PERLINDUNGAN DATA PRIBADI DAN AKUNTABILITAS PEMERINTAH DALAM DIGITALISASI PELAYANAN PUBLIK DI INDONESIA

Selvia Mutiara Fajar[1], Tasyabiratul Desjava Putri[2], Thesa Adelin Sidabutar[3]
selviamutiarafajar@gmail.com[1] , tbiratul@gmail.com[2] , adelinthesa@gmail.com[3]
Universitas Maritim Raja Ali Haji

ABSTRAK

Perlindungan data pribadi menjadi isu strategis di era digital, seiring meningkatnya penggunaan teknologi informasi dalam pelayanan publik. Pemerintah Indonesia telah mengesahkan Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 sebagai payung hukum utama yang mengatur hak- hak pemilik data, kewajiban pengendali data, serta sanksi bagi pelanggaran. UU ini juga memiliki efek ekstrateritorial, sehingga perusahaan asing yang mengolah data warga Indonesia wajib mematuhinya. Meski kerangka hukum sudah tersedia, implementasi masih menghadapi tantangan seperti keterbatasan SDM, infrastruktur, literasi masyarakat yang rendah, dan risiko baru akibat perkembangan teknologi. Untuk memperkuat akuntabilitas, diperlukan pembentukan lembaga independen pengawas data pribadi, audit keamanan secara rutin, transparansi publik dalam kasus kebocoran, serta edukasi literasi digital. Keberhasilan perlindungan data pribadi pada akhirnya bergantung pada keseriusan pemerintah, pengawasan yang efektif, dan partisipasi masyarakat.

Kata Kunci: Perlindungan Data Pribadi, UU PDP, Keamanan Siber, Akuntabilitas.

ABSTRACT

Personal data protection has become a strategic issue in the digital era, along with the growing use of information technology in public services. Indonesia enacted the Personal Data Protection Law (Law No. 27 of 2022) as the primary legal framework regulating data subjects' rights, data controllers' obligations, and sanctions for violations. This law also has extraterritorial effect, requiring foreign companies processing Indonesian citizens' data to comply. Despite this legal framework, implementation still faces challenges such as limited human resources, infrastructure gaps, low digital literacy, and emerging risks from new technologies. Strengthening accountability requires the establishment of an independent data supervisory authority, regular security audits, transparency in data breach cases, and public digital literacy education. Ultimately, the success of personal data protection in Indonesia depends on government commitment, effective oversight, and active citizen participation.

***Keywords**: Personal Data Protection, PDP Law, Cybersecurity, Account Ability.*

PENDAHULUAN

Kemajuan pesat dalam teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor, termasuk dalam penyelenggaraan layanan publik di Indonesia. Digitalisasi ini memberikan kemudahan dan meningkatkan efisiensi, namun juga menimbulkan tantangan besar terkait perlindungan dan keamanan data pribadi masyarakat. Pemerintah Indonesia menyadari pentingnya menjaga keamanan serta kerahasiaan data pribadi sebagai bagian dari hak fundamental warga negara sekaligus untuk membangun kepercayaan publik terhadap layanan digital. Oleh karena itu, pemerintah telah menetapkan berbagai regulasi dan kebijakan penting, salah satunya adalah Undang-Undang Pelindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, yang menjadi dasar hukum utama dalam pengelolaan dan perlindungan data pribadi di tanah air.

UU PDP memberikan pengaturan menyeluruh mengenai hak-hak pemilik data, kewajiban pengendali dan pengolah data, mekanisme persetujuan, serta sanksi pidana dan administratif

bagi pelanggar. Selain itu, pemerintah juga mengeluarkan regulasi teknis dan operasional melalui Peraturan Pemerintah, Peraturan Menteri, dan pedoman teknis yang mengatur keamanan siber, tata kelola data, serta penyimpanan data secara lokal. Penggunaan cloud lokal dan penerapan enkripsi merupakan langkah strategis untuk memastikan data layanan digital tetap berada dalam yurisdiksi Indonesia dan mengurangi risiko akses tidak sah dari luar negeri.

Meski regulasi dan kebijakan telah disusun secara komprehensif, pelaksanaannya di lapangan masih menghadapi berbagai kendala, terutama di tingkat daerah dan instansi pemerintah yang memiliki keterbatasan sumber daya manusia, infrastruktur, dan kesiapan teknis. Audit dan pemantauan pelanggaran data pribadi yang dilakukan oleh Kominfo dan BSSN menunjukkan peningkatan kasus kebocoran data, yang menandakan perlunya penguatan pengawasan dan penegakan hukum. Selain itu, kemunculan teknologi baru seperti kecerdasan buatan, big data, dan Internet of Things (IoT) menuntut regulasi yang adaptif dan responsif terhadap risiko privasi yang berkembang.

Pendahuluan jurnal ini bertujuan untuk mengkaji kebijakan pemerintah dalam menjamin keamanan dan kerahasiaan data pribadi masyarakat, mengidentifikasi tantangan dalam pelaksanaan UU PDP dan regulasi terkait, serta memberikan rekomendasi strategis guna memperkuat perlindungan data pribadi di era digital. Dengan demikian, diharapkan tercipta ekosistem digital yang aman, terpercaya, dan berkelanjutan yang mendukung pelayanan publik yang efektif sekaligus menghormati hak privasi warga negara.

METODOLOGI

Penelitian ini menggunakan spesifikasi penelitian deskriptif-analitis dengan tujuan menggambarkan serta menganalisis penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 dalam konteks akuntabilitas pemerintah. Jenis penelitian yang digunakan adalah penelitian hukum normatif-empiris, yakni memadukan kajian terhadap peraturan perundang-undangan dengan realitas implementasi di lapangan. Pendekatan yang digunakan adalah pendekatan yuridis- normatif untuk menelaah regulasi terkait perlindungan data pribadi serta pendekatan sosiologis untuk melihat tantangan praktis di masyarakat dan instansi pemerintah. Teknik pengumpulan data dilakukan melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur akademik, dan jurnal penelitian, serta dilengkapi dengan studi dokumentasi dan data sekunder dari laporan resmi pemerintah maupun media daring. Metode analisis data yang digunakan adalah analisis kualitatif dengan cara mereduksi, mengklasifikasi, serta menginterpretasikan data secara sistematis untuk memperoleh gambaran menyeluruh mengenai kesenjangan antara regulasi dan implementasi, serta menawarkan rekomendasi bagi penguatan perlindungan data pribadi di Indonesia.

HASIL DAN PEMBAHASAN

BAB I - Jaminan Keamanan Dan Kerahasiaan Data Pribadi Dalam Digitalisasi Pelayanan Publik

Digitalisasi pelayanan publik di Indonesia telah berkembang dengan sangat cepat. Hampir semua bidang layanan kini mulai beralih ke sistem berbasis elektronik. Misalnya, di bidang kesehatan pemerintah meluncurkan aplikasi PeduliLindungi dan SatuSehat, di bidang administrasi kependudukan tersedia layanan Dukcapil online, dan di berbagai daerah pemerintah sudah menyediakan platform pelayanan publik berbasis digital untuk mempermudah masyarakat mengurus berbagai dokumen. Perubahan ini membawa banyak manfaat seperti efisiensi waktu, kemudahan akses, dan penghematan biaya. Masyarakat

tidak perlu lagi datang langsung ke kantor pelayanan, cukup melalui aplikasi atau website yang tersedia.

Namun, perkembangan digitalisasi ini juga menghadirkan tantangan baru, yaitu ancaman kebocoran data pribadi. Data masyarakat yang tersimpan dalam sistem digital memiliki nilai yang sangat tinggi. Data seperti nomor induk kependudukan (NIK), alamat rumah, rekam medis, hingga data finansial bisa disalahgunakan untuk kepentingan tertentu, mulai dari kejahatan siber, penipuan, hingga jual beli data di pasar gelap digital. Oleh karena itu, penting bagi pemerintah untuk menjamin bahwa digitalisasi pelayanan publik tidak justru membuka peluang baru bagi pelanggaran privasi warga negara.1

Untuk merespons tantangan tersebut, pemerintah Indonesia telah membentuk kerangka hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini merupakan tonggak penting karena menjadi dasar hukum pertama yang secara khusus mengatur hak-hak pemilik data pribadi, kewajiban penyelenggara sistem elektronik (PSE), serta mekanisme perlindungan jika terjadi kebocoran data. UU PDP juga menekankan prinsip-prinsip dasar, seperti transparansi, tujuan yang jelas, keterbatasan pemrosesan data, keamanan data, serta akuntabilitas pengendali data.

Selain UU PDP, terdapat pula Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang mengatur lebih teknis mengenai tanggung jawab PSE, termasuk kewajiban menyediakan sistem yang andal, aman, serta dapat dipertanggungjawabkan. Dari sisi kelembagaan, pemerintah menugaskan Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN) untuk menjadi garda terdepan dalam menjaga keamanan sistem digital negara. Kominfo berfokus pada regulasi dan pengawasan, sementara BSSN menangani aspek teknis keamanan siber.2

Meski demikian, regulasi saja tidak cukup. Tantangan utama justru terletak pada implementasi di lapangan. Pemerintah sudah berusaha untuk menempatkan data pada server dalam negeri atau cloud lokal, menggunakan teknologi enkripsi, melakukan audit keamanan sistem, serta mewajibkan adanya pelaporan insiden kebocoran data. Namun faktanya, kasus kebocoran data masih sering terjadi. Contohnya, kebocoran data aplikasi eHAC Kementerian Kesehatan pada tahun 2021 dan serangan terhadap Pusat Data Nasional (PDN) pada tahun 2024 yang membuat banyak layanan digital pemerintah lumpuh. Kasus-kasus ini membuktikan bahwa meskipun aturan sudah ada, praktik keamanan siber dan budaya perlindungan data masih belum kuat.

Masalah lain adalah tingkat kesadaran masyarakat. Banyak warga yang masih belum memahami pentingnya menjaga kerahasiaan data pribadi, misalnya dengan mudah membagikan NIK atau foto KTP di media sosial. Padahal, perlindungan data pribadi tidak hanya tanggung jawab pemerintah, tetapi juga membutuhkan partisipasi aktif dari masyarakat sebagai pemilik data.3

Dengan demikian, dapat disimpulkan bahwa jaminan keamanan data pribadi dalam digitalisasi pelayanan publik dilakukan melalui kombinasi regulasi hukum, standar teknis keamanan, serta pengawasan kelembagaan. Akan tetapi, masih terdapat gap (kesenjangan) yang cukup besar antara aturan yang tertulis dengan praktik nyata di lapangan. Karena itu, perlu dilakukan perbaikan berkelanjutan, baik dari sisi penegakan hukum, peningkatan kapasitas teknis, maupun edukasi masyarakat. Tanpa langkah-langkah tersebut, digitalisasi pelayanan publik yang seharusnya membawa kemudahan justru bisa menimbulkan kerugian baru bagi masyarakat akibat penyalahgunaan data pribadi.

BAB II – Kebijakan Dan Regulasi Serta Kesesuaiannya Dengan Prinsip Akuntabilitas Publik

Sejauh mana kebijakan dan regulasi di Indonesia benar-benar mampu melindungi data pribadi warga negara, serta apakah kebijakan tersebut sudah sesuai dengan prinsip akuntabilitas publik yang menjadi landasan tata kelola pemerintahan yang baik.

Secara normatif, Undang-Undang Pelindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang cukup komprehensif. UU ini menegaskan berbagai hak subjek data, seperti hak untuk mengetahui tujuan penggunaan data pribadinya, hak akses untuk melihat data yang disimpan, hak untuk mengoreksi data yang keliru, hingga hak untuk menghapus data atau yang dikenal dengan istilah "right to be forgotten". Selain itu, UU PDP juga mengatur sanksi yang beragam, mulai dari sanksi administratif, perdata, hingga pidana bagi pihak-pihak yang melanggar ketentuan, baik itu instansi pemerintah maupun pelaku di sektor swasta. Hal ini merupakan kemajuan signifikan dibandingkan dengan sistem hukum sebelumnya yang hanya mengandalkan aturan sektoral yang terpisah-pisah dan belum menyeluruh.

Dari perspektif akuntabilitas publik, regulasi yang ada sudah mencerminkan beberapa prinsip utama yang sangat penting. Pertama, prinsip transparansi diwujudkan melalui kewajiban bagi penyelenggara sistem elektronik untuk memberitahukan kepada publik apabila terjadi kebocoran data pribadi. Kedua, prinsip pertanggungjawaban hukum ditegakkan dengan adanya mekanisme sanksi yang dapat dikenakan kepada pemerintah atau penyelenggara sistem elektronik (PSE) yang lalai dalam menjaga keamanan data. Ketiga, pengawasan diupayakan melalui rencana pembentukan otoritas perlindungan data pribadi yang bersifat independen, yang bertugas mengawasi kepatuhan terhadap regulasi dan memberikan perlindungan kepada subjek data.4

Namun demikian, dalam praktiknya masih terdapat sejumlah tantangan yang cukup signifikan. Pertama, regulasi turunan yang menjadi pedoman teknis pelaksanaan UU PDP belum semuanya diterbitkan, sehingga banyak detail operasional yang masih belum jelas dan membingungkan bagi pelaksana di lapangan. Kedua, otoritas independen yang dijanjikan oleh UU sebagai pengawas utama perlindungan data pribadi sampai saat ini belum terbentuk secara penuh dan belum beroperasi secara efektif. Hal ini menyebabkan pengawasan terhadap pelaksanaan UU PDP menjadi kurang optimal. Ketiga, terdapat ketimpangan kapasitas dan standar teknis di antara berbagai instansi pemerintah, terutama antara pusat dan daerah, sehingga penerapan keamanan data pribadi belum merata dan konsisten.

Dengan demikian, meskipun secara hukum Indonesia telah memiliki regulasi yang cukup kuat dan lengkap untuk melindungi data pribadi, implementasi di lapangan masih menunjukkan kelemahan yang nyata. Akuntabilitas publik dalam hal perlindungan data pribadi belum berjalan secara maksimal karena mekanisme pengawasan, transparansi, dan penegakan hukum belum sepenuhnya efektif dan merata. Oleh karena itu, perlu upaya lebih lanjut untuk memperkuat regulasi turunan, membentuk dan mengaktifkan lembaga pengawas independen, serta meningkatkan kapasitas teknis dan sumber daya di seluruh instansi terkait agar perlindungan data pribadi dapat benar-benar terlaksana sesuai dengan prinsip akuntabilitas publik.5

BAB III - Pertanggungjawaban Pemerintah atas Pelanggaran dan Kebocoran Data

Digitalisasi pelayanan publik membawa konsekuensi besar terhadap akuntabilitas pemerintah, khususnya dalam melindungi data pribadi masyarakat. Akuntabilitas ini tidak hanya berarti pemerintah harus mampu menyediakan layanan yang cepat dan efisien, tetapi juga memastikan bahwa data masyarakat yang mereka kelola tetap aman dan tidak

disalahgunakan. Apabila terjadi pelanggaran atau kebocoran data, maka tanggung jawab pemerintah akan diuji, apakah mampu memberikan perlindungan hukum, pemulihan bagi korban, serta transparansi informasi kepada publik.

Bentuk pertanggungjawaban pemerintah dalam kasus kebocoran data pada dasarnya sudah diatur dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) maupun aturan turunannya. Pemerintah memiliki kewajiban memberikan sanksi administratif kepada penyelenggara sistem elektronik (PSE) yang lalai, misalnya berupa peringatan, denda, penghentian sementara sistem, hingga kewajiban memperbaiki sistem yang bocor. Jika kebocoran dilakukan dengan sengaja oleh individu atau lembaga, maka dapat dikenakan sanksi pidana, baik berupa hukuman penjara maupun denda. Selain itu, masyarakat sebagai pemilik data juga berhak menuntut ganti rugi perdata apabila mengalami kerugian, baik secara materiil seperti kehilangan finansial maupun immateriil seperti hilangnya rasa aman dan privasi.6 Tidak kalah penting, pemerintah juga memikul tanggung jawab politik dengan cara memberi klarifikasi, menyampaikan permintaan maaf, dan melaporkan secara transparan kepada publik maupun DPR. Dengan demikian, pertanggungjawaban pemerintah tidak hanya berhenti pada aspek hukum, tetapi juga menyangkut kepercayaan publik terhadap negara.

Mekanisme penegakan perlindungan data pribadi sendiri tersedia melalui beberapa jalur. Masyarakat dapat melapor ke Kominfo atau BSSN apabila menjadi korban kebocoran data. Selain itu, jalur peradilan perdata maupun pidana juga terbuka bagi masyarakat untuk menuntut haknya. Dalam jangka panjang, UU PDP juga mengamanatkan pembentukan otoritas perlindungan data pribadi independen yang diharapkan mampu menjadi pengawas utama dan bertindak lebih profesional dalam menangani isu kebocoran data. Namun, mekanisme ini pada praktiknya masih menghadapi hambatan. Respons pemerintah seringkali lambat, proses penyelesaian kasus cenderung berbelit, dan transparansi penyampaian informasi kepada masyarakat masih minim.

Hal tersebut terlihat jelas dalam beberapa kasus kebocoran data yang pernah terjadi. Misalnya, pada kebocoran aplikasi eHAC Kementerian Kesehatan tahun 2021, data jutaan pengguna bocor dan diakses pihak tidak berwenang. Pemerintah pada saat itu dikritik karena dianggap lambat merespons serta kurang terbuka dalam menjelaskan penyebab kebocoran maupun langkah perbaikan yang dilakukan. Kasus serangan ransomware terhadap Pusat Data Nasional (PDN) pada tahun 2024 juga menunjukkan lemahnya kesiapan pemerintah menghadapi serangan siber berskala besar. Layanan publik sempat lumpuh selama beberapa waktu karena minimnya sistem cadangan (backup) yang bisa segera dipakai. Kondisi ini menimbulkan kerugian besar bagi masyarakat dan memperkuat kritik bahwa pertanggungjawaban pemerintah masih sebatas formalitas, belum benar-benar efektif melindungi hak warga negara.7

Kenyataan di atas menunjukkan bahwa meskipun bentuk pertanggungjawaban sudah diatur dengan cukup jelas, implementasi di lapangan masih jauh dari ideal. Kelemahan teknis dalam sistem keamanan, rendahnya transparansi pemerintah, belum optimalnya koordinasi antar lembaga, serta belum terbentuknya otoritas perlindungan data independen menjadi faktor yang memperburuk situasi. Ke depan, pemerintah harus menempatkan mekanisme remedial yang cepat, transparan, dan adil sebagai prioritas utama. Hal ini bisa dilakukan dengan memperkuat infrastruktur keamanan data, mempercepat pembentukan otoritas pengawas independen, melakukan audit sistem secara berkala, serta memastikan bahwa setiap korban kebocoran data mendapatkan kompensasi yang layak.

Dengan demikian, pertanggungjawaban pemerintah atas kebocoran data tidak cukup hanya sebatas penegakan hukum atau pemberian sanksi, melainkan juga menyangkut pemulihan kepercayaan masyarakat. Hanya dengan langkah yang nyata, cepat, dan

transparan, negara dapat menunjukkan komitmen serius bahwa digitalisasi pelayanan publik benar-benar membawa manfaat tanpa mengorbankan hak fundamental warga negara atas keamanan dan kerahasiaan data pribadinya.

BAB IV – Tantangan Utama dalam Menyeimbangkan Efisiensi dan Hak Privasi

Digitalisasi pelayanan publik membawa banyak manfaat, terutama dalam hal mempercepat proses dan meningkatkan kemudahan akses bagi masyarakat. Namun, di balik kemudahan tersebut, terdapat dilema yang cukup kompleks, yaitu bagaimana menyeimbangkan antara kebutuhan efisiensi layanan dengan kewajiban menjaga hak privasi warga negara. Pemerintah menghadapi sejumlah tantangan utama yang harus diatasi agar kedua aspek ini dapat berjalan beriringan secara harmonis.

Pertama, perkembangan teknologi digital seperti big data, kecerdasan buatan (AI), Internet of Things (IoT), dan teknologi biometrik berlangsung sangat cepat, jauh melampaui kecepatan penyusunan regulasi yang mengaturnya. Meskipun Undang- Undang Pelindungan Data Pribadi (UU PDP) baru disahkan pada tahun 2022, praktik digitalisasi layanan publik sudah berlangsung jauh sebelumnya. Hal ini menyebabkan adanya kesenjangan antara teknologi yang digunakan dengan aturan hukum yang mengaturnya, sehingga potensi risiko pelanggaran privasi menjadi lebih besar.8

Kedua, kapasitas teknis dan sumber daya manusia (SDM) di banyak instansi pemerintah, khususnya di tingkat daerah, masih sangat terbatas. Tidak semua instansi memiliki tenaga ahli keamanan siber yang memadai untuk menerapkan standar keamanan data secara konsisten. Ketidaksiapan ini berpotensi menimbulkan celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.

Ketiga, infrastruktur teknologi informasi yang digunakan oleh pemerintah masih menghadapi berbagai kerentanan. Beberapa sistem lama belum diperbarui atau diupgrade secara memadai, server yang digunakan belum sepenuhnya aman, dan praktik penting seperti enkripsi data serta audit keamanan secara berkala belum diterapkan secara menyeluruh. Kondisi ini meningkatkan risiko kebocoran data dan serangan siber yang dapat merugikan masyarakat.

Keempat, terdapat dilema antara kecepatan peluncuran layanan digital dengan aspek keamanan. Dalam upaya memenuhi tuntutan efisiensi dan percepatan pelayanan, sering kali layanan digital diprioritaskan untuk segera dirilis tanpa melalui pengujian keamanan yang matang. Akibatnya, layanan tersebut rentan terhadap berbagai ancaman keamanan yang dapat membahayakan data pribadi pengguna.

Kelima, kesadaran masyarakat terhadap pentingnya perlindungan data pribadi masih tergolong rendah. Banyak warga yang tanpa sadar memberikan data pribadi secara berlebihan atau kurang memperhatikan persetujuan penggunaan data. Hal ini menyebabkan pengawasan sosial terhadap pemerintah dan penyelenggara layanan digital menjadi terbatas, sehingga potensi penyalahgunaan data sulit terdeteksi dan dikendalikan.9

Keseluruhan tantangan ini menunjukkan bahwa perlindungan data pribadi bukan hanya soal adanya regulasi yang memadai, tetapi juga berkaitan erat dengan budaya privasi yang harus dibangun di masyarakat serta kesiapan teknis yang harus dimiliki oleh instansi pemerintah. Pemerintah dituntut untuk memperkuat kapasitas sumber daya manusia, memperbaiki infrastruktur teknologi, serta meningkatkan koordinasi antar lembaga agar efisiensi pelayanan publik digital tidak mengorbankan hak dasar warga negara atas privasi dan keamanan data pribadi mereka.

BAB V - Peran Keterlibatan Masyarakat Dan Transparansi Dalam Mewujudkan Akuntabilitas

Agar pemerintah benar-benar akuntabel dalam melindungi data pribadi masyarakat, maka keterlibatan masyarakat dan transparansi harus menjadi fondasi utama dalam tata

kelola data. Selama ini, perlindungan data seringkali dianggap sebagai urusan pemerintah dan penyelenggara sistem saja, padahal masyarakat sebagai pemilik data justru memiliki peran besar untuk mengawasi, mengkritisi, bahkan menuntut jika haknya dilanggar. Tanpa partisipasi publik dan keterbukaan informasi, regulasi yang ada hanya akan menjadi aturan di atas kertas, sementara praktiknya tetap rawan kebocoran dan penyalahgunaan.

Keterlibatan masyarakat bisa diwujudkan dalam beberapa cara. Pertama, melalui pengaduan publik. Pemerintah harus menyediakan saluran resmi yang mudah diakses oleh masyarakat untuk melaporkan dugaan pelanggaran atau kebocoran data. Misalnya, adanya pusat layanan pengaduan berbasis online yang responsif dan jelas tindak lanjutnya. Kedua, masyarakat juga dapat ikut serta dalam proses perumusan regulasi, misalnya melalui forum konsultasi publik, diskusi kebijakan, atau masukan dari lembaga swadaya masyarakat (LSM). Hal ini penting agar aturan yang dibuat tidak hanya berpihak pada kepentingan negara atau penyelenggara sistem, tetapi juga benar- benar melindungi hak warga negara.10 Ketiga, masyarakat sipil dapat melakukan advokasi hukum, termasuk mengajukan gugatan ke pengadilan apabila hak atas privasi dilanggar. Kehadiran kelompok masyarakat sipil yang aktif akan menjadi pengawas tambahan agar pemerintah tidak lepas tangan.

Selain keterlibatan masyarakat, transparansi juga menjadi kunci dalam mewujudkan akuntabilitas. Transparansi berarti pemerintah dan instansi penyelenggara layanan digital harus terbuka terhadap publik mengenai bagaimana data pribadi dikumpulkan, digunakan, dan dilindungi. Misalnya, setiap instansi wajib menyediakan kebijakan privasi yang jelas dan mudah dipahami. Tujuan pengumpulan data, cara pemrosesan, serta siapa saja pihak yang dapat mengaksesnya harus disampaikan secara terbuka, bukan disembunyikan dengan bahasa hukum yang rumit.

Lebih jauh lagi, jika terjadi kebocoran data, pemerintah wajib memberikan pemberitahuan insiden kepada masyarakat. Hal ini penting agar masyarakat bisa segera melindungi diri, misalnya dengan mengganti kata sandi, memblokir akun, atau mengajukan keberatan. Tanpa pemberitahuan yang cepat, masyarakat akan menjadi korban berulang karena tidak mengetahui bahwa datanya sudah disalahgunakan. Transparansi juga perlu ditegakkan melalui audit independen. Hasil audit tentang keamanan sistem dan kepatuhan terhadap regulasi sebaiknya dipublikasikan secara berkala agar masyarakat bisa ikut mengawasi. Dengan begitu, tidak ada lagi ruang bagi instansi untuk menutup-nutupi kelemahan sistemnya.

Melalui keterlibatan masyarakat dan transparansi, akan ada tekanan moral maupun politik bagi pemerintah untuk tidak lalai dalam menjaga data pribadi. Pemerintah tidak bisa lagi bekerja secara tertutup, melainkan harus terbuka dan siap diawasi. Di sisi lain, masyarakat juga akan merasa memiliki peran dalam menjaga ekosistem digital yang sehat. 11Partisipasi publik ini pada akhirnya akan meningkatkan kepercayaan masyarakat terhadap sistem digital pemerintah. Kepercayaan inilah yang menjadi modal sosial penting agar digitalisasi pelayanan publik dapat berjalan dengan lancar dan berkelanjutan.

Dengan kata lain, perlindungan data pribadi bukan hanya urusan regulasi dan teknologi, tetapi juga tentang hubungan timbal balik antara pemerintah dan masyarakat. Pemerintah dituntut untuk transparan, sementara masyarakat didorong untuk aktif berpartisipasi. Jika kedua hal ini berjalan seimbang, maka akuntabilitas dalam pengelolaan data pribadi bisa benar-benar terwujud, dan digitalisasi pelayanan publik di Indonesia dapat memberikan manfaat yang maksimal tanpa mengorbankan hak privasi warganya.12

KESIMPULAN

Digitalisasi layanan publik di Indonesia memang memberikan kemudahan dan mempercepat akses bagi masyarakat, tetapi juga menimbulkan tantangan serius terkait

perlindungan data pribadi. Pemerintah sudah menetapkan aturan yang cukup lengkap melalui UU Pelindungan Data Pribadi dan peraturan pendukung lainnya, serta membentuk lembaga pengawas dan standar keamanan teknis. Namun, pelaksanaannya di lapangan masih menghadapi berbagai kendala, seperti keterbatasan sumber daya dan infrastruktur yang belum memadai, serta adanya kesenjangan antara aturan yang ada dengan praktik nyata. Selain itu, kesadaran dan peran aktif masyarakat dalam mengawasi perlindungan data pribadi juga masih perlu ditingkatkan agar pemerintah bisa lebih bertanggung jawab. Dengan demikian, perlindungan data pribadi dalam digitalisasi layanan publik harus didukung oleh regulasi yang kuat, peningkatan kemampuan teknis, transparansi, dan partisipasi masyarakat agar hak privasi warga tetap terjaga tanpa menghambat kecepatan dan kemudahan layanan.

DAFTAR PUSTAKA

Abdullah, C., Durand, N., & Moonti, R. M. (2025). Transformasi Digital dan Hak atas Privasi: Tinjauan Kritis Pelaksanaan UU Perlindungan Data Pribadi (PDP) Tahun 2022 di Era Big Data. Amandemen: Jurnal Ilmu Pertahanan, Politik dan Hukum Indonesia, 2(3), 233–241.

Abdullah, Chairunnisa, Nursakina Durand, and Roy Marthen Moonti. "Transformasi Digital Dan Hak Atas Privasi: Tinjauan Kritis Pelaksanaan Perlindungan Data Pribadi (PDP) Tahun 2022 Di Era Big Data." Politik Dan Hukum Indonesia 2, no. 3 (2025): 233–41. https://doi.org/10.62383/amandemen.v2i3.1073.

Al Baihaqy, A. H., Yuwana, M. A. S., Adhi Surya, A. P., & Syaikhona Kholil, M. A. N. F. (2024). Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM. Wicarana, 3(1).

Andhika Pratama Adhi Surya M . Asif Nur Fauzi" 4, no. 156 (2025): 31–37. Iqbal, Husein Muhammad, Sapto Hermawan, and Asianto Nugroho. "Bentuk

Anggaini, R. P., Dahlian, P., & Mulyadi. (2024). Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional. Syntax Literate: Jurnal Ilmiah Indonesia, 10(5).

Azza Fitrahul Faizah, Ananda Fersa Dharmawan, Garry Gumelar Pratama, and Sinta Dewi Rosadi. "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura." Hakim: Jurnal Ilmu Hukum Dan Sosial 1 (2023).

Buala, J., Elisatris, G., & Yuanitasari, D. (2024). Penyalahgunaan Data Pribadi Konsumen Oleh Perusahaan: Kajian Yuridis dalam Perspektif UU Perlindungan Konsumen dan UU Perlindungan Data Pribadi. Jurnal Pendidikan Indonesia.

Faizah, A. F., Rosadi, S. D., Pratama, G. G., & Dharmawan, A. F. (2023). Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan Perbandingan Hukum Hong Kong dan Singapura. Hakim: Jurnal Ilmu Hukum dan Sosial.

Ham, Dalam Perspektif, Muhammad Asthi, Seta Ari, Abdul Hakim, and Al Baihaqy. "ANALISA DAMPAK KEBOCORAN DATA PUSAT DATA NASIONAL (PDN)

Iqbal, H. M., Hermawan, S., & Nugroho, A. (2024). Bentuk Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional Berdasarkan Hukum Administrasi Negara. Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara, 3(2).

Jefry, Buala, Elisatris Gultom, and Deviana Yuanitasari. "Penyalahgunaan Data Pribadi Konsumen Oleh Perusahaan: Kajian Yuridis Dalam Perspektif UU Perlindungan Konsumen Dan UU Perlindungan Data Pribadi." Jurnal Pendidikan Indonesia 6, no. 5 (2025): 1–7. https://doi.org/10.59141/japendi.v6i5.7709.

Jonathan Riko Mono, and Lewiandy. "Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi Dalam Insiden Serangan Siber Pusat Data Nasional Sementara." Jurnal Ilmu Hukum, Humaniora Dan Politik 5, no. 1 (2024): 467–77. https://doi.org/10.38035/jihhp.v5i1.3195.

Karnedi, G., & Alam, R. G. (2024). Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa. El-Mujtama: Jurnal Pengabdian Masyarakat, 5(3).

Karnedi, Gunawan, and RG Guntur Alam. “Evaluasi Regulasi Perlindungan Data Pribadi Di Indonesia: Komparasi Dengan GDPR Uni Eropa.” El-Mujtama: Jurnal Pengabdian Masyarakat 5, no. 3 (2025): 610–22. https://doi.org/10.47467/elmujtama.v5i3.8549.

Laelaturramadani. (2024). Tinjauan Terhadap Efektivitas Regulasi Perlindungan Data Pribadi di Indonesia. Mandalika Law Journal, 3(1).

Laelaturramadani. “Tinjauan Terhadap Efektivitas Regulasi Perlindungan Data Pribadi Di Indonesia.” Mandalika Law Journal 3, no. 1 (2025): 38–48. https://ojs.cahayamandalika.com/index.php/mlj/article/view/5469/4034.

Mono, J. R., & Lewiandy. (2024). Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi dalam Insiden Serangan Siber Pusat Data Nasional Sementara. Jurnal Ilmu Hukum, Humaniora dan Politik, 5(1), 467–477.

Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional Berdasarkan Hukum Administrasi Negara.” Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara 3, no. 2 (2025): 72–83.

Puspita D, Rini Anggaini. “Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional.” Syntax Literate ; Jurnal Ilmiah Indonesia 10, no. 5 (2025): 5397–5406. https://doi.org/10.36418/syntax- literate.v10i5.59084.

Rinjani, M. A., & Firmansyah, R. (2023). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum, 8(1).

Sembiring, F., & Pattihahuan, F. M. (2024). Peran Badan Siber dan Sandi Negara dalam Kasus Serangan Siber yang Mengakibatkan Kebocoran Data Pribadi Pusat Data Nasional Sementara 2 (PDNS2). Gloria Justitia, 5(1).

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. Journal Sains Student Research, 2(6).

Toding Bua, I., & Idris, N. I. (2024). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, 2(2).

Tommy, S., & Nasution, M. I. P. (2024). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN). Jurnal Ilmiah Ekonomi dan Manajemen; dan juga Jurnal Manajemen Ekonomi dan Bisnis, tergantung versi publikasinya.