Pidana Khusus Idulfitri 1445 Hijriah*. Diakses dari https://www.ditjenpas.go.id/159557-narapidana-dan-anak-binaan-muslim-terima-remisi-dan-pengurangan-masa-pidana-khusus-idulfitri-1445-hijriah#:~:text=Berdasarkan%20Sistem%20Database%20Pemasyarakatan%20per,dan%20Anak%20Binaan%201.640%20orang

Kejaksaan. Tingkatkan pelindungan *Data Pribadi, JAM DATUN Adakan Pelatihan dan Sertifikasi Data Protection Officer.* Diakses dari https://www.kejaksaan.go.id/conference/news/1839/read

Komdigi. *Polri Gunakan Teknologi Face Recognition untuk Pengamanan di PON Aceh-Sumut*. Diakses dari https://www.komdigi.go.id/berita/artikel-gpr/detail/polri-gunakan-teknologi-face-recognition-untuk-pengamanan-di-pon-aceh-sumut

Kompas. *Lapas di Indonesia "Overcrowded", Kapasitas 140.000, Penghuninya 265.000 Orang.* Diakses dari https://nasional.kompas.com/read/2024/06/13/07562511/lapas-di-indonesia-overcrowded-kapasitas-140000-penghuninya-265000-orang.

Kumparan. *Pakar Hukum: Tak Bisa Polisi Tetapkan Tersangka Hanya Pakai Face Recognition*. Diakses dari https://kumparan.com/kumparannews/pakar-hukum-tak-bisa-polisi-tetapkan-tersangka-hanya-pakai-face-recognition-1xt8l2EQ40V

Munawaroh, Nafiatul. *Tanggung Jawab BPJS atas Kebocoran Data Pribadi Pesertanya*. Diakses dari https://www.hukumonline.com/klinik/a/tanggung-jawab-bpjs-atas-kebocoran-data-pribadi-pesertanya-lt6389d13f91363/

Nurhadi, M. *Soroti Dugaan Kebocoran Data Kemenkes, Pakar Singgung Ancaman Foto Medis Pasien*. Diakses dari https://www.suara.com/bisnis/2022/01/07/112835/

soroti-dugaan-kebocoran-data-kemenkes-pakar-singgung-ancaman-foto-medis-pasien

Octavia, Shela dan Danu Damarjati. *MoU Penyadapan dengan 4 Provider Disoal, Kejagung Jamin Tak Sembarangan*. Diakses dari https://nasional.kompas.com/read/2025/06/26/20514751/mou-penyadapan-dengan-4-provider-disoal-kejagung-jamin-tak-sembarangan

Santoso, Audrey. *Kondisi Overcapacity Lapas hingga Rutan di Indonesia Capai 93 Persen*. Diakses dari https://news.detik.com/berita/d-8056099/kondisi-overcapacity-lapas-hingga-rutan-di-indonesia-capai-93-persen

Tempo. *Antisipasi Kendaraan Tanpa Pelat, Polri Terapkan Face Recognition untuk Tilang Elektronik*. Diakses dari https://www.tempo.co/arsip/antisipasi-kendaraan-tanpa-pelat-polri-terapkan-face-recognition-untuk-tilang-elektronik-261554

Tribrata. *Polri Terapkan Teknologi Face Recognition Dalam Pengamanan KTT G20*. Diakses dari https://tribratanews.polri.go.id/blog/none-22/polri-terapkan-teknologi-face-recognition-dalam-pengamanan-ktt-g20-51245

Sumber-sumber Lainnya

Focus Group Discussion (FGD) pada tanggal 23 Januari 2026

Hasil wawancara dengan Gatot Goei, Peneliti Center for Detention Studies (CDS), pada 19 Januari 2026

Hasil wawancara dengan Sriyana, Sekretaris Jenderal Lembaga Pelindungan Saksi dan Korban, pada 12 Januari 2026.

Kegiatan Pengembangan Kapasitas Pelindungan Data Pribadi dalam Sistem Peradilan Pidana Indonesia yang dilaksanakan oleh STHI Jentera dan dihadiri oleh perwakilan lembaga penegak hukum dari Kepolisian, Kejaksaan, Mahkamah Agung, LPSK dan Lembaga Pemasyarakatan, pada 11-12 Februari 2026

SEKOLAH TINGGI HUKUM
INDONESIA JENTERA

PSHK
Pusat Studi Hukum &
Kebijakan Indonesia

L e I P