Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan
Volume 2, Nomor. 2, Mei 2025
E-ISSN .: 3063-2803; P-ISSN .: 3063-279X; Hal. 100-114
DOI: https://doi.org/10.62383/desentralisasi.v2i2.653
Available online at: https://ejournal.appihi.or.id/index.php/Desentralisasi

Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024

Imanuel Toding Bua[1*], Nur Isdah Idris[2]
[1-2] Universitas Hasanuddin, Indonesia
Imanueltodingbua3@gmail.com[1] , *nurisdah@unhas.ac.id[2]*

Alamat: Jalan Perintis Kemerdekaan Km. 10 Tamalanrea, Kota Makassar, Sulawesi Selatan, Indonesia
*Korespondensi penulis: Imanueltodingbua3@gmail.com**

Abstract*. The 2024 data breach incident at Indonesia's National Data Center (PDN) marked a major crisis in the governance of national cybersecurity. This study examines the causes, threats, proposed solutions, and the roles of both the government and the public in responding to such breaches. The research employs a literature review and media framing analysis, focusing on news coverage and government policy responses. Findings indicate that systemic vulnerabilities, inadequate infrastructure readiness, and human factors are the primary causes of the breach. The resulting threats include economic and social losses, a decline in public trust, and the risk of data misuse. Proposed solutions involve strengthening regulations, enhancing technical capacity, and increasing public awareness through education. The active participation of civil society and swift government response are critical to restoring trust and preventing similar incidents in the future*

Keywords*: Cyber Security, Data Breach, National Data Center, Indonesia, Public Policy*.

Abstrak. Insiden kebocoran data pada Pusat Data Nasional (PDN) Indonesia tahun 2024 menandai krisis besar dalam tata kelola keamanan siber nasional. Penelitian ini menganalisis penyebab, ancaman, solusi, serta peran masyarakat dan pemerintah dalam menangani kebocoran data nasional. Metode yang digunakan adalah kajian literatur dan analisis framing media, dengan fokus pada pemberitaan dan kebijakan pemerintah. Hasil penelitian menunjukkan bahwa kelemahan sistem, kurangnya kesiapan infrastruktur, serta faktor manusia menjadi penyebab utama kebocoran. Ancaman yang muncul meliputi kerugian ekonomi dan sosial, penurunan kepercayaan publik, dan risiko penyalahgunaan data. Solusi yang diusulkan meliputi penguatan regulasi, peningkatan kapasitas teknis, dan edukasi masyarakat. Peran aktif masyarakat dan respons cepat pemerintah sangat krusial dalam memulihkan kepercayaan dan mencegah insiden serupa di masa depan.

Kata kunci: Keamanan Siber, Kebocoran Data, Pusat Data Nasional, Indonesia, Kebijakan Publik.

1. LATAR BELAKANG

Transformasi digital yang berlangsung pesat di Indonesia selama satu dekade terakhir telah mendorong pemerintah untuk melakukan sentralisasi data melalui pembentukan Pusat Data Nasional (PDN). Langkah ini diambil sebagai bagian dari upaya modernisasi tata kelola pemerintahan dan pelayanan publik berbasis teknologi informasi. PDN diharapkan menjadi tulang punggung infrastruktur digital nasional, menyatukan data dari berbagai instansi untuk meningkatkan efisiensi, integrasi, dan keamanan sistem pemerintahan6. Namun, pada 20 Juni 2024, PDN mengalami insiden besar berupa serangan siber yang menyebabkan data nasional terkunci oleh pelaku dan menuntut tebusan (ransomware). Serangan ini berdampak pada ratusan instansi pemerintah, memicu kekhawatiran publik terkait keamanan data pribadi, dan menyoroti efektivitas kebijakan keamanan siber nasional yang selama ini dijalankan.

Received: April 25, 2025; Revised: Mei 06, 2025; Accepted: Mei 20, 2025; Published: Mei 23, 2025

Insiden kebocoran data nasional tahun 2024 tidak hanya menjadi peristiwa teknis, tetapi juga fenomena sosial dan politik yang mengguncang kepercayaan masyarakat terhadap pemerintah. Dampaknya terasa luas, mulai dari gangguan layanan publik, potensi penyalahgunaan data pribadi, hingga meningkatnya kecemasan masyarakat akan keamanan digital di era keterbukaan informasi. Studi oleh Syahril et al. (2024) menunjukkan bahwa insiden kebocoran data besar seperti ini dapat menurunkan tingkat kepercayaan publik, bahkan memengaruhi kepatuhan warga negara terhadap kewajiban negara, seperti kepatuhan pajak, akibat persepsi bahwa pemerintah gagal melindungi data sensitif mereka. Kepercayaan publik yang menurun ini dapat berdampak domino terhadap efektivitas kebijakan publik dan stabilitas sosial.

Salah satu penyebab utama kebocoran data nasional adalah lemahnya implementasi kebijakan keamanan siber, baik dari aspek teknis maupun regulasi. Studi Tanjung & Febrianisa (2024) menyoroti bahwa penggunaan kata sandi yang lemah dan tidak adanya standar minimum keamanan yang ketat di banyak instansi pemerintah menjadi pintu masuk utama bagi peretas. Regulasi yang ada, seperti UU ITE dan beberapa peraturan turunan, dinilai belum cukup spesifik dan tegas dalam mengatur praktik keamanan teknis, seperti penggunaan autentikasi dua faktor, enkripsi, serta audit keamanan berkala. Selain itu, penegakan hukum yang lemah dan kurangnya sumber daya untuk pengawasan memperparah kerentanan sistem data nasional.

Evaluasi terhadap kebijakan dan regulasi keamanan siber di Indonesia mengungkapkan adanya gap antara regulasi, implementasi, dan perkembangan ancaman siber. Penelitian Bahtiar (2022) dan Sarjito (2024) mengidentifikasi bahwa regulasi sistem perlindungan data pribadi di Indonesia masih lemah dan belum komprehensif, ditandai dengan lambatnya pengesahan UU Perlindungan Data Pribadi (PDP) dan belum adanya standar yang jelas untuk perlindungan data di sektor publik maupun swasta. Sementara itu, ancaman siber terus berkembang dengan teknik yang semakin canggih, menuntut respons kebijakan yang adaptif dan kolaboratif lintas sektor.

Tantangan lain yang dihadapi adalah rendahnya kesadaran dan literasi keamanan siber di kalangan aparatur negara maupun masyarakat umum. Studi Nugroho et al. (2023) menegaskan bahwa praktik penggunaan kata sandi yang kuat dan kompleks masih jauh dari memadai di banyak organisasi pemerintah, membuat sistem rentan terhadap serangan brute force dan credential stuffing. Selain itu, pelatihan keamanan siber yang berkelanjutan dan audit sistem secara rutin belum menjadi budaya di birokrasi Indonesia, sehingga celah keamanan sering kali tidak terdeteksi hingga terjadi insiden besar.

Dampak kebocoran data nasional tidak hanya bersifat teknis, tetapi juga psikologis dan sosial. Dari perspektif akuntansi keperilakuan, Syahril et al. (2024) menunjukkan bahwa persepsi keamanan data yang rendah dapat menurunkan tingkat kepatuhan warga negara terhadap sistem, seperti kepatuhan pajak, karena hilangnya rasa percaya terhadap otoritas negara. Teori kepercayaan organisasi dan keadilan prosedural menegaskan bahwa kepercayaan publik sangat dipengaruhi oleh kemampuan pemerintah dalam menjaga keamanan data dan transparansi dalam menangani insiden. Jika pemerintah gagal menunjukkan respons yang cepat, transparan, dan efektif, maka krisis kepercayaan dapat semakin dalam dan berdampak pada stabilitas sosial.

Studi kasus kebocoran data nasional tahun 2024 juga memperlihatkan pentingnya kerja sama antara pemerintah, sektor swasta, dan masyarakat dalam membangun ekosistem keamanan siber yang tangguh. Mishra et al. (2022) menekankan bahwa kerja sama lintas sektor sangat penting untuk memperkuat pertahanan kolektif terhadap ancaman siber yang semakin rumit dan lintas batas. Kerjasama ini mencakup berbagi informasi ancaman, pengembangan standar keamanan global, dan harmonisasi regulasi antarnegara. Tanpa sinergi yang kuat, upaya perlindungan data nasional akan selalu tertinggal dari perkembangan teknik serangan siber.

Selain aspek regulasi dan teknis, aspek edukasi dan peningkatan kesadaran masyarakat menjadi faktor kunci dalam pencegahan kebocoran data di masa depan. Chaudhary et al. (2022) menegaskan bahwa program kesadaran siber yang dirancang dengan baik dapat mendorong praktik keamanan yang lebih baik di tingkat organisasi dan masyarakat. Edukasi berkelanjutan, pelatihan berbasis skenario, dan evaluasi kinerja keamanan harus menjadi bagian integral dari strategi nasional keamanan siber. Dengan demikian, masyarakat tak hanya menjadi objek perlindungan, tetapi juga menjadi subjek aktif dalam menjaga keamanan data pribadi dan nasional.

Akhirnya, insiden kebocoran data nasional tahun 2024 menjadi momentum penting bagi Indonesia untuk melakukan evaluasi menyeluruh terhadap tata kelola keamanan siber. Perlu ada pembaruan regulasi yang lebih adaptif, penguatan infrastruktur teknis, peningkatan kapasitas sumber daya manusia, serta kerjasama lintas sektor yang lebih erat. Hanya dengan langkah-langkah komprehensif dan berkelanjutan, Indonesia dapat membangun ekosistem digital yang aman, terpercaya, dan mendukung pertumbuhan ekonomi digital yang inklusif dan berkelanjutan.

2. KAJIAN TEORITIS

Kajian teoritis yang digunakan dalam penelitian ini mencangkup teori-teori yang berkaitan dengan keamanan siber, perlindungan data pribadi, dan kepercayaan publik. Teori kepercayaan organisasi Mayer et al. (1995) digunakan guna menjelaskan dampak dari kebocoran data nasional terhadap persepsi publik. Pendekatan freming media Entman (1993) juga di jadikan acuan dalam menganalisis kostruksi realitas oleh media massa. Penelitian terdahulu yeng relevan dengan penelitian ini seperti oleh Tanjung & Febrianisa (2024), dan Mishra et al. (2022) menjadi dasar konseptual dalam merumuskan permasalahan dan solusi kebijakan keamanan siber di Indonesia.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan kombinasi analisis isi (content analysis), analisis framing media, dan studi literatur terhadap regulasi serta kebijakan yang relevan. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam dan komprehensif mengenai fenomena kebocoran data nasional pada Pusat Data Nasional (PDN) tahun 2024, khususnya dari sisi penyebab, dampak, respons, dan solusi kebijakan yang diambil pemerintah, serta persepsi publik yang berkembang di media massa.

Analisis isi digunakan untuk mengkaji konten pemberitaan media daring yang membahas insiden kebocoran data PDN. Data primer berupa artikel berita diambil dari berbagai portal berita nasional, seperti Tempo.co, Kompas.com, CNN Indonesia, dan MetroTV News, yang secara intensif meliput peristiwa ini. Analisis dilakukan terhadap narasi, tema, dan sudut pandang yang diangkat media, serta bagaimana media membingkai peristiwa, aktor, dan solusi yang ditawarkan. Untuk mendalami konstruksi realitas yang dibangun media, penelitian ini mengadopsi konsep framing Robert N. Entman yang menyoroti elemen seleksi isu, penekanan aspek tertentu, dan pengabaian aspek lain dalam pemberitaan. Dengan metode ini, dapat diungkap bagaimana opini publik dibentuk dan bagaimana media berperan dalam membangun persepsi masyarakat terhadap kebijakan keamanan siber pemerintah.

Selain analisis isi dan framing media, penelitian ini juga melakukan studi literatur terhadap regulasi dan kebijakan yang berkaitan dengan keamanan siber dan perlindungan data di Indonesia. Literatur yang dikaji meliputi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP), serta kebijakan teknis dari Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN). Studi literatur ini bertujuan untuk menelaah kesesuaian dan

efektivitas kerangka hukum dalam mencegah dan menangani insiden kebocoran data, serta mengidentifikasi gap antara regulasi dan praktik di lapangan.

Pengumpulan data sekunder juga dilakukan melalui dokumen resmi pemerintah, siaran pers, dan laporan investigasi terkait insiden kebocoran data PDN. Data ini digunakan untuk melengkapi analisis, memastikan validitas informasi, dan memberikan gambaran utuh mengenai kronologi, respons, serta langkah mitigasi yang diambil pemerintah. Selain itu, penelitian ini mengacu pada hasil kajian akademik dan jurnal ilmiah yang membahas dampak kebocoran data terhadap kepercayaan publik, perilaku masyarakat, dan kepatuhan terhadap sistem negara, seperti yang diulas oleh Syahril et al. (2024) dalam konteks behavioral accounting dan persepsi keamanan data.

Analisis dilakukan secara tematik dan komparatif, dengan membandingkan temuan dari berbagai sumber untuk mengidentifikasi pola, perbedaan, dan konsistensi dalam pemberitaan maupun kebijakan. Penelitian ini juga memperhatikan aspek triangulasi data, yakni membandingkan data dari media, dokumen resmi, dan kajian akademik untuk meningkatkan keandalan hasil penelitian. Dalam proses analisis, peneliti secara sistematis mengelompokkan data berdasarkan kategori: penyebab kebocoran, dampak dan ancaman, solusi dan mitigasi, serta peran masyarakat dan pemerintah.

Penelitian ini juga mengadopsi pendekatan konseptual dan studi kasus (case approach) untuk mendalami kasus kebocoran data PDN sebagai studi utama. Pendekatan konseptual digunakan untuk memahami konsep-konsep kunci seperti keamanan siber, perlindungan data pribadi, dan kepercayaan publik, sedangkan studi kasus memungkinkan analisis mendalam terhadap dinamika, aktor, dan kebijakan yang terlibat dalam insiden ini.

Dengan pendekatan kualitatif yang integratif, penelitian ini tak hanya berfokus pada aspek teknis, tetapi juga memperhatikan dimensi sosial, hukum, dan komunikasi publik. Hasil dari metode ini diharapkan dapat memberikan gambaran holistik menyangkut kebijakan keamanan siber di Indonesia, serta saran strategis untuk mencegah terulangnya insiden kebocoran data nasional di masa depan.

4. HASIL DAN PEMBAHASAN

Penyebap Kebocoran Data Nasional

Kebocoran data nasional di Indonesia, khususnya pada kasus Pusat Data Nasional (PDN) tahun 2024, merupakan hasil dari kumpulan berbagai kelemahan sistemik yang telah lama menjadi sorotan para ahli dan praktisi keamanan siber. Penyebab utama insiden ini dapat dijabarkan secara mendalam dalam beberapa aspek, yaitu kelemahan infrastruktur dan sistem,

kurangnya kesiapan sumber daya manusia (SDM) dan prosedur, serta sentralisasi data yang belum diimbangi dengan proteksi optimal. Selain itu, faktor regulasi, budaya organisasi, dan dinamika ancaman siber global juga memperparah kerentanan sistem data nasional Indonesia.

Faktor utama yang menyebabkan kebocoran data nasional adalah lemahnya infrastruktur dan sistem keamanan siber di pemerintah Indonesia. Serangan ransomware yang menimpa PDN pada Juni 2024 terjadi akibat adanya celah keamanan yang belum diantisipasi dengan baik. Banyak sistem pemerintahan masih menggunakan perangkat lunak yang telah ketinggalan zaman (outdated), konfigurasi keamanan yang lemah, serta tidak adanya pemantauan dan audit sistem secara berkala. Studi Tanjung & Febrianisa (2024) menegaskan bahwa penggunaan kata sandi yang lemah seperti "Admin#1234", sangat rentan terhadap serangan brute force dan credential stuffing. Hal ini menunjukkan bahwa meskipun teknologi keamanan sudah tersedia, implementasinya di lapangan masih jauh dari memadai. kurangnya standar minimum keamanan yang tegas dan tidak adanya mekanisme enkripsi data yang kuat memperbesar risiko eksploitasi oleh pihak tidak bertanggung jawab. Nugroho et al. (2023) melalui evaluasi perangkat lunak password cracker, membuktikan bahwa sandi pendek dan sederhana sangat mudah dibobol, sehingga memperkuat argumen pentingnya penggunaan sandi yang kompleks dan sistem autentikasi berlapis. Ketiadaan firewall yang efektif, segmentasi jaringan, serta sistem deteksi dan respons insiden (IDS/IRS) juga menjadi celah yang sering dimanfaatkan oleh peretas.

Selain faktor teknis, aspek manusia dan prosedur operasional juga menjadi penyebab utama kebocoran data nasional. Prosedur keamanan siber di banyak instansi pemerintah masih belum siap dan matang. Banyak operator dan administrator sistem yang belum mendapatkan pelatihan keamanan siber secara berkala, sehingga respons terhadap serangan menjadi lamban dan tidak terkoordinasi. Tanjung & Febrianisa (2024) menyoroti bahwa lemahnya edukasi dan kesadaran keamanan siber di tingkat organisasi menyebabkan praktik-praktik dasar, seperti penggantian kata sandi secara rutin dan penggunaan autentikasi dua faktor, sering diabaikan. Ketiadaan simulasi serangan (penetration test) dan audit keamanan berkala juga membuat banyak celah keamanan tidak terdeteksi hingga akhirnya dieksploitasi oleh peretas. Selain itu, kurangnya budaya pelaporan insiden dan koordinasi antar lembaga memperlambat proses mitigasi dan pemulihan pasca insiden. Mishra et al. (2022) menekankan pentingnya kolaborasi lintas sektor dan pelatihan berkelanjutan untuk memperkuat ketahanan siber nasional.

Transformasi digital yang mendorong sentralisasi data melalui PDN memang bertujuan untuk meningkatkan efisiensi dan integrasi layanan publik. Namun, sentralisasi ini justru menjadi pedang bermata dua ketika tidak diimbangi dengan penguatan proteksi dan backup

data yang memadai. Sentralisasi data tanpa segmentasi dan proteksi berlapis memperbesar risiko kebocoran berskala masif jika terjadi satu titik kegagalan (single point of failure). Ketika PDN diserang ransomware, ratusan instansi pemerintah langsung terdampak karena tidak memiliki backup data yang terdistribusi dan sistem failover yang andal. Penelitian Bahtiar (2022) dan Sarjito (2024) mengidentifikasi bahwa regulasi perlindungan data pribadi di Indonesia masih lemah dan belum komprehensif. Belum adanya standar yang jelas untuk perlindungan data di sektor publik maupun swasta membuat sentralisasi data menjadi sangat berisiko. Selain itu, backup data yang seharusnya menjadi prosedur standar diabaikan oleh banyak instansi, sehingga proses pemulihan pasca serangan menjadi sangat lambat dan tidak efisien.

Kebocoran data nasional juga dipengaruhi oleh lemahnya regulasi dan penegakan hukum di bidang keamanan siber. UU ITE dan regulasi turunannya dinilai belum cukup spesifik dalam mengatur standar teknis keamanan data, seperti penggunaan enkripsi, audit keamanan, dan kewajiban pelaporan insiden. Studi Sarjito (2024) menegaskan bahwa regulasi yang tidak adaptif terhadap perkembangan teknologi dan ancaman siber membuat perlindungan data di Indonesia tertinggal dari negara-negara lain yang telah menerapkan standar global seperti GDPR. Penegakan hukum yang lemah dan kurangnya sanksi tegas terhadap pelanggaran keamanan data membuat banyak organisasi tidak serius dalam menerapkan kebijakan keamanan siber. Ketidakjelasan otoritas penegak hukum dan tumpang tindih kewenangan antar lembaga juga memperlambat proses investigasi dan penanganan insiden kebocoran data.

Budaya organisasi yang belum menempatkan keamanan siber sebagai prioritas utama juga menjadi penyebab mendasar kebocoran data nasional. Banyak pimpinan instansi yang masih menganggap keamanan siber sebagai biaya tambahan dan bukan investasi strategis. Akibatnya, alokasi anggaran untuk pembaruan sistem, pelatihan SDM, dan audit keamanan sering kali minim. Chaudhary et al. (2022) menegaskan bahwa program kesadaran siber yang dirancang dengan baik dapat mendorong praktik keamanan yang lebih baik di tingkat organisasi, namun hal ini belum menjadi budaya di banyak lembaga pemerintah Indonesia.

Perkembangan ancaman siber yang semakin rumit dan lintas batas juga menjadi tantangan besar bagi keamanan data nasional. Serangan ransomware, phishing, dan advanced persistent threat (APT) kini dilakukan oleh kelompok peretas internasional dengan sumber daya dan teknologi canggih. Mishra et al. (2022) menyoroti pentingnya kolaborasi internasional dan pertukaran informasi ancaman untuk memperkuat pertahanan kolektif. Tanpa

adaptasi strategi dan teknologi terbaru sistem data nasional Indonesia akan selalu menjadi target empuk bagi peretas global.

Kurangnya kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam membangun ekosistem keamanan siber yang tangguh juga memperbesar risiko kebocoran data nasional. Mishra et al. (2022) menekankan bahwa kerja sama lintas sektor sangat penting untuk memperkuat pertahanan kolektif terhadap ancaman siber yang semakin kompleks dan lintas batas. Tanpa adanya standar nasional yang jelas dan kolaborasi yang erat. upaya perlindungan data nasional akan selalu tertinggal dari perkembangan teknik serangan siber.

Ancaman Akibat Kebocoran Data Nasional

Kebocoran data nasional, seperti insiden yang terjadi pada Pusat Data Nasional (PDN) tahun 2024, menimbulkan berbagai ancaman serius yang berdampak luas pada aspek ekonomi, sosial, hingga psikologis masyarakat. Ancaman-ancaman ini tidak hanya bersifat langsung seperti kerugian finansial, tetapi juga berdampak jangka panjang terhadap kepercayaan publik dan stabilitas sistem digital nasional. Kebocoran data nasional membuka peluang besar bagi pelaku kejahatan siber untuk melakukan berbagai tindak kriminal seperti pemerasan, penipuan, hingga penyalahgunaan identitas. Data yang bocor sering kali berisi informasi sensitif seperti nomor induk kependudukan, data keuangan, hingga rekam jejak digital individu. Penelitian Tanjung & Febrianisa (2024) menegaskan bahwa lemahnya perlindungan data dan penggunaan kata sandi yang lemah membuat sistem sangat rentan terhadap serangan brute force dan credential stuffing yang dapat berujung pada pencurian data secara massal. Dampak ekonomi dari kebocoran data sangat signifikan. Perusahaan dan lembaga pemerintah yang menjadi korban harus mengeluarkan biaya besar untuk pemulihan sistem, investigasi, serta kompensasi kepada individu yang terdampak. Selain itu, masyarakat yang datanya bocor berisiko menjadi korban penipuan daring (phishing), pemerasan, hingga pencurian identitas yang dapat merugikan secara finansial dan psikologis. Studi Syahril et al. (2024) bahkan menemukan bahwa kebocoran data dapat memengaruhi perilaku ekonomi masyarakat, termasuk menurunnya kepatuhan terhadap sistem perpajakan akibat hilangnya rasa aman dan percaya pada pemerintah.

Salah satu dampak paling nyata dari kebocoran data nasional adalah penurunan tingkat kepercayaan masyarakat terhadap pemerintah dan penyelenggara layanan digital. Kepercayaan publik merupakan modal sosial yang sangat penting dalam pembangunan sektor digital. Ketika masyarakat merasa bahwa data pribadinya tidak aman mereka akan enggan menggunakan layanan digital pemerintah, bahkan bisa beralih ke jalur informal atau menghindari penggunaan

layanan sama sekali. Syahril et al. (2024) menyoroti bahwa krisis kepercayaan ini dapat berdampak domino pada berbagai sektor termasuk menurunnya kepatuhan pajak, keengganan masyarakat untuk berbagi data, hingga resistensi terhadap program digitalisasi pemerintah. Teori kepercayaan organisasi (Mayer, Davis, & Schoorman, 1995) menjelaskan bahwa kepercayaan dibangun atas dasar kemampuan, integritas, dan kebajikan. Ketika pemerintah gagal melindungi data maka ketiga pilar kepercayaan ini runtuh, memperparah krisis legitimasi dan efektivitas kebijakan publik.

Data yang bocor akibat insiden kebocoran nasional sangat mungkin diperjualbelikan di forum gelap (dark web) dan digunakan untuk berbagai kejahatan siber lain. Data pribadi yang bocor dapat dimanfaatkan untuk serangan spear phishing, rekayasa sosial (social engineering), hingga pembobolan akun keuangan dan media sosial. Tanjung & Febrianisa (2024) menekankan bahwa tanpa regulasi yang ketat dan implementasi teknologi keamanan yang kuat, data sensitif akan selalu menjadi komoditas berharga di pasar gelap. Risiko penyalahgunaan data tidak hanya berdampak pada individu tetapi juga dapat mengancam keamanan nasional. Data yang bocor dapat digunakan untuk memetakan jaringan sosial, melakukan pemerasan terhadap pejabat publik, atau bahkan sebagai alat spionase oleh aktor negara asing. Studi Sarjito (2024) menyoroti bahwa serangan siber terhadap data pemerintah, seperti kasus SolarWinds di Amerika Serikat, tidak hanya mengganggu operasional pemerintahan, tetapi juga merusak kepercayaan publik dan menimbulkan risiko strategis bagi keamanan negara.

Kebocoran data sering kali disertai dengan gangguan operasional pada layanan publik terutama jika insiden tersebut melibatkan serangan ransomware yang mengunci sistem penting. Pada kasus PDN 2024 ratusan instansi pemerintah tidak dapat mengakses data dan layanan digital selama beberapa hari, sehingga menghambat pelayanan kepada masyarakat. Gangguan ini tidak hanya menimbulkan kerugian ekonomi, tetapi juga menurunkan kualitas pelayanan publik dan menambah beban psikologis bagi masyarakat yang membutuhkan layanan penting. Kebocoran data juga berdampak pada aspek psikologis masyarakat seperti meningkatnya kecemasan, ketidakpastian, dan rasa tidak aman dalam menggunakan layanan digital. Studi Syahril et al. (2024) menunjukkan bahwa persepsi negatif terhadap keamanan data dapat memengaruhi perilaku masyarakat, termasuk menurunnya partisipasi dalam program-program pemerintah dan ekonomi digital. Efek psikologis ini, jika tidak segera ditangani, dapat menimbulkan resistensi sosial yang menghambat transformasi digital nasional.

Lembaga yang mengalami kebocoran data akan menghadapi tekanan hukum dan reputasi yang berat. Tanjung & Febrianisa (2024) menyebutkan bahwa lemahnya regulasi dan penegakan hukum di Indonesia membuat banyak organisasi belum siap menghadapi tuntutan

hukum dan kompensasi akibat kebocoran data. Reputasi lembaga yang tercoreng dapat berdampak jangka panjang terhadap kepercayaan pelanggan dan mitra kerja, serta menurunkan nilai ekonomi organisasi di mata investor.

Sektor ekonomi digital sangat bergantung pada kepercayaan dan keamanan data. Kebocoran data berskala nasional dapat menghambat pertumbuhan ekonomi digital, menurunkan minat investasi, dan memperlambat adopsi teknologi baru. Bahtiar (2022) menegaskan bahwa tanpa perlindungan data yang kuat, ekonomi digital Indonesia akan sulit bersaing di tingkat global dan rentan terhadap risiko sistemik akibat serangan siber.

Peran Masyarakat dan Pemerintah Dalam Menangani Kebocoran Data Nasional

a. Peran Masyarakat

Insiden kebocoran data nasional seperti yang terjadi pada Pusat Data Nasional (PDN) tahun 2024 memicu respons kritis dari masyarakat. Publik secara aktif menuntut transparansi dan akuntabilitas pemerintah dalam menangani insiden tersebut. Hal ini tercermin dari berbagai diskusi di media sosial, forum publik, hingga aksi protes yang menuntut penjelasan terbuka dari pemerintah dan pihak terkait. Penelitian Tanzil et al. (2024) menunjukkan bahwa pemberitaan media massa, terutama yang dibingkai secara kritis, turut memperkuat suara masyarakat dalam menuntut pertanggungjawaban dan perbaikan sistem keamanan siber nasional. Masyarakat tidak lagi pasif melainkan menjadi aktor penting yang menekan pemerintah agar bertindak cepat, tepat, dan transparan.

Kebocoran data berskala nasional telah meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi. Banyak individu dan komunitas mulai aktif mengikuti pelatihan literasi digital, seminar keamanan siber, serta kampanye perlindungan data pribadi. Masyarakat juga semakin selektif dalam membagikan data pribadi di internet dan lebih waspada terhadap potensi penipuan daring yang memanfaatkan data bocor. Studi Syahril et al. (2024) menegaskan bahwa peningkatan literasi digital masyarakat berkontribusi pada advokasi keamanan siber dan mendorong partisipasi aktif dalam mengawasi implementasi kebijakan perlindungan data.

Masyarakat kini berperan sebagai pengawas kebijakan publik. Mereka tidak hanya menuntut perbaikan tetapi juga aktif memantau tindak lanjut pemerintah melalui media massa, laporan resmi, dan kanal aduan publik. Selain pengawasan pada kebijakan publik masyarakat juga harus melakukan pengawasan pada data yang telah diambil oleh pemerintah. Masyarakat dapat menuntut traspalansi dan akuntabilitas untuk hak privasi dan keamanan siber, agar dapat meminimalisir penyalagunaan data masyarakat. Tekanan yang

diberikan masyarakat telah mendorong pemerintah untuk lebih terbuka dalam menginformasikan langkah-langkah mitigasi dan pemulihan pasca insiden. Media massa sebagai corong suara publik juga memainkan peran penting dalam merumuskan isu kebocoran data sehingga menjadi perhatian nasional (Tanzil et al., 2024). Dengan demikian, masyarakat berperan sebagai penggerak perubahan dan memastikan pemerintah tidak abai terhadap keamanan data warganya.

b. Peran Pemerintah

Pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo) serta Badan Siber dan Sandi Negara (BSSN) segera melakukan investigasi, klarifikasi, dan pemulihan layanan setelah insiden kebocoran data terjadi. Langkah-langkah ini meliputi identifikasi sumber serangan, penutupan celah keamanan, serta pemulihan akses layanan publik yang terdampak. Pemerintah juga menyampaikan klarifikasi kepada masyarakat melalui siaran pers resmi dan konferensi pers, meskipun respons awal sering kali dinilai kurang transparan dan lambat oleh publik (Tanzil et al., 2024). Insiden kebocoran data nasional telah menjadi momentum bagi pemerintah untuk melakukan evaluasi menyeluruh terhadap kebijakan keamanan siber. Pemerintah mempercepat proses pengesahan dan implementasi regulasi perlindungan data pribadi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). pemerintah juga melakukan reformasi kebijakan internal di berbagai instansi, memperketat standar keamanan teknis, serta memperkuat koordinasi lintas lembaga dalam penanganan insiden siber (Syahril et al., 2024).

Transparansi menjadi tuntutan utama masyarakat pasca insiden kebocoran data. Pemerintah didorong untuk lebih terbuka dalam menyampaikan informasi terkait kronologi insiden, dampak yang ditimbulkan, serta langkah mitigasi yang diambil. Studi Coombs (2007) menekankan pentingnya komunikasi krisis yang efektif untuk memulihkan kepercayaan publik dan reputasi organisasi. Dalam hal ini, pemerintah perlu mengadopsi strategi komunikasi yang proaktif, jujur, dan berbasis data agar masyarakat merasa dilibatkan dan mendapatkan informasi yang akurat.

Pemerintah harus menjelaskan dengan jelas tentang tujuan data yang diambil dari masyarakat. Seringkali pemerintah mengambil data masyarakat tenpa menjelaskan data tersebut untuk apa dan digunakan sebagai apa. Hal ini lah yang harus di perhatikan pemerintah agar tidak melanggar etika siber yang ada. Salsabil (2021) menjalaskan etika siber sebagai aturan yang tidak tertulis yang menjadi norma bagi semua pengguna siber di seluruh dunia. Selain aspek regulasi dan komunikasi pemerintah juga memperkuat infrastruktur keamanan siber dan meningkatkan kapasitas sumber daya manusia (SDM) di

bidang teknologi informasi. Pelatihan keamanan siber bagi pegawai pemerintah, audit sistem secara berkala, serta pembaruan perangkat lunak menjadi bagian dari upaya preventif untuk mencegah insiden serupa di masa depan. Pemerintah juga menggandeng sektor swasta dan akademisi dalam pengembangan teknologi deteksi dini dan sistem pertahanan siber nasional.

Solusi Untuk Pencegahan Kebocoran Data Nasional

Kebocoran data nasional yang terjadi di Indonesia khususnya pada insiden Pusat Data Nasional (PDN) tahun 2024 telah menjadi peringatan keras akan pentingnya penguatan sistem keamanan siber nasional. Untuk mencegah terulangnya insiden kebocoran data di masa depan, diperlukan solusi yang komprehensif, sistematis, dan berkelanjutan. Langkah pertama yang sangat penting adalah memperkuat kerangka regulasi perlindungan data pribadi di Indonesia. Pemerintah perlu mempercepat implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) yang telah lama dinanti serta memastikan bahwa sanksi terhadap pelanggaran keamanan data benar-benar ditegakkan. Studi Syahril et al. (2024) menegaskan bahwa kejelasan regulasi dan penegakan hukum yang tegas dapat meningkatkan kepercayaan publik dan memberikan efek jera bagi pelaku pelanggaran. Harus regulasi yang mengatur secara spesifik standar teknis minimum yang wajib diterapkan oleh seluruh institusi pengelola data baik disektor publik maupun swasta. Standar tersebut meliputi penggunaan enkripsi, autentikasi multi-faktor, audit keamanan berkala, serta kewajiban pelaporan insiden secara transparan dan tepat waktu. Penegakan hukum yang konsisten juga harus didukung oleh koordinasi antar lembaga penegak hukum, seperti Kominfo, BSSN, dan Kepolisian, agar tidak terjadi tumpang tindih kewenangan yang dapat memperlambat penanganan insiden.

Modernisasi infrastruktur teknologi informasi menjadi kebutuhan yang mendesak dalam menghadapi ancaman siber yang semakin canggih. Pemerintah dan seluruh institusi pengelola data harus melakukan audit keamanan secara rutin untuk mengidentifikasi dan menutup celah-celah keamanan yang ada. Implementasi sistem backup data yang terdistribusi dan terenskripsi juga menjadi langkah wajib, agar data tetap aman dan dapat dipulihkan dengan cepat jika terjadi serangan ransomware atau insiden serupa (Tanzil et al., 2024). Protokol keamanan harus diperbarui secara berkala sesuai dengan perkembangan ancaman siber global. Penggunaan perangkat lunak yang sudah ketinggalan zaman (outdated) harus dihentikan dan seluruh sistem harus menggunakan patch keamanan terbaru. penerapan Zero Trust Architecture, segmentasi jaringan, dan sistem deteksi serta respons insiden (IDS/IRS) dapat memperkuat pertahanan berlapis dan meminimalkan risiko akses tidak sah ke data sensitif.

Solusi lainnya adalah peningkatan edukasi dan kesadaran keamanan siber di seluruh lapisan masyarakat khususnya bagi pegawai pemerintah dan operator sistem informasi. Studi Chaudhary et al. (2022) menunjukkan bahwa program edukasi siber yang berkelanjutan dapat secara signifikan mengurangi risiko human error yang sering menjadi penyebab utama kebocoran data. Pemerintah perlu mengadakan pelatihan rutin tentang praktik keamanan siber seperti penggunaan kata sandi yang kuat, pengenalan phishing, serta prosedur pelaporan insiden. Selain itu, kampanye literasi digital kepada masyarakat umum harus digalakkan secara masif agar masyarakat memahami pentingnya perlindungan data pribadi dan tidak mudah menjadi korban kejahatan siber.

Penguatan pertahanan siber nasional tidak dapat dilakukan oleh pemerintah saja melainkan membutuhkan kolaborasi multi-pihak yang melibatkan sektor swasta, akademisi, dan masyarakat sipil. Mishra et al. (2022) menekankan pentingnya kerja sama lintas sektor dalam berbagi informasi ancaman, pengembangan standar keamanan bersama, serta harmonisasi regulasi. Kolaborasi ini dapat diwujudkan melalui pembentukan forum keamanan siber nasional yang melibatkan semua pemangku kepentingan termasuk BSSN, Kominfo, operator telekomunikasi, perusahaan teknologi, serta komunitas keamanan siber. Forum ini berfungsi sebagai wadah koordinasi, pertukaran informasi, serta pengembangan kapasitas bersama dalam menghadapi ancaman siber yang terus berkembang.

Selain aspek teknis dan regulasi transparansi dan akuntabilitas dalam penanganan insiden kebocoran data juga sangat penting untuk memulihkan kepercayaan publik. Pemerintah harus secara terbuka menginformasikan kronologi, dampak, dan langkah-langkah mitigasi yang telah diambil pasca insiden. Studi Coombs (2007) menekankan bahwa komunikasi krisis yang efektif dapat membantu memulihkan reputasi organisasi dan mengurangi dampak negatif terhadap persepsi publik. Pemerintah juga perlu menyediakan saluran pelaporan insiden yang mudah diakses oleh masyarakat dan memberikan perlindungan bagi pelapor (whistleblower) agar insiden dapat segera terdeteksi dan ditangani sebelum menimbulkan kerugian yang lebih besar.

Setiap institusi yang mengelola data nasional harus diwajibkan untuk memiliki sertifikasi keamanan siber seperti ISO 27001 atau standar internasional lainnya. Sertifikasi ini memastikan bahwa institusi telah menerapkan sistem manajemen keamanan informasi yang sesuai standar global. Audit eksternal secara berkala juga harus dilakukan untuk memastikan kepatuhan terhadap standar dan mengidentifikasi area yang perlu diperbaiki. Pemerintah juga perlu mendorong inovasi dan riset di bidang keamanan siber baik melalui pendanaan penelitian, inkubasi startup keamanan siber, maupun kerja sama dengan perguruan tinggi. Pengembangan

teknologi deteksi dini, kecerdasan buatan untuk analisis ancaman, serta sistem enkripsi generasi baru sangat diperlukan untuk menghadapi serangan yang semakin canggih dan terorganisir.

Kebijakan keamanan siber harus dievaluasi dan diperbarui secara berkala sesuai dengan dinamika ancaman dan perkembangan teknologi. Pemerintah perlu membentuk tim evaluasi independen yang bertugas menilai efektivitas kebijakan, mengidentifikasi kelemahan, serta memberikan rekomendasi perbaikan secara berkelanjutan.

5. KESIMPULAN DAN SARAN

Kebocoran data nasional pada PDN tahun 2024 menjadi peringatan keras bagi Indonesia untuk segera memperbaiki tata kelola keamanan siber. Penyebab utama insiden adalah kelemahan sistem, kurangnya kesiapan SDM, dan lemahnya regulasi. Dampak yang ditimbulkan sangat luas, mulai dari kerugian ekonomi hingga penurunan kepercayaan publik. Solusi yang diusulkan meliputi penguatan regulasi, modernisasi infrastruktur, edukasi, dan kolaborasi lintas sektor. Peran aktif masyarakat dan pemerintah sangat penting untuk mencegah kebocoran data serupa di masa depan dan membangun ekosistem digital yang aman dan terpercaya.

DAFTAR REFERENSI

Aln, J., Cherry, T., Jones, M., & McKee, M. (2010). Taxpayer information assistance services and tax compliance behavior. *Journal of Economic Psychology*, 31(4), 577–586. https://doi.org/10.1016/j.joep.2010.03.001

Bahtiar, R. (2022). Analisis regulasi perlindungan data pribadi di Indonesia. *Jurnal Hukum dan Teknologi*, 2(1), 45–60.

Chaudhary, S., et al. (2022). Cybersecurity awareness programs: Best practices and impact. *Journal of Information Security*, 11(3), 200–215.

CNN Indonesia. (2024, Juli 2). Data diklaim dari PDN 2021-2024 dijual Rp198 M di forum gelap. https://www.cnnindonesia.com/teknologi/20240702104538-192-1116574/data-diklaim-dari-pdn-2021-2024-dijual-rp198-m-di-forum-gelap

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Febrianisa, F., & Tanjung, M. F. (2024). Peran regulasi komunikasi dalam mengatasi pencurian data nasional pada 2024. *Jurnal Mahasiswa Komunikasi Cantrik*, 4(2), 93–102. https://doi.org/10.20885/cantrik.vol4.iss2.art2

JDIH DPR RI. (2024, Juli 4). Kebocoran data kembali terjadi, Sukamta: Ini alarm keras buat pemerintah! https://jdih.dpr.go.id/berita/detail/id/51640/t/Kebocoran+Data+Kembali+Terjadi%2C+Sukamta%3A+Ini+Alarm+Keras+Buat+Pemerintah%21

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024, Maret 20). Siaran pers No. 207/HM/KOMINFO/03/2024 tentang tangani kebocoran data pelanggan Dirjen Aptika: Kita sudah minta klarifikasi. https://www.komdigi.go.id/berita/pengumuman/detail/siaran-pers-no-207-hm-kominfo-03-2024-tentang-tangani-kebocoran-data-pelanggan-dirjen-aptika-kita-sudah-minta-klarifikasi

Kompas.com. (2024, Juli 4). Ramai soal data Kemenkominfo diduga bocor dan dijual Rp 1,9 miliar, benarkah? https://www.kompas.com/tren/read/2024/07/04/083000265/ramai-soal-data-kemenkominfo-diduga-bocor-dan-dijual-rp-1-9-miliar-benarkah

MetroTV News. (2024, Juli 2). Kebocoran data kembali terjadi, kerja Kominfo dan BSSN dipertanyakan. https://www.metrotvnews.com/read/bzGCzVPy-kebocoran-data-kembali-terjadi-kerja-kominfo-dan-bssn-dipertanyakan

Mishra, D., et al. (2022). Cybersecurity collaboration: A global perspective. *International Journal of Cyber Security*, 8(2), 101–119.

Nugroho, D. W., et al. (2023). Evaluasi kinerja password cracker pada berkas ZIP. *Jurnal Teknologi Informasi*, 5(1), 20–30.

Salsabil, L. S. (2021). Perkembangan Etika Siber dan Pengaturan Cyberlaw di Indonesia. *Dialektika Komunika: Jurnal Kajian Komunikasi dan Pembangunan Daerah*, *9*(1), 1-5. https://doi.org/10.33592/dk.v9i1.1211

Sarjito, A. (2024). Evaluasi regulasi perlindungan data dan kepercayaan publik di era digital. *Jurnal Ilmu Pemerintahan*, 10(1), 15–29.

Syahril, M. A. F., Hasan, H., & Hasan, N. (2024). Dampak kebocoran data Bjorka pada kepatuhan wajib pajak: Perspektif akuntansi keperilakuan. *Jurnal Akuntansi dan Keperilakuan*, (Special Issue), 109–112. https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/30073662/07c219f8-63b1-4b7c-95fb-a43521c2564b/596-Article-Text-2383-2-10-20250228.pdf

Tanzil Wahyu Ramadhan, I. D. F., & Permadi, D. (2024). Analisis framing pemberitaan peretasan Pusat Data Nasional (PDN) di media online Tempo.co. *Journal of Education Research*, 5(3), 3368–3379. https://doi.org/10.37985/jer.v5i3.1491