QISTINA: Jurnal Multidisiplin Indonesia
P-ISSN: 2964-6278 E-ISSN: 2964-1268
Vol. 4 No. 1 Juni 2025

Analisis Kebocoran Data NPWP dalam Sistem e-Government: Tinjauan Keamanan Informasi dan Kepercayaan Publik

Aila Azhara[1] Fachri Devio Rahmadi[2] M Rasul Pilihan[3] Mhd Tri Syahrofi[4] Nabil Abdilla[5] Natasya Alfatikha Maritza[6] Siti Fatimatuzzahro[7]
Universitas Riau, Kota Pekanbaru Baru, Provinsi Riau, Indonesia[1,2,3,4,5,6,7]
Email: aila.azhara3862@student.unri.ac.id[1] fachri.devio6843@student.unri.ac.id[2]
m.rasul6785@student.unri.ac.id[3] mhd.tri7414@student.unri.ac.id[4]
nabil.abdilla4560@student.unri.ac.id[5] natasya.alfatikha3732@student.unri.ac.id[6]
siti.fatimatuzzahro3779@student.unri.ac.id[7]

Abstrak

Fenomena digitalisasi layanan publik melalui sistem e-government di Indonesia menghadirkan kemudahan akses bagi masyarakat, namun sekaligus memunculkan tantangan serius terkait perlindungan data pribadi. Salah satu isu krusial yang mengemuka adalah kebocoran data Nomor Pokok Wajib Pajak (NPWP), yang berpotensi melemahkan kepercayaan publik terhadap layanan digital pemerintah. Penelitian ini bertujuan untuk mengidentifikasi faktor penyebab kebocoran data NPWP, mengevaluasi tingkat keamanan informasi dalam sistem e-government berdasarkan regulasi yang berlaku, serta menganalisis dampak insiden kebocoran terhadap kepercayaan publik. Di samping itu, penelitian ini juga mengkaji respons pemerintah dan merumuskan rekomendasi strategis untuk meningkatkan keamanan siber serta kepercayaan masyarakat. Jenis penelitian yang digunakan adalah penelitian kualitatif deskriptif berbasis studi literatur (library research). Sumber data sekunder terdiri atas jurnal ilmiah terkait e-government dan keamanan siber, peraturan perundang-undangan (UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dan PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik), laporan resmi, serta pemberitaan dari media terpercaya. Teknik analisis data dilakukan melalui analisis isi (content analysis) untuk mengkaji dokumen, regulasi, serta kasus kebocoran data, serta koding tematik untuk mengelompokkan informasi berdasarkan aspek keamanan, kepercayaan publik, dan kebijakan pemerintah. Hasil penelitian menunjukkan bahwa kebocoran data NPWP disebabkan oleh kelemahan teknis sistem, rendahnya standar kepatuhan terhadap kebijakan keamanan informasi, serta kurangnya responsivitas awal dari pihak terkait. Hal ini berdampak langsung pada penurunan kepercayaan publik terhadap layanan e-government. Studi ini juga membandingkan praktik keamanan data di Indonesia dengan negara lain seperti Estonia dan Singapura, yang telah mengadopsi pendekatan komprehensif berbasis keamanan siber dan tata kelola data yang kuat. Oleh karena itu, penelitian ini merekomendasikan peningkatan kebijakan keamanan data, penguatan kolaborasi antar lembaga, serta strategi pemulihan kepercayaan publik berbasis transparansi dan akuntabilitas.

Kata Kunci: E-Government, Kebocoran Data NPWP, Kepercayaan Publik, Keamanan Informasi, UU PDP

Abstract

The phenomenon of digitalization of public services through the e-Government system in Indonesia provides easy access for the public, but at the same time raises serious challenges related to personal data protection. One of the crucial issues that has emerged is the leakage of Taxpayer Identification Number (NPWP) data, which has the potential to increase public trust in government digital services. This study aims to identify the factors causing NPWP data leakage, distribute the level of information security in the e-Government system based on applicable regulations, and analyze the impact of leaks on public trust. In addition, this study also examines the government's response and formulates strategic recommendations to improve cybersecurity and public trust. The type of research used is descriptive qualitative research based on literature studies. Secondary data sources consist of scientific journals related to e-government and cybersecurity, laws and regulations (Law No. 27 of 2022 concerning Personal Data Protection and PP No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions), official reports, and news from trusted media. Data analysis techniques were carried out through content analysis to examine documents, regulations, and data leak cases, as well as thematic coding to group information

based on aspects of security, public trust, and government policy. The results of the study indicate that the NPWP data leak was caused by technical weaknesses in the system, low standards of compliance with information security policies, and a lack of initial responsiveness from related parties. This has a direct impact on reducing public trust in e-government services. This study also compares data security practices in Indonesia with other countries such as Estonia and Singapore, which have adopted a comprehensive approach based on cybersecurity and strong data governance. Therefore, this study recommends improving data security policies, strengthening collaboration between institutions, and strategies for restoring public trust based on transparency and accountability.
Keywords: *E-Government, NPWP Data Leak, Public Trust, Information Security, PDP Law*

PENDAHULUAN

Saat ini, digitalisasi merupakan suatu keniscayaan. Pemerintah sebagai aktor utama dalam suatu negara dituntut untuk mampu menguasai teknologi informasi dan digitalisasi guna memenuhi pelayanan kepada masyarakat secara lebih efektif, efisien, dan merata. Indonesia telah memasuki era Industri 4.0 yang ditandai dengan berkembangnya teknologi informasi dan komunikasi. Transformasi ini dapat dilihat dari berbagai aspek, terutama dari banyaknya aplikasi dan layanan berbasis teknologi yang dikembangkan oleh pemerintah (Fauzi et al., 2024). Digitalisasi pelayanan publik kini menjadi bagian integral dari agenda reformasi birokrasi dan modernisasi tata kelola pemerintahan. Dalam konteks ini, kepercayaan publik terhadap institusi negara menjadi faktor kunci yang menentukan keberhasilan adopsi teknologi digital. Kepercayaan tidak hanya berkaitan dengan persepsi masyarakat terhadap efektivitas pelayanan, tetapi juga mencakup persepsi atas perlindungan hak-hak dasar mereka, termasuk hak atas privasi dan keamanan data pribadi. Kepercayaan publik *(public trust)* berakar pada gagasan bahwa masyarakat bersedia berinteraksi dan bekerja sama dengan negara apabila mereka merasa negara bertindak secara transparan, akuntabel, dan responsif. Transparansi berarti pemerintah mampu membuka informasi publik dengan jelas dan mudah diakses. Akuntabilitas menuntut pemerintah untuk bertanggung jawab atas segala kebijakan, sistem, dan keputusan yang dibuat, terutama dalam hal perlindungan data pribadi. Responsivitas mencerminkan sejauh mana pemerintah tanggap terhadap keluhan, aspirasi, dan kebutuhan masyarakat yang disampaikan melalui kanal-kanal digital. Ketiga prinsip tersebut menjadi pondasi utama dalam membangun sistem e-government yang sehat. Dalam praktiknya, e-government di Indonesia telah diwujudkan melalui peluncuran sejumlah aplikasi digital seperti SP4N-LAPOR, PeduliLindungi, serta sistem administrasi dan perpajakan digital lainnya. Akan tetapi, tantangan besar muncul ketika infrastruktur teknologi informasi pemerintah tidak mampu menjamin keamanan data, yang berakibat pada menurunnya kepercayaan masyarakat. Salah satu kasus paling serius dalam beberapa tahun terakhir adalah kebocoran data Nomor Pokok Wajib Pajak (NPWP) pada tahun 2024 (Naylawati Bahtiar, 2022).

Kebocoran data NPWP tahun 2024 menjadi preseden buruk dalam sejarah transformasi digital pemerintahan Indonesia. Kasus ini memperlihatkan dengan jelas betapa rapuhnya sistem pengamanan data digital yang dikelola negara. NPWP merupakan identitas penting dalam sistem perpajakan nasional, yang diatur dalam Undang-Undang Nomor 16 Tahun 2000 tentang Ketentuan Umum dan Tata Cara Perpajakan yang telah diubah dengan Undang-Undang Nomor 7 Tahun 2021 tentang Harmonisasi Peraturan Perpajakan (Tobing et al., 2022). NPWP menyimpan data yang sangat sensitif, seperti nama lengkap, tempat dan tanggal lahir, alamat, serta status kependudukan yang juga tercantum dalam dokumen-dokumen identitas resmi lain seperti KTP, SIM, dan KK. Kebocoran data tersebut berimplikasi sangat luas — mulai dari

pencurian identitas, penyalahgunaan data untuk tindak pidana, hingga penipuan dengan modus digital yang semakin canggih. Dalam konteks sosial-politik, kebocoran data NPWP juga menciptakan krisis kepercayaan terhadap kredibilitas sistem perpajakan nasional yang seharusnya menjadi salah satu fondasi keuangan negara. Kasus kebocoran data Nomor Pokok Wajib Pajak (NPWP) pada tahun 2024 menjadi sorotan besar publik karena diduga melibatkan sekitar 6 juta data pribadi warga negara Indonesia, termasuk data milik Presiden Jokowi, anak-anaknya, dan sejumlah pejabat tinggi negara. Data tersebut diperdagangkan oleh akun anonim "Bjorka" di forum gelap Breach Forums, mencakup informasi sensitif seperti NIK, alamat, email, nomor telepon, dan bahkan data penghasilan. Pemerintah melalui Kementerian Keuangan, Kominfo, BSSN, dan Polri segera melakukan penyelidikan, meskipun Ditjen Pajak menyatakan belum menemukan jejak kebocoran dalam sistem mereka berdasarkan log 6 tahun terakhir. Presiden Jokowi menduga insiden ini terjadi akibat kelalaian seperti penggunaan sandi yang lemah dan sistem penyimpanan yang tidak terpisah. Meskipun demikian, publik menilai insiden ini mencerminkan lemahnya tata kelola keamanan siber dan perlindungan data nasional.

Berbagai pihak, termasuk DPR dan pengamat siber, mengkritik keras kegagalan pemerintah dalam mencegah kebocoran ini. DPR mendesak percepatan pembentukan Lembaga Perlindungan Data Pribadi sesuai amanat UU PDP yang sudah disahkan sejak 2022 namun belum berjalan efektif. Pakar keamanan menyebut risiko dari kebocoran ini sangat tinggi, mulai dari penipuan pajak hingga penyalahgunaan identitas. Kepercayaan masyarakat terhadap sistem digital pemerintah terancam, dan ini berdampak langsung pada legitimasi sistem perpajakan serta efektivitas layanan publik digital lainnya. Kasus ini membuka mata bahwa Indonesia perlu segera membenahi sistem keamanan data nasional, termasuk audit sistem digital, penguatan regulasi, peningkatan literasi siber, dan penegakan hukum yang tegas terhadap pelanggaran perlindungan data pribadi. Kasus kebocoran ini tidak berdiri sendiri. Sebelumnya, masyarakat Indonesia juga telah menghadapi berbagai insiden serupa. Pada tahun 2020, data 2,3 juta pemilih bocor dari sistem Komisi Pemilihan Umum (KPU), lalu disusul oleh kebocoran data 279 juta peserta BPJS Kesehatan (Naylawati Bahtiar, 2022). Bahkan Bank Indonesia pun tidak luput dari serangan siber yang mengekspos informasi penting milik institusi dan individu. Satu per satu institusi strategis negara menjadi korban pelanggaran keamanan siber. Hal ini menimbulkan pertanyaan besar mengenai kesiapan teknis dan kapasitas kelembagaan pemerintah dalam menjaga data masyarakat. Apabila data pajak — yang notabene merupakan data dengan tingkat kerahasiaan tinggi — dapat bocor ke ruang publik, maka tidak tertutup kemungkinan data-data lainnya seperti data kesehatan, data pendidikan, hingga data keuangan pribadi turut menjadi sasaran.

Kasus kebocoran data NPWP pada 2024 memiliki efek domino terhadap ketaatan warga negara. Pajak adalah instrumen vital dalam pembangunan nasional. Ketika warga tidak lagi percaya bahwa pemerintah mampu menjaga data pribadi mereka, maka akan timbul resistensi dalam menyampaikan laporan dan membayar kewajiban perpajakan secara jujur dan terbuka (Bua et al., 2025). Ini menjadi ancaman serius terhadap penerimaan negara yang bersumber dari pajak, sekaligus melemahkan daya dorong pembangunan nasional. Kepercayaan publik yang menurun juga memperburuk efektivitas kebijakan digital, karena masyarakat menjadi ragu untuk menggunakan layanan berbasis daring, menghindari aplikasi resmi, dan cenderung memilih jalur manual atau bahkan tidak patuh administrasi. Tantangan besar ini juga menunjukkan bahwa penguatan perlindungan hukum terhadap data pribadi menjadi sangat mendesak. Indonesia memang telah mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur hak-hak subjek data, tanggung jawab pengendali dan prosesor data, serta mekanisme sanksi terhadap pelanggaran. Namun,

pelaksanaan undang-undang ini masih menghadapi berbagai hambatan, mulai dari lemahnya koordinasi antar lembaga, keterbatasan sumber daya manusia di bidang keamanan siber, hingga minimnya literasi digital di kalangan pengguna dan penyelenggara layanan. Selain itu, UU PDP masih harus didukung dengan implementasi standar internasional seperti ISO/IEC 27001 untuk membangun sistem manajemen keamanan informasi (ISMS) yang menyeluruh dan berkelanjutan.

Dari sisi masyarakat, rendahnya kesadaran terhadap pentingnya privasi digital juga menjadi salah satu faktor penyebab kerentanan. Banyak warga yang masih secara sadar atau tidak sadar membagikan informasi pribadi mereka melalui media sosial, situs tidak resmi, atau dalam interaksi daring lainnya (Ham et al., 2025). Di sisi lain, kurangnya edukasi dan transparansi dari pemerintah mengenai risiko keamanan digital turut memperparah keadaan. Infrastruktur penyimpanan dan pengelolaan data pemerintah pun kerap kali masih menggunakan sistem yang usang, tidak terenkripsi dengan baik, atau tidak terintegrasi secara aman antar instansi. Ini membuka celah besar bagi serangan siber, baik dari dalam maupun luar negeri. Dengan demikian, kebocoran data NPWP 2024 harus dilihat sebagai momentum korektif yang mendorong semua pihak untuk memperkuat arsitektur keamanan data nasional. Pemerintah perlu menetapkan standar keamanan minimum yang wajib diterapkan oleh seluruh kementerian, lembaga, dan instansi pengelola data publik. Sistem audit independen terhadap keamanan siber juga harus diperkuat, agar setiap potensi celah bisa segera diperbaiki sebelum dimanfaatkan pihak yang tidak bertanggung jawab. Lebih penting lagi, harus ada transparansi dan komunikasi terbuka kepada masyarakat setiap kali terjadi insiden, disertai dengan solusi, kompensasi, dan langkah pemulihan yang nyata. Hal ini penting untuk menunjukkan bahwa pemerintah hadir dan bertanggung jawab, serta menjamin bahwa insiden serupa tidak akan terulang kembali di masa mendatang. Digitalisasi layanan publik tidak bisa dilepaskan dari isu kepercayaan publik. Kasus kebocoran data NPWP tahun 2024 adalah pelajaran pahit yang harus direspons dengan serius oleh seluruh elemen pemerintahan. Jika tidak ditangani secara struktural dan menyeluruh, bukan hanya sistem digital yang akan gagal, melainkan juga integritas dan legitimasi negara dalam mata rakyatnya. Oleh karena itu, pemerintah harus menyadari bahwa keamanan digital adalah bagian dari hak asasi warga negara yang wajib dilindungi secara serius dan sistematis.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif sebagai kerangka utama dalam mengkaji fenomena kebocoran data pribadi di ruang digital layanan publik, khususnya terkait data Nomor Pokok Wajib Pajak (NPWP) dalam sistem e-government di Indonesia. Studi literatur dipilih karena mampu memberikan pemahaman yang komprehensif terhadap dinamika kompleks yang melibatkan aspek teknologi informasi, regulasi perlindungan data, serta kepercayaan publik terhadap sistem digital pemerintah. Fokus penelitian diarahkan pada insiden-insiden kebocoran data NPWP yang merepresentasikan lemahnya sistem keamanan informasi dan belum optimalnya tata kelola data pribadi oleh institusi negara, yang pada gilirannya berdampak langsung terhadap menurunnya kepercayaan masyarakat. Sumber data dalam penelitian ini bersifat sekunder dan diperoleh dari berbagai literatur akademik, termasuk jurnal ilmiah nasional maupun internasional yang relevan dengan tema e-government, keamanan siber, dan manajemen data digital. Literatur dikumpulkan melalui basis data daring seperti Google Scholar, Sinta, dan DOAJ, dengan batas waktu publikasi antara tahun 2015 hingga 2025. Selain itu, digunakan pula dokumen resmi negara dan instrumen hukum yang mengatur keamanan informasi, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP No. 71/2019), serta Peraturan

BSSN dan kebijakan teknis dari Kementerian Komunikasi dan Informatika (Kominfo). Untuk memperkaya data empiris, juga dianalisis laporan insiden dan siaran pers dari BSSN dan Kominfo, serta pemberitaan media terpercaya seperti Katadata, Kompas, dan Tempo, dengan verifikasi silang untuk menjaga akurasi informasi yang dikumpulkan.

Analisis data dilakukan menggunakan metode analisis isi (content analysis), yang mencakup telaah sistematis terhadap dokumen hukum, laporan resmi, dan artikel media untuk mengidentifikasi struktur, kelemahan, serta tanggapan kebijakan terkait pengelolaan keamanan data NPWP. Proses analisis ini dikembangkan melalui analisis tematik, yang mencakup enam tahapan utama, yaitu familiarisasi data, pengkodean awal, pencarian tema, peninjauan tema, pendefinisian dan penamaan tema, serta penulisan laporan. Tema-tema utama yang diidentifikasi dalam proses ini antara lain: (1) faktor penyebab teknis dan kelembagaan dalam kebocoran data NPWP; (2) efektivitas regulasi keamanan informasi dalam sistem e-government; (3) dampak kebocoran data terhadap tingkat kepercayaan publik; (4) tanggapan dan strategi pemerintah dalam pemulihan sistem dan kredibilitas layanan digital; serta (5) pembelajaran dari praktik keamanan data di negara lain untuk memperkuat ketahanan siber nasional. Penelitian ini dibingkai oleh beberapa pendekatan teoretis, termasuk Teori Kepercayaan Publik yang menekankan pentingnya transparansi, akuntabilitas, dan responsivitas dalam menjaga hubungan antara pemerintah dan warga negara di era digital. Selain itu, digunakan juga konsep-konsep dari teori sistem informasi publik, serta prinsip-prinsip keamanan informasi yang mengacu pada standar internasional (misalnya ISO/IEC 27001) sebagai dasar untuk menilai kelayakan dan kerentanan sistem. Untuk menjamin validitas dan reliabilitas hasil penelitian, diterapkan strategi triangulasi sumber melalui perbandingan informasi dari regulasi, literatur ilmiah, dan media massa. Selain itu, dilakukan validasi konseptual melalui diskusi akademik sejawat (peer debriefing) dan audit trail dalam bentuk dokumentasi proses analisis yang transparan dan sistematis.

HASIL PENELITIAN DAN PEMBAHASAN

Kebocoran data NPWP yang paling buruk adalah kasus yang diinisiasi oleh akun Bjorka. Insiden ini melibatkan kebocoran data pribadi, termasuk data NPWP, yang dibocorkan melalui situs open source dan diperjualbelikan. Aktornya adalah peretas yang mengidentifikasi dirinya sebagai Bjorka, dan sistem yang bocor diduga berasal dari sistem DJP. Bentuk kebocoran data adalah data pribadi, termasuk data NPWP, yang mencakup data pribadi seperti nama, alamat, dan informasi lainnya. Bjorka adalah seorang hacker anonim yang namanya mencuat karena berbagai aksi peretasan yang menggemparkan Indonesia. Salah satu aksinya yang paling heboh adalah klaimnya berhasil meretas data pribadi lebih dari 6 juta wajib pajak, termasuk data tokoh penting seperti Presiden Joko Widodo dan Gibran Rakabuming Raka. Meskipun identitas aslinya belum terungkap, Bjorka dikenal aktif di forum-forum internet dan sering mempublikasikan data yang ia klaim diperoleh dari sistem pemerintahan atau perusahaan besar di Indonesia. Bjorka pertama kali menarik perhatian ketika ia merilis data pribadi sejumlah pejabat tinggi. Sejak saat itu, aksinya semakin berani, dengan meretas data sensitif warga negara, termasuk data vaksinasi dan informasi pribadi lainnya. Aksi terbarunya, yaitu kebocoran data Nomor Pokok Wajib Pajak (NPWP), menjadi sorotan besar dan mengundang kekhawatiran terkait keamanan data di Indonesia, (https://www.codepolitan.com/, 2024). Kasus kebocoran data NPWP (Nomor Pokok Wajib Pajak) merupakan sebuah insiden yang menimbulkan kekhawatiran besar terkait perlindungan data pribadi warga negara Indonesia.

Presiden Joko Widodo mengungkapkan bahwa kebocoran ini disebabkan oleh keteledoran dalam pengelolaan password dan penyimpanan data yang tidak aman (Tempo, 2023). Dalam konteks ini, penting untuk menganalisis bagaimana pemerintah merespons insiden ini dan langkah-langkah yang diambil untuk memulihkan kepercayaan publik.Respon

pemerintah terhadap kebocoran data, melalui pernyataan Presiden Jokowi, menekankan pentingnya mitigasi terhadap kebocoran data ini. Jokowi meminta Kementerian Komunikasi dan Informatika serta Kementerian Keuangan untuk segera mengambil langkah-langkah yang diperlukan (Tempo, 2023). Hal ini menunjukkan keseriusan pemerintah dalam menangani masalah keamanan data, terutama yang berkaitan dengan informasi sensitif seperti NPWP. Evaluasi Internal yang dilakukan oleh Menteri Keuangan Sri Mulyani juga meminta Direktorat Jenderal Pajak untuk melakukan evaluasi menyeluruh terhadap insiden ini. Ini mencakup analisis terhadap sistem yang ada dan identifikasi celah keamanan yang mungkin ada (Tempo, 2023) serta melakukan koordinasi dengan Badan Siber dan Sandi Negara (BSSN), yang dimana Pemerintah juga melibatkan BSSN untuk membantu dalam mitigasi dan perbaikan sistem keamanan data. Ini menunjukkan bahwa pemerintah tidak hanya mengandalkan satu lembaga, tetapi melakukan kolaborasi lintas sektoral untuk mengatasi masalah ini, (https://www.codepolitan.com/, 2024).

Terkait hal ini, Kementerian Kominfo menyatakan telah meminta klarifisikasi pada DJP Kementerian Keuangan. Langkah ini didasarkan pada PP nomor 71 tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik (PP PSTE). Tidak hanya itu, Kominfo juga terus berkoordinasi dengan pihak terkait lainnya soal dugaan kebocoran data wajib pajak ini. Dirjen Informasi dan Komunikasi Publik Kementerian Kominfo, Prabu Revolusi juga mengatakan UU PDP mengatur ketentuan pidana terhadap setiap orang yang dengan sengaja melawan hukum, seperti mengungkapkan Data Pribadi yang bukan miliknya atau menggunakan data Data Pribadi yang bukan miliknya dapat dipidana dengan pidana penjara paling lama 4 tahun dan/atau pidana denda paling banyak 4 miliar rupiah. Sementara menggunakan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak 5 miliar rupiah. [22.32, 9/6/2025] Aila Azhara (Aza): ak 4 miliar rupiah. Sementara menggunakan Data Pribadi yang bukan miliknya dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak 5 miliar rupiah. Prabu Revolusi selaku Dirjen Informasi dan Komunikasi Publik Kementerian Kominfo mengatakan "Kementerian Komunikasi dan Informatika (Kemenkominfo) mendukung penuh dan telah bekerja sama dengan Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia, dan Direktorat Jenderal Pajak (DJP) Kementerian Keuangan, untuk melakukan investigasi dan mitigasi atas dugaan kebocoran data pribadi."

Kebocoran ini dapat terjadi akibat kelemahan sistem keamanan, serangan siber, kesalahan manusia, atau tindakan internal yang menyalahgunakan akses data. Dampaknya cukup serius, karena data NPWP yang bocor dapat disalahgunakan untuk tindakan penipuan, pencurian identitas, maupun kejahatan siber lainnya, sehingga merugikan individu maupun negara. Pemerintah Indonesia melalui Direktorat Jenderal Pajak (DJP) dan Kementerian Komunikasi dan Informatika terus berupaya memperkuat sistem keamanan data perpajakan, termasuk penerapan teknologi enkripsi dan audit keamanan secara berkala, guna mencegah kejadian serupa di masa mendatang. Selain itu, pengaturan perlindungan data pribadi sedang diperkuat melalui Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), yang bertujuan memberikan sanksi tegas terhadap pelanggaran keamanan data. Kasus kebocoran data NPWP menegaskan pentingnya peningkatan sistem keamanan dan kesadaran akan perlindungan data pribadi di era digital saat ini. Kebocoran data pribadi yang dilakukan oleh peretas Bjorka terhadap 6,6 juta data wajib pajak dari Direktorat Jenderal Pajak (DJP) telah mengguncang ranah keamanan siber Indonesia. Insiden ini tidak hanya mengekspos data sensitif warga negara, termasuk Indonesia Presiden Joko Widodo dan para menteri, tetapi juga berpotensi menimbulkan dampak serius terhadap kepercayaan publik pada sistem keamanan nasional.

Kebocoran data NPWP (Nomor Pokok Wajib Pajak) yang melibatkan sekitar 6 juta data pribadi warga Indonesia pada tahun 2024 merupakan manifestasi dari berbagai kelemahan sistemik dalam pengelolaan keamanan informasi pada infrastruktur *e-government* nasional. Insiden ini bukan hanya mencerminkan kegagalan teknis semata, tetapi juga mengindikasikan adanya permasalahan kompleks yang melibatkan aspek teknologi, sumber daya manusia, tata kelola organisasi, dan kerangka regulasi yang saling berinteraksi dan memperkuat kerentanan sistem secara keseluruhan. Berdasarkan analisis terhadap berbagai sumber literatur dan laporan investigasi, faktor-faktor penyebab kebocoran data NPWP dapat dikategorikan ke dalam lima dimensi utama yang saling berinteraksi dan memperkuat kerentanan sistem secara keseluruhan. Berdasarkan artikel (KEUANGAN, 2022), terdapat tiga faktor utama yang menjadi penyebab kebocoran data, khususnya data pribadi. Ketiga faktor tersebut adalah:

1. Kesalahan Manusia *(human error)*: Kelemahan Dasar dalam Perilaku Digital. Human error merupakan faktor penyebab kebocoran data yang paling signifikan karena memanfaatkan kelemahan alamiah manusia dalam berinteraksi dengan teknologi digital. Dalam konteks kebocoran data NPWP Indonesia, human error tidak hanya terbatas pada "keteledoran password" yang disebutkan Presiden Jokowi, tetapi mencakup jangkauan perilaku yang lebih luas. Fitrah manusia yang hobi mempraktekkan kebiasaan ekonomis, di antaranya dengan mencari *free software* atau aplikasi bajakan (yang biasanya memberikan iming-iming free trial atau bonus-bonus lainnya), "memaksa" pengguna untuk secara sukarela memasukkan data pribadi berupa nomor telepon di situs atau aplikasi yang tidak terjamin keamanannya. Perilaku ini dilakukan tanpa kesadaran akan risiko keamanan yang ditimbulkan. Dalam konteks sistem pemerintahan, human error merupakan salah satu faktor utama yang menyebabkan kebocoran atau kerentanan data. Kesalahan ini dapat muncul dalam berbagai bentuk perilaku atau kelalaian yang tampaknya sepele, namun berdampak besar terhadap keamanan sistem. Salah satu contohnya adalah penggunaan password yang lemah atau mudah ditebak oleh petugas sistem. Praktik ini memudahkan pihak yang tidak berwenang untuk mengakses sistem tanpa kesulitan berarti. Selain itu, kebiasaan berbagi kredensial login antara beberapa pengguna demi alasan efisiensi operasional juga sangat berisiko, karena menyulitkan pelacakan aktivitas pengguna dan meningkatkan peluang penyalahgunaan data. Masalah lain muncul ketika protokol keamanan yang telah ditetapkan diabaikan karena dianggap menghambat produktivitas. Padahal, protokol tersebut dibuat untuk melindungi integritas sistem dan data. Kurangnya kehati-hatian dalam mengelola akses ke sistem yang berisi data sensitif juga dapat menyebabkan pihak yang tidak berwenang memperoleh informasi yang seharusnya dilindungi. Terakhir, ketidaksadaran terhadap pentingnya prosedur backup dan recovery data menjadikan sistem rawan kehilangan data penting apabila terjadi insiden seperti serangan siber atau kerusakan teknis. Semua contoh tersebut menunjukkan bahwa edukasi dan peningkatan kesadaran keamanan siber di lingkungan pemerintahan sangatlah penting untuk meminimalkan risiko yang timbul akibat human error. Human error dalam konteks sistem e-government tidak bisa dianggap sepele, karena konsekuensinya bersifat sistemik dan meluas. Sistem pemerintahan digital menyimpan dan mengelola data jutaan warga negara, mulai dari informasi identitas pribadi hingga data keuangan dan kependudukan. Oleh karena itu, satu kesalahan kecil yang dilakukan oleh operator atau petugas sistem dapat menimbulkan dampak yang sangat besar. Sebagai contoh, kasus kebocoran data NPWP yang pernah terjadi menunjukkan betapa seriusnya akibat dari kelalaian manusia. Dalam insiden tersebut, sekitar 6 juta data pribadi warga Indonesia terekspos dan berpotensi disalahgunakan. Ini bukan hanya mengancam privasi individu, tetapi juga dapat merusak kepercayaan publik terhadap sistem digital pemerintahan, bahkan membuka peluang bagi

tindak kejahatan siber seperti penipuan, pencurian identitas, hingga manipulasi data. Selain itu, dampak sistemik dari human error juga bisa menyebabkan gangguan operasional pemerintahan, kerugian finansial, dan ketidakstabilan kebijakan publik jika data yang bocor digunakan untuk menyebarkan disinformasi atau mempengaruhi proses pengambilan keputusan. Oleh karena itu, penguatan kapasitas SDM, literasi digital, dan penerapan sistem pengamanan berlapis menjadi sangat penting dalam ekosistem e-government.

2. Serangan Malware. Serangan malware menjadi salah satu faktor utama yang turut berkontribusi signifikan terhadap kebocoran data, terlebih dengan tingkat kecanggihan yang terus berkembang seiring kemajuan teknologi. Salah satu celah yang sering dimanfaatkan oleh malware adalah kelalaian pengguna dalam memeriksa email, baik saat menerima maupun mengirim, yang tanpa disadari dapat membuka pintu bagi infeksi malware masuk ke dalam sistem. Malware pada dasarnya adalah program yang dirancang untuk merusak dengan menyusup ke sistem komputer. Salah satu jenis malware yang berbahaya yaitu spyware. Menurut Kaspersky, salah satu vendor antivirus yang sudah mendunia, spyware merupakan software yang didesain untuk masuk ke dalam perangkat komputer. Spyware mempunyai kemampuan mengumpulkan data-data pribadi user dan mengirimnya kepada pihak ketiga tanpa persetujuan user. Kemampuan ini memungkinkan penyerang untuk mengakses data sensitif secara diam-diam dan dalam jangka waktu yang panjang.
3. *Social Engineering* : Manipulasi Psikologis untuk Eksploitasi Keamanan. Social engineering merupakan faktor ketiga yang memanfaatkan kelemahan psikologis manusia untuk mengakses sistem dan data yang dilindungi. Social engineering adalah penggunaan manipulasi psikologis untuk mengumpulkan data sensitif seperti nama lengkap, username, password, dan sebagainya melalui media elektronik dengan menyamar sebagai pihak yang dapat dipercaya. Biasanya phishing memanfaatkan email untuk mengelabui korbannya. Email yang dikirimkan pelaku dapat berisi sesuatu yang mengatasnamakan pihak tertentu dan memancing korban untuk mengklik tautan yang tercantum di dalamnya. Bahkan, banyak kasus di mana pelaku mengirimkan SMS yang berisi tautan dengan iming-iming bonus pulsa, yang dapat merupakan kail untuk memancing "ikan-ikan" yang tergoda dengan umpan yang melambai-lambai memanggil untuk diklik. Dalam kasus kebocoran data NPWP, teknik social engineering menjadi salah satu metode yang sangat efektif digunakan oleh penyerang untuk mendapatkan akses ke sistem tanpa harus meretas secara teknis.

Teknik ini memanfaatkan kelemahan psikologis manusia, seperti kepercayaan, rasa ingin tahu, atau ketidaktahuan, untuk mengecoh target agar memberikan informasi atau akses yang seharusnya bersifat rahasia. Salah satu bentuknya adalah spear phishing, yaitu serangan siber yang ditargetkan secara spesifik kepada petugas pajak atau administrator sistem melalui email atau pesan lain yang tampak meyakinkan. Tujuannya adalah memancing korban agar membuka tautan berbahaya atau menyerahkan kredensial login. Metode lain adalah pretexting, di mana penyerang menyamar sebagai petugas IT atau pihak berwenang, lalu menghubungi korban dengan dalih untuk melakukan pembaruan sistem atau pengecekan keamanan, padahal tujuannya adalah memperoleh akses. Baiting juga sering digunakan, yakni dengan memberikan iming-iming seperti software gratis, update sistem palsu, atau informasi menarik yang sebenarnya mengandung malware. Ketika korban tertarik dan mengakses file tersebut, sistem bisa langsung terinfeksi. Terakhir, teknik quid pro quo melibatkan tawaran bantuan palsu, seperti layanan dukungan teknis, sebagai imbalan dari informasi login atau akses ke sistem. Semua teknik ini berbahaya karena sulit dikenali, dan dalam konteks sistem e-government, dampaknya bisa sangat besar karena menyangkut data pribadi jutaan warga.

Ketiga faktor penyebab kebocoran data yaitu human error, malware, dan social engineering tidak bekerja secara terpisah, melainkan saling terhubung dan memperkuat satu sama lain dalam menciptakan multiple attack vectors yang kompleks dan berbahaya. Human error sering kali menjadi titik awal terjadinya pelanggaran keamanan, seperti penggunaan password yang lemah atau kelalaian dalam mengecek keaslian email. Celah ini dapat dimanfaatkan oleh malware, yang masuk ke dalam sistem melalui file atau tautan berbahaya dan kemudian digunakan untuk melakukan reconnaissance atau mengumpulkan informasi internal yang berguna untuk serangan lanjutan. Informasi yang diperoleh dari malware ini kemudian bisa mendukung serangan social engineering, di mana penyerang menggunakan data yang dikumpulkan untuk menciptakan skenario penipuan yang lebih meyakinkan. Melalui taktik seperti spear phishing atau pretexting, korban dapat secara tidak sadar menginstal malware tambahan atau bahkan memberikan akses sistem secara langsung. Dengan kata lain, ketika ketiga faktor ini bekerja secara bersamaan, mereka membentuk rantai serangan yang sangat sulit dihentikan jika tidak diantisipasi sejak awal. Oleh karena itu, strategi perlindungan data tidak cukup hanya mengandalkan aspek teknis, tetapi juga harus mencakup peningkatan kesadaran dan literasi digital pada setiap level pengguna.

Pengelolaan data NPWP (Nomor Pokok Wajib Pajak) dalam sistem e-government menjadi salah satu elemen penting dalam upaya modernisasi administrasi perpajakan di Indonesia. Seiring dengan pesatnya perkembangan teknologi dan digitalisasi layanan publik, pengelolaan data wajib pajak secara elektronik menuntut penerapan standar keamanan informasi yang ketat. Hal ini bertujuan untuk melindungi kerahasiaan, integritas, dan ketersediaan data NPWP dari berbagai ancaman, seperti kebocoran data, penyalahgunaan, dan serangan siber. Oleh karena itu, regulasi yang mengatur keamanan informasi dalam pengelolaan data NPWP sangat diperlukan sebagai landasan hukum yang menjamin perlindungan data pribadi wajib pajak serta mendukung terciptanya sistem administrasi perpajakan yang terpercaya dan akuntabel. Dalam rangka menjamin keamanan dan perlindungan data NPWP, pemerintah Indonesia telah mengatur berbagai regulasi yang menjadi payung hukum bagi pelaksanaan sistem e-government, khususnya dalam pengelolaan data perpajakan. Beberapa regulasi utama yang mengatur hal ini antara lain:

1. Landasan Hukum Utama. Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia diatur dalam Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, (PANrB, 2020) Sistem Pemerintahan Berbasis Elektronik (SPBE) yang bertujuan untuk mewujudkan tata kelola pemerintahan yang terpadu, efisien, dan transparan melalui pemanfaatan teknologi informasi dan komunikasi. Dalam peraturan ini, aspek keamanan informasi menjadi salah satu pilar utama, khususnya dalam domain layanan digital publik seperti sistem administrasi perpajakan. SPBE menekankan pentingnya pengelolaan keamanan siber secara terintegrasi, perlindungan data pribadi, serta kepatuhan terhadap standar interoperabilitas dan integritas sistem digital, termasuk dalam pengelolaan data NPWP oleh Direktorat Jenderal Pajak. Dengan demikian, SPBE menjadi kerangka kerja nasional yang mendukung penguatan sistem e-government agar mampu memberikan layanan yang aman, andal, dan berkelanjutan kepada masyarakat. Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) harus dilaksanakan dengan mengedepankan prinsip keterpaduan dan integrasi antar instansi pemerintah. Hal ini mengharuskan Instansi Pusat maupun Pemerintah Daerah untuk menerapkan unsur-unsur SPBE secara konsisten dan menyeluruh, sesuai dengan kerangka kerja yang telah ditetapkan dalam Tata Kelola SPBE dan Manajemen SPBE. Tata kelola SPBE mencakup pengaturan kebijakan, prosedur, dan pengawasan agar pelaksanaan sistem elektronik pemerintahan dapat berjalan dengan baik dan sesuai standar yang berlaku. Sementara itu, manajemen SPBE menitikberatkan

pada perencanaan, pengelolaan sumber daya, pengendalian risiko, dan evaluasi berkelanjutan guna menjaga efektivitas, efisiensi, dan kesinambungan pelaksanaan SPBE. Dengan penerapan prinsip-prinsip tersebut secara terpadu, diharapkan layanan pemerintahan berbasis elektronik, termasuk pengelolaan data NPWP, dapat memberikan pelayanan publik yang transparan, akuntabel, serta aman bagi seluruh pemangku kepentingan. (Wiki Provinsi Gorontalo, 2024)

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan regulasi cyber law pertama yang disahkan di Indonesia pada tanggal 21 April 2008. UU ini menjadi dasar hukum utama dalam mengatur penggunaan teknologi informasi dan transaksi elektronik di berbagai sektor, termasuk pemerintahan dan layanan publik. Pada tahun 2016, UU ITE mengalami revisi melalui Undang-Undang Nomor 19 Tahun 2016 guna memperkuat ketentuan-ketentuan yang berkaitan dengan keamanan informasi, perlindungan data, serta penanganan tindak pidana di dunia digital. Dengan adanya UU ITE, implementasi sistem elektronik seperti e-government mendapatkan landasan hukum yang kokoh untuk menjamin keabsahan, keamanan, dan integritas transaksi serta komunikasi elektronik di Indonesia. UU ITE menetapkan perlindungan terhadap data elektronik dengan memastikan keamanan, keutuhan, dan kerahasiaannya dalam sistem elektronik. Transaksi elektronik diakui sah secara hukum, termasuk penggunaan tanda tangan digital. UU ini juga memberikan dasar hukum untuk menindak pelanggaran, dengan sanksi pidana bagi pihak yang meretas, menyalahgunakan, atau merusak data elektronik. Relevansi UU ITE terhadap data NPWP sangat penting karena menjadi dasar hukum dalam pengelolaan dan perlindungan data perpajakan secara elektronik. UU ini memberikan legitimasi bagi sistem perpajakan digital, memastikan data wajib pajak, termasuk NPWP, terlindungi dari akses ilegal atau penyalahgunaan, serta menetapkan sanksi tegas bagi pelanggaran yang menyangkut data tersebut. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah mengalami perubahan melalui disahkannya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008. UU ini resmi disahkan oleh Presiden Joko Widodo pada 2 Januari 2024. Perubahan ini mencerminkan upaya pemerintah untuk menyempurnakan regulasi di bidang informasi dan transaksi elektronik, dengan fokus pada penguatan perlindungan hak masyarakat, penyesuaian terhadap perkembangan teknologi digital, serta pengaturan yang lebih jelas mengenai pencemaran nama baik, perlindungan anak di ruang digital, dan kewajiban Penyelenggara Sistem Elektronik (PSE) (INVESTASI, n.d.)
3. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan regulasi komprehensif pertama di Indonesia yang secara khusus mengatur pelindungan data pribadi. Disahkan pada 17 Oktober 2022, UU ini menjadi tonggak penting dalam memastikan hak konstitusional warga negara atas privasi dan kendali atas data pribadi mereka, terutama di tengah pesatnya perkembangan teknologi digital. UU PDP menetapkan hak-hak subjek data kewajiban bagi pengendali dan pemroses data, serta sanksi tegas bagi pihak yang menyalahgunakan data pribadi. Prinsip keabsahan dan keadilan mengharuskan bahwa data pribadi dikumpulkan dan diproses secara sah, adil, dan transparan. Pembatasan tujuan berarti bahwa data pribadi hanya boleh dikumpulkan untuk tujuan yang spesifik dan sah, serta tidak digunakan untuk tujuan lain yang tidak sesuai. Prinsip kecukupan menekankan bahwa data yang dikumpulkan harus memadai, relevan, dan terbatas pada apa yang diperlukan untuk tujuan pemrosesan. Akurasi mengharuskan data pribadi yang dikumpulkan akurat, lengkap, tidak menyesatkan, dan mutakhir. Terakhir,

prinsip keamanan menuntut penerapan langkah-langkah teknis dan organisasi yang tepat untuk melindungi data pribadi dari akses, pengungkapan, pengubahan, atau penghancuran yang tidak sah. Prinsip-prinsip ini sejalan dengan ketentuan dalam Pasal 16 UU PDP, yang menyatakan bahwa pengumpulan data pribadi harus dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan. Pemrosesan data pribadi juga harus sesuai dengan tujuan yang telah ditentukan, menjamin hak subjek data pribadi, dilakukan secara akurat dan dapat dipertanggungjawabkan, serta dilindungi dari akses yang tidak sah. UU PDP mengatur perlindungan data pribadi dengan prinsip utama: data harus diproses secara sah dan adil, digunakan hanya untuk tujuan jelas, cukup dan relevan, akurat dan diperbarui, serta dilindungi dengan keamanan yang memadai. UU PDP membedakan dua jenis data pribadi, yaitu data pribadi umum seperti nama, jenis kelamin, kewarganegaraan, agama, dan status perkawinan, serta data pribadi spesifik yang meliputi informasi sensitif seperti data kesehatan, biometrik, genetika, orientasi seksual, pandangan politik, catatan kejahatan, data anak, dan data keuangan pribadi. Wajib pajak sebagai subjek data memiliki berbagai hak yang dijamin dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Hak-hak ini memberikan kendali penuh kepada individu atas data pribadinya. Salah satunya adalah hak akses, yaitu hak untuk mengetahui dan mendapatkan informasi mengenai data pribadi yang sedang diproses oleh pengendali data. Selain itu, subjek data juga berhak melakukan rectifikasi atau perbaikan terhadap data yang tidak akurat atau sudah tidak sesuai. Dalam kondisi tertentu, subjek data berhak untuk meminta penghapusan data pribadi yang tidak lagi relevan atau apabila pemrosesan data melanggar hukum. Tidak hanya itu, mereka juga memiliki hak untuk memindahkan data pribadinya dari satu pengendali ke pengendali lainnya, yang dikenal sebagai hak portabilitas, guna memastikan kelancaran layanan dan keberlanjutan kontrol atas data pribadi tersebut. Pengendali data pribadi memiliki tanggung jawab besar dalam memastikan bahwa setiap proses pengumpulan, penyimpanan, dan penggunaan data dilakukan sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pengolahan data wajib dilakukan secara terbatas dan spesifik, serta harus sah menurut hukum dan transparan kepada subjek data. Setiap aktivitas pemrosesan data juga harus sesuai dengan tujuan yang telah ditentukan sebelumnya, dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan. Lebih jauh, pengendali data diwajibkan untuk menjamin keamanan data pribadi dari berbagai bentuk ancaman, seperti akses tanpa izin, pengungkapan yang tidak sah, perubahan yang tidak sah, penyalahgunaan, perusakan, atau bahkan penghilangan data. Perlindungan ini menjadi penting untuk menjamin hak-hak subjek data dan menjaga kepercayaan publik terhadap sistem yang menggunakan data pribadi. UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menetapkan sanksi tegas bagi pihak yang melanggar ketentuan perlindungan data pribadi. Pelanggaran dapat dikenai sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data, penghapusan atau pemusnahan data pribadi, serta denda administratif yang dapat mencapai 2% dari pendapatan tahunan atau penerimaan tahunan berdasarkan variabel pelanggaran. Selain itu, pelanggaran yang bersifat serius juga dapat dikenai sanksi pidana, dengan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah). Ketentuan ini menunjukkan komitmen pemerintah dalam menegakkan perlindungan hak privasi warga negara di era digital.

4. Peraturan Menteri Keuangan terkait Keamanan Data Perpajakan. PMK Nomor 112/PMK.03/2022 tentang NPWP (direvisi dengan PMK Nomor 136 Tahun 2023). Peraturan Menteri Keuangan (PMK) Nomor 112/PMK.03/2022 mengatur penggunaan

Nomor Pokok Wajib Pajak (NPWP) bagi berbagai kategori wajib pajak, termasuk orang pribadi, badan, dan instansi pemerintah. Peraturan ini menetapkan bahwa mulai 14 Juli 2022, wajib pajak orang pribadi yang merupakan penduduk Indonesia menggunakan Nomor Induk Kependudukan (NIK) sebagai NPWP, sementara wajib pajak lainnya menggunakan NPWP dengan format 16 digit. Peraturan ini kemudian diperbarui melalui PMK Nomor 136 Tahun 2023, yang memperpanjang masa transisi penggunaan format NPWP lama hingga 30 Juni 2024, memberikan waktu tambahan bagi wajib pajak dan instansi terkait untuk menyesuaikan sistem administrasi mereka. Langkah ini mencerminkan upaya pemerintah dalam meningkatkan efisiensi dan keamanan data perpajakan melalui integrasi sistem identitas nasional dan perpajakan. Peraturan Menteri Keuangan (PMK) Nomor 59/PMK.03/2022 merupakan perubahan atas PMK Nomor 231/PMK.03/2019 yang mengatur tata cara pendaftaran dan penghapusan Nomor Pokok Wajib Pajak (NPWP), serta pengukuhan dan pencabutan Pengusaha Kena Pajak (PKP). Peraturan ini menekankan pentingnya keamanan data dalam proses administrasi perpajakan. Dalam pelaksanaannya, dilakukan verifikasi identitas wajib pajak untuk mencegah penyalahgunaan data. Selain itu, terdapat persyaratan dokumentasi yang harus dipenuhi untuk memastikan keabsahan dan keamanan data yang disampaikan. Seluruh aktivitas terkait pendaftaran dan penghapusan NPWP dicatat secara sistematis, membentuk jejak audit (audit trail) yang dapat digunakan untuk keperluan pengawasan dan penegakan hukum. Langkah-langkah ini bertujuan untuk meningkatkan transparansi, akuntabilitas, dan perlindungan data pribadi dalam sistem perpajakan nasional.

5. Mekanisme Pengamanan Informasi. Mekanisme pengamanan informasi dalam sistem perpajakan di Indonesia didasarkan pada prinsip-prinsip keamanan data yang tercantum dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Salah satu prinsip utama adalah duty of care (kewajiban kehati-hatian), yaitu kewajiban bagi pengendali data untuk menjaga kerahasiaan dan integritas data pribadi, termasuk data wajib pajak, dari akses atau penyalahgunaan yang tidak sah. Prinsip ini menekankan tanggung jawab moral dan hukum dalam melindungi data pribadi. Berdasarkan Pasal 36C UU KUP yang mengatur Komite Pengawas Perpajakan (Komwasjak) dan asas kerahasiaan dalam UU PDP yang menegaskan perlindungan data pribadi dari pihak yang tidak berhak. Selain itu, UU PDP juga mengadopsi prinsip least privilege (prinsip Hak Akses minimum), yang berarti akses terhadap data hanya diberikan kepada pihak yang benar-benar memerlukan untuk menjalankan tugasnya. Prinsip ini menyatakan bahwa pengguna atau entitas dalam sistem komputer hanya boleh diberikan hak akses dan izin yang diperlukan untuk menyelesaikan tugas yang spesifik. Dalam konteks pengelolaan data NPWP, prinsip ini diterapkan dengan cara memastikan bahwa setiap pengguna maupun aplikasi hanya memiliki akses terhadap data dan fungsi yang benar-benar mereka perlukan untuk menjalankan tugas atau proses tertentu. Akses yang diberikan dibatasi secara ketat berdasarkan peran dan tanggung jawab masing-masing pihak dalam organisasi. Selain itu, hak akses yang telah diberikan akan ditinjau secara berkala untuk memastikan bahwa tidak ada kelebihan wewenang yang berpotensi menimbulkan risiko terhadap keamanan dan kerahasiaan data perpajakan. Pendekatan ini tidak hanya meningkatkan efisiensi, tetapi juga meminimalkan kemungkinan terjadinya kebocoran atau penyalahgunaan data.

Selanjutnya yang terakhir yaitu prinsip *data minimization* (minimalisasi data) juga menjadi bagian integral dari UU PDP, di mana pengumpulan data pribadi dibatasi hanya pada informasi yang relevan dan diperlukan sesuai dengan tujuan pengolahan. Hal ini bertujuan untuk mengurangi risiko penyalahgunaan data dan memastikan bahwa data yang dikumpulkan

tidak berlebihan. Penerapan prinsip ini dalam pengelolaan data NPWP mencakup pengumpulan data pribadi yang benar-benar relevan dan dibutuhkan untuk kepentingan administrasi perpajakan, tanpa mengambil informasi yang berlebihan. Data yang sudah tidak lagi diperlukan akan dihapus sesuai dengan ketentuan yang berlaku, guna menghindari penyimpanan yang tidak efisien dan potensi penyalahgunaan. Selain itu, durasi penyimpanan data juga dibatasi sesuai peraturan, sehingga data tidak disimpan lebih lama dari yang diperlukan untuk tujuan awal pengumpulannya. Langkah-langkah ini mencerminkan komitmen terhadap prinsip data minimization yang menjadi bagian penting dalam tata kelola data yang aman dan bertanggung jawab. Kebocoran data Nomor Pokok Wajib Pajak (NPWP) yang melibatkan 6 juta data pribadi warga negara Indonesia pada September 2024 telah menimbulkan dampak signifikan terhadap ekosistem digital pemerintahan Indonesia. Insiden ini tidak hanya mempertanyakan efektivitas sistem keamanan siber nasional, tetapi juga mengancam fondasi kepercayaan publik yang menjadi prasyarat fundamental bagi keberhasilan transformasi digital pemerintahan. Dampak langsung dari insiden ini adalah meningkatnya rasa ketidakpercayaan masyarakat terhadap layanan digital pemerintah, terutama dalam hal perlindungan data pribadi dan transparansi pengelolaannya. Ketika masyarakat merasa bahwa data sensitif mereka tidak aman di tangan institusi negara, partisipasi dalam layanan digital seperti pelaporan pajak daring, layanan administrasi kependudukan, hingga sistem jaminan sosial elektronik berpotensi menurun drastis. Kejadian ini juga membuka ruang bagi penyebaran disinformasi dan memicu keresahan publik yang dapat dimanfaatkan oleh aktor-aktor yang tidak bertanggung jawab, baik di ranah politik maupun ekonomi. Kebocoran data NPWP tidak hanya menjadi insiden keamanan siber semata, tetapi juga menimbulkan serangkaian dampak sistemik yang mengganggu ekosistem digital pemerintahan. Dampak-dampak tersebut mencakup berbagai aspek, mulai dari krisis kepercayaan publik hingga terganggunya implementasi kebijakan transformasi digital yang sedang dijalankan oleh pemerintah. Berikut beberapa dampak yang ditimbulkan dari kebocoran data NPWP terhadap kepercayaan publik:

1. krisis kepercayaan publik. Kebocoran data NPWP secara langsung mengikis kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi informasi pribadi yang bersifat sensitif dan rahasia. Hal ini menjadi semakin serius karena kepercayaan publik merupakan elemen krusial dalam mendukung keberhasilan digitalisasi layanan pemerintahan. Kondisi kebocoran data NPWP ini tidak hanya menimbulkan kekhawatiran individu, tetapi juga menciptakan keraguan sistemik yang mendalam mengenai kompetensi dan kredibilitas pemerintah dalam mengelola data pribadi secara aman dan bertanggung jawab. Ketidakmampuan pemerintah dalam menjaga kerahasiaan data sensitif seperti NPWP dapat menimbulkan persepsi bahwa mekanisme perlindungan data selama ini kurang memadai, sehingga menggerus kepercayaan publik secara menyeluruh terhadap sistem administrasi digital negara. Keraguan ini berimplikasi luas, termasuk menurunnya partisipasi aktif masyarakat dalam layanan digital yang sangat bergantung pada integritas data pribadi. Dari sisi psikologis, dampak kebocoran data ini jauh lebih kompleks dan mendalam. NPWP merupakan identitas finansial yang melekat erat dengan informasi perpajakan dan kondisi keuangan seseorang, sehingga pelanggaran atas data tersebut berarti ancaman langsung terhadap privasi dan keamanan finansial warga negara. Hilangnya rasa aman akan perlindungan data finansial tidak hanya menimbulkan kekhawatiran individual, melainkan juga memicu trauma kolektif yang meluas dalam masyarakat. Trauma ini dapat berupa rasa cemas yang berkelanjutan, ketidakpercayaan terhadap sistem digital, hingga kecenderungan untuk menghindari penggunaan layanan digital pemerintah yang mengharuskan pengisian data pribadi. Karena sifatnya yang menyangkut aspek fundamental

kehidupan ekonomi dan sosial, trauma ini berpotensi bertahan dalam jangka panjang, menghambat proses digitalisasi pemerintah, dan merusak hubungan antara warga dengan institusi negara.

2. Penurunan Partisipasi dalam Program Digital Pemerintah. Kebocoran data NPWP menimbulkan keengganan masyarakat untuk berpartisipasi secara aktif dalam ekosistem digital pemerintahan. Ketidakamanan data pribadi menyebabkan masyarakat menjadi ragu untuk mengikuti program pemerintah atau memberikan informasi yang akurat dan lengkap. Fenomena ini berpotensi menghambat percepatan digitalisasi layanan publik yang tengah diupayakan oleh pemerintah, mengingat partisipasi publik merupakan faktor kunci dalam keberhasilan implementasi layanan digital tersebut. Kepercayaan yang telah rusak sulit untuk dipulihkan dan membutuhkan langkah nyata yang transparan dan akuntabel dari pemerintah. Keengganan ini dapat ditunjukkan melalui perilaku seperti, penurunan intensitas penggunaan platform digital pemerintah, pengisian data secara tidak lengkap atau disengaja tidak akurat, hingga penolakan total terhadap layanan publik berbasis digital yang mensyaratkan input data pribadi yang dianggap sensitif. Fenomena ini mencerminkan bentuk resistensi masyarakat terhadap sistem yang dianggap tidak mampu menjamin perlindungan privasi, dan pada akhirnya dapat menghambat efektivitas serta efisiensi transformasi digital yang tengah diupayakan oleh pemerintah.
3. Implikasi terhadap Kepatuhan Wajib Pajak. Dalam sistem perpajakan modern, kepercayaan wajib pajak terhadap otoritas pajak merupakan salah satu faktor utama yang memengaruhi tingkat kepatuhan *sukarela (voluntary compliance)*. Kepercayaan ini mencakup keyakinan bahwa data pribadi dan informasi sensitif yang diserahkan akan dikelola secara aman dan bertanggung jawab oleh pemerintah. Namun, kebocoran data NPWP yang melibatkan jutaan warga negara Indonesia menjadi pukulan serius terhadap fondasi kepercayaan tersebut. Insiden ini tidak hanya menimbulkan kekhawatiran atas potensi penyalahgunaan data pribadi, tetapi juga merusak persepsi masyarakat terhadap integritas dan keamanan sistem perpajakan secara keseluruhan. Sebuah studi yang dipublikasikan dalam jurnal akademik oleh STIH Amsir mengungkapkan bahwa kebocoran data NPWP oleh peretas Bjorka telah menimbulkan guncangan signifikan terhadap persepsi keamanan wajib pajak di Indonesia. Analisis terhadap kasus ini menunjukkan bahwa informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Kebocoran data NPWP jelas merupakan pelanggaran terhadap ketentuan ini, yang dapat memperkuat persepsi negatif wajib pajak terhadap kemampuan pemerintah dalam melindungi data mereka.
4. Dampak Jangka Panjang terhadap Transformasi Digital. Kebocoran data NPWP membawa konsekuensi serius terhadap agenda transformasi digital pemerintahan, terutama dalam jangka panjang. Keamanan dan kepercayaan merupakan dua fondasi utama dalam membangun ekosistem digital yang inklusif dan berkelanjutan. Ketika insiden kebocoran data terjadi berulang, hal ini secara langsung menurunkan tingkat kepercayaan publik terhadap sistem digital pemerintah. Penurunan kepercayaan tersebut akan berdampak pada lambatnya adopsi teknologi digital oleh masyarakat dalam berbagai layanan publik, mulai dari sistem perpajakan, layanan kependudukan, kesehatan, hingga pendidikan. Sebagaimana diberitakan oleh Kompas (2024), "Maraknya kebocoran data pribadi dari berbagai instansi penyelenggara platform digital tentu saja menurunkan kepercayaan" yang pada akhirnya dapat merusak fondasi penerimaan masyarakat terhadap sistem digital yang tengah dikembangkan. Tanpa dukungan publik yang kuat, program digitalisasi pemerintah akan kehilangan efektivitas dan legitimasi, karena teknologi bukan hanya soal perangkat, tetapi juga tentang kepercayaan antara negara dan warganya. Dalam jangka panjang, resistensi

masyarakat terhadap platform digital bisa memperlambat pencapaian visi pemerintahan digital yang efisien, transparan, dan partisipatif. Oleh karena itu, penguatan regulasi perlindungan data pribadi, transparansi dalam tata kelola informasi digital, serta langkah-langkah pemulihan kepercayaan publik menjadi hal yang sangat mendesak untuk menjamin keberlanjutan transformasi digital nasional.

Kebocoran data NPWP merupakan cerminan nyata dari lemahnya sistem keamanan siber nasional. Kurangnya kesiapan institusi dalam menghadapi serangan siber sehingga mengguncang fondasi kepercayaan publik yang menjadi syarat utama keberhasilan transformasi digital pemerintahan. Ketika data pribadi, khususnya yang bersifat finansial seperti NPWP, tidak dapat dijamin keamanannya, maka resistensi masyarakat terhadap layanan digital pemerintah menjadi keniscayaan. Penurunan partisipasi, keraguan terhadap akurasi sistem, serta potensi pelanggaran hukum oleh pihak ketiga menunjukkan bahwa dampak kebocoran ini bersifat sistemik dan jangka panjang. Seperti diungkapkan oleh Pratama Persadha, pakar keamanan siber, rentetan kebocoran data di Indonesia telah mencoreng reputasi negara di mata dunia dan menunjukkan lemahnya kepedulian terhadap keamanan siber. Di sisi lain, implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) yang belum optimal juga memperparah situasi. Belum terbentuknya lembaga pengawas perlindungan data menunjukkan bahwa sistem perlindungan belum berjalan sesuai amanat regulasi. Oleh karena itu, diperlukan langkah strategis dan komprehensif berupa penguatan regulasi, investasi pada teknologi keamanan, serta peningkatan literasi digital aparat dan masyarakat. Hanya dengan pendekatan yang terintegrasi, kepercayaan publik dapat dipulihkan dan visi e-government yang akuntabel, aman, dan inklusif dapat diwujudkan.

KESIMPULAN

Kebocoran data pribadi dalam sistem e-government Indonesia telah memperlihatkan risiko serius terhadap keamanan informasi publik dan mendorong keterpurukan kepercayaan masyarakat terhadap pelayanan digital pemerintah. Implikasi pertama adalah menurunnya legitimasi sistem e-government dan menghambat partisipasi warga dalam layanan publik. Studi dari Kabupaten Sidoarjo menunjukkan bahwa penerapan manajemen keamanan informasi dengan mengacu pada standar ISO 27001 mampu meningkatkan ketahanan sistem terhadap ancaman siber, serta mengurangi potensi kebocoran data akibat kesalahan prosedural, (SEPTIONO, 2017). Namun, hal ini hanya efektif jika diiringi dengan pelatihan rutin dan audit keamanan berkala yang menyeluruh. Dampak kedua adalah keterbatasan infrastruktur dan kesiapan sumber daya manusia. Penelitian tentang e-government di Kecamatan Tallo menemukan bahwa rendahnya literasi digital masyarakat dan resistensi terhadap sistem digital membuat kebijakan keamanan tetap rentan, bahkan dengan fisik dan protokol yang memadai. Ini menegaskan bahwa keamanan data tidak hanya relevan pada level teknologi, tetapi juga pada percepatan pemahaman dan kesiapan sosial. Untuk merespons tantangan tersebut, diperlukan rekomendasi kebijakan berlapis dan strategi pemulihan kepercayaan yang komprehensif. Pertama, pemerintah harus memperluas cakupan pengelolaan keamanan informasi dengan memastikan setiap lembaga menerapkan ISO 27001 dan menerapkan audit internal dan eksternal secara rutin – bukan hanya inisiasi di beberapa kota besar. Bukti implementasi di Surabaya menunjukkan pengurangan insiden keamanan dan peningkatan kepercayaan publik setelah komitmen terpadu antara teknis dan kebijakan, (Ratny et al., 2024). Kedua, edukasi dan sosialisasi tentang keamanan data perlu diintegrasikan dalam program e-government di tingkat desa dan kelurahan. Studi di Sumbawa Barat menegaskan pentingnya transparansi dan akuntabilitas sebagai fondasi kepercayaan

masyarakat; maka kanal pengaduan digital, laporan publik berkala, serta pelibatan masyarakat dalam evaluasi sistem harus diutamakan, . Kombinasi antara penguatan teknologi, regulasi, serta pemberdayaan publik diyakini dapat memulihkan kepercayaan dan menjamin keberlangsungan layanan digital pemerintah yang aman dan inklusif. (Jaya et al., 2025)

DAFTAR PUSTAKA

Bua, I. T., & Idris, N. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. 2, 100–114.

Fauzi, A. R. … Negara, A. (2024). Digitalisasi terhadap Pelayanan Publik (Implementasi Digitalisasi Terhadap Pelayanan Publik di Pemerintah Kota Kediri dan Kabupaten Jember) Digitalization of Public Services (Implementation of Digitalization of Public Services in the Kediri City Govern. 7(10), 3727–3734. https://doi.org/10.56338/jks.v7i10.6146

Ham, D. P. … Baihaqy, A. (2025). Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) Andhika Pratama Adhi Surya M . Asif Nur Fauzi. 4(156), 31–37. https://www.codepolitan.com/. (2024). Siapa Bjorka Sebenarnya? Hacker di Balik Kebocoran Data NPWP. https://www.codepolitan.com/blog/siapa-bjorka-sebenarnya-hacker-di-balik-kebocoran-data-npwp/

INVESTASI, K. B. K. D. (n.d.). UU 1/2024: Perubahan Kedua UU No. 11 Tahun 2008 tentang ITE. https://jdih.maritim.go.id/uu-12024-perubahan-kedua-uu-no-11-tahun-2008-tentang-ite#:~:text=Undang-Undang No. 1 Tahun,atau berpotensi melanggar hak anak

Jaya, I., & Yamin, A. (2025). Pengaruh Penerapan E-Government , Akuntabilitas , dan Transparansi terhadap Tingkat Kepercayaan Masyarakat kepada Pemerintah Kabupaten Sumbawa Barat. 8, 5075–5080.

KEUANGAN, K. (2022). https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html. https://www.djkn.kemenkeu.go.id/artikel/baca/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html

Naylawati Bahtiar. (2022). Darurat Kebocoran Data : Kebutuhan Regulasi Pemerintah. -, 2(1), 1–16. file:///C:/Users/user/Downloads/32144-Article Text-109597-1-10-20240320.pdf

PANrB. (2020). Sistem Pemerintahan Berbasis Elektronik (SPBE). https://www.menpan.go.id/site/kelembagaan/sistem-pemerintahan-berbasis-elektronik-spbe-2

Ratny, F. … Rahman, Y. (2024). Implementasi E-Government Dalam. 7, 8888–8893.

Septiono, M. (2017). Manajemen Keamanan Informasi (Studi Kasus Layanan E-government Pemerintah Kota Surabaya). https://etd.repository.ugm.ac.id/penelitian/detail/128822

Tobing, E. G. L., & Kusmono, K. (2022). Modernisasi Administrasi Perpajakan: NIK Menjadi NPWP. Jurnal Pajak Indonesia (Indonesian Tax Review), 6(2), 183–193. https://doi.org/10.31092/jpi.v6i2.1674

Wiki Provinsi Gorontalo. (2024). Dasar Hukum Pelaksanaan dan Pengelolaan SPBE. https://wiki.gorontaloprov.go.id/