KEAMANAN DATA KEPENDUDUKAN DI ERA KOMUNIKASI DIGITAL

(Studi pada Penyedia Layanan Telekomunikasi Smartfren Kota Metro)

Budi Ariyanto*[1], Rosdiana Rahmadhani*[2], Khaliza Zhahwa Nazwa*[3]
*[1*2*3]Universitas Islam Negeri Jurai Siwo Lampung
e-mail: budiariyanto@metrouniv.ac.id

Abstrak: Perkembangan komunikasi digital membawa kemudahan dalam pengelolaan administrasi kependudukan, namun sekaligus memunculkan ancaman serius terhadap keamanan data pribadi. Sejak 2020, Indonesia berkali-kali mengalami insiden kebocoran data berskala besar yang mengungkap berbagai kelemahan dalam ekosistem perlindungan data. Tujuan penelitian ini menganalisis secara mendalam bagaimana sistem data kependudukan dikelola, batas kemampuan teknis yang dimiliki instansi di tingkat bawah, peran pemerintah melalui regulasi, dan berbagai insiden nyata yang memperlihatkan risiko kebocoran data. Menggunakan pendekatan kualitatif. Hasil penelitian menunjukkan bahwa melalui komunikasi digital yang integratif dan kolaboratif antar pemangku kepentingan, upaya perlindungan data pribadi dapat diwujudkan secara optimal

Kata kunci: *Komunikasi Digital, Keamanan Data, Layanan Telekomunikasi, Perlindungan Data Pribadi.*

Abstract: *The development of digital communication has brought convenience to the management of population administration, yet it simultaneously poses serious threats to personal data security. Since 2020, Indonesia has repeatedly experienced large-scale data breach incidents that reveal various weaknesses within the data protection ecosystem. The purpose of this research is to analyze in depth how population data systems are managed, the technical capability limits of agencies at the grassroots level, the role of government through regulations, and various real-world incidents that demonstrate the risks of data leakage. Using a qualitative approach, the results of the study indicate that through integrative and collaborative digital communication among stakeholders, personal data protection efforts can be achieved optimally.*

Keywords: *Digital Communication, Data Security, Telecommunication Services, Personal Data Protection.*

PENDAHULUAN

Beberapa tahun terakhir, isu keamanan data kependudukan menjadi salah satu topik paling diperdebatkan di Indonesia. Kekhawatiran masyarakat terhadap penyalahgunaan Nomor Induk Kependudukan (NIK) semakin meningkat ketika muncul banyak laporan kebocoran data pribadi sejak tahun 2020 (Novita et al., 2024). Di sisi lain, masyarakat juga mempertanyakan apakah instansi yang mengelola layanan publik benar-benar dapat menjamin keamanan data mereka. Keresahan ini wajar karena NIK merupakan identitas dasar yang terhubung dengan hampir semua sistem administrasi, mulai dari layanan kesehatan, pendidikan, perbankan, bantuan sosial, hingga ruang digital. Berbagai proses komunikasi yang dilakukan tidak sebatas pada satu individu, melainkan harus ada langkah yang bersinergi. Sinergi untuk mengelola data dan menjamin keamanannya.

Senada dengan penelitian Adinda Putri Aisyah, berjudul Perlindungan Data Pribadi dan Etika Media Sosial di Era Digital. Penelitian ini mengungkapkan bahwa keamanan data pribadi harus terjamin, karena teknologi dan informasi merubah pola masyarakat dalam kehidupannya (Aisyah et al., 2024). relevan dengan penelitian ini bahwa di era digital masyarakat terus dipengaruhi oleh berbagai kemajuan teknologi, namun sistem komunikasi digital yang dibangun minim atas jaminan keamanan data. Persoalan ini berlarut dengan maraknya berbagai isu dan kejadian yang tidak berkaitan dengan keamanan data privasi.

Berbagai kejadian yang telah terjadi dalam keamanan data kependudukan menjadi cermin bahwa sistem komunikasi digital belum efektif dan perlu langkah strategis yang dilakukan. Hal ini juga merepresentasikan bahwa keamanan di era digital terus mengalami perkembangan, upaya-upaya baik pencegahan maupun proses penanganannya harus dikelola dan lebih diperkuat. Pengelolaan yang baik akan memberikan dampak signifikan dalam meningkatkan kepercayaan masyarakat kepada penyedia layanan.

Sesuai dengan konteks inilah penting untuk memahami bahwa keamanan data

bukan hanya persoalan teknis, melainkan juga berkaitan dengan tata kelola, kebijakan, serta kesiapan institusi menghadapi ancaman siber global. Era komunikasi digital telah mempercepat perubahan sistem administrasi menjadi serba online, tetapi perubahan cepat tersebut tidak sepenuhnya diiringi kesiapan keamanan yang memadai. Oleh sebab itu, artikel ini berupaya menganalisis komunikasi digital dalam mengelola keamanan data pada penyedia layanan telekomunikasi Smartfren cabang kota Metro.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian deskriptif-analitis yang menggambarkan serta menganalisis keamanan data kependudukan pada penyedia layanan telekomunikasi Smartfren kota Metro. Pendekatan ini guna mendapatkan pemahaman mendalam terkait persoalan keamanan data di era komunikasi digital, dimana semua proses registrasi di layanan telekomunikasi wajib menyertakan data kependudukan.

Pendekatan deskriptif digunakan untuk memaparkan fakta dan peristiwa (Moleong, 2014) terkait kebocoran data kependudukan, sedangkan pendekatan analitis digunakan untuk mengkaji komunikasi digital, keterlibatan pihak ketiga, serta efektivitas kebijakan perlindungan data yang diterapkan pemerintah.

Studi ini dilakukan sejak tahun 2025 guna mendapatkan data yang lengkap, peneliti melakukan wawancara mendalam kepada informan yaitu karyawan Smartfren kota Metro yang enggan disebutkan namanya. Sebagaimana yang menjadi fokus dalam penelitian ini yaitu mendeskripsikan komunikasi digital dalam mengelola keamanan data yang terjadi dan dialami langsung oleh penyedia layanan telekomunikasi Smartfren Kota Metro. Pendekatan ini digunakan untuk memperoleh data yang menyeluruh dan mendalam terkait keamanan data di Smartfren Kota Metro. Dari uraian diatas desain penelitian keamanan data dapat digambarkan dalam diagram sebagai berikut:

Gambar 1. Diagram Keamanan Data

Gambar 1 merupakan model kerangka perlindungan data terintegrasi yang disusun oleh peneliti berdasarkan sintesis antara konsep keamanan data digital dengan fakta empiris yang ditemukan di lokasi penelitian. Diagram ini menggambarkan bahwa keamanan data bukan hanya bergantung pada infrastruktur teknologi seperti enkripsi, melainkan merupakan ekosistem yang melibatkan aspek kebijakan kualitas sumber daya manusia (literasi digital), dan tata kelola kelembagaan (audit dan respons insiden) yang saling berkesinambungan.

Teknik analisis data yang digunakan yakni analisis deskriptif kualitatif, dengan tahapan reduksi data, penyajian data secara naratif, serta penarikan kesimpulan berdasarkan pola dan kecenderungan yang ditemukan (Rijali, 2018). Analisis dilakukan dengan mengaitkan fakta empiris dengan konsep keamanan data, tata kelola digital, dan kebijakan publik. Pendekatan yang dicirikan dengan tujuan penelitian untuk memahami fenomena yang mendalam yang tidak memerlukan kuantifikasi(Abdussamad, 2021). Sehingga dalam penelitian ini menganalisis komunikasi yang tepat dalam pengelolaan data kependudukan. Jaminan keamanan data menjadi hak seluruh masyarakat. Masyarakat memiliki kewajiban dalam registrasi kartu SIM yang dikeluarkan oleh

penyedia layanan telekomunikasi. Penyedia juga memberikan hak masyarakat untuk dijamin keamanan data kependudukannya. Proses saling menguntungkan inilah yang layak dijadikan indikator keberhasilan dalam mengelola keamanan data. Adanya sinergi yang terintegrasi baik komunikasi pembuat kebijakan dan masyarakat sebagai penggunanya.

HASIL DAN PEMBAHASAN

Sebelum membahas risiko kebocoran data, penting memahami struktur pengelolaan data itu sendiri. Proses komunikasi digital perlu dilakukan sebagai bagian terpenting dalam pengelolaan data privasi yaitu adanya integrasi kebijakan (Halim et al., 2025) di tingkat bawah seperti outlet atau kantor layanan. Petugas sebenarnya tidak memiliki akses langsung ke server pusat yang menyimpan data kependudukan. Mereka hanya menggunakan aplikasi layanan sesuai prosedur yang telah ditentukan, sehingga mereka juga tidak dapat memastikan secara teknis apakah sistem pusat pernah diretas atau tidak. Namun dalam pelaksanaannya perlu perlindungan secara internal yang dapat dilakukan, berupa pembaharuan kebijakan internal perusahaan (Adam & Wiraguna, 2025). Pengelolaan data ini menjadi kewajiban setiap orang, bahwa perlu adanya manajemen yang baik dan aman, meskipun data ini tidak sepenuhnya tiap individu yang mengelola dan menjagannya.

Manajemen Data Kependudukan

Data kependudukan dikelola secara terpusat oleh instansi terkait terutama Ditjen Dukcapil yang kemudian diawasi oleh Kominfo dari sisi kebijakan dan regulasi keamanan data. Berbagai Langkah strategis telah dilakukan oleh Dukcapil, sebagaimana perluasan kolaborasi dengan instansi eksternal dan percepatan pelayanan (Giyanti & Tukiman, 2025). Artinya pengelolaan semakin diperketat dengan pola komunikasi yang efektif dan mengintegrasi berbagai pihak, serta tepat sasaran dalam menjangkau masyarakat. Hal ini menandakan bahwa kebijakan tidak sebatas diatas penguasa. Dengan demikian, kemampuan mereka untuk memberikan jawaban tentang keamanan sistem terbatas pada pengetahuan prosedural, bukan teknis. Komunikasi

digital yang melibatkan seluruh pihak dan instansi terkait sebagai bentuk upaya perlindungan data privasi. Dapat dipahami bahwa komunikasi yang bersifat integral, dengan menjalin kerjasama dengan berbagai pemangku kebijakan hingga masyarakat sebagai penggunan terus dilakukan sebagai langkah yang diambil dalam menjamin keamanan data kependudukan.

Akan tetapi, keterbatasan akses di tingkat dan kesadaran masyarakat terkait haknya terhadap keamanan data privasi (Valentina & Prastiyanti, 2025). Mengingat bawah tidak menutup fakta bahwa Indonesia telah beberapa kali mengalami insiden kebocoran data besar sejak 2020. Kasus-kasus tersebut menunjukkan bahwa meskipun pusat telah menerapkan sistem keamanan, ancaman kebocoran tetap menjadi realitas. Pada tahun 2021, publik dikejutkan dengan dugaan kebocoran 279 juta data penduduk yang disebut-sebut berkaitan dengan sistem keanggotaan kesehatan nasional. Data tersebut dikabarkan dijual di forum internasional, lengkap dengan NIK, tanggal lahir, hingga informasi status kesehatan. Meskipun pemerintah melakukan investigasi dan menerbitkan klarifikasi, insiden ini telah memunculkan keraguan besar terhadap keamanan sistem nasional.

Tidak berhenti di situ, sejak 2019 hingga pertengahan 2023, Kementerian Komunikasi dan Informatika (Kominfo) mencatat setidaknya 94 insiden kebocoran data pribadi yang melibatkan berbagai lembaga, mulai dari layanan digital, perusahaan telekomunikasi, hingga fasilitas kesehatan. Setelah 2020, sejumlah kasus baru terus bermunculan, seperti kebocoran data pengguna aplikasi digital, data registrasi kartu SIM, hingga informasi pasien dari beberapa layanan kesehatan. Bahkan, pada 2022 dan 2023, terdapat laporan mengenai kebocoran data paspor, data riwayat kredit, serta data pribadi pelanggan operator telekomunikasi yang beredar di internet (Syifa Nurul Sabila & Wira Atman, 2025). Rentetan insiden tersebut menunjukkan bahwa ancaman terhadap data pribadi bukan sekadar kemungkinan, melainkan fakta yang terus berulang.

Adapun hal serupa juga pernah terjadi pada penyedia layanan telekomunikasi

Smartfren cabang kota Metro Jl Brigjend Sutiyoso. Kejadian penyalahgunaan data kependudukan oleh oknum yang tidak bertanggung jawab. Sebagaimana diungapkan oleh karyawan Smartfren bahwa dalam merespon kejadian tersebut, pihaknya menerima laporan yang kemudian di lakukan pelaporan ke Kominfo sebagai pemegang database secara utuh. Smartfren dalam hal ini menjadi jembatan dalam komunikasi antara pengguna dengan Kominfo.

Keterbatasan akses terhadap basis data ini merupakan langkah dan upaya dari satu induk yang memegang data kependudukan sebagai bentuk pencegahan kebocoran data. Tidak dapat dipungkiri bahwa kebocoran data yang pernah terjadi bersumber dari pihak ketiga yang tidak berkaitan secara langsung dengan penyedia layanan maupun Kementerian Komunikasi dan Informatika (Kominfo). Umumnya, kebocoran tersebut dilakukan oleh pihak yang mencoba atau dengan sengaja membobol sistem keamanan dengan berbagai kepentingan. Kominfo dan Smartfren terus menjalin komunikasi serta menegaskan bahwa mereka tetap bertanggung jawab penuh terhadap keamanan data. Komunikasi ini dilakukan sebagai bentuk pengelolaan data pribadi yang merupakan hak masyarakat, sehingga fokus pada pelayanan yang diberikan Smartfren kepada masyarakat dapat berjalan secara optimal. Namun demikian, pihak terkait juga menyadari bahwa upaya pembobolan data terus dilakukan. Meskipun tidak terdapat persoalan yang tampak secara langsung, Smartfren tetap konsisten menjaga keamanan data dan memfasilitasi pengguna agar dapat menikmati layanan secara prima.

Komunikasi Digital sebagai Upaya Menjaga Keamanan Data

Fenomena ini menunjukkan adanya beberapa lapisan masalah. *Pertama*, sistem komunikasi digital yang digunakan oleh berbagai lembaga sering kali belum menerapkan standar keamanan tertinggi. Sebagian sistem masih menggunakan protokol lama yang rentan dibobol. Smartfren juga melakukan komunikasi digital dengan menjalin kerjasama antara Kominfo, Ditjen Dukcapil dan pihak terkait untuk mengelola keamanan data.

Kedua, ada kemungkinan kebocoran terjadi bukan dari server utama, tetapi dari

pihak ketiga yang bekerja sama dengan instansi pemerintah atau penyedia layanan. Pihak ini sering melakukan registrasi kartu SIM dengan nomor induk kependudukan secara ganda, sehingga berakibat data yang tidak terverifikasi secara baik dan benar.

Ketiga, manusia tetap menjadi titik lemah terbesar. Banyak kebocoran terjadi akibat kelalaian, kesalahan input, atau penyalahgunaan akses oleh pihak yang tidak bertanggung jawab. Ada beberapa gejala dimana piha tertentu dengan sengaja menginput data dengan asal teregistrasi, tanpa ada sebuah perhitungan apakah berdampak baik atau sebaliknnya. Inilah faktor yang sering terjadi, hanya berorientasi pada kepentingan profit saja, tanpa memperhitungkan dampaknya.

Keempat, ekosistem keamanan digital Indonesia masih berkembang, sehingga belum seluruh lembaga siap menghadapi serangan siber skala besar. Smartfren terus melakukan peningkatan keamanan secara internal, namun tidak bisa berdiri sendiri tanpa sinergi dan kolaborasi dari berbagai pihak. Komunikasi digital terus dilakukan dengan menjalin kerjasama guna mewujudkan keamanan data privasi sebagai hak setiap warga masyarakat.

Berdasarkan uraian diatas muncul spekulasi apakah sistem pusat yang menyimpan NIK pernah diretas. Secara resmi, pemerintah tidak pernah mengonfirmasi adanya peretasan langsung pada server utama yang menyimpan data kependudukan. Namun, berbagai kebocoran data pada 2020 ke atas menunjukkan bahwa jalur tidak langsung, seperti integrasi sistem, aplikasi lain, atau celah keamanan pihak ketiga, dapat menjadi pintu masuk bocornya data. Artinya, sistem pusat mungkin tidak diretas secara langsung, tetapi ekosistem digital di sekitarnya memiliki banyak celah yang membuat data tetap bisa bocor (Lesmana & Nasution, 2025). Adapun kebocoran data yang terjadi menunjukkan perlunya alternatif penyelesaian persoalan keamanan data melalui komunikasi yang integratif antara pemegang kekuasaan, penyedia layanan telekomunikasi dalam hal ini Smartfren serta pengguna. Ketiga pihak tersebut harus menjalin kerja sama yang berkelanjutan.

Maka, perlindungan data di Indonesia sesungguhnya adalah persoalan yang

jauh lebih kompleks dibanding sekadar apakah server diretas atau tidak. Ia melibatkan kesiapan infrastruktur, kualitas kebijakan, standar keamanan lembaga, serta kedewasaan masyarakat dalam menjaga data pribadinya. Ketika satu komponen lemah, seluruh ekosistem bisa terancam. Ini menjelaskan mengapa meskipun pemerintah telah mengeluarkan Undang-Undang Perlindungan Data Pribadi, risiko kebocoran tetap menghantui karena pelaksanaannya membutuhkan waktu, anggaran, serta komunikasi yang integratif antar lintas lembaga yang kuat. Penyedia layanan telekomunikasi memiliki kewajiban untuk pencegahan dan penanganan pasca kejadian (Anindya & Subiyanto, 2025). Upaya ini perlu dilakukan secara optimal, sebagai bentuk tanggung jawab dan kewajibannya.

Sebagaimana dalam pengelolaan data kependudukan dapat dilakukan dengan berbagai upaya, namun hal yang tidak dapat dipisahkan yaitu komunikasi. Komunikasi digital menjadi bagian dalam proses menjaga keamanan data kependudukan, terutama komunikasi yang melibatkan berbagai pemangku kebijakan (Asrianti et al., n.d.). Sering dimaknai sebagai komunikasi integral, antara pemerintah sebagai pembuat kebijakan dengan mengintegrasi kekuatan masyarakat dalam menjaganya. Langkah ini juga diperkuat oleh penyedia layanan telekomunikasi seperti Smartfren.

SIMPULAN

Berdasarkan uraian tersebut, dapat disimpulkan bahwa keamanan data kependudukan di Indonesia menghadapi tantangan serius, terutama sejak maraknya kebocoran data pada tahun 2020. Meskipun sistem terpusat telah dilengkapi dengan berbagai lapisan pengamanan, fakta bahwa data tetap bocor melalui celah lain menunjukkan bahwa perlindungan data memerlukan pendekatan yang bersifat sistemik. Pemerintah perlu memperkuat regulasi serta melakukan audit keamanan secara berkelanjutan, penyedia layanan wajib memperketat pengelolaan dan pembatasan akses data, sementara masyarakat harus semakin berhati-hati dalam membagikan data pribadi. Hanya melalui komunikasi digital yang integratif dan kolaboratif antar pemangku kepentingan, upaya perlindungan data pribadi dapat

diwujudkan secara optimal.

DAFTAR PUSTAKA

Abdussamad, Z. (2021). *Metode Penelitian Kualitatif*. CV. syakir Media Press.

Adam, M. Z., & Wiraguna, S. A. (2025). Menghadapi Tantangan Baru Dalam Menjaga Etika Komunikasi,. *Jurnal Multidisiplin Ilmu Sosial*.

Aisyah, A. P., Aprilia, A., Andini, P., Syahida, S., Azzahra, S. M., & Supriyandi. (2024). Perlindungan Data Pribadi dan Etika Media Sosial di Era Digital. *Jurnal Pendidikan Tambusai*, *8*(2), 28235–28240.

Anindya, R. P., & Subiyanto, A. E. (2025). Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(3), 1105–1112. https://doi.org/10.31004/riggs.v4i3.2105

Asrianti, N. F., Alghazali, M. G., & Putri, I. Y. (n.d.). *Kasus Kebocoran Data Pada Pusat Data Nasional KOMINFO : Pentingnya Keamanan Cloud di Era Digitalisasi*. *1*, 24–33.

Giyanti, M. E. P., & Tukiman. (2025). Analisis Prosedur Dan Tantangan Digitalisasi

Layanan Kependudukan Melalui Plavon Dukcapil Di Mal Pelayanan Publik Kabupaten Sidoarjo. *Future Academia : The Journal of Multidisciplinary Research on Scientific and Advanced*, *3*(4), 1693–1706. https://doi.org/10.61579/future.v3i4.667

Halim, Z., Islam, U., Sumatera, N., Irwan, M., Nasution, P., Islam, U., & Sumatera, N. (2025). *Strategi Manajemen Data Privasi dalam Era Digital pada Perusahaan dan Bisnis Modern*. *2*(3), 474–485.

Lesmana, R., & Nasution, M. I. P. (2025). Kebocoran Data di Media Sosial : Analisis Pola dan Strategi Pencegahannya. *Journal of Internet and Software Engineering*, *2*(10), 74–80. https://doi.org/10.62017/tektonik

Moleong, L. J. (2014). *Metode Penelitian Kualitatif*. PT Remaja Rosdakarya.

Novita, F., Nugroho, P., Listanto, M. F., & Amelia, N. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65.

Rijali, A. (2018). *Analisis Data Kualitatif*. *17*(33), 81–95.

Syifa Nurul Sabila, & Wira Atman. (2025). Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia. *Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial Dan Politik*, *2*(3), 142–154. https://doi.org/10.62383/sosial.v2i3.1998

Valentina, R. W., & Prastiyanti, R. A. (2025). Perlindungan Data Pribadi : Tantangan dan Solusi di Era Big Data yang Berkaitan dengan Hukum Telematika. *Hukum Dinamika Ekselensia*, *7*(2), 33–47.