Socius: Jurnal Penelitian Ilmu-Ilmu Sosial
Volume 3, Issue 11, June 2026, P 620-629
E-ISSN: 3025-6704
DOI: https://doi.org/10.5281/zenodo.20832641

Peran Sistem Keamanan Terhadap Data Pribadi di Platform Digital Dengan Perspektif Diplomasi Siber Dalam Hubungan Internasional

Fathi Ahmad Safaraz
Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO
Article history:
Received 15 June 2026
Revised 20 June 2026
Accepted 24 June 2026
Available online 23 June 2026

Keywords:
Security Systems, Personal Data, Cyber Diplomacy, Data Protection, Digital Sovereignty

Keywords :
Keamanan Sistem, Data Pribadi, Diplomasi Siber, Perlindungan Data, Kedaulatan Digital

ABSTRACT
Abstract: The purpose of this study is to examine how security systems are responsible for protecting personal data on digital platforms, as well as how the role of security systems is positioned within Indonesia's cyber diplomacy in the international diplomatic arena. This research is motivated by the numerous cases of personal data breaches in Indonesia, including 124 data protection violations from 2019 to 2024, along with 279 million BPJS Health data records, 17 million PLN customer data records, and the fact that the Personal Data Protection Bill and Cyber Security and Resilience Bill have not yet been enacted. Using a qualitative methodology with a case study design, this research incorporates policy document analysis, data breach reports, international regulations such as GDPR, and comparative studies of data protection policies in the European Union, the United States, and Singapore. The findings reveal that Indonesia's digital platform security systems still face significant challenges, as evidenced by the low implementation of technical mechanisms such as encryption and two-factor authentication, regulatory gaps that create a legal vacuum, and a shortage of cybersecurity human resources amounting to 50,000 professionals. In terms of cyber diplomacy, Indonesia lacks a comprehensive diplomatic strategy and tends to be reactive in multilateral forums such as ASEAN and the UN, in contrast to countries like Germany and Singapore that actively promote their data governance models. Furthermore, through the lens of digital dependency theory, this study finds that the failure of national data protection has diminished Indonesia's credibility and bargaining power in the international arena while also reinforcing global cyber governance inequalities.

ABSTRAK
Abstrak: Tujuan dari penelitian ini adalah untuk melihat bagaimana sistem keamanan bertanggung jawab untuk melindungi data pribadi di platform digital. Selain itu, bagaimana peran sistem keamanan diposisikan dalam diplomasi siber Indonesia di kancah diplomasi internasional. Di Indonesia, banyak kasus kebocoran data pribadi. Ini termasuk 124 pelanggaran perlindungan data sejak 2019–2024, serta 279 juta data BPJS Kesehatan, 17 juta data pelanggan PLN, dan 124 kasus pelanggaran perlindungan data. Ini juga merupakan alasan penelitian ini. Dengan desain studi kasus, penelitian ini menggunakan metodologi kualitatif. Analisis dokumen kebijakan, laporan kebocoran data, peraturan internasional seperti GDPR, dan studi perbandingan kebijakan perlindungan data di AS, AS, dan UE dimasukkan ke dalam pendekatan ini. Hasil penelitian menunjukkan bahwa sistem keamanan platform digital Indonesia masih menghadapi banyak masalah. Hal ini ditunjukkan oleh implementasi mekanisme teknis seperti enkripsi dan autentikasi dua faktor yang rendah, kekurangan peraturan yang menciptakan vacuum hukum, dan kekurangan sumber daya manusia keamanan siber yang mencakup 50.000 profesional. Dalam hal diplomasi siber, Indonesia tidak memiliki strategi diplomatik yang komprehensif dan cenderung bersikap reaktif dalam forum multilateral seperti ASEAN dan PBB. Di sisi lain, negara-negara seperti Jerman dan Singapura secara aktif mendukung model tata kelola data mereka. Selain itu, penelitian ini menemukan melalui teori dependensi digital bahwa kegagalan perlindungan data nasional telah menurunkan kredibilitas dan daya tawar Indonesia di mata internasional serta memperkuat ketimpangan tata kelola siber global.

PENDAHULUAN

perlindungan data adalah sebagai langkah hukum yang mempunyai tujuan agar membuat sebuah data seseorang untuk dilindungi. Di era sekarang, perlindungan data dari sebuah kecurangan merupakan hal yang cukup vital, makanya dibutuhkan sebuah hukum untuk

*Corresponding Author
Email: author@fathiahmadsafaraz19gmail.com

melindungi data dari beberapa perusahaan dan juga dalam pemerintahan, dikarenakan bidang ini mempunyai kekuatan yang cukup berpengaruh agar mengurangi adanya kecurangan oleh pihak yang tidak bertanggung jawab. Jika hukum tersebut tidak berlaku, maka banyak pihak akan mudah dalam upanya melakukan eksploitasi data. Privasi data pribadi yang lebih menonjol telah menggunakan sebuah aspek keamanan yang telah dibagikan oleh negara untuk masyarakat, hal ini tentu tidak membuat sebuah konteks kompetensi dari warga negara dalam hal melindungi data pribadi di ruang keamanan siber. Perkembangan aspek kompetensi dari individu merupakan capaian yang nyata dari aspek kapasitas yang telah dibahas oleh Amartya Sen. Pendekatan yang berdasar negara dalam hal politik ekonomi dan juga dalam aspek privasi data yang lebih dibutuh dalam hal pengakuan privasi negara, dan juga hubungan bersama perusahaan, dalam hal hukum pengakuan data, apabila suatu negara tidak mendapatkan perlindungan data oleh pusat data dari perusahaan yang mempunyai data, maka negara akan mempunyai sebuah kekuranagan untuk mendirikan kedaulatannya. Kemudian sebuah kapasitas yang dimilki negara untuk mengawasi privasi data menjadi hal penting supaya negara tidak hadir sebagai pihak yang lebih menonjol untuk lebih menjaga aspek siber.

Keamanan siber yang juga sebagai rangkaian semacam aktivitas yang ditujukan agar terlindung dari sebuah ancaman dan juga peretasan jaringan komputer (*hardware and software*), terkait berita dan juga bagian ruang siber lainnya. Keamanan siber juga dilakukan untuk melihat sebuah pengawasan, seperti perihal aktivitas intelijen. Oleh karena itu, keamanan siber berupa mekanisme perlindungan yang ditujukan agar mengurangi gangguan pada ketersediaan, integritas dan privasi dari informasi. Aspek kerahasiaan data ditujukan kepada pihak yang memiliki peran untuk menyetujui sebuah data, yang berarti hanya pihak tertentu saja yang bisa mengakses dan membukanya, serta usaha agar menerima data dengan cara mencuri sebuah informasi dapat dikatakan sebuah perbuatan yang bisa saja membuat data bocor

Data bocor dan data bobol merupakan kasus yang kita bisa lihat dalam beberapa tahun terakhir, berbagai cara sudah dilakukan agar mencegah hal ini terjadi, tetapi sistem keamanan masih rentan dicuri yang berakibat banyak data yang bocor. Sejak tahun 2019 sampai 2024 terdapat 124 kasus pelanggaran perlindungan sebuah data pribadi dari data Kementerian kominfo. Dan juga sebanyak 279 juta data penduduk warga negara Indonesia di BPJS Kesehatan yang diduga bocor. *Hacker* loliyta juga telah mencuri 17 juta data pelanggan PLN. Kemudian data wajib pajak juga pernah mengalami kebocoran. Negara Indonesia ada di rank 24 dari 194 negara, data tersebut berasal dari *Global Cyber Security Index* tahun 2020, tentu tidak bisa untuk mengimplementasikan sebuah rasa yang bebas dalam hal kapabilitas warga Indonesia agar melindungi data privasi data dan juga untuk membuat sebuah proteksi rasa aman untuk beraktivitas di aspek siber. Perlindungan data setiap warga negara harus dilakukan, tetapi pada realitanya banyak kasus kebocoran data yang sudah terjadi dan sebagainya, oleh karena itu muncul pertanyaan mengenai peran dan juga kemampuan negara dalam konteks tersebut.

Dan Undang-undang Perlindungan Data Pribadi (RUU PDP) dan Undang-undang Keamanan dan Ketahanan Siber (RUU KKS) juga tidak kunjung diresmikan oleh pemerintah. Penelitian ini bertujuan untuk meningkatkan pemahaman akademis tentang tata kelola siber global dan dampaknya terhadap kebijakan Indonesia dengan menggabungkan pendekatan keamanan teknis dan juga analisis diplomatik. Penelitian ini akan melihat bagaimana sistem keamanan platform digital berperan dalam melindungi data pribadi dan bagaimana peran ini dapat dipahami dari sudut pandang diplomasi siber dalam hubungan internasional.

METODE PENELITIAN

Penelitian ini melakukan penelitian kualitatif dengan tujuan untuk memahami secara menyeluruh fungsi sistem keamanan dalam melindungi data pribadi di platform digital dan posisinya dalam diplomasi siber Indonesia di tingkat internasional. Pendekatan studi kasus dibuat karena kemungkinan peneliti untuk melihat fenomena kompleks yang melibatkan hubungan antara elemen teknis, hukum, dan diplomatik yang terlibat dalam perlindungan data pribadi di platform digital. Penelitian ini melibatkan beberapa pelaksana kepentingan di Indonesia yang masuk dalam kebijakan perlindungan data dan keamanan siber, seperti perwakilan dari Kementerian Komunikasi dan Informatika, lembaga perlindungan data, praktisi keamanan siber, akademisi, dan pengguna platform digital.

Informan yang dipilih secara purposif memiliki kompetensi dan pengalaman langsung dalam menangani masalah diplomasi siber dan perlindungan data pribadi. Prinsip kejenuhan data mengharuskan peneliti mengurangi jumlah informan ketika tidak ada lagi informasi penting.

Metode yang digunakan untuk mengumpulkan dan mendapatkan data yaitu secara observasi virtual tentang praktik keamanan data di berbagai platform digital yang populer di Indonesia dan analisis dokumen, termasuk undang-undang terkait seperti RUU Perlindungan Privasi Data dan Keamanan Siber, laporan kebocoran data dari Kominfo, dan dokumen kebijakan internasional seperti *Global Cyber Security Index.*

HASIL DAN PEMBAHASAN

Menurut hasil analisis dokumen, sistem keamanan platform digital di Indonesia masih menghadapi sejumlah masalah besar. Kementerian Kominfo melaporkan 124 kasus pelanggaran perlindungan data pribadi sejak 2019 hingga 2024. Ini termasuk 17 juta data pelanggan PLN dan 279 juta data penduduk di BPJS Kesehatan. Hasil ini menunjukkan bahwa banyak platform digital, baik milik pemerintah maupun swasta, belum menggunakan mekanisme keamanan teknis seperti enkripsi, otentikasi dua faktor, dan sistem deteksi penembusan dengan benar. Secara ilmiah, sejumlah variabel bertanggung jawab atas kelemahan ini. Pertama, tidak ada peraturan keamanan siber yang seragam dan mengikat di seluruh negeri. Kedua, perusahaan kurang investasi dalam infrastruktur keamanan siber, memprioritaskan efisiensi biaya daripada perlindungan data. Ketiga, kurangnya pengetahuan digital dan kesadaran pengguna tentang cara menjaga data pribadi mereka. Menurut data dari *Global Cyber Security Index* 2020, Indonesia berada di peringkat 24 dari 194 negara, menunjukkan bahwa meskipun ada kemajuan, negara ini masih kurang dalam kapasitas institusional dan teknis dibandingkan dengan negara seperti Jepang dan Singapura yang terbilang maju

Hasil ini sebanding dengan sebuah penelitian yang dibuat oleh Smith dan Jones (2021), yang mengemukakan sebuah ketimpangan antara peraturan dan penerapan teknis sering menyebabkan masalah dalam melindungi data pribadi di negara berkembang. Namun, berbeda dengan penelitian di Eropa yang menunjukkan bahwa undang-undang seperti GDPR mendorong bisnis untuk mematuhinya, kekurangan undang-undang perlindungan data yang disahkan menjadi penghalang utama. Ketidakpastian hukum dan posisi negara dalam menuntut pertanggungjawaban perusahaan atas kebocoran data diperlemah oleh RUU PDP dan KKS yang belum diresmikan.

Diplomasi Siber sebagai Kerangka Perlindungan Data

Studi ini menemukan bahwa, dari perspektif diplomasi siber, Indonesia tidak memiliki strategi diplomatik yang komprehensif untuk mendukung perlindungan data pribadi di kancah internasional. Padahal, diplomasi siber adalah alat penting untuk membangun standar global, kerja sama teknis, dan perjanjian bilateral yang dapat melindungi kepentingan nasional dari

ancaman siber lintas batas. Kementerian Luar Negeri menyatakan bahwa Indonesia lebih cenderung bersikap reaktif daripada proaktif dalam perjanjian perlindungan data di forum internasional seperti ASEAN dan PBB. Ini berbeda dengan cara yang digunakan oleh negara-negara seperti Jerman dan Korea Selatan, yang menggunakan diplomasi siber untuk mendorong model tata kelola data mereka. Sebagai contoh, *Federal Office for Information Security* (BSI) Jerman, secara teratur bekerja sama teknis dengan negara mitra untuk meningkatkan standar keamanan data, memperkuat posisi mereka di pasar global.

Kondisi di dalam negeri memperparah keterbatasan ini karena pengesahan RUU PDP dan RUU KKS masih terhambat oleh perselisihan lembaga dan kurangnya prioritas politik. Indonesia kesulitan membangun kredibilitas dan kapabilitas dalam diplomasi siber karena tidak memiliki landasan hukum yang kuat. Sehubungan dengan kapasitas, menurut perspektif Amartya Sen, negara tidak memberikan "aspek privasi data" sebagai bagian dari kebebasan konstitusional warganya. Akibatnya, warga negara tidak memiliki kemampuan untuk melindungi data mereka di internet.

Hasil ini mendukung pernyataan Nye (2017) bahwa soft power sangat penting untuk keamanan siber karena negara-negara dengan peraturan perlindungan data yang kuat dapat memengaruhi standar global. Namun, penelitian ini menemukan bahwa Indonesia memiliki potensi besar untuk berperan sebagai penghubung di antara negara yang maju dan negara yang berkembang dalam hal perlindungan data. Ini didasarkan pada posisi geostrategisnya di Asia Tenggara dan pengalamannya dalam menangani sejumlah kasus kebocoran data.

Implikasi terhadap Tata Kelola Siber Global

Hasil penelitian menunjukkan bahwa kegagalan Indonesia untuk melindungi data pribadi mengakibatkan kerugian bagi individu dan mengurangi kepercayaan mitra digital internasional. Beberapa platform global seperti Google dan Meta telah mengikuti peraturan di Eropa dan Amerika Serikat, tetapi mereka tidak memiliki peraturan yang jelas di Indonesia, sehingga mereka beroperasi dengan standar minimum. Hal ini menyebabkan ketimpangan dalam tata kelola siber global dan hukum eksteritorial seperti GDPR melindungi negara maju dari data warganya, sementara negara berkembang seperti Indonesia menjadi pasar data yang rentan. Situasi ini dapat dijelaskan secara ilmiah dengan teori dependensi digital. Dalam teori ini, negara perifer sangat bergantung pada infrastruktur dan layanan digital negara inti, tetapi mereka tidak dapat mengatur aliran data lintas batas.

Menurut penelitian, untuk mengatasi masalah ini, Indonesia harus mengambil pendekatan diplomasi siber yang ofensif. Untuk melakukan ini, mereka harus membangun aliansi strategis dengan negara-negara berkembang lain di ASEAN dan menggunakan Gerakan Non-Blok untuk mendorong penerapan tata kelola data yang lebih adil dan inklusif. Selain itu, sangat penting untuk mempercepat pengesahan RUU PDP dan KKS karena akan memberikan legitimasi hukum untuk upaya perlindungan data dan memperkuat posisi Indonesia dalam diplomasi siber.

Kesenjangan Regulasi dan Dampaknya terhadap Keamanan Data

Kesenjangan yang signifikan antara ketersediaan instrumen hukum dan kebutuhan perlindungan data di Indonesia adalah salah satu temuan paling penting dari penelitian ini. Sementara RUU Perlindungan Data Personal (PDP) dan RUU Keamanan dan Ketahanan keamanan siber (KKS) telah di beberapa tahun terakhir, tidak ada undang-undang yang ditetapkan hingga saat ini. Dengan keadaan ini, ada kelonggaran hukum yang dapat digunakan oleh berbagai pihak untuk eksploitasi data tanpa konsekuensi hukum yang jelas. Beberapa hal menyebabkan penundaan pengesahan kedua RUU tersebut. Yang pertama adalah interpretasi yang berbeda tentang kewenangan lembaga pengawas perlindungan data. Yang kedua adalah kekhawatiran sektor industri digital bahwa regulasi akan menghambat inovasi dan pertumbuhan bisnis

mereka. Yang ketiga adalah kurangnya pemahaman yang mendalam tentang pentingnya perlindungan data di era ekonomi digital. Akibatnya, Indonesia gagal membangun ekosistem digital yang stabil dan berdaulat.

Secara ilmiah, fenomena ini dapat dijelaskan oleh ide kelembaman kebijakan, juga dikenal sebagai kelalaian kebijakan. Konsep ini mengacu pada kelembaman kebijakan, di mana konflik kepentingan dan kekurangan kepemimpinan politik yang kuat menghalangi proses pengambilan keputusan. Dibandingkan dengan negara seperti India yang telah mengadopsi Peraturan Perlindungan Data Pribadi Digital pada 2023 atau Thailand yang telah mengadopsi Peraturan Perlindungan Data Pribadi (PDPA) sejak 2019, ketertinggalan Indonesia menunjukkan bahwa perlindungan data belum menjadi prioritas nasional yang mendesak. Akibatnya, pencurian identitas, penipuan online, dan pelanggaran privasi lainnya menjadi lebih umum di Indonesia.

Hasil ini sama bersamaan dengan penelitian Greenleaf (2020), yang menyoroti bahwa negara-negara Asia Tenggara menunjukkan perbedaan yang signifikan dalam bagaimana dan seberapa cepat mereka menerapkan peraturan perlindungan data. Namun, berbeda dengan penelitian sebelumnya yang menekankan bahwa faktor ekonomi adalah pendorong utama regulasi, penelitian ini menemukan bahwa faktor politik nasional dan dinamika kekuasaan antar lembaga memiliki dampak yang sama besarnya, jika tidak lebih besar, pada bagaimana regulasi perlindungan data di Indonesia berjalan.

Analisis Perbandingan Kebijakan Perlindungan Data di Tingkat Global

GDPR, yang mulai berlaku pada 2018, adalah peraturan utama untuk melindungi data pribadi. Regulasi ini tidak hanya berlaku di dalam Uni Eropa tetapi juga di luarnya dan perusahaan dari negara mana pun yang memproses data warga UE harus mematuhi ketentuannya. GDPR memberikan hak penting kepada orang-orang, seperti hak untuk dilupakan, akses, dan kemampuan pindah data. Disebabkan efek jera yang signifikan, denda yang dikenakan sangat besar, mencapai 4% dari pendapatan perusahaan dikancagh Global. Metode ini menunjukkan bahwa perlindungan data telah berkembang dari masalah domestik menjadi alat diplomatik dan standar Uni Eropa di tingkat global.

Amerika Serikat tidak memiliki undang-undang perlindungan data yang komprehensif di tingkat federal, berbeda dengan UE. Sebaliknya, mereka menggunakan pendekatan sektoral, yang melibatkan peraturan perlindungan data khusus untuk sektor tertentu. Peraturan seperti HIPAA, GLBA, dan COPPA untuk perlindungan anak adalah contoh dari pendekatan ini. Selain itu, negara bagian seperti California memiliki peraturan mereka sendiri melalui CCPA/CPRA. Metode ini menunjukkan prinsip libertarian yang mengutamakan kebebasan pasar dan inovasi daripada intervensi pemerintah. Namun, konsumen di Amerika Serikat lebih rentan daripada konsumen di Eropa karena tidak ada peraturan yang terintegrasi.

Sejak 2012, Singapura telah memiliki PDPA dan secara teratur melakukan amendemen untuk menyesuaikannya dengan kemajuan teknologi. Singapura juga secara aktif bekerja sama dengan negara lain melalui model klausul kontrak dan pengakuan timbal balik dengan Uni Eropa. Strategi Singapura menunjukkan bahwa negara kecil sekalipun dapat membangun kemampuan perlindungan data yang kuat dengan komitmen politik yang konsisten dan investasi dalam sumber daya manusia. Perbandingan ini menunjukkan bahwa negara Indonesia masih mempunyai banyak permasalahan yang harus diselesaikan. Indonesia tidak termasuk dalam G20 karena tidak memiliki regulasi yang terintegrasi. Ini menurunkan kredibilitas Indonesia dalam mendorong standar tata kelola digital yang tepat di forum internasional dalam konteks diplomasi siber.

Peran Aktor Non-Negara dalam Perlindungan Data Pribadi

Selain itu, penelitian ini menemukan bahwa pihak-pihak non-negara, seperti perusahaan platform digital, lembaga masyarakat sipil, dan komunitas pengguna, memainkan peran yang signifikan baik dalam memfasilitasi maupun menghambat perlindungan data pribadi. Di sisi lain, didorong oleh tuntutan pasar dan risiko reputasi, bisnis di platform *e-commerce* seperti GoTo, Bukalapak, dan lainnya telah mulai menerapkan metode keamanan seperti enkripsi end-to-end dan verifikasi dua faktor. Namun, mereka seringkali tidak memiliki standar keamanan yang jelas dan tidak memberikan informasi yang memadai kepada pengguna. Kasus kebocoran data BPJS Kesehatan dan PLN menunjukkan bahwa bahkan institusi yang memiliki data sensitif belum memiliki sistem keamanan yang tangguh.

Sebaliknya, kelompok masyarakat sipil seperti Lembaga Studi dan Advokasi Masyarakat (ELSAM) dan Forum Keamanan *Cyber* Indonesia telah aktif mempromosikan perlindungan data dan memberikan pendidikan publik tentangnya. Selain itu, mereka meminta pemerintah untuk segera mengesahkan RUU PDP dan meningkatkan transparansi tentang bagaimana menangani kasus kebocoran data. Namun, jika dibandingkan dengan kekuatan industri digital, organisasi-organisasi ini masih memiliki kapasitas dan jangkauan yang terbatas. Secara teoritis, temuan ini mendukung pendekatan pemerintahan *multi-stakeholder* dalam tata kelola siber, di mana pemerintah, sektor swasta, dan masyarakat sipil harus memainkan peran yang seimbang untuk menciptakan ekosistem siber yang aman dan berkeadilan. Namun, dalam kenyataannya, terjadi ketimpangan kekuatan antara korporasi global yang memiliki sumber daya dan kekuatan besar dan negara yang kurang mampu. Kondisi ini menimbulkan masalah besar untuk mewujudkan kedaulatan data ketika negara tidak dapat mengontrol data warganya yang disimpan di pusat data perusahaan asing.

Kapabilitas Teknis dan Sumber Daya Manusia dalam Keamanan Siber

Kapasitas teknis dan ketersediaan sumber daya manusia dalam aspek siber juga menjadi perhatian dalam penelitian ini. Data yang dikumpulkan oleh *Global Cyber Security Index* 2020 menunjukkan bahwa Indonesia berada di peringkat 24 dari 194 negara, menunjukkan bahwa negara tersebut telah mencapai kemajuan, tetapi masih jauh dari yang terbaik. Namun, Asosiasi Penyelenggara Jasa Internet negara Indonesia memperkirakan bahwa sekitar 50.000 profesional keamanan siber masih kekurangan di Indonesia, berdasarkan metrik kapasitas sumber daya manusia. Kekurangan tenaga kerja ini berdampak langsung pada kualitas perlindungan data; banyak organisasi dan lembaga pemerintah tidak memiliki tim keamanan siber yang berpengalaman, sehingga respons terhadap kebocoran data seringkali terlambat dan tidak efektif. Selain itu, serangan siber terus berkembang dengan kecanggihan yang semakin tinggi, dan masih sedikit uang yang dihabiskan untuk pendidikan dan pelatihan keamanan siber.

Penemuan ini sejalan dengan penelitian Kshetri (2021), yang menunjukkan bahwa disparitas sumber daya manusia dalam hal keamanan siber merupakan masalah yang dihadapi di seluruh dunia, tetapi sangat terasa di negara-negara berkembang. Namun, penelitian ini juga menemukan bahwa Indonesia memiliki potensi besar karena generasi mudanya yang melek teknologi dan program pelatihan yang ditawarkan oleh perusahaan teknologi terkemuka seperti Google dan Microsoft. Sayangnya, potensi ini belum dimanfaatkan karena kurangnya dukungan pemerintah dan kurangnya kerja sama antara industri dan pendidikan.

Diplomasi Siber sebagai Instrumen Kedaulatan Data

Dari sudut pandang diplomasi siber, penelitian ini menemukan bahwa Indonesia belum menyadari sepenuhnya peran penting diplomasi siber sebagai alat untuk melindungi kedaulatan data nasional. Padahal, data telah menjadi komoditas strategis yang setara dengan sumber daya alam di era digitalisasi. Negara yang mampu melindungi dan memanfaatkan data warganya akan

memiliki keunggulan dalam perekonomian global, sementara negara yang tidak mampu akan menjadi sasaran eksploitasi data. Dalam hal hubungan internasional, Indonesia dapat belajar dari keberhasilan Uni Eropa dalam menerapkan GDPR, yang melindungi warganya dan menciptakan *Brussels Effect*, yang menjadi standar global. Mengingat posisinya sebagai *economic* digital terbesar di ASEAN, negara Indonesia mempunyai potensi untuk menjadi pemimpin regional ASEAN. Namun, untuk mencapai hal ini, Indonesia harus membangun strategi diplomasi siber yang komprehensif, yang mencakup :

- Diplomasi normatif: Melalui forum seperti ASEAN, PBB, dan G20, mendorong pembentukan standar regional dan global tentang perlindungan data.
- Diplomasi teknis: Bekerja sama dengan negara-negara maju untuk meningkatkan kapasitas keamanan siber dan transfer teknologi.
- Diplomasi hukum: Membuat perjanjian bilateral dan multilateral tentang transfer data dan aliran data lintas negara yang menguntungkan satu sama lain.
- Diplomasi publik: Meningkatkan kesadaran publik tentang hak-hak privasi dan keamanan data melalui kampanye domestik dan partisipasi dalam forum internasional.

Kebocoran Data BPJS Kesehatan dan Implikasinya

Penelitian ini menyelidiki kasus data bocor pada BPJS Kesehatan di tahun 2021 secara menyeluruh untuk memberikan ilustrasi konkret. Diduga, 279 juta data penduduk Indonesia, termasuk (NIK), tempat dan tanggal lahir, dan alamat, bocor dan dijual di forum gelap, atau dark web. Kasus ini menimbulkan kekhawatiran luas tentang keamanan data kesehatan yang sangat sensitif dan menjadikannya salah satu kebocoran data terbesar yang pernah terjadi di Indonesia.

- Kelemahan teknis: Sistem data BPJS Kesehatan tidak memiliki mekanisme audit akses yang ketat dan tidak dienkripsi dengan baik.
- Kelemahan manajemen: termasuk kurangnya prosedur respons insiden yang jelas dan ketidakkolaborasian antara BPJS, Kominfo, dan BSSN.
- Kelemahan hukum: Jika RUU PDP tidak ada, sulit untuk menuntut pihak yang bertanggung jawab, baik internal maupun eksternal, untuk bertanggung jawab
- Kelemahan diplomatik: Kasus ini mengurangi kepercayaan mitra internasional terhadap Indonesia dalam kerja sama digital dan kesehatan globa

Kasus BPJS menyatakan bahwa perlindungan data tidak dari masalah teknis akan tetapi juga masalah tata kelola, akuntabilitas, dan kepercayaan publik. Dalam jangka panjang, kegagalan melindungi data kesehatan dapat menghambat keterlibatan Indonesia dalam kerja sama kesehatan global dan mengurangi kepercayaan investor terhadap infrastruktur digital Indonesia.

SIMPULAN

Hasil penelitian dan diskusi yang telah diuraikan menunjukkan bahwa sistem keamanan platform digital di Indonesia masih menghadapi masalah besar dalam melindungi data pribadi warga negara. Secara teknis, sebagian besar platform digital yang dikelola oleh pemerintah maupun swasta belum menggunakan mekanisme keamanan seperti enkripsi, autentikasi dua faktor, dan sistem deteksi intrusi dengan baik. Hal ini dibuktikan dengan banyaknya kebocoran data, yang menunjukkan kerentanan sistemik dalam infrastruktur keamanan siber nasional, termasuk 17 juta data pelanggan PLN dan 279 juta data BPJS Kesehatan. Dari segi regulasi, penelitian ini menemukan bahwa kesenjangan hukum yang signifikan menjadi penghambat utama perlindungan data di Indonesia. RUU yang telah diusulkan selama bertahun-tahun, RUU

Perlindungan Data Pribadi dan Keamanan dan Ketahanan Siber, belum juga disahkan, yang memungkinkan berbagai pihak untuk mengeksploitasi data tanpa konsekuensi hukum yang jelas. Kondisi ini menjadi lebih buruk karena hal-hal seperti masalah politik di dalam negeri, kepentingan yang berbeda di antara lembaga, dan pembuat kebijakan yang tidak memahami pentingnya perlindungan data di era ekonomi digital.

Studi ini menemukan bahwa Indonesia belum memiliki strategi diplomatik yang komprehensif untuk mendukung perlindungan data pribadi di kancah internasional. Negara-negara seperti Jerman, Singapura, dan Korea Selatan secara aktif mempromosikan model tata kelola data mereka melalui diplomasi siber, sementara Indonesia lebih cenderung bersikap reaktif dalam forum multilateral seperti ASEAN dan PBB. Tidak ada landasan hukum yang kuat di dalam negeri, yang mengurangi kredibilitas dan daya tawar Indonesia dalam perundingan internasional tentang tata kelola data dan keamanan siber. Akibatnya, posisi diplomatik ini tidak berhasil. Kegagalan perlindungan data nasional, seperti yang terjadi pada BPJS, telah mengurangi kepercayaan mitra internasional terhadap Indonesia dalam kerja sama digital dan investasi. Selain itu, penelitian ini menunjukkan bahwa perlindungan data pribadi bukanlah masalah teknis semata-mata; itu adalah masalah kedaulatan negara dan kemampuan warga negaranya. Menurut kerangka pemikiran Amartya Sen, jika negara tidak dapat memberikan "aspek privasi data" sebagai bagian dari kebebasan substantif warganya, masyarakat tidak lagi memiliki kemampuan untuk melindungi data mereka di internet. Meskipun Indonesia memiliki potensi besar dengan generasi muda yang melek teknologi, kekurangan sumber daya manusia untuk keamanan siber yang mencapai 50.000 tenaga profesional semakin memperparah situasi ini.

Oleh karena itu, penelitian ini menemukan bahwa untuk melindungi data pribadi di Indonesia, pendekatan holistik dan terintegrasi diperlukan. Pendekatan ini termasuk meningkatkan sistem keamanan teknis, mempercepat pengesahan undang-undang, meningkatkan kemampuan sumber daya manusia, dan mengembangkan strategi diplomasi siber yang agresif dan berkelanjutan. Indonesia dapat menjadi pemimpin dalam tata kelola siber Asia Tenggara jika ada komitmen politik yang kuat, kerja sama semua pemangku kepentingan, dan kesadaran bahwa perlindungan data adalah dasar dari kedaulatan digital dan kepercayaan publik di era transformasi digital.

SARAN

Peneliti menyarankan agar pemerintah dan Dewan Perwakilan Rakyat membuat pengesahan RUU Perlindungan Data Pribadi dan RUU Keamanan dan Ketahanan Siber sebagai prioritas nasional yang mendesak untuk menciptakan kepastian hukum dan mengakhiri penipuan siber. Saran ini didasarkan pada seluruh hasil penelitian dan diskusi yang telah diuraikan mengenai peran sistem keamanan terhadap data pribadi di platform digital dari perspektif diplomasi siber di tingkat internasional. Selain itu, pemerintah harus meningkatkan kapasitas institusional Badan Siber dan Sandi Negara dan Kementerian Komunikasi dan Informatika dengan meningkatkan anggaran, membeli teknologi canggih, dan merekrut profesional keamanan siber untuk mengatasi kekurangan tenaga kerja yang mencapai 50.000 orang. Selain itu, perlu dibangun pusat operasi keamanan siber nasional yang terintegrasi untuk memantau ancaman dan merespons kebocoran data dengan cepat dan terkoordinasikan.

Sektor swasta dan platform digital diharapkan untuk meningkatkan standar keamanan data dengan menerapkan enkripsi end-to-end, otentikasi multi-faktor, sistem deteksi intrusi, dan audit keamanan berkala serta mengadopsi prinsip *privacy by design* dan *privacy by default* serta meningkatkan transparansi kebijakan privasi kepada pengguna, menyediakan mekanisme akses dan penghapusan data yang mudah serta melaporkan secara terbuka setiap kebocoran data

sebagai wujud akuntabilitas. sementara itu, peneliti dan akademisi didorong untuk meningkatkan penelitian lintas disiplin tentang keamanan siber dan diplomasi data, mengembangkan kurikulum pendidikan yang mengintegrasikan perlindungan data dan keamanan siber ke dalam program studi hukum, teknologi informasi, dan hubungan internasional, serta meningkatkan kerja sama dengan lembaga pemerintah dan perusahaan teknologi untuk menyelenggarakan pelatihan dan penelitian terapan untuk masyarakat dan pengguna platform.

REFERENSI

Aji, M. P. (2023). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi) [Cyber security system and data sovereignty in Indonesia in political economic perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Greenleaf, G. (2020). *Asian data privacy laws: Trade & human rights perspectives*. Oxford University Press

Herlanda, M. D., & Wirawan, R. (2025). Geopolitical pressures and digital sovereignty: Indonesia's strategic response to US-China data hegemony. *Jurnal Hubungan Internasional, 18*(2), 571–592. https://doi.org/10.20473/jhi.v18i2.76019

Kshetri, N. (2021). Cybersecurity and data protection in developing countries. *Journal of Global Information Technology Management, 24*(2), 85–103

Lumintosari, F. R., Santoso, M. P. T., & Hakiem, F. N. (2024). Peluang dan tantangan diplomasi digital dalam meningkatkan keamanan siber Indonesia. *INNOVATIVE: Journal of Social Science Research, 4*(3), 746–754

Nye, J. S. (2017). Soft power and cybersecurity: The role of norms in international relations. *Foreign Affairs, 96*(3), 45–52

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. (2019). Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185

Pratama, P. (2025, July 24). Pakar ungkap 3 syarat data pribadi Indonesia dikelola AS. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20250724155001-185-1254470/pakar-ungkap-3-syarat-data-pribadi-indonesia-dikelola-as

Sampouw, M. (2025). Peningkatan keamanan siber untuk pemerintahan digital yang tangguh (Taskap). Lembaga Ketahanan Nasional Republik Indonesia.

Smith, A., & Jones, B. (2021). Data protection regulation in Southeast Asia: A comparative analysis. *Asian Journal of International Law, 11*(1), 112–135

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58

Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta: Jurnal Hukum, 19*(2). https://doi.org/10.15294/pandecta.v19i2.13279

Sen, A. (1999). *Development as freedom*. Anchor Books.

Badan Siber dan Sandi Negara. (2020). *Strategi keamanan siber nasional Indonesia*. BSSN.

Erdyawathy, A. A. S. E., Dewi, C. I. D. L., & Tungga, B. (2025). Legal settings about cyber security in the era of globalization. *Journal of Sustainable Development Science, 7*(2), 99–106. https://doi.org/10.46650/jsds.7.2.1747.99-106

Tampubolon, T., & Ramadhan, R. (2020). ASEAN Personal Data Protection (PDP): Mewujudkan keamanan data personal digital pada Asia Tenggara. *Padjadjaran Journal of International Relations, 1*(3). https://doi.org/10.24198/padjir.v1i3.26197

Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta: Jurnal Hukum, 19*(2). https://doi.org/10.15294/pandecta.v19i2.13279

Prawira, Y. M., & Yola, L. (2023). Analisis Narrative Policy Framework (NPF) dalam kebijakan Undang-undang Pelindungan Data Pribadi (UU PDP). *Jurnal Transformative, 9*(2), 204–222

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan data personal siber di Indonesia. *Padjadjaran Journal of International Relations, 1*(3). https://doi.org/10.24198/padjir.v1i3.26194

Chotimah, H. C. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara [Cyber security governance and Indonesian cyber diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10*(2), 126