KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 1: Pengenalan Keamanan Siber

Subtopik 1.3: Peraturan dan Kebijakan Terkait

ACCESS CONTROL

NETWORK SECURITY

DATA PROTECTION

EMAIL VIRUS THREAT

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun. Peraturan dan kebijakan adalah pondasi dalam menjaga keamanan siber. Tanpa aturan yang jelas, baik ASN maupun masyarakat akan kesulitan memahami hak dan kewajiban di ruang digital. Oleh karena itu, Subtopik 1.3 ini menghadirkan penjelasan mengenai regulasi penting, seperti Surat Edaran Bersama Mendagri–BSSN Tahun 2025 dan Peraturan Kepala BSSN Tahun 2024, yang menjadi acuan dalam melindungi data serta memastikan pelayanan publik berjalan aman.

Melalui pemahaman regulasi ini, ASN dapat lebih disiplin dalam mengelola data instansi, sedangkan masyarakat semakin sadar akan hak dan kewajiban digitalnya. Dengan demikian, aturan bukan sekadar dokumen hukum, tetapi pedoman nyata untuk menciptakan ekosistem digital yang aman, terpercaya, dan bermanfaat bagi semua. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa subtopik ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari Subtopik 1.3 ini, peserta diharapkan mampu:

1. Menjelaskan isi pokok dari SEB Mendagri–BSSN 2025 dan Perka BSSN 2024.
2. Menghubungkan peraturan tersebut dengan peran ASN maupun masyarakat dalam menjaga keamanan siber.
3. Memahami konsekuensi apabila regulasi ini tidak dipatuhi, baik dalam pelayanan publik maupun kehidupan digital sehari-hari.

Sasaran Peserta

1. ASN: agar memahami kewajiban hukum dalam mengelola data instansi, melaporkan insiden, dan menerapkan standar keamanan sesuai peraturan.
2. Masyarakat: agar mengetahui hak perlindungan data pribadi dan pentingnya patuh terhadap aturan digital untuk menjaga keamanan bersama.

A. Latar Belakang Regulasi

Perkembangan teknologi digital di Indonesia beberapa tahun terakhir membawa perubahan besar dalam tata kelola pemerintahan maupun kehidupan masyarakat. Layanan publik yang dulu serba manual kini beralih ke sistem elektronik: mulai dari administrasi kependudukan, sistem perizinan, pelayanan kesehatan, hingga transaksi keuangan. Transformasi ini memberi manfaat berupa efisiensi, transparansi, dan kemudahan akses.

Namun, di sisi lain, transformasi digital juga melahirkan tantangan baru: **ancaman keamanan siber yang semakin kompleks.** Beberapa kasus yang mencuat antara tahun 2020–2024, seperti kebocoran data kependudukan, jual-beli data pribadi di forum gelap, hingga serangan ransomware pada rumah sakit, menunjukkan bahwa risiko siber nyata dan dapat mengganggu stabilitas pelayanan publik. Salah satu kelemahan yang ditemukan adalah **belum meratanya kesiapan pemerintah daerah** dalam menghadapi insiden siber. Banyak daerah belum memiliki **Computer Security Incident Response Team (CSIRT)**, prosedur penanganan insiden masih belum seragam, serta koordinasi dengan pusat sering terlambat. Kondisi ini berpotensi memperbesar kerugian masyarakat jika terjadi serangan.

Untuk menjawab permasalahan tersebut, pemerintah pusat melalui **Badan Siber dan Sandi Negara (BSSN)** bersama **Kementerian Dalam Negeri (Kemendagri)** menerbitkan **Surat Edaran Bersama (SEB) Mendagri–BSSN 2025**. Dokumen ini menekankan pentingnya kolaborasi pusat–daerah dalam membangun sistem keamanan siber yang tangguh. Selain itu, **Peraturan Kepala (Perka) BSSN 2024** diterbitkan untuk memberikan **standar teknis** bagi instansi pemerintah, terutama di daerah. Regulasi ini menjawab kebutuhan akan panduan yang lebih rinci: bagaimana melakukan enkripsi data, bagaimana klasifikasi informasi, serta bagaimana standar audit dan prosedur penanganan insiden harus dilakukan.

Dengan demikian, **SEB Mendagri–BSSN 2025** dan **Perka BSSN 2024** hadir bukan sekadar sebagai dokumen hukum, melainkan sebagai **jawaban atas kebutuhan nyata**

di lapangan. Regulasi ini juga menjadi pelengkap dari kebijakan nasional yang lebih luas, seperti **Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi** dan **Strategi Keamanan Siber Nasional (BSSN, 2023)**. Bagi ASN, pemahaman regulasi ini berarti kesadaran akan tanggung jawab hukum dalam menjaga data publik dan memastikan keberlangsungan layanan digital. Bagi masyarakat, pemahaman ini memberi kepastian bahwa data pribadi mereka dilindungi oleh aturan hukum, sekaligus memberi kanal resmi untuk melaporkan insiden.

Kronologi Regulasi Keamanan Siber Indonesia (2017–2025)

Tahun	Regulasi / Dokumen	Isi Pokok	Implikasi bagi ASN & Masyarakat
2017	Peraturan Presiden No. 53 Tahun 2017 tentang BSSN	Membentuk Badan Siber dan Sandi Negara sebagai lembaga khusus keamanan siber nasional	ASN mulai memiliki lembaga rujukan resmi dalam keamanan siber; masyarakat mendapat payung hukum perlindungan data strategis
2018	Roadmap Keamanan Siber Nasional (BSSN)	Menetapkan arah pembangunan keamanan siber nasional	Pemda mulai diarahkan memperkuat sistem digital; masyarakat mulai dikenalkan literasi siber
2020–2022	Meningkatnya insiden kebocoran data (BPJS, Dukcapil, dsb.)	Menjadi pemicu percepatan regulasi perlindungan data pribadi	ASN dituntut lebih disiplin dalam mengelola data; masyarakat sadar risiko data bocor
2022	UU No. 27 Tahun 2022 tentang Pelindungan Data	Mengatur hak masyarakat atas data pribadi dan kewajiban	ASN wajib patuh standar perlindungan data; masyarakat punya hak

Tahun	Regulasi / Dokumen	Isi Pokok	Implikasi bagi ASN & Masyarakat
	Pribadi (PDP)	pengendali data	hukum bila data disalahgunakan
2023	Strategi Keamanan Siber Nasional (BSSN)	Menetapkan kerangka kerja keamanan siber nasional dan prioritas sektor kritis	ASN di daerah diarahkan mengikuti strategi nasional; masyarakat mendapat jaminan keamanan lebih kuat
2024	Peraturan Kepala BSSN Tahun 2024 tentang Standar Teknis Keamanan Informasi	Menetapkan standar teknis enkripsi, audit, klasifikasi data, dan SOP insiden	ASN punya panduan praktis menjaga data instansi; masyarakat terlindungi dengan standar minimal keamanan data
2025	Surat Edaran Bersama Mendagri–BSSN Tahun 2025	Memperkuat kolaborasi pusat–daerah, wajib pembentukan CSIRT daerah, pelatihan ASN, dan pelaporan insiden ke BSSN	ASN di daerah wajib membentuk CSIRT dan ikuti pelatihan; masyarakat mendapat kanal resmi melapor jika terjadi insiden

B. Pokok Isi SEB Mendagri–BSSN 2025

Surat Edaran Bersama (SEB) antara **Menteri Dalam Negeri** dan **Badan Siber dan Sandi Negara (BSSN)** tahun 2025 merupakan dokumen penting yang memperkuat peran pemerintah daerah dalam menjaga keamanan siber. Regulasi ini hadir karena

banyak daerah sebelumnya masih belum memiliki mekanisme tangguh untuk mencegah maupun menangani insiden siber.

1. Penguatan Infrastruktur Keamanan Siber

SEB menekankan bahwa pemerintah daerah wajib memperkuat infrastruktur teknologi informasinya, termasuk server, jaringan, aplikasi layanan publik, dan basis data kependudukan.

a. **Bagi ASN:** memastikan perangkat kantor, aplikasi, dan jaringan tidak menggunakan sistem usang atau tidak terproteksi.
b. **Bagi masyarakat:** berhak mengakses layanan publik digital yang lebih aman dan tidak mudah diretas.

2. Pembentukan CSIRT Daerah

Salah satu poin utama SEB adalah kewajiban pembentukan **Computer Security Incident Response Team (CSIRT)** di setiap pemerintah daerah. Tim ini bertugas:

a. Mengidentifikasi insiden siber sejak dini.
b. Menangani laporan masyarakat terkait kebocoran data atau serangan digital.
c. Berkoordinasi langsung dengan BSSN untuk pemulihan sistem.
d. Melakukan edukasi keamanan digital ke ASN dan masyarakat.

Makna bagi ASN: setiap pegawai yang bekerja dengan data publik tahu ke mana harus melapor jika ada insiden.

Makna bagi masyarakat: ada kanal resmi, bukan sekadar mengeluh di media sosial, ketika data atau layanan digital terganggu.

3. Kewajiban Pelaporan Insiden ke BSSN

SEB menegaskan bahwa insiden siber **tidak boleh ditutupi atau diselesaikan secara internal saja.** Setiap kejadian wajib dilaporkan ke BSSN melalui mekanisme resmi.

a. **Contoh untuk ASN:** jika aplikasi SIMPEG diretas, ASN tidak boleh sekadar menutup aplikasi dan diam. Laporan harus dibuat secara formal ke BSSN.

b. **Contoh untuk masyarakat:** warga yang menemukan upaya phishing mengatasnamakan pemda bisa melaporkannya melalui kanal resmi yang dikelola CSIRT daerah.

4. Peningkatan Kapasitas ASN

SEB juga mengamanatkan peningkatan kapasitas ASN, bukan hanya teknisi IT, melainkan seluruh pegawai yang terlibat dalam pengelolaan data dan layanan publik.

a. Pelatihan rutin tentang dasar keamanan informasi.
b. Sertifikasi tertentu bagi ASN yang mengelola sistem kritis.
c. Simulasi tanggap insiden di lingkungan kerja.

5. Ringkasan Tabel SEB 2025

Aspek Utama	Isi SEB Mendagri–BSSN 2025	Implikasi untuk ASN	Implikasi untuk Masyarakat
Infrastruktur	Pemda wajib memperkuat server, aplikasi, dan database	ASN pastikan aplikasi instansi aman & terproteksi	Warga dilayani lewat sistem yang lebih aman
CSIRT Daerah	Wajib dibentuk di setiap pemerintah daerah	ASN tahu prosedur pelaporan insiden	Warga punya kanal resmi untuk melapor insiden
Pelaporan Insiden	Insiden wajib dilaporkan ke BSSN	ASN tidak boleh menutup-nutupi masalah	Warga tahu ada mekanisme nasional menangani laporan
Peningkatan Kapasitas ASN	ASN wajib ikut pelatihan & sertifikasi dasar	ASN semakin sadar dan kompeten	Dampaknya: pelayanan publik lebih profesional

C. Pokok Isi Perka BSSN 2024

Peraturan Kepala (Perka) BSSN 2024 diterbitkan untuk memberikan **standar teknis dan prosedural** dalam penerapan keamanan informasi di instansi pemerintah. Jika SEB 2025 lebih menekankan koordinasi pusat–daerah, maka Perka 2024 fokus pada **langkah teknis yang harus dilaksanakan ASN sehari-hari.**

1. Standar Minimal Enkripsi Data

Perka mewajibkan penggunaan teknologi enkripsi untuk melindungi data, terutama data pribadi dan dokumen penting.

a. **ASN:** tidak boleh menyimpan data rahasia (misalnya NIK, gaji pegawai, rencana anggaran) tanpa perlindungan enkripsi.
b. **Masyarakat:** lebih terlindungi karena data yang mereka serahkan ke pemda tidak bisa dengan mudah diakses pihak yang tidak berwenang.

2. Audit Keamanan Sistem Elektronik

Setiap instansi pemerintah daerah wajib melakukan audit keamanan secara berkala. Audit ini menilai apakah aplikasi pelayanan publik, sistem administrasi, dan jaringan internet aman dari peretasan.

a. **ASN:** bertanggung jawab menyediakan akses data dan informasi untuk keperluan audit.
b. **Masyarakat:** berhak mendapatkan pelayanan publik dari sistem yang sudah diuji keamanannya.

3. Klasifikasi Data

Perka mengatur bahwa data harus dikelompokkan ke dalam kategori tertentu:

a. **Data biasa:** data umum yang tidak sensitif.
b. **Data terbatas:** data yang hanya boleh diakses ASN tertentu.
c. **Data rahasia:** data sangat sensitif yang hanya boleh diakses pejabat berwenang dengan izin khusus.

Contoh: dokumen SOP bisa termasuk data biasa, laporan internal bisa termasuk data terbatas, sedangkan data kependudukan detail (NIK, KK, biometrik) termasuk data rahasia.

4. SOP Penanganan Insiden Siber

Perka menetapkan prosedur baku:

1. **Deteksi dini:** mengenali tanda-tanda serangan (misalnya akses mencurigakan).
2. **Isolasi:** memutus sistem terdampak agar serangan tidak menyebar.
3. **Pemulihan:** mengembalikan data & layanan ke kondisi normal.
4. **Pelaporan:** menyampaikan insiden ke CSIRT daerah dan BSSN.

ASN: tidak boleh mengambil keputusan sendiri (misalnya langsung menghapus data yang diduga terinfeksi), tetapi wajib mengikuti SOP.

Masyarakat: mendapat kepastian bahwa insiden ditangani sesuai prosedur resmi, bukan sembarangan.

5. Ringkasan Tabel Perka 2024

Aspek Teknis	Ketentuan Perka 2024	Implikasi untuk ASN	Implikasi untuk Masyarakat
Enkripsi data	Data wajib dilindungi dengan enkripsi standar nasional	ASN wajib mengenkripsi dokumen sensitif	Data pribadi warga lebih terlindungi
Audit keamanan	Audit berkala atas sistem elektronik pemda	ASN harus siap mendukung audit	Layanan publik dijamin lebih aman
Klasifikasi data	Data dibagi: biasa, terbatas, rahasia	ASN wajib tahu kategori data sebelum membagikan	Warga tahu data sensitif tidak boleh sembarangan
SOP insiden siber	Deteksi → Isolasi → Pemulihan →	ASN wajib ikuti prosedur saat ada	Warga yakin insiden ditangani sesuai

Aspek Teknis	Ketentuan Perka 2024	Implikasi untuk ASN	Implikasi untuk Masyarakat
	Pelaporan	serangan	standar resmi

6. Makna Perka 2024

Dengan adanya Perka ini, pemerintah daerah memiliki panduan jelas untuk mengelola data dan sistem informasi. Bagi ASN, aturan ini menuntut disiplin dalam setiap langkah pengelolaan data. Bagi masyarakat, aturan ini memberikan jaminan perlindungan hukum atas data pribadi yang mereka percayakan kepada pemerintah.

D. Ilustrasi Kasus Hipotetis

Untuk memahami pentingnya regulasi SEB Mendagri–BSSN 2025 dan Perka BSSN 2024, mari kita bayangkan sebuah skenario di Kabupaten Klungkung.

Kasus: Serangan Ransomware pada Sistem Perizinan Online

Pada suatu pagi, sistem **perizinan online** Kabupaten Klungkung tiba-tiba tidak bisa diakses. Masyarakat yang hendak mengurus izin usaha dan dokumen lain hanya melihat tampilan layar hitam dengan pesan: *"Data Anda telah kami kunci. Bayar 100 juta rupiah jika ingin mengakses kembali."*

Di sisi ASN, muncul kepanikan: layanan terhenti, antrean warga menumpuk, dan berita mulai menyebar di media sosial bahwa sistem pemerintah daerah diretas.

Bagaimana jika tanpa SEB & Perka?

1. ASN bingung, tidak ada tim khusus (CSIRT) yang bertugas.
2. Masing-masing staf mencoba "mematikan server" atau "menghapus file yang dicurigai", sehingga bukti serangan hilang.
3. Masyarakat marah karena tidak ada kejelasan, bahkan sebagian menuduh data pribadi mereka ikut bocor.
4. Layanan terhenti berhari-hari, kepercayaan publik menurun drastis.

Bagaimana jika dengan SEB & Perka?

1. ASN segera melapor ke **CSIRT Daerah**, sesuai SEB 2025.
2. CSIRT melakukan **isolasi server** dan menghubungi BSSN untuk pendampingan.
3. Prosedur **SOP insiden** dari Perka 2024 dijalankan: deteksi → isolasi → pemulihan → pelaporan.
4. Masyarakat diberi informasi resmi melalui kanal komunikasi pemda, sehingga tidak terjadi kepanikan.
5. Dalam 2 hari, layanan berhasil dipulihkan tanpa harus membayar uang tebusan.

Pesan dari Kasus Hipotetis ini

1. **ASN** belajar bahwa aturan bukan sekadar dokumen, tetapi pedoman praktis yang bisa menyelamatkan instansi dari krisis.
2. **Masyarakat** memahami bahwa ada prosedur resmi yang melindungi data mereka, bukan sekadar janji.
3. **Pemerintah daerah** membuktikan kredibilitasnya dengan bertindak cepat, transparan, dan sesuai aturan.

E. Hubungan dengan Regulasi Nasional Lain

Agar lebih dipahami, penting untuk menempatkan SEB Mendagri–BSSN 2025 dan Perka BSSN 2024 dalam kerangka regulasi nasional yang lebih luas. Dua aturan ini pada dasarnya merupakan **instrumen operasional** yang mendukung kebijakan strategis tingkat nasional.

1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

a. UU PDP adalah dasar hukum utama bagi perlindungan hak privasi masyarakat.
b. ASN yang mengelola data pribadi wajib menaati prinsip UU ini: legalitas, keadilan, transparansi, keamanan, dan akuntabilitas.
c. Masyarakat memperoleh **hak hukum** untuk menuntut jika data pribadinya disalahgunakan.

d. SEB 2025 dan Perka 2024 menjadi perangkat implementasi UU PDP di level daerah.

2. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN)

a. Perpres ini membentuk **BSSN** sebagai lembaga utama keamanan siber di Indonesia.
b. Tanpa Perpres ini, BSSN tidak akan punya otoritas menerbitkan Perka maupun mengeluarkan SEB bersama Kemendagri.
c. Bagi ASN, Perpres ini memastikan ada satu lembaga pusat yang bisa dijadikan rujukan.
d. Bagi masyarakat, Perpres ini menjamin adanya lembaga khusus yang bertugas melindungi ruang digital Indonesia.

3. Strategi Keamanan Siber Nasional (BSSN, 2023)

a. Dokumen strategis ini menjadi peta jalan penguatan keamanan siber di Indonesia.
b. Fokus pada sektor-sektor kritis: pemerintahan, energi, kesehatan, dan keuangan.
c. ASN di daerah diarahkan untuk mengintegrasikan sistem kerjanya dengan strategi nasional.
d. SEB 2025 & Perka 2024 merupakan **penjabaran teknis** strategi ini di level implementasi.

4. Keterkaitan Antar-Regulasi

Agar lebih jelas, berikut diagram hubungan regulasi:

5. Makna bagi ASN dan Masyarakat

a. **ASN:** harus memahami bahwa peraturan teknis (SEB/Perka) adalah bentuk konkret kewajiban hukum nasional. Kepatuhan bukan sekadar disiplin kerja, tetapi juga bentuk tanggung jawab hukum.
b. **Masyarakat:** menyadari bahwa perlindungan data pribadi mereka tidak hanya janji, tetapi dijamin secara berlapis mulai dari UU hingga aturan teknis di daerah.

F. Dampak Jika Tidak Dipatuhi

Peraturan dan kebijakan keamanan siber tidak dibuat hanya untuk menambah dokumen birokrasi, tetapi untuk melindungi kepentingan publik. Jika SEB Mendagri–BSSN 2025 dan Perka BSSN 2024 tidak dipatuhi, dampaknya bisa serius dan merugikan

banyak pihak.

1. Dampak bagi ASN & Pemerintah Daerah

a. **Gangguan Layanan Publik**, Layanan kependudukan, perizinan online, hingga kesehatan digital bisa terhenti akibat serangan siber. ASN akan kewalahan menghadapi komplain masyarakat.

b. **Sanksi Administratif & Reputasi**, ASN atau instansi yang lalai dapat dikenai teguran atau sanksi administratif. Lebih dari itu, reputasi pemerintah daerah bisa tercoreng karena dianggap tidak profesional.

c. **Beban Biaya Tinggi**, Pemulihan sistem setelah serangan lebih mahal daripada pencegahan. Anggaran daerah bisa terkuras untuk menebus serangan ransomware atau membangun sistem darurat.

2. Dampak bagi Masyarakat

a. **Pencurian Data Pribadi**, Tanpa perlindungan yang baik, data masyarakat (NIK, KK, rekening, rekam medis) bisa dicuri dan diperdagangkan di forum gelap.

b. **Kerugian Finansial**, Penipuan digital semakin mudah dilakukan jika data masyarakat bocor. Banyak warga bisa kehilangan tabungan atau jatuh ke dalam jebakan pinjaman online ilegal.

c. **Hilangnya Kepercayaan**, Jika masyarakat tidak percaya pada layanan digital pemerintah, mereka enggan menggunakannya. Transformasi digital pun terhambat.

3. Dampak bagi Negara

a. **Melemahnya Ketahanan Siber Nasional**, Serangan pada level daerah bisa menjadi pintu masuk untuk serangan lebih besar ke sistem nasional.

b. **Krisis Reputasi Internasional**, Kebocoran data besar dapat membuat Indonesia dianggap tidak serius menjaga keamanan siber, sehingga menurunkan kepercayaan investor global.

c. **Hambatan Transformasi Digital**, Program *Smart City* dan pemerintahan digital tidak akan berhasil jika aturan dasar seperti SEB & Perka diabaikan.

Pertanyaan Reflektif

1. Jika suatu aplikasi layanan publik (misalnya e-KTP atau perizinan online) tiba-tiba berhenti karena serangan siber, menurut Anda apa dampak yang paling cepat dirasakan masyarakat?
2. Mengapa ASN yang bukan tenaga IT tetap perlu memahami isi SEB Mendagri–BSSN 2025 dan Perka BSSN 2024?
3. Jika Anda sebagai masyarakat menemukan data pribadi Anda (misalnya NIK atau rekening bank) disalahgunakan, ke mana seharusnya Anda melapor berdasarkan aturan yang berlaku?

DAFTAR PUSTAKA

Alfaridzah, A. L., Firlana, H., & Astuti, R. K. (2025). IMPLEMENTASI DAN DAMPAK SISTEM MANAJEMEN SDM BERBASIS E-GOVERNMENT DI INDONESIA. *Jurnal Kajian Pemerintah (JKP)*, *11*(1), 145–156.

Badan Siber dan Sandi Negara. (2024). *Peraturan Kepala BSSN tentang Standar Teknis Keamanan Sistem Elektronik Pemerintah Daerah.* Jakarta: BSSN.

Badan Siber dan Sandi Negara & Kementerian Dalam Negeri. (2025). *Surat Edaran Bersama Mendagri–BSSN tentang Penguatan Keamanan Siber Pemerintah Daerah.* Jakarta.

Darmayadi, A., Aprilia, F. S., Somantri, Y. K., Pamungkas, F. A., Nurfadhilah, A., & Sinambela, S. W. (2025). *Strategy and Implementation of Indonesian Cyber Diplomacy in the Framework of Bilateral and Multilateral Cooperation in the Digital Era*. Atlantis Press SARL. https://doi.org/10.2991/978-2-38476-442-6_11

Fatanah, D. Y., Putri, E. R. D., Z, W. O. A., Faturachman Alputra Sudirman, & Saidin. (2025). ANALISIS BIBLIOMETRIK BIROKASI DIGITAL DAN KEAMANAN DATA DI INDONESIA TAHUN 2023-2024. *Jurnal Ilmu Pemerintahan*, *13*(02), 191–206.

Maharani, M. A., & Atman, W. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia. *Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial Dan Politik*, *2*(3), 344–354. https://doi.org/10.62383/sosial.v2i3.2291

Mubarak, Z. Y., & Triwibowo, R. N. (2025). REGULATORY TRANSFORMATION OF THE DIGITAL ECONOMY AND THE CHALLENGES OF PERSONAL DATA PROTECTION IN INDONESIA: A LITERATURE REVIEW. *INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS (IJEFE)*, *2*(1), 187–196.

Nurrizky, A., & Nugroho, W. (2025). Analisis Kebijakan Otoritas Jasa Keuangan dalam Upaya Menanggulangi Cyber Crimedi Sektor Perbankan. *Recht Studiosum Law*

Review, *02*(1), 2961–7812. https://doi.org/10.32734/rslr.v4i1.18452

Pradevi, B., Wibisono, I. W., & Seba, R. O. (2025). Kebijakan Pemerintahan Joko Widodo dalam Menghadapi Ancaman Cyber di Sektor Infrastruktur Energi Indonesia. *SOSMANIORA (Jurnal Ilmu Sosial Dan Humaniora)*, *4*(3), 908–917. https://doi.org/10.55123/sosmaniora.v4i3.6424

Presiden Republik Indonesia. (2017). *Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.* Jakarta: Sekretariat Negara. https://peraturan.bpk.go.id/Home/Details/74041

Rotib, A. A., Windasari, S., Bagaskoro, B., Frihadi, A., & Abdurohman. (2025). Leveraging Blockchain Technology to Enhance Data Integrity and Transparency in Government Data Centers. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *5*(1), 126–133. https://doi.org/10.51903/teknik.v5i1.891

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.* Jakarta: Kementerian Hukum dan HAM. https://peraturan.bpk.go.id/Home/Details/216819

Syafitri, N., & Hendrawarman. (2025). Legal Review of Cyber Crime: Case of Attack Ransomware On Center Data National Temporary Surabaya 2. *Journal Critical Legal Review*, *2*(3), 37–57.