KEGAGALAN PERLINDUNGAN DATA PRIBADI PASCA UU PDP: ANALISIS KOMPARATIF KASUS KEBOCORAN DATA DI INDONESIA (2024–2025)

Sherly Julia Nanda Saputri[1], Adji Prasetiyo Ramadhan[2], Bagus Islamudin Al Faqih[3], Bastomi Baharsyah[4]
sherlysaputri209@gmail.com[1], adjiprasetiyo2005@gmail.com[2], bagus.islamudin05@gmail.com[3], bastomibaharsyah@uinjambi.ac.id[4]
Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi

ABSTRAK

Kebocoran data pribadi di Indonesia terus meningkat meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah berlaku penuh sejak 17 Oktober 2024. Fenomena ini menimbulkan pertanyaan mendasar mengenai efektivitas regulasi tersebut dalam mencegah insiden kebocoran data, sekaligus menyoroti tanggung jawab etika profesi bagi pengelola sistem teknologi informasi. Penelitian ini bertujuan menganalisis secara komparatif tiga kasus kebocoran data terbaru di Indonesia, yaitu insiden ransomware pada Pusat Data Nasional Sementara (PDNS 2) pada Juni 2024, dugaan kebocoran data Nomor Pokok Wajib Pajak (NPWP) pada September 2024, serta dugaan kebocoran 128 juta data registrasi kartu SIM pada Oktober 2025. Penelitian menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus komparatif, bersumber dari rilis resmi instansi, pemberitaan media terverifikasi, dan literatur akademik terkait. Hasil analisis menunjukkan pola serupa pada ketiga kasus, yaitu lambannya pengakuan resmi, minimnya transparansi awal kepada publik, serta lemahnya mekanisme akuntabilitas akibat belum terbentuknya Lembaga Pelindungan Data Pribadi (LPDP) yang diamanatkan UU PDP. Penelitian ini merekomendasikan percepatan pembentukan LPDP serta penguatan pendidikan etika profesi bagi tenaga teknologi informasi dalam pengelolaan data pribadi.

Kata Kunci: Kebocoran Data, UU PDP, Etika Profesi Teknologi Informasi, Keamanan Siber, Perlindungan Data Pribadi.

PENDAHULUAN

Perkembangan teknologi informasi dan transformasi digital di Indonesia mendorong hampir seluruh layanan publik maupun privat bertumpu pada pengelolaan data secara elektronik. Ketergantungan ini di satu sisi meningkatkan efisiensi layanan, namun di sisi lain memperbesar risiko kebocoran data pribadi. Ramadhani dan Suhardiman (2026) mencatat rentetan insiden besar dalam satu dekade terakhir, mulai dari kebocoran 2,3 juta data pemilih (2014), 1,3 juta data pengguna aplikasi eHAC (2020), 1,3 miliar data registrasi kartu SIM (2022), hingga 6 juta data NPWP dan 4,7 juta data pegawai negeri sipil pada 2024 — menunjukkan bahwa kebocoran data berskala besar telah menjadi pola berulang, bukan insiden yang berdiri sendiri.

Pemerintah Indonesia sesungguhnya telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sejak 17 Oktober 2022, dengan masa transisi dua tahun sebelum berlaku penuh pada 17 Oktober 2024. Namun, sejumlah insiden kebocoran data besar justru terjadi tepat pada periode menjelang dan setelah UU PDP berlaku penuh, yaitu insiden ransomware pada Pusat Data Nasional Sementara (PDNS 2) pada 20 Juni 2024 yang melumpuhkan layanan di 210–282 instansi pemerintah dan menimbulkan kerugian ekonomi langsung diperkirakan Rp300 miliar (Puannandini, Faridl, & Buwana, 2026), dugaan kebocoran sekitar 6 juta data Nomor Pokok Wajib Pajak (NPWP) pada September 2024, serta dugaan kebocoran 128,3 juta data registrasi kartu SIM pada Oktober 2025. Fenomena ini menimbulkan pertanyaan kritis: mengapa

kebocoran data masih terus terjadi meski payung hukum sudah tersedia?

Salah satu penjelasan yang mengemuka adalah belum terbentuknya Lembaga Pelindungan Data Pribadi (LPDP) yang diamanatkan Pasal 58 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi sebagai otoritas pengawas independen, meski telah lebih dari tiga tahun sejak UU tersebut disahkan. Ramadhani dan Suhardiman (2026) mengidentifikasi tiga kesenjangan kritis akibat kekosongan lembaga ini: kesenjangan pengawasan (supervisory gap), kesenjangan penegakan sanksi (sanction enforcement gap), dan kesenjangan pemulihan hak (remedy gap) bagi korban. Puannandini, Faridl, dan Buwana (2026) menemukan pula adanya kekosongan hukum mengenai tanggung jawab negara, ketidakjelasan rezim hukum yang berlaku, serta ketiadaan mekanisme ganti rugi yang memadai bagi korban kebocoran data pada institusi publik.

Berdasarkan uraian tersebut, penelitian ini merumuskan tiga permasalahan: (1) bagaimana pola kegagalan perlindungan data pada kasus-kasus kebocoran data periode 2024–2025 dilihat dari sisi tanggung jawab etika profesi pengelola sistem; (2) sejauh mana implementasi UU PDP efektif dalam mencegah dan menangani insiden-insiden tersebut di lapangan; dan (3) apa implikasi kekosongan Lembaga PDP terhadap akuntabilitas dan hak subjek data yang dirugikan.

Penelitian ini bertujuan untuk menganalisis secara komparatif ketiga kasus tersebut guna mengidentifikasi pola kegagalan yang berulang, mengevaluasi efektivitas UU PDP dalam praktik, serta merumuskan implikasinya bagi etika profesi teknologi informasi. Secara akademik, penelitian ini diharapkan memperkaya literatur mengenai keamanan data dan etika profesi TI di Indonesia; secara praktis, hasilnya diharapkan menjadi bahan masukan bagi pembuat kebijakan maupun praktisi TI dalam mengelola data pribadi secara lebih bertanggung jawab.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus komparatif (comparative case study), yang bertujuan mengidentifikasi pola persamaan dan perbedaan di antara beberapa kasus kebocoran data yang terjadi dalam kurun waktu berbeda namun berada pada rezim hukum yang relatif sama.

Sumber data yang digunakan adalah data sekunder, meliputi: (1) rilis resmi dan keterangan pers instansi terkait (Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara, Direktorat Jenderal Pajak); (2) pemberitaan media arus utama yang telah diverifikasi (Antara, CNN Indonesia, Kompas, Kontan, Metro TV News); (3) laporan lembaga riset keamanan siber dan hukum (Sibermate.com, Hukumonline); dan (4) literatur akademik berupa artikel jurnal nasional terkait kebijakan keamanan siber dan etika profesi TI sebagaimana diuraikan pada bagian Tinjauan Pustaka.

Teknik analisis data menggunakan analisis isi (content analysis) lintas kasus, dengan langkah: (1) deskripsi kronologi masing-masing kasus; (2) identifikasi dimensi pembanding (entitas terdampak, penyebab, jenis data, skala, respons institusi, dan kaitan dengan regulasi); (3) penyusunan tabel analisis komparatif; dan (4) interpretasi temuan dalam kerangka etika profesi teknologi informasi dan efektivitas regulasi perlindungan data pribadi.

HASIL DAN PEMBAHASAN

1. Kasus Pusat Data Nasional Sementara 2 (PDNS 2), Juni 2024

Pada 20 Juni 2024, Pusat Data Nasional Sementara (PDNS 2) di Surabaya mengalami serangan ransomware yang dilakukan oleh kelompok yang dikenal dengan

nama Brain Cipher, sebuah varian dari ransomware LockBit 3.0. Rusyda (2025) mencatat bahwa serangan ini berdampak pada 282 instansi pemerintah, di mana hanya 44 instansi yang memiliki cadangan data (backup) sehingga dapat segera pulih, sementara 239 instansi lainnya mengalami gangguan layanan tanpa cadangan data sama sekali. Pelaku meminta tebusan senilai delapan juta dolar Amerika Serikat, dan kerugian finansial diperkirakan mencapai miliaran rupiah, meliputi biaya pemulihan sistem, hilangnya pendapatan akibat layanan terganggu, serta potensi denda akibat pelanggaran perlindungan data. Yang paling mencolok dari investigasi Rusyda (2025) adalah temuan bahwa pengelola PDNS menggunakan kata sandi yang sangat lemah dan mudah ditebak untuk mengamankan server penting tersebut — sebuah indikasi konkret kelalaian teknis dan etis dalam pengelolaan sistem oleh pihak yang seharusnya bertanggung jawab penuh atas keamanan data. Puannandini, Faridl, dan Buwana (2026) menyimpulkan bahwa insiden ini mengungkap kekosongan hukum mengenai tanggung jawab negara, ketidakjelasan rezim hukum yang berlaku, serta minimnya transparansi dalam penanganan insiden, yang berakar dari fragmentasi regulasi dan lemahnya koordinasi antarlembaga. Temuan ini sejalan dengan Rambe dan Hermawan (2025), yang menekankan bahwa lemahnya infrastruktur teknis dan tidak adanya sistem backup yang memadai membuat satu titik kegagalan (single point of failure) berdampak sistemik ke ratusan instansi sekaligus.

2. Kasus Kebocoran Data NPWP, September 2024

Pada 18 September 2024, seorang konsultan keamanan siber mengungkap dugaan kebocoran sekitar 6 juta data Nomor Pokok Wajib Pajak (NPWP) yang diperjualbelikan di forum peretasan BreachForums oleh aktor yang dikenal dengan nama Bjorka. Data yang bocor diduga mencakup Nomor Induk Kependudukan, NPWP, alamat, email, nomor telepon, dan tanggal lahir, termasuk data milik sejumlah pejabat tinggi negara. Direktorat Jenderal Pajak Kementerian Keuangan pada awalnya membantah adanya kebocoran dari sistem informasinya sendiri, dengan menyatakan tidak ditemukan indikasi kebocoran berdasarkan penelusuran log akses dalam enam tahun terakhir. Kasus ini kemudian ditindaklanjuti secara lintas lembaga oleh Kementerian Komunikasi dan Informatika, Badan Siber dan Sandi Negara, dan Direktorat Jenderal Pajak, namun sumber pasti kebocoran hingga naskah ini disusun belum dipublikasikan secara resmi dan konklusif. Pola respons defensif semacam ini turut menegaskan kesenjangan kepatuhan (compliance gap) yang diidentifikasi Ferdiansyah, Amalga, dan Muttaqin (2026) antara kewajiban normatif UU PDP dan kesiapan operasional institusi pengendali data di lapangan.

3. Dugaan Kebocoran Data Registrasi SIM, Oktober 2025

Pada 19 Oktober 2025, kembali muncul klaim kebocoran data berskala besar yang dikaitkan dengan aktor Bjorka, kali ini berupa 128.293.821 rekam data registrasi kartu SIM prabayar dalam format .SQL. Data yang diklaim bocor mencakup Nomor Induk Kependudukan, nomor telepon, nama operator seluler, dan tanggal registrasi kartu. Hingga naskah ini disusun, klaim tersebut masih berstatus dugaan dan belum ada konfirmasi resmi tunggal dari otoritas terkait mengenai sumber maupun validitas penuh data yang beredar. Berulangnya klaim kebocoran berskala ratusan juta data dalam rentang waktu relatif singkat memperkuat argumen Ferdiansyah, Amalga, dan Muttaqin (2026) bahwa UU PDP masih bersifat prinsipil dan belum menetapkan standar teknis minimum yang eksplisit, sehingga insiden semacam ini cenderung terus berulang tanpa mekanisme audit dan akuntabilitas yang memadai.

4. Analisis Komparatif

Tabel 1 menyajikan perbandingan ketiga kasus berdasarkan enam dimensi analisis.

Dimensi	**PDNS 2 (Juni 2024)**	**Kebocoran Data NPWP (September 2024)**	**Dugaan Kebocoran Data Registrasi SIM (Oktober**

			2025)
Entitas terdampak	Kementerian Komunikasi dan Informatika (pengelola Pusat Data Nasional Sementara)	Direktorat Jenderal Pajak, Kementerian Keuangan	Kementerian Komunikasi dan Digital (data registrasi kartu SIM prabayar)
Dugaan penyebab	Serangan ransomware Brain Cipher (varian LockBit 3.0); sentralisasi data tanpa backup terdistribusi	Diduga diretas oleh aktor bernama Bjorka; data dijual di forum peretasan BreachForums	Diduga diunggah oleh aktor bernama Bjorka di forum gelap dalam format .SQL
Jenis data	Data lintas 210–282 instansi pemerintah; layanan keimigrasian dan layanan publik lain terganggu	NIK, NPWP, alamat, email, nomor telepon, tanggal lahir, termasuk data pejabat tinggi negara	NIK, nomor telepon, nama operator seluler, tanggal registrasi kartu SIM
Skala dugaan	210–282 instansi pemerintah terdampak; kerugian ekonomi langsung diperkirakan Rp300 miliar	Sekitar 6 juta data wajib pajak	Diklaim sekitar 128,3 juta rekam data
Respons awal institusi	Mengakui insiden, menolak membayar tebusan, melakukan pemulihan bertahap	Awalnya membantah kebocoran dari sistem internal, kemudian berkoordinasi lintas lembaga	Belum ada konfirmasi resmi tunggal; klaim masih berstatus dugaan
Kaitan dengan UU PDP	Terjadi menjelang UU PDP berlaku penuh (17 Oktober 2024); menyoroti kesiapan infrastruktur negara	Terjadi sebelum UU PDP berlaku penuh; memunculkan wacana potensi gugatan wajib pajak	Terjadi setelah UU PDP berlaku penuh; menyoroti belum terbentuknya Lembaga PDP sebagai pengawas

Tabel 1. Analisis komparatif tiga kasus kebocoran data di Indonesia (2024–2025)

Perbandingan pada Tabel 1 menunjukkan pola yang berulang pada ketiga kasus, yaitu: pertama, institusi yang terdampak cenderung menunjukkan respons defensif pada tahap awal, baik berupa penyangkalan (kasus NPWP) maupun keterlambatan konfirmasi resmi (kasus registrasi SIM), sebelum akhirnya mengakui atau melakukan investigasi lebih lanjut; kedua, ketiga kasus melibatkan data instansi pemerintah atau data yang dikelola atas nama negara, yang seharusnya memiliki standar keamanan lebih tinggi dibanding sektor swasta; ketiga, dua dari tiga kasus (PDNS 2 dan registrasi SIM) terjadi setelah UU PDP berlaku penuh pada 17 Oktober 2024, namun belum menunjukkan perbaikan signifikan dalam pencegahan maupun kecepatan penanganan insiden, memperkuat argumen Ferdiansyah, Amalga, dan Muttaqin (2026) mengenai adanya kesenjangan kepatuhan (compliance gap).

5. Diskusi: Implikasi terhadap Etika Profesi TI dan Efektivitas UU PDP

Ditinjau dari perspektif etika profesi teknologi informasi, ketiga kasus ini mencerminkan pelanggaran terhadap prinsip dasar tanggung jawab profesional sebagaimana diuraikan Zarkasyi (2022), khususnya prinsip keamanan dan kepercayaan data. Pengelola sistem pada institusi-institusi tersebut idealnya menerapkan prinsip privacy-by-design, yakni mengintegrasikan perlindungan data sejak tahap perancangan sistem, bukan sekadar sebagai respons reaktif setelah insiden terjadi — sejalan dengan Pilar Pertama model MSPBEP yang diusulkan Mardhiyah dan Nurmiati (2026), yaitu fondasi etika (ethical foundation), yang tanpanya standar profesi hanya akan menjadi aturan formal tanpa implementasi nyata. Pola respons yang cenderung defensif dan lambat pada ketiga kasus juga menunjukkan lemahnya budaya akuntabilitas profesional, di mana pengakuan kesalahan secara terbuka dan cepat kepada publik masih dianggap sebagai risiko reputasi ketimbang kewajiban etis dan hukum.

Dari sisi efektivitas regulasi, temuan ini memperkuat argumen Ramadhani dan

Suhardiman (2026) bahwa UU PDP hingga saat ini belum berjalan optimal, salah satunya karena Lembaga Pelindungan Data Pribadi sebagai otoritas pengawas independen yang diamanatkan Pasal 58 belum juga terbentuk meski telah lebih dari tiga tahun sejak pengesahan undang-undang tersebut. Tanpa otoritas pengawas yang berwenang, sanksi administratif sebagaimana diatur dalam Pasal 57 UU PDP, termasuk denda hingga dua persen dari pendapatan tahunan pelaku usaha, tidak dapat ditegakkan secara efektif — penegakan hukum pun bersifat reaktif dan hanya menyasar pelaku teknis, bukan institusi yang lalai menjaga data (Ramadhani & Suhardiman, 2026). Temuan ini konsisten dengan Monica dan Permatasari (2025), yang menggunakan teori sistem hukum Lawrence Friedman untuk menunjukkan bahwa persoalan utama bukan pada substansi UU PDP, melainkan pada struktur hukum (legal structure) yang belum mampu melakukan pengawasan secara efektif, serta dengan Gustryan dan Hoesein (2025), yang menegaskan bahwa tantangan utama perlindungan data di Indonesia bukan ketiadaan regulasi, melainkan lemahnya implementasi dan koordinasi kelembagaan. Puannandini, Faridl, dan Buwana (2026) bahkan merekomendasikan konstruksi doktrin tanggung jawab negara berbasis strict liability sebagai solusi atas kekosongan hukum ini, sementara Rusyda (2025) menegaskan urgensi pembentukan peraturan pelaksana pemerintah dan lembaga pengawas independen guna menjamin efektivitas perlindungan data pribadi. Akibatnya, subjek data yang dirugikan pada ketiga kasus di atas tidak memiliki mekanisme pengaduan yang terlembaga secara khusus, dan hanya dapat menempuh jalur pelaporan kepada kepolisian, Kementerian Komunikasi dan Digital, atau upaya hukum perdata yang cenderung memakan waktu lebih panjang — sebagaimana diatur dalam ketentuan pidana Pasal 67, 68, dan 70 UU PDP yang dikaji Putri, Mahendrawati, dan Ujianti (2024).

KESIMPULAN

Berdasarkan analisis komparatif terhadap tiga kasus kebocoran data di Indonesia periode 2024–2025, dapat disimpulkan bahwa: (1) pola kegagalan perlindungan data pada ketiga kasus menunjukkan kesamaan berupa respons awal yang defensif, lambannya transparansi kepada publik, dan lemahnya penerapan prinsip privacy-by-design pada tahap perancangan sistem, yang mencerminkan belum kuatnya budaya etika profesi TI di institusi-institusi terkait; (2) implementasi UU PDP hingga saat ini belum efektif mencegah maupun menangani insiden kebocoran data secara cepat dan akuntabel, sebagaimana ditunjukkan oleh berlanjutnya insiden besar bahkan setelah UU PDP berlaku penuh; dan (3) kekosongan Lembaga Pelindungan Data Pribadi berimplikasi langsung pada lemahnya mekanisme akuntabilitas dan minimnya saluran pemulihan hak bagi subjek data yang dirugikan.

Saran

Bagi pembuat kebijakan, penelitian ini merekomendasikan percepatan pembentukan Lembaga Pelindungan Data Pribadi beserta peraturan turunannya agar mekanisme pengawasan, audit kepatuhan, dan penegakan sanksi dapat berjalan efektif. Bagi institusi pengelola data, khususnya instansi pemerintah, diperlukan penguatan arsitektur keamanan data melalui segmentasi dan sistem cadangan (backup) yang terdistribusi guna mengurangi risiko kegagalan sistemik. Bagi profesional dan pendidikan teknologi informasi, penelitian ini menekankan pentingnya penguatan pendidikan etika profesi yang mengintegrasikan prinsip privacy-by-design serta budaya transparansi dan akuntabilitas dalam pengelolaan data pribadi, sejalan dengan tuntutan hukum yang kini melekat pada profesi tersebut sejak berlakunya UU PDP.

DAFTAR PUSTAKA

Ferdiansyah, D., Amalga, R. S. G., & Muttaqin, M. F. (2026). UU Perlindungan Data Pribadi vs keamanan siber: Analisis kesenjangan dan implikasinya terhadap insiden data di Indonesia. Pasinformatik, 5(2). https://journal.unpas.ac.id/index.php/pasinformatik/article/download/64673/36257

Gustryan, M., & Hoesein, Z. A. (2025). Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam perlindungan data dan privasi di era ekonomi digital. Jurnal Minfo Polgan, 14(2), 3331–3344. https://doi.org/10.33395/jmp.v14i2.15746

Mardhiyah, N., & Nurmiati, E. (2026). Pengembangan model standar profesi berbasis etika bagi profesionalisme TI. Jurnal Analisis, Teknologi, dan Inovasi Sistem Informasi (JATINOM), 1(1), 69–79. https://jurnal.tau.ac.id/index.php/jatinom/article/download/1253/717/5372

Monica, R. D., & Permatasari, E. T. (2025). Tinjauan efektifitas hukum Undang-Undang Perlindungan Data Pribadi dalam kasus kebocoran data di Indonesia. HUNILA: Jurnal Ilmu Hukum dan Integrasi Peradilan, 4(2), 103–116. https://doi.org/10.53491/hunila.v4i2.2077

Puannandini, D. A., Faridl, F., & Buwana, S. A. N. (2026). Tanggung jawab hukum negara atas kebocoran data publik di era interkoneksi digital nasional: Analisis kasus serangan siber PDNS Kementerian Komunikasi dan Digital. Jurnal Pendidikan Tambusai, 10(1), 3627–3635. https://doi.org/10.31004/jptam.v10i1.36643

Putri, N. M. D. G., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2024). Perlindungan hukum terhadap data pribadi warga negara Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022. Jurnal Preferensi Hukum, 5(2), 240–245. https://doi.org/10.22225/jph.5.2.2024.240-245

Ramadhani, G., & Suhardiman, C. (2026). Kebuntuan pembentukan Lembaga Pelindungan Data Pribadi dan implikasinya terhadap efektivitas UU PDP di Indonesia. Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora (JURRISH), 5(2), 793–805. https://doi.org/10.55606/jurrish.v5i2.8513

Rambe, R., & Hermawan, F. F. (2025). The impact of ransomware on Indonesia's national data security: Case study of Kominfo data leaks. Indonesian Journal on Computing (Indo-JC), 10(1), 1–11. https://doi.org/10.21108/indojc.v10i1.8976

Rusyda, N. K. (2025). Perlindungan hukum terhadap subjek data kebocoran data oleh badan publik menurut UU Nomor 27 Tahun 2022. Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, 2(3), 247–262. https://doi.org/10.62383/desentralisasi.v2i3.940

Sembiring, F., & Pattihahuan, F. M. (2024). Peran Badan Siber dan Sandi Negara dalam kasus serangan siber yang mengakibatkan kebocoran data pribadi Pusat Data Nasional Sementara 2 (PDNS2). Gloria Justitia, 5(1), 4–6. https://doi.org/10.25170/gloriajustitia.v5i1.6807

Zarkasyi, Z. (2022). Etika profesi dalam bidang teknologi informasi. Jurnal Teknologi Terapan and Sains 4.0, 3(1), 719–724. https://doi.org/10.29103/tts.v3i1.8870

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

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

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Metrotvnews.com. (2025, 19 Oktober). Bjorka muncul lagi, klaim 128 juta data SIM bocor. https://www.metrotvnews.com/read/bw6CgM4o-bjorka-muncul-lagi-klaim-128-juta-data-sim-bocornomor-tokoh-publik-ikut-terseret

Investortrust.id. (2024, 21 September). Data NPWP Jokowi dan 6 juta wajib pajak bocor, Kemenkominfo klarifikasi ke DJP. https://www.investortrust.id