

BAB 2

GAMBARAN UMUM PELEMBAGAAN PELINDUNGAN DATA PRIBADI DI SEKTOR TELEKOMUNIKASI

2.1 Sektor Telekomunikasi dan Data Pribadi di Indonesia

Sektor telekomunikasi di Indonesia mengalami pertumbuhan yang cepat dalam sepuluh tahun terakhir, dengan jangkauan jaringan seluler yang semakin luas dan tingginya penggunaan layanan data digital. Ini terlihat dari statistik resmi yang menunjukkan bahwa mayoritas penduduk Indonesia aktif menggunakan ponsel dan internet, dengan tingkat adopsi internet mencapai sekitar 72,78% pada tahun 2024, yang menandakan peningkatan akses digital di kalangan masyarakat. Selain itu, lebih dari 68% populasi Indonesia menggunakan telepon seluler, menandakan bahwa layanan mobile telah menjadi elemen penting dalam kehidupan modern di negara ini (Badan Pusat Statistik, 2025, hlm. 27, 39).

Kondisi ini sejalan dengan nilai Indeks Masyarakat Digital Indonesia (IMDI) yang terus meningkat setiap tahunnya. Pada tahun 2022, skor nasional bermula di angka 37,80 dan terus mengalami peningkatan hingga mencapai skor 44,53 pada tahun 2025. Kenaikan rata-rata tahunan ini mencerminkan adanya upaya masif dalam pemerataan akses internet dan peningkatan literasi digital di berbagai wilayah Indonesia. Meskipun secara standar, skor tersebut masih berada di bawah angka 50. Kenaikan menunjukkan bahwa kesiapan masyarakat dalam mengadopsi teknologi digital semakin matang seiring berjalannya waktu (Komdigi, 2025).

Tabel 2.1 Skor Indeks Masyarakat Digital Indonesia (IMDI): Nasional vs DKI Jakarta (2022-2025)

Tahun	Perolehan Skor Indeks Masyarakat Digital Indonesia (IMDI)	
	Indonesia	Provinsi DKI Jakarta
2022	37,80	47,78
2023	43,18	49,15
2024	43,34	50,50
2025	44,53	56,97

Sumber: Dashboard IMDI 2022, Dashboard IMDI 2023, Dashboard IMDI 2024, GoodStats 2025

Berdasarkan data pada tabel di atas, Provinsi DKI Jakarta secara konsisten mencatat perolehan skor yang jauh melampaui jumlah rata-rata nasional. Pada tahun 2024, DKI Jakarta mencapai skor 50,50 dan mengalami lonjakan signifikan menjadi 56,97 pada tahun 2025. Dominasi skor ini memposisikan Jakarta sebagai wilayah dengan kesiapan digital tertinggi di Indonesia. Hal tersebut didukung oleh ketersediaan infrastruktur yang mapan serta tingginya penetrasi penggunaan teknologi digital dalam aktivitas ekonomi dan pekerjaan. Selisih skor yang cukup lebar antara DKI Jakarta dengan rata-rata nasional juga mengindikasikan bahwa Jakarta menjadi pusat gravitasi utama dalam percepatan transformasi digital di tingkat provinsi.

Kartu *Subscriber Identity Module* (SIM) adalah elemen yang krusial dalam jaringan seluler, karena tidak hanya berfungsi untuk mengidentifikasi pengguna dalam jaringan, tetapi juga sebagai akses ke berbagai layanan digital yang terhubung, seperti perbankan elektronik, dompet digital, dan aplikasi yang berbasis

pada identitas. Oleh sebab itu, informasi yang berkaitan dengan kartun SIM biasanya mencakup data sensitif seperti nomor telepon, identitas kependudukan, alamat, dan lokasi, yang perlu dijaga kerahasiaannya oleh penyedia layanan telekomunikasi.

Dalam konteks perlindungan data pribadi, sektor telekomunikasi sangat penting karena banyaknya dan sensitifnya data yang ditangani. Penyalahgunaan atau kebocoran data pribadi dalam sektor ini tidak hanya berdampak buruk pada individu yang datanya terpapar, tetapi juga dapat mengurangi kepercayaan masyarakat terhadap layanan telekomunikasi secara keseluruhan. Misalnya, dalam proses pendaftaran SIM, data kependudukan harus dikonfirmasi dan disimpan dengan tingkat keamanan yang memadai agar risiko kebocoran atau penyalahgunaan dapat diminimalisir.

2.2 Gambaran Umum Pelindungan Data Pribadi di Sektor Telekomunikasi

Undang-Undang Pelindungan Data Pribadi (UU PDP) ini berfungsi sebagai kerangka hukum yang menyeluruh untuk mengatur prinsip dasar pelindungan data, hak subjek data, tanggung jawab bagi pengendali dan pengolah data, serta cara untuk menegakkan hukum pelindungan data pribadi. Tujuan undang-undang ini adalah memberikan kepastian hukum bagi subjek data dan menjelaskan tanggung jawab organisasi yang menangani data pribadi.

UU PDP menginstruksikan bahwa data pribadi harus diproses dengan cara yang sah, adil, dan transparan, serta memiliki tujuan yang jelas dan tidak melebihi batas kebutuhan pemrosesan. Selain itu, pengendali data wajib menjaga keamanan

data dengan menerapkan kontrol teknis dan organisasi, di samping itu terdapat pemerian hak akses, perbaikan, dan penghapusan kepada subjek data sesuai dengan ketentuan hukum yang berlaku. Ketentuan ini menunjukkan bahwa perlindungan data pribadi bukan hanya masalah teknis, melainkan juga bagian dari hak asasi manusia dan kepercayaan masyarakat terhadap layanan digital (Simanjuntak, 2024, hlm. 6).

Dalam sektor telekomunikasi, kebijakan perlindungan data pribadi menempatkan operator sebagai pihak yang bertanggung jawab untuk mematuhi prinsip-prinsip tersebut. Operator seluler harus memastikan bahwa sistem pendaftaran, penyimpanan, dan pengolahan data dilakukan sesuai dengan ketentuan dalam UU PDP serta memenuhi standar keamanan yang tepat. Penelaahan hukum menunjukkan bahwa tanpa adanya kerangka hukum yang kuat seperti UU PDP, praktik pengelolaan data sebelumnya cenderung terpecah dalam berbagai peraturan sektoral yang tidak spesifik dan menyeluruh.

2.3 Kelembagaan dan Peran Aktor Terkait dalam Pelindungan Data Pribadi

2.3.1 Kementerian Komunikasi dan Digital sebagai Regulator dan Pengawas

Kementerian Komunikasi dan Digital (Komdigi) memiliki peran utama dalam penerapan kebijakan perlindungan data pribadi di Indonesia, terutama setelah diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (JDIH, 2022). Dalam konteks kebijakan publik, Komdigi berfungsi sebagai pengatur di sektor komunikasi dan informatika serta bertindak sebagai pengawas bagi penyelenggara sistem elektronik, termasuk penyedia layanan telekomunikasi.

Sebagai regulator, Komdigi memiliki tanggung jawab untuk merancang dan mengimplementasikan kebijakan di bidang telekomunikasi dan sistem elektronik yang sejalan dengan prinsip perlindungan data pribadi. Tugas ini mencakup pembuatan standar kepatuhan, bimbingan terhadap pelaku industri, serta penguatan manajemen penyelenggaraan layanan digital agar sesuai dengan aturan yang berlaku. Dalam hal layanan kartu SIM prabayar, peranan regulator Komdigi terlihat dari pengaturan pendaftaran kartu SIM dan kewajiban pengendali data untuk menjaga keamanan dan kerahasiaan informasi pelanggan.

Di samping fungsi regulasi, Komdigi juga melaksanakan tugas pengawasan terhadap penerapan kebijakan perlindungan data pribadi. Pada awal penerapan Undang-Undang Pelindungan Data Pribadi, Komdigi bertindak sebagai pengawas secara administratif sebelum munculnya otoritas perlindungan data pribadi yang mandiri sesuai amanat undang-undang. Pengawasan ini dilakukan dengan cara memonitor kepatuhan penyelenggara sistem elektronik, menangani laporan dari masyarakat, dan berkoordinasi lintas sektor untuk menanggapi dugaan pelanggaran data pribadi.

Dalam industri telekomunikasi, fungsi pengawasan Komdigi sangat penting mengingat banyaknya data pribadi yang ditangani oleh operator seluler. Pendaftaran kartu SIM prabayar yang mengharuskan penggunaan data kependudukan menjadikan Komdigi sebagai pihak utama dalam memastikan bahwa kebijakan pemerintah terkait perlindungan data pribadi dilaksanakan secara konsisten oleh penyelenggara layanan. Dengan demikian, Komdigi berfungsi tidak

hanya sebagai penyusun kebijakan, tetapi juga sebagai jembatan antara norma hukum perlindungan data pribadi dan praktik di tingkat industri.

Keberadaan Komdigi dalam konteks perlindungan data pribadi menggambarkan bahwa pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tidak dapat dipisahkan dari peran aktif pemerintah dalam mengawasi kebijakan publik. Peran ini sangat penting untuk memastikan bahwa hak privasi masyarakat sebagai subjek data tetap terjaga saat layanan telekomunikasi semakin menyatu dengan kehidupan digital sehari-hari.

2.3.2 PT Telekomunikasi Seluler (Telkomsel) sebagai Penyelenggara

PT Telekomunikasi Selular (Telkomsel) adalah salah satu penyedia layanan telekomunikasi terbesar di Indonesia yang didirikan pada 26 Mei 1995 sebagai anak perusahaan dari PT Telekomunikasi Indonesia (Telkomsel, 2025b). jangka panjang, sehingga jumlah data pribadi pelanggan tanpa kontrak yang dikumpulkan dan dikelola oleh Telkomsel menjadi sangat besar. Sebagai penyedia layanan seluler terkemuka dengan jangkauan jaringan di seluruh Indonesia, Telkomsel memiliki pelanggan yang sangat banyak, terutama dalam segmen kartu SIM prabayar yang mendominasi sektor telekomunikasi di Indonesia. Keunggulan dalam layanan prabayar ini menunjukkan bahwa mayoritas pengguna seluler di Indonesia lebih memilih untuk menggunakan layanan prabayar tanpa adanya komitmen kontrak jangka panjang. Dalam memberikan layanan telekomunikasi, Telkomsel tidak hanya bertindak sebagai penyedia komunikasi, tetapi juga sebagai pengelola data pribadi pelanggan, terutama dalam proses pengelolaan data yang diperoleh melalui registrasi kartu SIM dan penggunaan layanan.

Sebagai entitas bisnis yang terikat pada regulasi nasional, Telkomsel mengatur pengelolaan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi. Aturan dalam undang-undang tersebut kemudian diuraikan lebih lanjut ke dalam kebijakan internal perusahaan yang bersifat terstruktur dan operasional. Kebijakan ini berfungsi sebagai alat untuk mengimplementasikan kebijakan negara di tingkat organisasi.

Gambar 2. 1 Logo Telkomsel



Sumber: Laman Resmi Telkomsel, 2021

2.3.3 Struktur kebijakan internal Telkomsel dalam pengelolaan

a) Peraturan Direksi (PD)

Peraturan Direksi adalah pedoman strategis paling tinggi di dalam perusahaan yang berfungsi untuk mengadaptasi kewajiban hukum dari undang-undang ke dalam kebijakan perusahaan. Dalam hal perlindungan data pribadi, PD menjadi landasan bagi pengaturan umum mengenai tata kelola data pelanggan dan tanggung jawab unit yang relevan.

b) Peraturan Perusahaan (PR)

Peraturan Perusahaan berperan sebagai aturan lanjutan yang mengikat seluruh insan perusahaan dalam melaksanakan kebijakan perlindungan data

pribadi. PR menetapkan standar kepatuhan internal serta panduan perilaku organisasi dalam pengelolaan data pelanggan.

c) Surat Edaran

Surat edaran difungsikan sebagai alat untuk menyebarluaskan dan menegaskan kebijakan tertentu yang bersifat teknis atau situasional, termasuk penyesuaian prosedur dalam pengelolaan data pribadi sejalan dengan perkembangan regulasi dan teknologi.

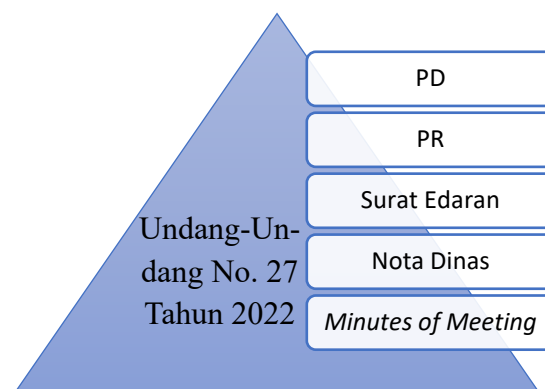
d) Nota Dinas

Nota dinas adalah alat administratif internal yang mengatur pelaksanaan teknis kebijakan, mencakup pembagian tugas dan tanggung jawab di antara unit kerja dalam pengelolaan dan pengamanan data pribadi pelanggan.

e) *Minutes of Meeting* (Notulen Rapat)

Minutes of Meeting berfungsi sebagai dokumentasi mengenai keputusan dan kesepakatan internal yang berkaitan dengan evaluasi, penguatan, atau penyesuaian kebijakan pengelolaan data pribadi, serta tindak lanjut terhadap isu atau insiden tertentu.

Gambar 2. 2 Struktur Kebijakan Perusahaan



Sumber: Diolah Oleh Peneliti, Mentor lapangan,2025

Melalui kerangka kebijakan internal tersebut, Telkomsel menegaskan komitmennya sebagai sebuah lembaga dalam mengaplikasikan kebijakan perlindungan data pribadi ke dalam praktik di dalam organisasi, sehingga tidak hanya bersifat teoritis, tetapi juga dilaksanakan dalam kegiatan operasional sehari-hari.

2.3.4 Layanan Kartu SIM Prabayar Telkomsel (Simpati) sebagai Objek Penelitian

Layanan kartu SIM prabayar Telkomsel, terutama produk Simpati, adalah salah satu layanan telekomunikasi yang paling banyak digunakan oleh masyarakat Indonesia. Menurut informasi dari Business Update, terdapat 159,66 juta pengguna Telkomsel yang terdiri dari 7,5 juta pengguna pascabayar dan 152,1 juta pengguna prabayar. Karakteristik layanan prabayar lebih banyak diminati karena kemudahan aksesnya, sifatnya yang fleksibel, dan tidak adanya kebutuhan kontrak jangka panjang, sehingga Simpati digunakan oleh berbagai kalangan masyarakat, mulai dari pelajar hingga pekerja di sektor informal.

Sebagai layanan prabayar, penggunaan kartu SIM Simpati mengharuskan proses pendaftaran yang mengharuskan pelanggan untuk memberikan data identitas diri. Data tersebut lalu dikelola oleh Telkomsel sebagai bagian dari sistem administrasi dan operasional layanan telekomunikasi. Situasi ini menjadikan Simpati sebagai subjek yang relevan untuk diteliti dalam mengkaji penerapan kebijakan perlindungan data pribadi, khususnya karena jumlah data yang dikumpulkan dan tingkat interaksi data yang tinggi

Gambar 2. 3 Produk Kartu SIM Prabayar Telkomsel (Simpati)



Sumber: Laman Resmi Telkomsel, 2025

Pemilihan layanan Simpati untuk penelitian ini didasarkan pada fakta bahwa layanan ini mewakili kelompok pengguna terbesar dari Telkomsel. Oleh karena itu, cara pengelolaan data pribadi dalam layanan ini mempunyai dampak langsung terhadap perlindungan hak privasi masyarakat secara umum.

2.3.5 Skema Alur Pengelolaan Data Pribadi Pelanggan Telkomsel

Berdasarkan Kebijakan Privasi Telkomsel dan peraturan nasional mengenai perlindungan data pribadi, pengelolaan data pelanggan di Telkomsel terdiri dari beberapa langkah utama yang menggambarkan cara penyedia layanan telekomunikasi menjalankan tanggung jawab hukum dalam konteks perlindungan data nasional, langkah utama sebagai berikut:

1. **Komitmen terhadap Pedoman dan Dasar Hukum**

Pengaturan data pribadi dimulai dengan komitmen resmi Telkomsel sebagai penyedia layanan telekomunikasi untuk memenuhi kewajiban yang ditetapkan oleh pemerintah. Komitmen ini tercermin dalam Kebijakan Privasi perusahaan yang sesuai dengan peraturan yang berlaku, khususnya terkait perlindungan informasi

pribadi. Inisiatif ini berfungsi sebagai dasar etis yang menjamin bahwa setiap proses pengaturan data dilakukan dengan prinsip transparansi, akuntabilitas, dan kepatuhan terhadap kebijakan publik di bidang perlindungan data pribadi.

2. Pengumpulan Data Pribadi

Proses pengumpulan data dilakukan sebagai bagian dari implementasi aturan pendaftaran kartu SIM yang telah ditetapkan oleh pemerintah. Untuk layanan kartu SIM prabayar, data yang dikumpulkan meliputi data identitas kependudukan, seperti Nomor Induk Kependudukan (NIK) dan Kartu Keluarga (KK), yang digunakan untuk keperluan verifikasi identitas pengguna. Pengumpulan ini menjadi dasar hubungan layanan antara Telkomsel dan pelanggan, sekaligus menunjukkan kepatuhan operator terhadap peraturan yang berlaku.

3. Pengolahan dan Pemanfaatan

Data untuk Tujuan Spesifik Data pribadi yang telah dihimpun kemudian diproses dan digunakan secara terbatas sesuai dengan tujuan yang sah, seperti yang diungkapkan dalam pedoman perusahaan dan regulasi resmi. Tujuan tersebut mencakup penyediaan layanan telekomunikasi, manajemen administrasi pelanggan, pemeliharaan keamanan jaringan, peningkatan kualitas layanan, serta pemenuhan kewajiban hukum. Langkah ini

memperlihatkan penerapan prinsip pembatasan tujuan dalam kebijakan perlindungan data pribadi.

4. Penyimpanan Data Pribadi

Informasi pribadi pelanggan disimpan dalam sistem yang memiliki perlindungan teknis dan organisatoris sebagai wujud tanggung jawab pengendali data dalam menjaga keamanan informasi. Data disimpan selama periode yang diperlukan untuk mencapai tujuan pengumpulannya atau sesuai dengan peraturan retensi data yang ditetapkan oleh peraturan perundang-undangan.

5. Koreksi dan Pembaruan Data

Selama data masih dikuasai oleh pengendali data, pelanggan mempunyai hak untuk memperbaiki dan memperbarui informasi pribadi jika terdapat kesalahan atau perubahan. Pemberian hak ini adalah bagian dari pemenuhan hak subjek data sebagaimana diatur dalam kebijakan perlindungan data pribadi dan juga menunjukkan komitmen untuk menghormati hak privasi pengguna layanan.

6. Pengungkapan Data kepada Pihak Ketiga

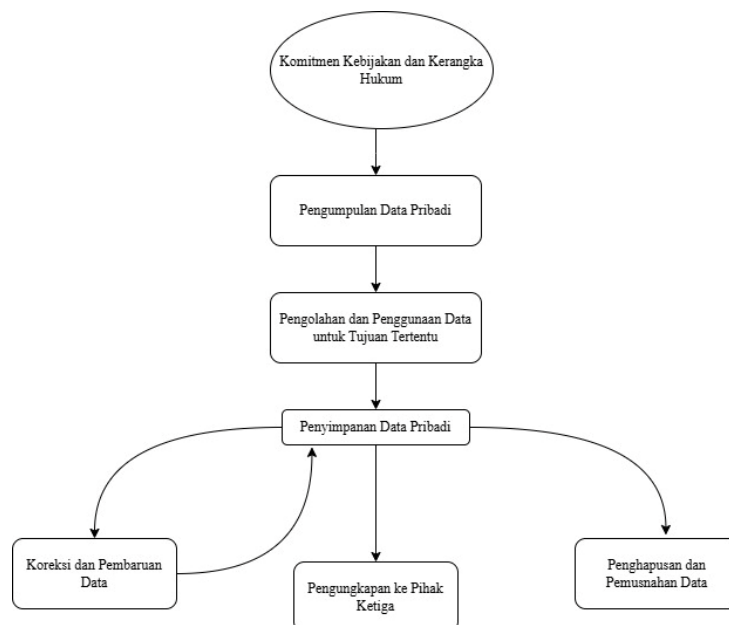
Dalam situasi tertentu, informasi pribadi pelanggan mungkin akan dibagikan kepada pihak ketiga, baik itu mitra kerja maupun instansi pemerintah. Pengungkapan ini hanya dilakukan berdasarkan dasar hukum yang sah, seperti persetujuan dari subjek data atau kewajiban hukum yang ditetapkan oleh pemerintah. Tahapan ini menjadi aspek penting dalam pengawasan pelaksanaan kebijakan perlindungan data

pribadi, karena terkait langsung dengan prinsip pembatasan pengungkapan data.

7. Penghapusan dan Pemusnahan Data

Langkah terakhir dalam pengelolaan data pribadi adalah penghapusan atau pemusnahan data. Data akan dihapus atau dimusnahkan ketika tidak lagi dibutuhkan untuk tujuan pengumpulannya atau apabila tidak ada dasar hukum yang mengharuskan penyimpanan data. Dalam konteks layanan kartu SIM Prabayar, tahap ini relevan ketika nomor pelanggan sudah tidak aktif dalam rentang waktu tertentu sesuai dengan ketentuan yang berlaku.

Gambar 2. 4 Skema Alur Pengelolaan Data Pribadi Pelanggan Telkomsel



Sumber: Diolah oleh Peneliti, Telkomsel, 2023; T-PAS Telkomsel, t.t.

Secara umum, proses pengelolaan informasi pribadi pelanggan di Telkomsel menunjukkan bahwa pengelolaan data dilakukan secara teratur dan berkelanjutan, dimulai dari pengumpulan hingga penghapusan data. Proses ini memberikan penjelasan tentang bagaimana kebijakan perlindungan data pribadi diimplementasikan dalam praktik operasional penyedia layanan telekomunikasi, serta mencerminkan upaya pengelola data dalam memenuhi kewajiban hukum dan memastikan perlindungan hak privasi pengguna layanan kartu SIM prabayar.

2.4 Gambaran Umum Isu Pelindungan Data Pribadi di Sektor Telekomunikasi

Isu perlindungan data pribadi di bidang telekomunikasi kian mendapat perhatian seiring dengan eskalasi ancaman keamanan siber yang menargetkan identitas konsumen layanan digital. Di lingkungan digital masa kini, nomor telepon genggam tidak lagi sekadar alat komunikasi, melainkan terintegrasi dengan berbagai aplikasi penting, termasuk perbankan daring, platform media sosial, dompet digital, dan layanan administrasi pemerintah. Hal ini menempatkan data identitas pengguna sebagai sumber daya berharga yang sekaligus rentan terhadap eksploitasi ilegal.

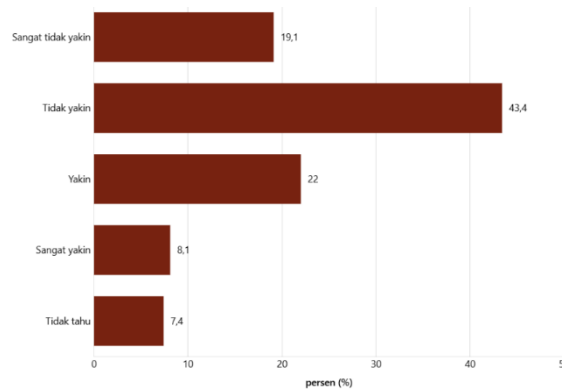
Menurut laporan *Threat Landscape* dari European Union Agency for Cybersecurity (ENISA), ancaman keamanan siber yang paling umum dalam beberapa tahun belakangan didominasi oleh serangan yang melibatkan manipulasi perilaku manusia atau *social engineering*. Ancaman jenis ini meliputi teknik seperti phishing dan distribusi malware yang memanfaatkan kecerobohan pengguna untuk mengakses data sensitif tanpa izin. ENISA menyoroti bahwa serangan tersebut secara sistematis memanfaatkan kesalahan manusia, sehingga menjadikan data

identitas sebagai fokus utama dalam berbagai modus kejahatan siber. Dalam hal ini, informasi pribadi seperti Nomor Induk Kependudukan (NIK), nomor telepon, dan alamat email menjadi sasaran prioritas karena dapat dimanfaatkan untuk penipuan daring, penguasaan akun, atau penyalahgunaan identitas.

Situasi ini sangat berkaitan dengan industri telekomunikasi, terutama layanan kartu SIM prabayar, di mana proses pendaftaran mengharuskan pengguna menyampaikan data kependudukan yang bersifat rahasia. Pengumpulan data identitas dalam skala besar oleh penyedia layanan telekomunikasi menempatkan sektor ini dalam risiko tinggi terhadap kebocoran data jika tidak didukung oleh mekanisme keamanan dan regulasi perlindungan data pribadi yang cukup kuat

Selain risiko teknis, masalah perlindungan data pribadi juga sangat terkait dengan tingkat kepercayaan masyarakat terhadap keamanan platform digital. Hasil survei nasional yang dirilis oleh Katadata Insight Center mengungkapkan bahwa sebagian besar warga Indonesia masih skeptis terhadap kondisi keamanan siber domestik. Survei yang dipublikasi oleh Databoks Katadata mencatat bahwa 62,5% responden menyatakan kurang percaya pada keamanan siber di Indonesia, sedangkan sekitar 30,1% responden menyatakan percaya, dan sisanya sebesar 7,4% menyatakan tidak memiliki pengetahuan pasti mengenai situasi keamanan siber.

Gambar 2. 5 Tingkat Keyakinan Responden Terhadap Keamanan Siber Indonesia (2023)



Sumber: Databoks Katadata, 2023

Rendahnya tingkat kepercayaan masyarakat ini menunjukkan adanya jurang antara peningkatan penggunaan layanan digital dengan pandangan masyarakat mengenai keamanan data pribadi. Di bidang telekomunikasi, situasi ini berpotensi mengganggu ikatan kepercayaan antara konsumen dan penyedia layanan, mengingat operator telekomunikasi menangani data identitas rahasia dalam volume besar dan berperan sebagai pintu masuk utama dalam ekosistem digital yang bergantung pada nomor ponsel.

Oleh karena itu, masalah perlindungan data pribadi di sektor telekomunikasi tidak hanya melibatkan jumlah insiden kebocoran data, tetapi juga pola ancaman keamanan siber yang bersifat sistematis serta pandangan masyarakat terhadap pengelolaan data pribadi. Gambaran ini menegaskan bahwa perlindungan data pribadi merupakan agenda kebijakan publik yang rumit, yang mencakup aspek teknologi, regulasi, dan kepercayaan sosial, serta menjadi latar belakang krusial

dalam memahami penerapan kebijakan perlindungan data pribadi pada layanan kartu SIM Prabayar di Indonesia.

2.5 Gambaran Umum Daerah Khusus Ibukota Jakarta sebagai Lokasi Penelitian

Daerah Khusus Ibukota (DKI) Jakarta merupakan wilayah dengan intensitas pemanfaatan layanan telekomunikasi dan aktivitas digital yang sangat tinggi dibandingkan daerah lain di Indonesia. Posisi Jakarta sebagai pusat pemerintahan, kegiatan ekonomi, serta penyelenggaraan layanan publik nasional menjadikan wilayah ini sebagai simpul utama interaksi antara penyedia layanan telekomunikasi, institusi pemerintah, dan masyarakat pengguna layanan digital. Tingginya tingkat mobilitas penduduk dan aktivitas ekonomi turut mendorong kebutuhan akan layanan komunikasi yang cepat, stabil, dan terintegrasi dengan berbagai platform digital.

Berdasarkan data Badan Pusat Statistik (2025), tingkat penetrasi internet dan kepemilikan telepon seluler di DKI Jakarta secara konsisten berada jauh di atas rata-rata nasional. Tercatat, sebanyak 87,84% penduduk Jakarta mengakses internet pada tahun 2024, menempati peringkat kedua tertinggi secara nasional setelah Kepulauan Riau (89,26%), sementara rata-rata nasional berada di angka 72,78%. Selain itu, 83,43% penduduk Jakarta memiliki atau menguasai telepon seluler, menempatkan Jakarta pada posisi ketiga tertinggi di Indonesia. Mayoritas penduduk menggunakan telepon seluler sebagai sarana utama untuk mengakses internet, baik untuk keperluan komunikasi, pekerjaan, transaksi ekonomi, maupun akses layanan publik berbasis elektronik. Hal ini menunjukkan ketergantungan

masyarakat Jakarta yang tinggi terhadap layanan telekomunikasi, khususnya berbasis kartu SIM dalam kehidupan sehari-hari.

Intensitas penggunaan layanan digital di DKI Jakarta juga terlihat dari frekuensi akses internet yang sangat tinggi, dengan 96,34% pengguna internet di wilayah ini mengakses layanan minimal sekali sehari, lebih besar dibandingkan rata-rata nasional (92,92%). Dominasi akses internet yang dilakukan melalui telepon seluler juga sangat signifikan, di mana secara nasional sebanyak 99,08% pengguna internet menggunakan ponsel sebagai perangkat utama akses, pola yang relevan dan berlaku umum untuk Jakarta mengingat tingginya kepemilikan telepon seluler di wilayah ini.

Tabel 2. 2 Indikator Kunci Telekomunikasi Digital: DKI Jakarta vs Nasional (2024)

No	Indikator	DKI Jakarta	Rata-rata Nasional
1.	Tingkat Penetrasi Internet	87,84% (tertinggi ke-2)	72,78%
2.	Kepemilikan Telepon Seluler	83,43% (tertinggi ke3)	68,65%
3.	Frekuensi Akses Internet Intens	96,34%	92,92% (nasional)
4.	Dominasi Akses Internet via Telepon Seluler	≈ 99,08% (data nasional berlaku umum)	99,08%

Sumber: Diolah Oleh Peneliti, Badan Pusat Statistik, 2025, Tabel 7, 10, 11 dan Gambar 15

Tingginya penggunaan layanan telekomunikasi di Jakarta juga berimplikasi pada besarnya volume data pribadi yang diproses oleh penyelenggara layanan.

Setiap aktivitas komunikasi dan akses layanan digital melibatkan pengelolaan data identitas pengguna, termasuk nomor telepon dan data kependudukan yang dihimpun melalui proses registrasi kartu SIM prabayar. Oleh karena itu, DKI Jakarta menjadi wilayah dengan intensitas pemrosesan data pribadi yang sangat tinggi dan sekaligus berpotensi memiliki risiko pelanggaran data pribadi yang lebih besar jika tidak didukung oleh kebijakan perlindungan data yang efektif.

Selain itu, karakteristik masyarakat Jakarta yang heterogen baik dari segi latar belakang sosial, ekonomi, maupun tingkat literasi digital, menjadikan wilayah ini sangat relevan untuk mengkaji implementasi kebijakan perlindungan data pribadi dari perspektif pengguna layanan. Keberadaan kantor pusat berbagai penyedia layanan telekomunikasi serta instansi pemerintah yang berwenang di Jakarta juga memudahkan peneliti untuk memperoleh gambaran komprehensif tentang praktik pengelolaan data pribadi dan pengawasan kebijakan di sektor telekomunikasi. Dengan data dan kondisi tersebut, DKI Jakarta dipilih sebagai lokasi penelitian yang representatif untuk menggambarkan dinamika perlindungan data pribadi di lingkungan perkotaan dengan tingkat penggunaan layanan telekomunikasi yang sangat tinggi.