



Keamanan Data Publik: Strategi Perlindungan dalam Infrastruktur Digital Pemerintahan



I Ketut Adi Purnama¹

¹ Magister Ilmu Hukum Universitas Suryakencana

Article Info

Corresponding Author:

Penulis Korespondensi

✉ ketutadipurnama@unsur.ac.id

History:

Submitted: 09-04-2025

Revised: 14-04-2025

Accepted: 21-04-2025

Kata Kunci:

Perlindungan Data, keamanan data, regulasi

Keyword:

Data protection, data security, regulation

Abstrak

Pemerintah mendorong pengembangan teknologi informasi untuk memasukkan sistem informasi terintegrasi untuk meningkatkan efisiensi dan kualitas layanan publik. Namun, penerapan sistem ini menghadapi berbagai tantangan, terutama dalam aspek perlindungan data. Data yang dikendalikan pemerintah seringkali sensitif. B. Data pribadi warga negara, karena manajemen yang aman diperlukan untuk mencegah risiko penyalahgunaan. Artikel ini bertujuan untuk menganalisis kerangka kerja hukum, teknis dan pedoman untuk perlindungan data dalam sistem informasi negara. Studi ini menggunakan undang-undang kontrol yudisial dengan pendekatan hukum dan studi kasus untuk mengimplementasikan sistem perlindungan data di lembaga pemerintah. Hasilnya menunjukkan bahwa sementara peraturan perlindungan data seperti 2022 Nomor Legal 27 ada untuk melindungi data pribadi, implementasinya masih menghadapi berbagai hambatan. Hambatan-hambatan ini termasuk infrastruktur teknis yang terbatas, kurangnya kemampuan digital, persepsi tentang pentingnya keamanan data di antara pejabat pemerintah, dan pemantauan penegakan peraturan yang lemah.

Abstract

The government is promoting the development of information technology to implement integrated information systems aimed at improving the efficiency and quality of public services. However, the implementation of such systems faces various challenges, particularly in the area of data protection. Government-controlled data is often sensitive—especially personal data of citizens which requires secure management to prevent the risk of misuse. This article aims to analyze the legal frameworks, technical aspects, and guidelines related to data protection within national information systems. The study adopts a judicial review approach by analyzing relevant laws and applying case studies to examine the implementation of data protection systems in government institutions. The findings indicate that while data protection regulations, such as Law No. 27 of 2022 on Personal Data Protection, are in place to safeguard personal information, their implementation still encounters numerous obstacles. These include limited technical infrastructure, a lack of digital capabilities, low awareness of data security among government officials, and weak enforcement monitoring.



Copyright © 2025 by
Jurnal Hukum Mimbar
Justitia.

All writings published in this journal are personal views of the authors and do not represent the views of the Constitutional Court.

 <https://doi.org/10.35194/jhmj.v10i2.5113>

A. PENDAHULUAN

1. Latar Belakang

Sistem Informasi Pemerintah Mengambil Peran Penting Dalam Meningkatkan Efisiensi Dan Kemanjuran Layanan Sektor Publik. Dalam Konteks Yang Ditandai Dengan Transformasi Digital Yang Semakin Cepat, Pemanfaatan Teknologi Informasi Melampaui Fungsinya Hanya Sebagai Instrumen Pendukung; Itu Muncul Sebagai Komponen Penting Dalam Penyederhanaan Proses Birokrasi, Optimalisasi Distribusi Sumber Daya, Dan Percepatan Pemberian Layanan Kepada Masyarakat. Penyebaran Sistem Informasi Terintegrasi Memberdayakan Pemerintah Untuk Mengurangi Redundansi Data, Menambah Transparansi, Dan Memperkuat Akuntabilitas Dalam Kerangka Pengambilan Keputusan¹.

Digitalisasi Juga Memberikan Pengaruh Yang Menguntungkan Pada Masyarakat Dengan Memfasilitasi Akses Yang Lebih Besar Ke Informasi Publik Dan Layanan Administrasi. Misalnya, Aplikasi Layanan Terintegrasi Seperti Sistem Informasi Administrasi Kependudukan (Siak) Dan Platform Layanan Lisensi Online Mencontohkan Bagaimana Kemajuan Teknologi Dapat Mengurangi Beban Temporal Dan Keuangan Yang Terkait Dengan Berbagai Tugas Administrasi.

Meskipun Demikian, Di Tengah Keuntungan Beragam Ini, Adopsi Sistem Informasi Pemerintah Juga Menimbulkan Tantangan Yang Signifikan, Terutama Mengenai Privasi Dan Keamanan Data. Ketergantungan Yang Meningkat Pada Teknologi Digital Membuat Data Pribadi Individu Semakin Rentan Terhadap Potensi Penyalahgunaan. Ancaman Yang Muncul, Termasuk Peretasan, Pelanggaran Data, Dan Penggunaan Informasi Yang Tidak Bertanggung Jawab, Telah Menjadi Masalah Mendesak Yang Memerlukan Perhatian Segera. Situasi Ini Memaksa Pemerintah Untuk Memprioritaskan Tidak Hanya Pembentukan Infrastruktur Digital Tetapi Juga Peningkatan Kerangka Kerja Peraturan Dan Perlindungan Hukum Yang Berkaitan Dengan Manajemen Data².

“Penjagaan Data Pribadi Merupakan Hak Fundamental Yang Diakui Oleh Banyak Negara, Termasuk Indonesia, Sebagaimana Diartikulasikan Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Uu Pdp)” (Direktorat Jenderal Aptika, 2023). Pemberlakuan Undang-Undang Pdp Memberikan Kerangka Hukum Yang Kuat Yang Bertujuan Melindungi Hak-Hak Individu Mengenai Data Pribadi Mereka, Sementara Secara Bersamaan Memaksakan Kewajiban Pada Entitas Pemerintah Dan Administrator Sistem Informasi Untuk

¹ S E Yoyo Sudaryo Et Al., *Digital Marketing Dan Fintech Di Indonesia* (Penerbit Andi, 2020).

² Feri Sulianta, *Social Informatics: Kajian Interaksi Teknologi \& Masyarakat* (Feri Sulianta, 2024).

Memastikan Keamanan Data Tersebut. Selain Itu, Undang-Undang Tersebut Bercita-Cita Untuk Menumbuhkan Kepercayaan Publik Pada Layanan Digital Pemerintah, Yang Merupakan Fondasi Penting Untuk Upaya Transformasi Digital.

Sebagai Mekanisme Implementasi, Uu Pdp Menggambarkan Berbagai Dimensi Perlindungan Data Pribadi, Yang Meliputi Pengumpulan, Pengolahan, Penyimpanan, Dan Penghancuran Data. Pemerintah Diberi Mandat Untuk Menjamin Bahwa Data Pribadi Individu Dikelola Dengan Cara Yang Sah, Transparan, Dan Sesuai Dengan Standar Perlindungan Data Yang Diterima Secara Internasional. Ini Mencakup Adopsi Teknologi Keamanan Informasi Seperti Enkripsi, Firewall, Dan Sistem Otentikasi Faktor Ganda, Di Samping Pengawasan Ketat Aksesibilitas Data.

Sebaliknya, Pelaksanaan Sistem Informasi Pemerintah Yang Efektif Memerlukan Kolaborasi Erat Antara Beragam Pemangku Kepentingan, Termasuk Entitas Pemerintah, Swasta, Dan Publik. Meningkatkan Kesadaran Publik Mengenai Pentingnya Perlindungan Data Pribadi, Bersama Dengan Pembentukan Mekanisme Pengaduan Yang Efisien Untuk Pelanggaran Data, Merupakan Langkah Penting Untuk Menumbuhkan Ekosistem Digital Yang Aman Dan Dapat Dipercaya³.

Mengingat Konteks Ini, Pemeriksaan Sistem Informasi Pemerintah Mengenai Pengamanan Data Pribadi Menjadi Sangat Relevan. Wacana Ini Tidak Hanya Meneliti Hambatan Yang Dihadapi Tetapi Juga Mengidentifikasi Peluang Yang Dapat Dimanfaatkan Untuk Mengaktualisasikan Layanan Publik Yang Efisien, Inklusif, Dan Aman Di Era Digital⁴.

Pengenalan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Uu Pdp) Menandai Tonggak Penting Dalam Ranah Perlindungan Data Di Indonesia. Berfungsi Sebagai Dasar Hukum, Undang-Undang Ini Menetapkan Bahwa Setiap Individu Memiliki Hak Atas Data Pribadi Mereka Dan Hak Untuk Diberitahu Tentang Pemanfaatannya. Pemerintah Dan Operator Sistem Informasi Berkewajiban Untuk Mematuhi Prinsip-Prinsip Perlindungan Data Yang Mencakup Legalitas, Transparansi, Pembatasan Tujuan, Dan Keamanan Pemrosesan Data⁵.

Seperti Yang Dijelaskan Oleh Direktorat Jenderal Aplikasi Informatika (Aptika) Dalam Publikasi Ilmiahnya, “Penjagaan Data Pribadi Melampaui Akuntabilitas Semata-Mata Penyelenggara Sistem; Itu Memerlukan Partisipasi Publik Yang Terlibat Dalam Menjaga

³ S Helmi Et Al., *Digitalisasi Tata Kelola Pemerintahan Gampong Dalam Mewujudkan Percepatan Pelayanan Dan Pembangunan Melalui Sistem Informasi Gampong (Sigap)* (Cv. Green Publisher Indonesia, 2024).

⁴ Nurmadi Harsa Sumarta And Djoko Karyono, *Auditor Internal Dan Konsultan Bisnis Desa: Sebuah Wacana Strategis* (Pandiva Buku, 2023).

⁵ Pemerintah Indonesia, “Undang-Undang Perlindungan Data Pribadi (Uu Pdp)” (Jakarta, 2022).

Kerahasiaan Data Mereka. Undang-Undang Pdp Menggambarkan Kewajiban Pengelola Data Untuk Memastikan Bahwa Proses Pengumpulan, Pemrosesan, Dan Penyimpanan Data Dilakukan Secara Etis Dan Sesuai Dengan Undang-Undang Hukum” (Aptika, 2023).

Selain Itu, Peraturan Tersebut Mencakup Konsekuensi Bagi Entitas Yang Melanggar Ketentuannya, Mulai Dari Dampak Administratif Hingga Hukuman Pidana. Misalnya, Pasal 65 Undang-Undang Pdp Menetapkan Denda Besar Bagi Individu Yang Bersalah Atas Penggunaan Data Pribadi Yang Tidak Tepat. Ini Diantisipasi Untuk Memberikan Pengaruh Pencegah Dan Mempromosikan Kehati-Hatian Yang Lebih Besar Di Antara Manajer Data Dalam Pengoperasian Sistem Informasi⁶.

Namun Demikian, Pemberlakuan Undang-Undang Pdp Menghadapi Tantangan Yang Berat. Hambatan Utama Adalah Kurangnya Infrastruktur Yang Memadai, Baik Secara Teknologi Maupun Dalam Hal Sumber Daya Manusia. Banyak Lembaga Pemerintah, Terutama Di Daerah Pinggiran, Terus Mengandalkan Sistem Informasi Yang Tidak Cukup Aman Dan Rentan Terhadap Ancaman Cyber. Sebaliknya, Literasi Digital Masyarakat Menghadirkan Rintangan Yang Signifikan Juga. Menurut Laporan Kementerian Komunikasi Dan Informatika (Kominfo), Tingkat Literasi Digital Di Kalangan Orang Indonesia Tetap Pada Tingkat Menengah, Mengakibatkan Kurangnya Pemahaman Yang Meluas Mengenai Risiko Yang Terkait Dengan Data Pribadi Mereka (Kominfo, 2023).

Kominfo Lebih Lanjut Mengamati Bahwa Dalam Beberapa Tahun Terakhir, Frekuensi Insiden Kebocoran Data Di Indonesia Terus Meningkat. “Terjadinya Kebocoran Data Sangat Memprihatinkan Karena Berkaitan Dengan Data Pribadi Jutaan Warga. Ini Menunjukkan Bahwa Protokol Keamanan Data Saat Ini Memerlukan Peningkatan, Baik Melalui Kemajuan Teknologi Maupun Peningkatan Kesadaran Publik,” Tegas Laporan Resmi Dari Kominfo (2023).

Peluang Signifikan Dalam Pembentukan Sistem Informasi Pemerintah Yang Aman Disediakan Oleh Dukungan Teknologi Yang Terus Berkembang. Teknologi Seperti Blockchain, Misalnya, Memiliki Potensi Untuk Berfungsi Sebagai Solusi Untuk Memastikan Transparansi Dan Integritas Data. Selain Itu, Penerapan Kecerdasan Buatan (Ai) Dapat Memfasilitasi Deteksi Dan Pencegahan Ancaman Cyber Secara Real-Time. Namun Demikian, Adopsi Teknologi Ini Memerlukan Investasi Besar Dan Upaya Kolaboratif Lintas Sektor⁷.

⁶ Irfani Arhani, “Sanksi Pelaku Tindak Pidana Cyber Phishing Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi” (Fakultas Syariah Dan Hukum Uin Syarif Hidayatullah Jakarta, 2024).

⁷ Hartatik Hartatik Et Al., *Tren Technopreneurship: Strategi \& Inovasi Pengembangan Bisnis Kekinian Dengan Teknologi Digital* (Pt. Sonpedia Publishing Indonesia, 2023).

Keamanan Data Pribadi Merupakan Masalah Terpenting Karena Data Individu Sering Digunakan Sebagai Dasar Untuk Pengambilan Keputusan Oleh Entitas Pemerintah Dan Swasta. Dalam Kerangka Ini, Pelanggaran Perlindungan Data Tidak Hanya Berdampak Buruk Pada Individu Tetapi Juga Membahayakan Kepercayaan Publik Terhadap Lembaga Pemerintah. Seperti Yang Diartikulasikan Oleh Dirjen Aptika, “Pelanggaran Data Pribadi Dapat Mengakibatkan Kerugian Material, Kerusakan Reputasi, Dan Bahkan Mengancam Hak Dasar Warga Negara Untuk Mengalami Keamanan Dalam Interaksi Digital Mereka” (Aptika, 2023)⁸.

Selain Itu, Laporan Dari Badan Cyber Dan Kata Sandi Negara (Bssn) Menunjukkan Peningkatan Tahunan Yang Signifikan Dalam Insiden Keamanan Siber Di Indonesia. Pada Tahun 2023, Bssn Mendokumentasikan Lebih Dari 700 Juta Upaya Serangan Siber, Terutama Terkait Dengan Kebocoran Data Pribadi Melalui Sistem Yang Tidak Cukup Aman (Bssn, 2023). Kenyataan Ini Menggarisbawahi Urgensi Penguatan Langkah-Langkah Perlindungan Untuk Data Pribadi, Terutama Di Sektor Publik Yang Mengawasi Pengelolaan Data Dalam Skala Besar. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Uu Pdp) Telah Dirumuskan Untuk Mengatasi Kebutuhan Mendesak Ini⁹.

Pasal 1 Undang-Undang Perlindungan Data Pribadi (Pdp) Menggambarkan Data Pribadi Sebagai “Setiap Data Mengenai Seseorang Yang Dapat Diidentifikasi Atau Dapat Diidentifikasi Baik Secara Individu Maupun Kolektif Melalui Informasi Tambahan.” Undang-Undang Ini Menggarisbawahi Perlunya Pengumpulan Dan Pengelolaan Data Pribadi Dilakukan Dengan Persetujuan Individu, Menggunakan Data Tersebut Semata-Mata Untuk Tujuan Yang Sah. Dalam Kerangka Sistem Informasi Pemerintah, Uu Pdp Menetapkan Bahwa Entitas Publik Diberi Mandat Untuk Menunjuk Petugas Perlindungan Data (Dpo) Untuk Menjamin Kepatuhan Terhadap Prinsip-Prinsip Manajemen Data Yang Aman. Menteri Komunikasi Dan Informatika (Menkominfo) Menjelaskan, “Penunjukan Dpo Adalah Inisiatif Strategis Untuk Memastikan Bahwa Setiap Instansi Publik Memiliki Individu Yang Sepenuhnya Bertanggung Jawab Atas Pengamanan Data Pribadi, Sehingga Mengurangi Potensi Penyalahgunaan Data” (Kominfo, 2023).

Selain Itu, Perlindungan Data Harus Didukung Oleh Mekanisme Audit Dan Evaluasi Yang Sistematis. Dalam Konteks Ini, Uu Pdp Mengharuskan Pemerintah Membangun Sistem Yang Efektif Untuk Menangani Pengaduan Dan Melakukan Penyelidikan Untuk Mengatasi

⁸ R M Gatot Hery Djatmiko, *Transformasi Kebijakan Administrasi Publik Menuju Era Society 5.0* (Indramayu: Penerbit Adab, 2023).

⁹ Aldi Dinata Saputra, Frans Dione, And Irfan Uluputty, “Pengelolaan Keamanan Informasi Dan Persandian Di Dinas Komunikasi Dan Informatika Provinsi Kalimantan Timur,” *Jurnal Teknologi Dan Komunikasi Pemerintahan* 5, No. 2 (2023): 159–187.

Setiap Dugaan Pelanggaran Data. “Masyarakat Memiliki Hak Untuk Mendapat Informasi Tentang Pengelolaan Data Mereka, Termasuk Hak Untuk Menyuarakan Keberatan Dalam Kasus Pelanggaran,” Tegas Kominfo Dalam Laporan Tahunannya (Kominfo, 2023). Transformasi Digital Yang Aman Dan Efektif Dari Operasi Pemerintah Memerlukan Sinergi Antara Regulasi, Teknologi, Dan Kesadaran Publik. Inisiatif Seperti Penyebaran Uu Pdp, Penyediaan Pelatihan Keamanan Siber, Dan Peningkatan Infrastruktur Digital Sangat Penting Untuk Mencapai Ekosistem Digital Yang Berkelanjutan. Seperti Yang Diartikulasikan Oleh Direktur Eksekutif Institut Tik Indonesia, Heru Sutadi, “Kemanjuran Perlindungan Data Pribadi Tidak Hanya Bergantung Pada Kemajuan Teknologi Tetapi Juga Pada Transformasi Budaya Dan Kesadaran Kolektif Mengenai Pentingnya Privasi” (Heru Sutadi, 2023)¹⁰.

Tujuan Artikel Ini Adalah Untuk Menggarisbawahi Pentingnya Penegakan Hukum Dan Jalan Hukum Bagi Korban Penipuan Media Sosial, Dengan Tujuan Membantu Individu Yang Menghadapi Tantangan Hukum Yang Terkait Dengan Penipuan Media Sosial Dan Meningkatkan Kesadaran Publik Tentang Signifikansi Dan Potensi Risiko Yang Melekat Dalam Evolusi Kontemporer Media Sosial.

2. Perumusan Masalah

1. Bagaimana peran sistem informasi pemerintah dalam meningkatkan efisiensi dan efektivitas layanan sektor publik di era digital?
2. Apa saja tantangan utama yang dihadapi pemerintah dalam mengimplementasikan sistem informasi yang aman dan terintegrasi, terutama terkait perlindungan data pribadi?
3. Sejauh mana Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dapat memberikan perlindungan hukum terhadap pengelolaan data pribadi dalam sistem informasi pemerintah?.

3. Metode Penelitian

Penyelidikan ini menggunakan metodologi kualitatif melalui kerangka studi perpustakaan, dengan tujuan mencapai pemahaman yang komprehensif tentang perlindungan data dalam sistem informasi pemerintah. Metodologi ini memfasilitasi pemeriksaan variabel yang berkaitan dengan kebijakan dan praktik perlindungan data, di samping hambatan yang dihadapi dalam pelaksanaannya di sektor publik. Strategi pengumpulan data yang digunakan dalam penyelidikan ini dilakukan melalui tinjauan literatur yang menggabungkan beragam sumber sekunder, termasuk artikel ilmiah, jurnal elektronik, monograf, dan publikasi

¹⁰ Annisa Fitri Anggraeni Et Al., *Institusi Keuangan Dan Pasar Modal* (Pt. Sonpedia Publishing Indonesia, 2025).

pemerintah yang berkaitan dengan subjek perlindungan data. Misalnya, kontribusi ilmiah yang membahas perlindungan data pribadi, kebijakan pemerintah yang terkait dengan Undang-Undang Perlindungan Data Pribadi (PDP Act), dan penyebaran sistem informasi yang aman dalam entitas pemerintah merupakan referensi utama untuk penelitian ini (Fauzi et al., 2023). Selain itu, penelitian ini menggunakan analisis data sekunder, yang melibatkan agregasi data dari jurnal, artikel, dokumen pemerintah, dan laporan relevan yang sebelumnya telah disebarluaskan oleh sarjana lain.

Tujuan dari metodologi penelitian ini adalah untuk menjelaskan fungsi signifikan dari kebijakan dan peraturan hukum dalam menjaga data pribadi dalam sistem informasi pemerintah. Diharapkan bahwa pembaca akan memperoleh pemahaman tentang sifat penting perlindungan data pribadi dalam kerangka kerja pemerintah dan memahami berbagai hak dan perlindungan hukum yang dapat digunakan untuk mencegah pelanggaran data dan penyalahgunaan.

B. HASIL DAN PEMBAHASAN

Sistem informasi pemerintah berbasis digital semakin rentan terhadap potensi pelanggaran data pribadi. Akibatnya, sangat penting untuk membangun kerangka hukum yang kuat yang bertujuan melindungi data pribadi warga negara. Indonesia, sebagai negara yang terus berkembang dalam digitalisasi proses pemerintahan, telah memberlakukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam upaya bersama untuk memberikan perlindungan terhadap data pribadi¹¹.

Menurut Direktur Jenderal Aplikasi Informatika, “UU PDP memiliki tujuan untuk memastikan pengelolaan data pribadi dilakukan secara transparan, akuntabel dan aman” (Kementerian Komunikasi dan Informatika, 2023). Berdasarkan kerangka legislatif ini, setiap entitas yang terlibat dalam pengelolaan data pribadi, termasuk lembaga pemerintah, diamanatkan untuk mematuhi prinsip-prinsip dasar perlindungan data, yang mencakup persetujuan subjek data, transparansi, dan akuntabilitas dalam tata kelola data.

Terlepas dari adanya langkah-langkah regulasi, ancaman terhadap keamanan data pribadi tetap menjadi perhatian yang cukup besar. Menurut laporan tahun 2023 oleh Badan Siber dan Kata Sandi Negara (BSSN), serangan cyber yang menargetkan lembaga pemerintah Indonesia telah meningkat tajam dalam beberapa tahun terakhir. “Pada tahun 2022, BSSN mencatat lebih dari 2.000 insiden cyber yang sebagian besar ditujukan untuk membobol sistem yang mengelola

¹¹ Taufiq A Gani, *Kedaulatan Data Digital Untuk Integritas Bangsa* (Aceh: Syiah Kuala University Press, 2023).

data pribadi warga” (BSSN, 2023).

Bentuk utama dari serangan ini termasuk phishing, penyisipan malware, dan upaya peretasan yang diarahkan pada sistem yang tidak diperkuat secara memadai. Fenomena ini menggambarkan bahwa, meskipun ada kebijakan, pelaksanaan langkah-langkah perlindungan mengenai data pribadi dalam sistem informasi pemerintah tetap tidak cukup efektif. Faktor yang berkontribusi terhadap situasi ini adalah ketidakcukupan infrastruktur keamanan yang digunakan oleh lembaga pemerintah, ditambah dengan kurangnya kesadaran mengenai pentingnya keamanan data di antara personel pemerintah¹².

Pemerintah Indonesia telah melakukan berbagai inisiatif untuk meningkatkan perlindungan data pribadi, termasuk pembentukan tim khusus seperti Cyber Security Incident Response Team (CSIRT) di setiap kementerian atau lembaga yang bertugas mengelola sistem informasi. Selain itu, pemerintah mulai mengadopsi teknologi enkripsi yang lebih canggih dan desain sistem cadangan yang aman untuk mengurangi risiko kehilangan data. “Inisiatif ini bertujuan untuk meningkatkan respons cepat terhadap ancaman dan memastikan keberlanjutan layanan digital yang aman bagi masyarakat” (Kementerian Komunikasi dan Informatika, 2023).

Penerapan teknologi blockchain juga secara progresif diintegrasikan ke dalam proyek-proyek pemerintah tertentu, seperti pengelolaan arsip dan data populasi. Blockchain dianggap memiliki potensi untuk meningkatkan keamanan data karena arsitekturnya yang terdesentralisasi, yang menghalangi manipulasi tanpa persetujuan semua pihak yang terlibat.

Meskipun inisiatif yang dilakukan oleh pemerintah menandakan komitmen untuk mengatasi perlindungan data, masih banyak tantangan dalam hal penegakan hukum dan kepatuhan terhadap peraturan. Tantangan utama adalah sumber daya manusia yang masih belum cukup yang dilengkapi untuk mengelola sistem informasi yang aman dengan mahir. Selain itu, penerapan teknologi canggih seperti enkripsi dan blockchain belum diadopsi secara seragam di seluruh lembaga pemerintah¹³.

“Implementasi perlindungan data yang konsisten di seluruh sektor pemerintah membutuhkan peningkatan kapasitas SDM, pembiayaan yang memadai, serta dukungan legislatif untuk memastikan bahwa setiap kebijakan yang diterapkan sesuai dengan standar internasional” (Schwartz & Solove, 2014). Seseorang harus menggunakan kebijaksanaan dan kehati-hatian ketika mengasimilasi informasi dari platform media sosial, tetap bijaksana dalam

¹² Alwi Putra Supendi, “Analisa Kerentanan Aplikasi Web Menggunakan Framework Mitre Att&Ck Dengan Metode Simulasi Red Team: Studi Kasus Di Pt. Nurul Fikri Cipta Inovasi” (Sekolah Tinggi Teknologi Terpadu Nurul Fikri, 2024).

¹³ Heri Heriyanto, “Analisis Perbandingan Regulasi Dan Perlindungan Hukum Atas Privasi Data Pasien Di Tiga Negara Asia Tenggara (Indonesia, Singapura, Dan Laos),” *Jurnal Ners* 7, No. 2 (2023): 1247–1259.

penggunaan media sosial di tengah kemajuan teknologi saat ini.

Sebuah studi kasus kebocoran data dalam sistem EKTP pada tahun 2022 menunjukkan bahwa itu rentan terhadap sistem informasi status dalam melindungi data pribadi. Berdasarkan laporan yang dikeluarkan oleh Komite Hubungan Masyarakat, lebih dari satu juta data pribadi yang tercantum dalam sistem EKTP telah membocorkan celah dalam enkripsi yang digunakan. "Kejadian ini menunjukkan bahwa pemerintah berusaha untuk mengamankan data pribadi. Kesenjangan keamanan yang sebelumnya tidak dikenali dapat menyebabkan kerugian yang signifikan bagi masyarakat" (Komisi Informasi Publik, 2022). Data ini tidak hanya menghubungkan masalah teknis dalam penanganan sistem informasi, tetapi juga membuka diskusi yang lebih luas mengenai sensitivitas serangan cyber dan potensi penyalahgunaan informasi pribadi¹⁴.

Dalam era digital yang semakin progresif, data pribadi adalah salah satu aset paling berharga yang perlu dianggap serius. Setiap orang menyimpan data dalam berbagai sistem negara bagian dan pribadi, termasuk informasi sensitif seperti identitas pribadi, status pekerjaan, alamat dan data keuangan. Keamanan data pribadi adalah tanggung jawab utama pemerintah, terutama ketika sistem seperti e-KTP menjadi salah satu platform terpenting bagi layanan publik. Hilangnya data e-KTP pada tahun 2022 menunjukkan bahwa ada pedoman dan peraturan yang terkait dengan perlindungan data pribadi yang tidak dapat menyebabkan masalah besar. Kesenjangan keamanan yang ditemukan dalam sistem enkripsi EKTP membuktikan bahwa teknologi yang digunakan tidak cukup memenuhi syarat untuk memaksimalkan perlindungan data pribadi warga negara¹⁵.

Insiden tersebut, yang melibatkan data e-KTP yang bocor, telah menetapkan preseden untuk kepercayaan publik dalam sistem digital yang dikendalikan pemerintah. Pemerintah daerah mempertanyakan sejauh mana pemerintah dapat menjamin keamanan data pribadi yang terdaftar di berbagai sistem elektronik. Sementara itu, kebocoran telah memicu urgensi untuk menilai langkah-langkah keamanan yang diterapkan pada sistem enkripsi dan berbagai tugas publik, terutama keselamatan yang mempengaruhi manajemen data pribadi warga negara.

Selanjutnya, insiden ini meningkatkan pentingnya keberlanjutan dalam mengimplementasikan sistem keamanan yang bergantung pada langkah-langkah teknis serta peraturan yang ketat dan pengawasan maksimum. Dalam konteks ini, pemerintah harus

¹⁴ Peti Savitri And Others, *Transformasi Digital Dalam Industri Perbankan: Implikasi Terhadap Akuntansi Dan Teknologi Informasi* (Penerbit Nem, 2024).

¹⁵ Almasari Aksenta Et Al., *Literasi Digital: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 Dan Society 5.0* (Pt. Sonpedia Publishing Indonesia, 2023).

memastikan bahwa semua pedoman atau sistem, termasuk data pribadi seperti e-KTP, diimplementasikan. Ini dapat mengatasi berbagai ancaman potensial dari serangan siber dan kesalahan manusia yang dapat membahayakan privasi dan integritas data. Sebagai langkah pertama, evaluasi teknologi yang digunakan, seperti pengujian berkala sistem enkripsi dan keamanan data, harus dilakukan untuk mencegah resolusi data di masa depan¹⁶.

Untuk mengatasi masalah yang timbul dari kebocoran data e-KTP pada tahun 2022, penting bagi pemerintah untuk fokus pada peningkatan teknis serta memperkuat kerangka kerja peraturan dan pengawasan yang ada. Langkah utama adalah memperbarui sistem enkripsi yang digunakan untuk penyimpanan dan manajemen. Teknik enkripsi yang lebih canggih dan aman harus diimplementasikan untuk memprediksi potensi kebocoran data di masa depan. Selain itu, penggunaan sistem keamanan dalam teknologi blockchain juga merupakan alternatif yang lebih aman, dengan mempertimbangkan metode transparan dan tidak berubah untuk mencegah manipulasi data oleh pihak yang tidak bertanggung jawab.

Selain aspek teknis, keberhasilan melindungi data pribadi juga sangat tergantung pada persepsi dan pemahaman menyeluruh dari pihak -pihak yang relevan, baik manajer negara, bisnis dan masyarakat. Dalam hal ini, pendidikan dan pelatihan tentang pentingnya melindungi data pribadi harus dikelola secara rutin oleh pejabat pemerintah yang mengelola data pribadi dan publik, subjek data. Pemerintah harus memperkuat sosialisasi hak -hak individu mengenai perlindungan data pribadi dan mekanisme yang dapat dimasukkan dalam hal pelanggaran hak -hak ini.

Peraturan yang ada seperti Undang -Undang No. 27 untuk melindungi data pribadi juga harus digunakan secara konsisten. Undang -undang memberikan dasar hukum yang kuat untuk mengatur pengumpulan, penyimpanan, penggunaan, dan distribusi data pribadi oleh unit negara bagian dan swasta. Namun, penerapan Undang -Undang ini harus didukung oleh pengawasan yang efektif dan otoritas penegak hukum yang ketat dari pihak -pihak yang telah terbukti melanggar ketentuan perlindungan data pribadi.

Memantau implementasi pedoman untuk data pribadi tidak hanya harus dilakukan oleh lembaga, tetapi juga oleh berbagai pihak terkait, seperti Komisi Informasi, Siber dan Badan Sandi Negara (BSSN), dan lembaga independen dengan pengetahuan ahli di bidang cybersecurity. Selain itu, mekanisme penelitian dan evaluasi berkelanjutan diperlukan untuk memastikan bahwa sistem yang ada terus diperbarui dan dapat semakin terpapar pada

¹⁶ Concilianus Laos Mbato, Fajar Sungging, And Others, *Pendidikan Indonesia Masa Depan: Tantangan, Strategi, Dan Peran Universitas Sanata Dharma* (Sanata Dharma University Press, 2022).

perkembangan teknis yang kompleks¹⁷.

Penting juga untuk dicatat bahwa dalam era yang semakin digital, penggunaan data pribadi tidak hanya terbatas pada sektor publik, tetapi juga mempengaruhi sektor swasta, seperti platform media sosial, perusahaan e-commerce dan teknologi. Oleh karena itu, pedoman perlindungan data pribadi harus mempertimbangkan perlindungan data yang dikelola oleh sektor swasta dengan akses luas ke data pribadi individu. Kolaborasi sektor publik dan swasta adalah kunci untuk menciptakan ekosistem perlindungan data yang komprehensif untuk semua pemangku kepentingan.

Untuk mengatasi masalah yang timbul dari kebocoran data e-KTP pada tahun 2022, penting bagi pemerintah untuk fokus pada perbaikan teknis dan memperkuat kerangka kerja peraturan yang ada dan pengawasan yang ada. Langkah utama adalah memperbarui sistem enkripsi yang digunakan untuk penyimpanan dan manajemen. Teknik enkripsi yang lebih canggih dan aman harus diimplementasikan untuk memprediksi potensi kebocoran data di masa depan. Selain itu, penggunaan sistem keamanan dalam teknologi blockchain juga merupakan alternatif yang lebih aman, dengan mempertimbangkan metode transparan dan tidak berubah untuk mencegah manipulasi data oleh pihak yang tidak bertanggung jawab¹⁸.

Selain aspek teknis, keberhasilan melindungi data pribadi juga sangat tergantung pada persepsi dan pemahaman umum dari pihak -pihak yang relevan, baik manajer nasional, bisnis dan masyarakat. " Dalam hal ini, pendidikan dan pelatihan tentang pentingnya melindungi data pribadi harus dikelola secara rutin oleh pejabat pemerintah yang mengendalikan data dan penerbit pribadi, serta mereka yang terkena dampak. Pemerintah harus memperkuat sosialisasi hak -hak individu dalam kaitannya dengan melindungi data pribadi dan mekanisme yang dapat dimasukkan dalam melanggar hak -hak ini. Peraturan yang ada seperti

Undang -Undang Perlindungan Data Pribadi No. 27 juga harus digunakan secara konsisten. Undang -undang memberikan dasar hukum yang kuat untuk mengatur pengumpulan, penyimpanan, penggunaan, dan distribusi data pribadi sesuai dengan unit negara bagian dan pribadi. Namun, penerapan Undang -Undang ini harus didukung oleh pengawasan yang efektif dan penegakan hukum yang ketat oleh para pihak yang telah terbukti melanggar ketentuan perlindungan data pribadi¹⁹.

¹⁷ Rafi Alfian Hibrizie Et Al., "Pandangan Islam Tentang Kesejahteraan Hidup Ekonomis," *Student Scientific Creativity Journal* 1, No. 3 (2023): 349–369.

¹⁸ Zainal Fadri And S Fil, "Era Digital Dan Dampaknya Terhadap Administrasi Publik," *Reformasi Birokrasi Dalam Administrasi Publik: Tantangan Dan Peluang Di Era Digital* 61 (2024).

¹⁹ Sinta Ardhilatul Jannah, "Pengaruh Promosi Dan Kualitas Pelayanan Terhadap Minat Investasi Logam Mulia Pada Pegadaian Unit Pembantu Syariah Pasar Iii Muara Enim." (Uin Raden Fatah Palembang, 2017).

Memantau implementasi pedoman untuk data pribadi harus dilakukan tidak hanya oleh lembaga tetapi juga oleh berbagai pihak terkait, termasuk: Selanjutnya, mekanisme penelitian dan evaluasi berkelanjutan diperlukan untuk memastikan bahwa sistem yang ada terus diperbarui dan semakin terpapar pada perkembangan teknis yang kompleks.

Penting juga untuk dicatat bahwa dalam era yang semakin digital, penggunaan data pribadi tidak hanya terbatas pada sektor publik, tetapi juga mempengaruhi sektor swasta, seperti platform media sosial, perusahaan e-commerce dan teknologi. Oleh karena itu, pedoman untuk melindungi data pribadi harus mempertimbangkan perlindungan data yang dikelola oleh sektor swasta dengan akses luas ke data pribadi individu. Kolaborasi sektor publik dan swasta adalah kunci untuk menciptakan ekosistem perlindungan data yang komprehensif untuk semua yang terlibat.

Selain itu, perkembangan teknologi seperti kecerdasan buatan (AI) dan data besar semakin membawa tantangan baru untuk mengelola dan melindungi data pribadi. Menggunakan AI dalam pemrosesan data dapat meningkatkan efisiensi, tetapi jika tidak dipantau, itu juga meningkatkan risiko potensial. Oleh karena itu, pemerintah harus mengeluarkan peraturan yang mengatur penggunaan teknologi ini untuk memastikan bahwa data pribadi tetap dilindungi dari penyalahgunaan dan kebocoran. Misalnya, penggunaan AI dalam pengelolaan data pribadi hanya dilakukan oleh pihak yang diverifikasi dan dijamin memiliki standar keamanan yang tinggi.

Selanjutnya, pengenalan perlindungan data pribadi harus dimulai lebih awal di bidang pelatihan dan pendidikan. Misalnya, kurikulum pendidikan sekolah dan universitas harus mencakup materi yang berkaitan dengan keamanan siber dan hak pribadi sehubungan dengan privasi dan data pribadi. Orang-orang yang terlatih lebih sadar akan risiko yang ada dan data pribadi lebih berhati-hati tentang media sosial, transaksi online dan dialog dengan lembaga publik.

Penegakan Hukum juga memainkan peran penting dalam konteks ini. Pemerintah harus memberikan sanksi yang ketat kepada mereka yang telah terbukti melanggar perlindungan data pribadi. Sanksi ini harus mencakup tidak hanya individu, tetapi juga bisnis dan lembaga yang tidak memenuhi kewajiban mereka untuk melindungi data pribadi. Diharapkan bahwa hukuman yang jelas dan keras akan mendorong pihak-pihak yang relevan untuk bijaksana dan mengikuti peraturan yang ada.

Sementara itu, sektor swasta, yang memiliki akses yang sangat baik ke data pribadi, juga merupakan mitra utama dalam upaya perlindungan data. Perusahaan teknologi, e-commerce, dan penyedia layanan digital lainnya harus transparan tentang bagaimana data pribadi klien

mereka dikelola, disimpan, dan dilindungi. Anda juga perlu memiliki kontrol yang lebih baik atas hak Anda atas data pribadi. B. Hak untuk mengakses data yang diperlukan, atau untuk memodifikasi atau menghapus data. Membuat kode etik atau pedoman untuk perlindungan data pribadi yang diterima dari sektor swasta dapat meningkatkan kepercayaan publik dalam penggunaan platform digital.

Selanjutnya, sistem perlindungan data yang kuat membutuhkan budaya transparansi dan akuntabilitas, tidak hanya dihentikan dengan perlindungan dan peraturan teknis yang ketat. Pemerintah dan perusahaan harus memiliki pedoman untuk segera memberi tahu publik jika terjadi pelanggaran atau kebocoran data. Pengguna yang datanya terancam oleh kebocoran harus menerima informasi yang jelas dan terperinci tentang langkah-langkah yang harus mereka ambil untuk mengatasi kerugian yang mungkin terjadi akibat kebocoran. B. Risiko pencurian identitas atau penyalahgunaan data pribadi.

Pada saat yang sama, keterlibatan masyarakat menjadi semakin penting dalam memelihara dan melindungi data pribadi Anda sendiri. Dalam hal ini, pengakuan tentang pentingnya pengaturan perlindungan data harus terus dibangun di berbagai platform digital. Salah satu cara untuk melakukan ini adalah dengan memberikan informasi yang lebih jelas tentang pedoman perlindungan data dan persyaratan untuk menggunakan aplikasi yang biasanya digunakan oleh publik. B. Media Sosial atau Platform Belanja Online. Masyarakat harus bijaksana untuk berbagi data pribadi dan memahami konsekuensi yang mungkin terjadi ketika data berada di tangan yang salah.

Keseluruhan, kerja sama yang kuat antara pemerintah, sektor swasta dan masyarakat diperlukan untuk memastikan perlindungan data pribadi yang efektif. Kebocoran data e-KTP yang terjadi pada tahun 2022 harus dinamis untuk membuat sistem yang lebih aman, lebih efisien dan transparan untuk data pribadi. Dengan pedoman, teknologi yang lebih maju dan kesadaran publik yang lebih tinggi, Indonesia dapat menciptakan ekosistem digital yang aman dan andal yang memungkinkan orang untuk secara aktif berpartisipasi dalam transformasi digital tanpa memastikan ancaman terhadap perlindungan dan keselamatan data.

Untuk mencapai tujuan ini, pemerintah juga harus mempertimbangkan penerapan prinsip-prinsip perlindungan data yang lebih komprehensif, sebagaimana ditentukan dalam Peraturan Perlindungan Data Umum (GDPR) yang digunakan oleh Uni Eropa. Prinsip-prinsip seperti "data yang diminimalkan," di mana data yang dikumpulkan terbatas pada tujuan hukum, dan "dilupakan," di mana orang dapat meminta penghapusan data pribadi, dapat dirujuk dalam pedoman Indonesia untuk melindungi data pribadi. Prinsip-prinsip ini memberi publik jaminan yang lebih besar untuk mengendalikan data pribadi Anda dan mengurangi kemungkinan

penyalahgunaan pihak ketiga.

Selanjutnya, penting bahwa pemerintah tetap inovatif dalam pengembangan sistem keamanan inovatif yang mengembangkan tantangan pengembangan teknologi. Misalnya, pengembangan teknologi Internet of Things (IoT) di mana banyak perangkat terhubung ke Internet dan mengumpulkan data pribadi pengguna harus menjadi masalah serius yang melindungi data yang dihasilkan dari perangkat ini. Penggunaan standar keamanan yang lebih ketat dan teknologi terbaru, seperti enkripsi ujung ke ujung, dapat meningkatkan perlindungan data yang mengalir melalui jaringan digital.

Termasuk sektor swasta untuk perlindungan data pribadi juga harus difasilitasi menggunakan sertifikasi keamanan data. Pemerintah dapat mendorong bisnis untuk mengelola data pribadi mereka untuk mendapatkan sertifikat keamanan spesifik yang menunjukkan mereka memenuhi standar perlindungan data yang tinggi. Ini memberi konsumen dan publik lebih percaya diri bahwa mereka bertanggung jawab untuk mempertahankan perlindungan data untuk data yang dikendalikan perusahaan.

Salah satu tantangan yang sering muncul dalam perlindungan data pribadi adalah ketidaksetaraan akses dan pemahaman keamanan data antara berbagai tingkat masyarakat. Orang yang tinggal dari jarak jauh atau tidak memiliki akses yang memadai ke teknologi seringkali merupakan target utama dari berbagai jenis penipuan atau serangan siber yang dapat merusak privasi. Oleh karena itu, penting bagi pemerintah untuk memastikan bahwa perlindungan data pribadi dan pelatihan keamanan siber didistribusikan secara merata di semua tingkat masyarakat. Kampanye pendidikan yang lebih intensif di bidang teknologi yang terjangkau dapat membantu meningkatkan persepsi publik dan pengetahuan tentang memelihara data pribadi.

Tidak hanya itu, pemerintah juga harus memprioritaskan prinsip transparansi pada setiap langkah untuk melindungi data pribadi. Setiap pedoman yang diterapkan harus diungkapkan dengan jelas kepada masyarakat sehingga Anda dapat menemukan hak Anda untuk mengelola dan melindungi data pribadi Anda. Pemerintah juga harus membuat saluran yang efektif bagi masyarakat untuk melaporkan pelanggaran atau kebocoran data dan menerima dukungan jika mereka menjadi korban data.

juga penting bagi Indonesia untuk memperkuat kerja sama internasional dalam perlindungan data pribadi. Banyak data pribadi di internet disimpan tidak hanya di Jerman tetapi juga di luar negeri. Oleh karena itu, pengaturan untuk melindungi data pribadi harus diterapkan dengan mempertimbangkan peraturan dan peraturan internasional yang berlaku sehingga Indonesia masih dapat melindungi data pribadi warga negara, bahkan jika disimpan atau

diproses di luar negeri. Apa yang dapat kita lakukan adalah secara aktif terlibat dalam forum internasional yang membahas perlindungan data dan cybersecurity, serta memperkuat kerja sama dengan negara -negara dengan peraturan perlindungan data yang kuat.

Tantangan dalam melindungi data pribadi akan berkembang dengan inovasi teknologi cepat dan perubahan sosial. Oleh karena itu, sementara pedoman perlindungan data pribadi tidak boleh statis, mereka harus terus beradaptasi dengan teknologi yang ada dan dinamika ancaman. Pemerintah perlu mempertahankan fleksibilitas dalam merancang pedoman yang dapat merespons dengan cepat pengembangan teknologi baru tanpa mempengaruhi aspek melindungi hak asasi manusia dan privasi individu.

Data EKTP akan menjadi peristiwa yang mengecewakan pada tahun 2022, tetapi ini dapat digunakan sebagai pelajaran yang berharga untuk meningkatkan sistem perlindungan data pribadi Indonesia. Dengan peningkatan pedoman, memperkuat infrastruktur keamanan dan meningkatkan kesadaran publik, Indonesia memiliki kesempatan untuk menciptakan sistem yang lebih aman dalam mengelola data pribadi. Keberhasilan dalam melindungi data pribadi akan meningkatkan kepercayaan warga negara dan sektor swasta, dan mempromosikan pertumbuhan ekonomi digital yang lebih terintegrasi dan aman untuk semua warga negara. Dengan prosedur spesifik yang digunakan secara menyeluruh, Indonesia adalah contoh dari keadaan di mana ia dapat menjaga keseimbangan antara pengembangan teknologi dan perlindungan privasi masyarakat²⁰.

Penting untuk merujuk pada peraturan internasional yang sudah ada di negara -negara maju, seperti Peraturan Perlindungan Data Umum (GDPR) yang diterapkan oleh Uni Eropa untuk meningkatkan sistem perlindungan data pribadi Indonesia. Peraturan ini menjadi prioritas daripada prinsip "minimalisasi data". Ini berarti bahwa data yang dikumpulkan terbatas pada tujuan hukum dan "hak untuk melupakan." Seperti yang dinyatakan Komisi Eropa, "GDPR memberikan perlindungan yang lebih baik bagi individu sehubungan dengan privasi dan kontrol atas data pribadi" (Komisi Eropa, 2018). Prinsip -prinsip ini bisa menjadi referensi penting bagi Indonesia dalam mengembangkan pedoman yang lebih komprehensif untuk data pribadi.

Selanjutnya, pemerintah Indonesia harus memperkuat kerangka hukumnya sehubungan dengan perlindungan data pribadi dengan menegakkan undang -undang yang tidak hanya fokus pada pengumpulan dan pemrosesan data, tetapi juga pada penggunaan teknologi terbaru untuk meningkatkan keamanan data. Menerapkan teknologi enkripsi dan tindakan pencegahan yang lebih kuat ketika berurusan dengan data potensial dan kebocoran melalui pengujian keamanan

²⁰ Hadi Prabowo, *Birokrasi Dan Pelayanan Publik* (Bandung: Bimedia Pustaka Utama, 2022).

yang lebih ketat sangat dibutuhkan. Seperti yang ditunjukkan BSSN (Siber dan State Sandi Agency), "Keamanan siber harus menjadi prioritas utama dalam mengelola data pribadi, dan pemantauan sistem yang mengelola data harus dilakukan secara berkelanjutan" (BSSN, 2023). Selain itu, teknologi yang dikembangkan dan prosedur keamanan tutup dapat membantu menutup kesenjangan keamanan dalam sistem EKTP atau platform lain yang mengelola data pribadi²¹.

Pemerintah juga perlu lebih transparan dalam mengelola data pribadi dan untuk memastikan bahwa orang memiliki pemahaman yang jelas tentang bagaimana mereka menggunakannya. Keterbukaan pedoman ini meningkatkan kepercayaan publik pada sistem yang ada. Seperti yang disarankan UNCTAD (Konferensi PBB

tentang perdagangan dan pengembangan), "Transparansi dalam pengelolaan data pribadi adalah kunci untuk membangun kepercayaan antara penyelenggara dan individu yang terlibat dalam data" (UNCTAD, 2022). Oleh karena itu, pemerintah harus memastikan bahwa setiap pedoman diimplementasikan secara transparan sehubungan dengan data pribadi dan umumnya dipertimbangkan.

Sektor swasta memainkan peran yang sangat penting dalam melindungi data pribadi, karena banyak perusahaan mengumpulkan dan memproses data pribadi pengguna. Dalam hal ini, bisnis harus mematuhi standar perlindungan data yang ketat dan membuka untuk mengelola data pribadi mereka. Sebagaimana dinyatakan oleh Komisi Eropa tentang Perlindungan dan Pengadaan Data Pribadi, "perusahaan yang mengumpulkan data pribadi harus memastikan bahwa data dilindungi dengan langkah-langkah keamanan yang sesuai dan tidak digunakan untuk tujuan lain tanpa persetujuan individu" (European Protection Commission, 2020). Oleh karena itu, sertifikat keamanan data dari bisnis dan lembaga yang mengelola data pribadi sangat penting untuk meningkatkan akuntabilitas dan keandalan publik.

telah menjadi semakin kompleks dengan perkembangan teknologi yang cepat seperti Internet of Things (IoT), yang umumnya digunakan, dan tantangan dalam melindungi data pribadi menjadi semakin kompleks. Data yang dihasilkan oleh perangkat IoT harus dijaga agar tetap aman sehingga tidak jatuh ke tangan yang salah. Misalnya, laporan dari pemeriksaan teknologi MIT menyatakan bahwa "menggunakan perangkat IoT yang terkait dengan Internet tanpa perlindungan yang tepat dapat meningkatkan kemungkinan kebocoran utama data pribadi" (Technology Review, 2023). Oleh karena itu penting bagi pemerintah untuk menggunakan standar keamanan yang lebih ketat untuk perangkat IoT yang tersebar di seluruh

²¹ Rezqi Awaliyah, "Manajemen Pembinaan Jamaah Haji Pada Kementerian Agama Kabupaten Sinjai" (Universitas Islam Negeri Alauddin, 2018).

pasar untuk mengembangkan peraturan yang dapat memprediksi perkembangan ini.

Komunitas sebagai pemilik data pribadi harus diizinkan untuk lebih menyadari hak Anda atas data pribadi Anda. Anda perlu tahu cara melindungi data pribadi Anda di dunia maya dan dalam kehidupan sehari-hari Anda. Pemerintah dan lembaga terkait harus menyediakan saluran informasi yang mudah diakses oleh publik untuk melindungi dan melaporkan data pribadi ketika mereka melanggar data pribadi. Dalam hal ini, Laporan Internasional Privasi mengingatkan kami bahwa "pendidikan tentang privasi dan perlindungan data pribadi harus menjadi bagian penting dari upaya untuk mengasah persepsi digital masyarakat" (Privacy International, 2021).

Dengan langkah-langkah yang lebih luas, termasuk pembaruan pedoman yang terkait dengan standar internasional, penggunaan teknologi yang lebih aman dan meningkatkan kesadaran publik untuk perlindungan data pribadi, Indonesia dapat menciptakan sistem yang lebih aman ketika mengelola data pribadi warga negara. Pemerintah harus memastikan bahwa semua pedoman yang diterapkan dimaksudkan untuk melindungi hak-hak individu dan mempertahankan privasi data publik dari kemungkinan kebocoran dan penyalahgunaan yang mungkin tidak menguntungkan.

Secara keseluruhan, upaya untuk melindungi data pribadi membutuhkan kerja sama antara pemerintah, sektor swasta dan masyarakat. Tanpa langkah keseluruhan dan berkelanjutan, melindungi data pribadi Anda tetap menjadi tantangan utama. Namun, kerja sama yang erat dan penerapan pedoman yang tepat memastikan bahwa Indonesia dilindungi dari seluruh masyarakat dan menciptakan ekosistem digital yang andal. Seperti yang dinyatakan Perwakilan Perlindungan Data Pribadi Uni Eropa, "Keamanan Data Pribadi adalah dasar kepercayaan dalam transformasi teknologi ekonomi digital, dan karenanya harus menjadi prioritas dalam semua pedoman" (Komisaris Perlindungan Data Pribadi Uni Eropa, 2021)²².

C. KESIMPULAN

Di era transformasi digital yang semakin pesat, sistem informasi pemerintah telah memainkan peran yang sangat penting dalam meningkatkan efisiensi dan efektivitas layanan publik. Melalui digitalisasi proses birokrasi, penyederhanaan alur pelayanan, serta integrasi data antarinstansi, sistem informasi memungkinkan distribusi sumber daya yang lebih optimal dan layanan yang lebih cepat, transparan, serta responsif terhadap kebutuhan masyarakat. Inovasi

²²H M Harry Mulya Zein And Sisca Septiani, *Digitalisasi Pemerintahan Daerah: Katalis Untuk Integrasi Dan Optimasi Good Governance* (Sada Kurnia Pustaka, 2024).

seperti SIAK dan layanan perizinan daring merupakan contoh nyata manfaat konkret dari pemanfaatan teknologi informasi dalam sektor publik.

Namun demikian, penerapan sistem informasi yang aman dan terintegrasi tidak terlepas dari berbagai tantangan signifikan, terutama dalam aspek perlindungan data pribadi. Pemerintah masih menghadapi kendala berupa keterbatasan infrastruktur teknologi, kurangnya sumber daya manusia yang kompeten di bidang keamanan siber, dan rendahnya literasi digital di kalangan masyarakat. Situasi ini memperbesar risiko kebocoran data, penyalahgunaan informasi, serta serangan siber yang dapat merusak kepercayaan publik terhadap layanan digital pemerintah.

Menjawab tantangan tersebut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai tonggak penting dalam memberikan kerangka hukum yang kuat untuk perlindungan hak individu atas data pribadinya. UU ini mengatur dengan jelas prinsip-prinsip legalitas, transparansi, dan keamanan dalam pengelolaan data, serta mewajibkan instansi pemerintah untuk menunjuk Petugas Perlindungan Data (DPO) dan menerapkan teknologi keamanan informasi. Meskipun pelaksanaannya masih menghadapi berbagai hambatan, UU PDP memberikan dasar normatif yang strategis untuk memperkuat tata kelola data dalam sistem informasi pemerintah dan membangun kepercayaan publik terhadap ekosistem digital nasional.

DAFTAR PUSTAKA

- Aksenta, Almasari, Irmawati Irmawati, Achmad Ridwan, Nur Hayati, Sepriano Sepriano, Herlinah Herlinah, Ayupitha Tiara Silalah, et al. *LITERASI DIGITAL: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 Dan Society 5.0*. Jambi: PT. Sonpedia Publishing Indonesia, 2023.
- Anggraeni, Annisa Fitri, Apriyanto Apriyanto, Andi Rustam, Tri Kunawangsih Purnamaningrum, and Niar Astaginy. *Institusi Keuangan Dan Pasar Modal*. Jambi: PT. Sonpedia Publishing Indonesia, 2025.
- Arhani, Irfani. "Sanksi Pelaku Tindak Pidana Cyber Phishing Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2024.
- Awaliyah, Rezqi. "Manajemen Pembinaan Jamaah Haji Pada Kementerian Agama Kabupaten Sinjai." Universitas Islam Negeri Alauddin, 2018.
- Djarmiko, R M Gatot Hery. *Transformasi Kebijakan Administrasi Publik Menuju Era Society 5.0*. Indramayu: Penerbit Adab, 2023.

- Fadri, Zainal, and S Fil. *Era Digital Dan Dampaknya Terhadap Administrasi Publik. Reformasi Birokrasi Dalam Administrasi Publik: Tantangan Dan Peluang Di Era Digital*. Vol. 1. Agam: Yayasan Tri Edukasi Ilmiah, 2024.
- Gani, Taufiq A. *Kedaulatan Data Digital Untuk Integritas Bangsa*. Aceh: Syiah Kuala University Press, 2023.
- Hartatik, Hartatik, Arief Yanto Rukmana, Efitra Efitra, Iqbal Ramadhani Mukhlis, Almasari Aksenta, Luh Putu Rara Ayu Ratnaningrum, and Zefri Efdison. *TREN TECHNOPRENEURSHIP: Strategi & Inovasi Pengembangan Bisnis Kekinian Dengan Teknologi Digital*. Jambi: PT. Sonpedia Publishing Indonesia, 2023.
- Helmi, S, M IP, S Nofriadi, M IP, Effendi Hasan, S Muliawati, M IP, et al. *Digitalisasi Tata Kelola Pemerintahan Gampong Dalam Mewujudkan Percepatan Pelayanan Dan Pembangunan Melalui Sistem Informasi Gampong (Sigap)*. Cirebon: CV. Green Publisher Indonesia, 2024.
- Heriyanto, Heri. "Analisis Perbandingan Regulasi Dan Perlindungan Hukum Atas Privasi Data Pasien Di Tiga Negara Asia Tenggara (Indonesia, Singapura, Dan Laos)." *Jurnal Ners* 7, no. 2 (2023): 1247–1259. <https://journal.universitaspahlawan.ac.id/index.php/ners/article/view/16760>.
- Hibrizie, Rafi Alfian, Pranata Acun Sandriya, Rizky Fadillah Adrian, M Backtiar, and Yayat Suharyat. "Pandangan Islam Tentang Kesejahteraan Hidup Ekonomis." *Student Scientific Creativity Journal* 1, no. 3 (2023): 349–369. <https://journal.amikveteran.ac.id/index.php/sscj/article/download/1983/1568>.
- Indonesia, Pemerintah. *Undang-Undang Perlindungan Data Pribadi (UU PDP)*. Indonesia: Jakarta, 2022.
- Jannah, Sinta Ardhilatul. "Pengaruh Promosi Dan Kualitas Pelayanan Terhadap Minat Investasi Logam Mulia Pada Pegadaian Unit Pembantu Syariah Pasar III Muara Enim." Uin Raden Fatah Palembang, 2017.
- Mbato, Concilianus Laos, Fajar Sungging, and others. *Pendidikan Indonesia Masa Depan: Tantangan, Strategi, Dan Peran Universitas Sanata Dharma*. Depok: Sanata Dharma University Press, 2022.
- Prabowo, Hadi. *Birokrasi Dan Pelayanan Publik*. Bandung: Bimedia Pustaka Utama, 2022.
- Saputra, Aldi Dinata, Frans Dione, and Irfan Uluputty. "Pengelolaan Keamanan Informasi Dan Persandian Di Dinas Komunikasi Dan Informatika Provinsi Kalimantan Timur." *Jurnal Teknologi Dan Komunikasi Pemerintahan* 5, no. 2 (2023): 159–187. http://eprints.ipdn.ac.id/14787/1/30.0981_Aldi_Dinata_Saputra_Pengelolaan_Keamanan_Informasi_dan_Persandian_di_Dinas_Komunikasi_dan_Informatika_Provinsi_Kalimantan_Timur.pdf.
- Savitri, Peti, and others. *Transformasi Digital Dalam Industri Perbankan: Implikasi Terhadap Akuntansi Dan Teknologi Informasi*. Pekalongan: Penerbit NEM, 2024.

Sulianta, Feri. *SOCIAL INFORMATICS: Kajian Interaksi Teknologi & Masyarakat*. Feri Sulianta, 2024.

Sumarta, Nurjadi Harsa, and Djoko Karyono. *Auditor Internal Dan Konsultan Bisnis Desa: Sebuah Wacana Strategis*. bantul: Pandiva Buku, 2023.

Supendi, Alwi Putra. "Analisa Kerentanan Aplikasi Web Menggunakan Framework Mitre ATT & CK Dengan Metode Simulasi Red Team: Studi Kasus Di PT. Nurul Fikri Cipta Inovasi." Sekolah Tinggi Teknologi Terpadu Nurul Fikri, 2024.

Yoyo Sudaryo, S E, M MM, S Pd Nunung Ayu Sofiati Efi, S E Mohamad Arfiman Yosep, S T Budi Nurdiansyah, M H SE, and others. *Digital Marketing Dan Fintech Di Indonesia*. Yogyakarta: Penerbit Andi, 2020.

Zein, H M Harry Mulya, and Sisca Septiani. *Digitalisasi Pemerintahan Daerah: Katalis Untuk Integrasi Dan Optimasi Good Governance*. Banten: Sada Kurnia Pustaka, 2024.