KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 2: Ancaman Siber yang Sering Terjadi

Subtopik 2.3: Kebocoran Data

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. Subtopik ini membahas fenomena kebocoran data, salah satu isu paling serius di era digital. Kasus kebocoran data di Indonesia beberapa tahun terakhir tidak hanya menimpa sektor swasta, tetapi juga instansi pemerintah. Hal ini menunjukkan bahwa keamanan siber bukan hanya tanggung jawab teknisi IT, melainkan kewajiban seluruh pihak, terutama ASN dan masyarakat yang berinteraksi dengan data setiap hari.

Subtopik ini disusun agar ASN dan masyarakat dapat memahami pentingnya pengelolaan data secara aman dan sesuai kebijakan pemerintah, sementara masyarakat semakin sadar untuk menjaga kerahasiaan data pribadinya. 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 modul 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 ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Menjelaskan pengertian dan jenis kebocoran data dalam konteks pemerintahan dan kehidupan sehari-hari.
2. Mengidentifikasi penyebab umum kebocoran data di Indonesia.
3. Memahami dampak kebocoran data terhadap kepercayaan publik dan keamanan nasional.
4. Mengetahui langkah pencegahan serta tanggung jawab ASN dan masyarakat dalam melindungi data pribadi.

Sasaran Peserta

1. ASN: agar mampu menjaga kerahasiaan data instansi dan tidak sembarangan membagikan akses ke sistem informasi pemerintahan.
2. Masyarakat: agar lebih berhati-hati dalam mengelola dan membagikan data pribadi di berbagai platform digital.

A. Pengantar: Mengapa Isu Kebocoran Data Penting di Tahun 2025

Kebocoran data bukan lagi sekadar berita yang muncul sesekali di media nasional, ia sudah menjadi ancaman nyata yang menyentuh kehidupan masyarakat sehari-hari dan memengaruhi kepercayaan publik terhadap pemerintah. Di tahun 2025, dunia digital Indonesia berkembang sangat pesat. Hampir seluruh layanan publik, mulai dari administrasi kependudukan, pajak daerah, hingga layanan kesehatan, sudah terhubung secara daring (online). Namun, kemudahan ini juga membuka peluang baru bagi kejahatan siber.

Setiap data yang dikumpulkan dan disimpan oleh pemerintah daerah maupun masyarakat memiliki **nilai ekonomi dan strategis** yang tinggi. Data bukan hanya kumpulan angka atau dokumen digital, melainkan identitas dan aset bangsa. Ketika data bocor, maka bukan hanya individu yang dirugikan, tetapi juga **pemerintahan dan negara** yang kehilangan kepercayaan publik.

Pada tahun 2024–2025, laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan peningkatan signifikan pada jumlah insiden kebocoran data di Indonesia. Banyak dari kasus tersebut terjadi karena **kelalaian manusia (*human error*)** dan **pengelolaan sistem yang belum memenuhi standar keamanan digital nasional**. Artinya, ancaman terbesar tidak selalu berasal dari hacker atau pelaku kejahatan dunia maya, tetapi bisa juga dari kesalahan kecil yang dilakukan tanpa sadar oleh pegawai atau pengguna biasa.

Sebagai contoh, kebocoran data bisa terjadi hanya karena seseorang menyimpan file data kependudukan di penyimpanan daring (*cloud*) tanpa kata sandi, atau karena ASN mengirimkan dokumen rahasia lewat email pribadi. Di sisi lain, masyarakat sering kali tanpa sadar memberikan data pribadi seperti **NIK, nomor rekening, atau alamat rumah** kepada pihak yang tidak jelas identitasnya.

Khusus di tingkat daerah, termasuk Kabupaten Klungkung, kesadaran terhadap keamanan data menjadi semakin penting seiring dengan peningkatan layanan digital

publik seperti **SIAK Terpusat, e-Office, dan layanan perizinan online.** Data-data dari sistem ini menjadi sasaran empuk bagi pihak tidak bertanggung jawab, karena mengandung informasi lengkap tentang warga dan aktivitas pemerintahan.

Oleh sebab itu, memahami isu kebocoran data bukan hanya tugas tenaga IT atau tim keamanan siber, melainkan tanggung jawab bersama antara **ASN dan masyarakat.** ASN bertugas menjaga keamanan data milik instansi dan layanan publik, sementara masyarakat harus melindungi data pribadinya agar tidak mudah disalahgunakan.

Dalam konteks tata kelola pemerintahan modern, kebocoran data berdampak langsung terhadap **kepercayaan publik.** Sekali data bocor, kepercayaan sulit dikembalikan. Warga akan ragu memberikan data kepada pemerintah, dan sistem digital bisa kehilangan efektivitasnya. Maka dari itu, menjaga keamanan data di era digital bukan sekadar soal teknis, tetapi juga **soal etika, tanggung jawab, dan integritas.**

B. Definisi dan Jenis Kebocoran Data

1. Definisi Kebocoran Data

Kebocoran data adalah **peristiwa ketika informasi pribadi, rahasia, atau penting diakses, disalin, atau disebarluaskan oleh pihak yang tidak berwenang.** Dalam konteks pemerintahan dan kehidupan masyarakat, kebocoran data dapat terjadi baik karena serangan siber maupun karena kelalaian manusia. Data yang bocor tidak selalu langsung terlihat sering kali baru disadari setelah muncul penyalahgunaan, seperti kasus penipuan, pencurian identitas, atau penyebaran data pribadi di media sosial dan forum daring. Di lingkungan instansi pemerintah, kebocoran data bisa berasal dari berbagai sumber, seperti:

a. penggunaan akun pribadi untuk pekerjaan kedinasan,
b. file penting disimpan di *cloud* tanpa pengaman,
c. atau kurangnya kontrol akses terhadap sistem internal.

💬 *Contoh sederhana:* Jika seorang ASN tanpa sengaja mengunggah file daftar penerima bantuan sosial ke internet tanpa kata sandi, data tersebut bisa diambil siapa pun dan disalahgunakan untuk penipuan.

2. Jenis-Jenis Kebocoran Data

Kebocoran data dapat dibedakan berdasarkan **jenis informasi** yang bocor dan **asal insiden** terjadinya. Berikut beberapa jenis yang umum di Indonesia pada tahun 2020–2025:

a. Kebocoran Data Pribadi

Terjadi ketika informasi individu seperti **Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), alamat rumah, nomor rekening bank, email, atau nomor telepon** tersebar tanpa izin. Kasus ini paling sering dimanfaatkan untuk:

- penipuan digital (phishing atau pinjaman online ilegal),
- penjualan data di forum gelap (*dark web*),
- atau penyalahgunaan untuk kampanye dan iklan tidak sah.

📍 *Contoh:* Kasus kebocoran data SIM card pada tahun 2022 yang mengungkap jutaan data pengguna karena lemahnya sistem registrasi.

b. Kebocoran Data Pemerintahan

Jenis ini mencakup data yang dikelola oleh instansi pemerintah pusat maupun daerah, seperti:

- dokumen perencanaan dan keuangan,
- arsip pelayanan publik (SIAK, perizinan, kepegawaian),
- atau laporan internal instansi.

Kebocoran di sektor ini berpotensi mengganggu stabilitas pemerintahan dan menurunkan kepercayaan publik.

📍 *Contoh:* Gangguan pada portal layanan publik di beberapa daerah tahun 2023 akibat celah keamanan server lama yang belum diperbarui.

c. Kebocoran Data Kesehatan

Data medis memiliki nilai tinggi di pasar gelap karena memuat informasi

pribadi sekaligus rekam riwayat kesehatan. Kebocoran ini dapat menyebabkan penyalahgunaan asuransi atau manipulasi identitas pasien. Rumah sakit dan puskesmas kini menjadi target utama *ransomware*.

- *Contoh:* Serangan siber terhadap sistem rumah sakit besar di Indonesia tahun 2023 yang mengakibatkan ribuan data pasien bocor.

d. Kebocoran Data Pendidikan

Dengan meningkatnya penggunaan aplikasi e-learning dan database sekolah digital, data siswa dan guru juga berisiko bocor. Data pendidikan sering kali memuat NISN, alamat, nilai, dan bahkan data keluarga.

- *Contoh:* Kebocoran data dari platform pembelajaran daring tahun 2024 yang memperjualbelikan jutaan data pelajar secara ilegal.

e. Kebocoran Data Digital Modern (AI, Biometrik, dan Sensor)

Tahun 2025 ditandai dengan makin banyaknya data berbasis **kecerdasan buatan (AI)** dan **biometrik**, seperti sidik jari, wajah, atau suara. Data jenis ini memiliki risiko tinggi karena tidak bisa diubah seperti kata sandi. Sekali bocor, identitas digital seseorang sulit dilindungi kembali.

- *Contoh:* Kasus kebocoran data kamera pengawas (CCTV) berbasis AI di beberapa kota besar yang digunakan untuk profiling warga.

3. Mengapa ASN dan Masyarakat Harus Peduli?

a. Karena setiap orang **menjadi bagian dari rantai data.** ASN mengelola data publik, masyarakat menjadi sumber datanya.

b. Sekali data bocor, sulit dikendalikan penyebarannya dan dampaknya bisa menular ke banyak sistem lain.

c. Menjaga data berarti menjaga **kepercayaan, integritas, dan keamanan bersama.**

C. Penyebab Umum Kebocoran Data

Kebocoran data tidak terjadi begitu saja. Dalam banyak kasus, penyebabnya bukan semata-mata serangan dari luar, melainkan **kombinasi antara kelalaian manusia, lemahnya sistem keamanan, dan rendahnya kesadaran digital.** Di bawah ini dijelaskan beberapa penyebab paling umum yang sering ditemui di lingkungan pemerintahan daerah maupun masyarakat.

1. Kelalaian Manusia (*Human Error*)

   Faktor ini menjadi penyebab paling sering dan paling sulit diantisipasi. Banyak kebocoran data justru terjadi karena tindakan sederhana yang tidak disengaja. Contohnya:

   a. Mengirim dokumen penting ke alamat email yang salah.
   b. Menyimpan file di penyimpanan awan (*cloud*) tanpa kata sandi.
   c. Mengunggah data publik di situs tanpa proteksi.
   d. Menggunakan *password* yang mudah ditebak seperti "12345" atau "admin123".

   Di instansi pemerintah, kasus semacam ini sering terjadi karena pegawai belum memahami standar keamanan digital, atau terburu-buru dalam bekerja. Padahal, satu kesalahan kecil bisa membuka jalan bagi peretas untuk masuk ke sistem.

   💡 *Pesan penting:* Kesadaran setiap individu lebih berpengaruh daripada sekadar teknologi canggih.

2. Serangan Siber (*Cyber Attack*)

   Serangan dari luar masih menjadi ancaman serius, terutama dalam bentuk:

   a. ***Phishing*:** penipuan lewat email atau pesan yang meniru instansi resmi.
   b. ***Malware* dan *ransomware*:** virus yang mencuri atau mengunci data lalu meminta tebusan.

c. ***SQL Injection* atau *DDoS Attack*:** menyerang sistem basis data atau membuat layanan tidak bisa diakses.

Serangan ini sering menyasar sistem pemerintah daerah karena banyak data sensitif tersimpan di dalamnya, sementara perlindungannya belum selalu maksimal.

Berdasarkan laporan BSSN tahun 2024, lebih dari **40% serangan siber di Indonesia menargetkan instansi publik.**

🧠 *Contoh lokal:* Jika server layanan kependudukan diserang *ransomware*, masyarakat bisa kesulitan mengurus KTP, KK, atau surat penting lainnya selama berhari-hari.

3. Sistem Keamanan yang Lemah

Beberapa instansi dan lembaga masih menggunakan:

a. sistem lama yang belum diperbarui,
b. aplikasi internal tanpa enkripsi,
c. server dengan pengaturan keamanan standar.

Sistem semacam ini rentan ditembus oleh peretas, terutama jika tidak diaudit secara berkala. Kadang, server penyimpanan dibiarkan aktif 24 jam tanpa pemantauan, padahal koneksi terus terbuka ke jaringan luar.

⚙️ *Catatan penting:* Keamanan data bukan hanya tentang antivirus, tapi juga pengelolaan server, akses pengguna, dan pembaruan sistem secara rutin.

4. Akses Internal Tidak Terkendali

Bukan hanya pihak luar yang berisiko menyebabkan kebocoran data. Di banyak kasus, **orang dalam (*insider*)** baik karena kelalaian maupun niat buruk menjadi sumber kebocoran. Penyebabnya bisa beragam:

a. Pegawai yang menyalahgunakan akses data.
b. Mantan pegawai yang masih memiliki akun aktif.
c. Tidak adanya pembatasan hak akses berdasarkan jabatan.

Misalnya, pegawai dengan akses penuh ke data kependudukan seharusnya hanya membuka data sesuai tugasnya. Namun, tanpa sistem kontrol, data bisa disalin atau dikirim keluar tanpa jejak.

🔐 *Solusi utama:* Terapkan sistem ***role-based access control*** (RBAC), yaitu hak akses sesuai jabatan atau kebutuhan kerja.

5. Penggunaan Platform Digital Tidak Aman

Kebocoran juga sering terjadi karena ASN atau masyarakat menggunakan aplikasi yang tidak resmi, misalnya:

a. mengirim data penting lewat aplikasi pesan instan pribadi,
b. menyimpan arsip kantor di Google Drive pribadi,
c. atau memakai Wi-Fi publik tanpa pengamanan.

Kebiasaan ini memberi peluang besar bagi pihak luar untuk mencuri data. Peretas kini memanfaatkan jaringan publik atau aplikasi bajakan untuk menyusup dan menyalin informasi secara diam-diam.

📱 *Pesan utama:* Gunakan hanya platform dan jaringan yang sudah diverifikasi instansi atau pemerintah.

6. Kurangnya Edukasi dan Budaya Keamanan Siber

Banyak ASN dan masyarakat masih menganggap keamanan data sebagai hal teknis yang tidak berhubungan langsung dengan pekerjaan sehari-hari. Padahal, kesalahan kecil seperti membuka lampiran email mencurigakan atau membagikan data tanpa izin sudah cukup untuk memicu kebocoran besar. Budaya keamanan siber perlu ditanamkan sejak awal:

a. ASN wajib mengikuti pelatihan keamanan data secara rutin.
b. Masyarakat perlu diedukasi melalui media sosial, sekolah, dan layanan publik.
c. Pemerintah daerah bisa membuat kampanye seperti *"Klungkung Aman Data, Aman Digital."*

📣 *Pesan utama:* Keamanan data adalah perilaku, bukan hanya perangkat lunak.

D. Dampak Kebocoran Data

Kebocoran data bukan hanya sekadar kehilangan file atau bocornya informasi pribadi. Dampaknya bisa **meluas ke berbagai sektor kehidupan pemerintahan, ekonomi, sosial, bahkan keamanan nasional.** Ketika data jatuh ke tangan yang salah, kerugian yang ditimbulkan tidak hanya dirasakan oleh individu, tetapi juga oleh masyarakat luas dan lembaga pemerintah. Berikut adalah tiga lapisan utama dampak kebocoran data:

1. **Dampak bagi Pemerintah Daerah dan ASN**

   Pemerintah daerah, termasuk ASN sebagai pengelola data publik, memegang tanggung jawab besar dalam menjaga kerahasiaan dan integritas informasi.

   Kebocoran data di sektor ini menimbulkan beberapa risiko besar:

   a. Hilangnya Kepercayaan Publik

      Begitu data masyarakat bocor, kepercayaan terhadap pemerintah akan langsung menurun. Warga menjadi ragu untuk menyerahkan data pribadinya, misalnya saat mendaftar layanan digital seperti **SIAK Terpusat, perizinan online, atau aplikasi bantuan sosial.**

      💬 *Contoh nyata:* Jika data penerima bantuan sosial bocor ke publik, warga bisa merasa haknya dilanggar, dan program bantuan kehilangan legitimasi.

   b. Gangguan Operasional dan Pelayanan Publik

      Kebocoran data bisa menyebabkan sistem pemerintahan terganggu. Misalnya:

      - Server dilumpuhkan karena serangan *ransomware*.
      - Dokumen penting terhapus atau diubah.
      - Pelayanan publik seperti pembuatan KTP, izin usaha, atau administrasi kepegawaian terganggu.

Gangguan ini membuat pemerintah tidak bisa melayani masyarakat secara optimal dan menurunkan produktivitas ASN.

c. Risiko Hukum dan Disiplin ASN

Kebocoran data yang diakibatkan oleh kelalaian ASN bisa menimbulkan sanksi administratif, bahkan hukum, sesuai dengan **UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022)**. ASN wajib menjaga kerahasiaan data sesuai **kode etik dan peraturan perundangan.**

⚖️ *Poin penting:* Setiap pegawai negeri yang memegang akses data publik harus memahami bahwa penyalahgunaan atau kelalaian dalam melindungi data termasuk pelanggaran serius.

2. Dampak bagi Masyarakat

Kebocoran data masyarakat berpotensi menimbulkan **kerugian langsung dan tidak langsung.** Sering kali, korban bahkan tidak menyadari bahwa datanya telah digunakan oleh pihak lain.

a. Pencurian Identitas (*Identity Theft*)

Data pribadi seperti NIK, nomor rekening, atau foto KTP sering disalahgunakan untuk membuat akun palsu atau mengajukan pinjaman online ilegal. Akibatnya, korban bisa tiba-tiba menerima tagihan atas nama dirinya tanpa pernah merasa meminjam.

💡 *Contoh:* Kasus pinjaman online ilegal yang menggunakan data hasil kebocoran dari registrasi SIM card.

b. Kerugian Finansial dan Penipuan Digital

Masyarakat bisa kehilangan uang karena tertipu oleh pihak yang memanfaatkan data bocor untuk mengaku sebagai pihak resmi (seperti bank, lembaga pemerintah, atau toko online). Modus yang sering digunakan termasuk phishing melalui WhatsApp, email, dan media sosial.

c. Gangguan Privasi dan Tekanan Sosial

Kebocoran data pribadi seperti alamat, nomor telepon, atau foto pribadi

dapat menyebabkan pelecehan daring (*cyber harassment*) dan tekanan psikologis. Bagi masyarakat kecil, kehilangan rasa aman digital sama beratnya dengan kehilangan barang berharga.

3. Dampak bagi Negara dan Keamanan Nasional

Dampak kebocoran data tidak berhenti di tingkat individu atau daerah. Ketika data strategis bocor, misalnya data kependudukan, keuangan, atau infrastruktur digital maka stabilitas nasional ikut terancam.

a. Ancaman terhadap Ketahanan Nasional

Data adalah aset strategis. Jika data warga, instansi, atau sistem pemerintahan jatuh ke pihak asing atau kelompok kriminal internasional, maka bisa digunakan untuk spionase, manipulasi kebijakan, atau serangan digital lanjutan.

Contoh: Serangan siber terkoordinasi terhadap sistem pelayanan publik bisa melumpuhkan layanan administratif di beberapa daerah sekaligus.

b. Gangguan terhadap Reputasi Pemerintah Indonesia

Setiap kebocoran besar yang terjadi akan menjadi sorotan nasional dan internasional. Kredibilitas pemerintah dalam mengelola data warganya akan dipertanyakan, terutama dalam kerja sama internasional dan investasi digital.

c. Dampak Sosial dan Ekonomi Jangka Panjang

Ketika masyarakat kehilangan kepercayaan terhadap keamanan data, mereka menjadi enggan menggunakan layanan digital. Hal ini dapat memperlambat transformasi digital yang sedang dijalankan oleh pemerintah pusat dan daerah.

E. Upaya Pencegahan dan Mitigasi Kebocoran Data

Kebocoran data bisa dicegah asalkan ada **disiplin, kesadaran, dan sistem pengamanan yang diterapkan secara konsisten.** Pencegahan bukan hanya tanggung

jawab petugas IT, tetapi juga setiap ASN dan masyarakat yang mengakses, menyimpan, atau membagikan informasi digital. Langkah-langkah berikut dibagi berdasarkan peran masing-masing pihak agar mudah diterapkan di lapangan.

1. Upaya Pencegahan untuk ASN

ASN memegang peran penting karena mereka adalah **penjaga utama data publik.** Kebanyakan kebocoran yang terjadi di instansi pemerintah daerah berawal dari hal-hal sederhana yang seharusnya bisa dihindari. Berikut praktik terbaik (*best practices*) yang wajib diterapkan:

a. Gunakan Perangkat dan Akun Resmi Instansi

- Semua pekerjaan kedinasan harus dilakukan menggunakan akun dan perangkat resmi, misalnya domain email **@klungkungkab.go.id**.
- Hindari menyimpan dokumen dinas di media pribadi seperti WhatsApp, Google Drive pribadi, atau laptop keluarga.
- Gunakan jaringan internet kantor atau VPN yang disediakan instansi.

📌 *Alasan:* Setiap data yang keluar dari sistem resmi sulit diawasi dan berpotensi bocor tanpa disadari.

b. Terapkan Pengamanan Berlapis

- Gunakan **kata sandi yang kuat** dan ubah secara berkala.
- Aktifkan **autentikasi dua langkah (2FA)** untuk semua akun penting.
- Hindari mengklik tautan mencurigakan dari email atau pesan tidak dikenal.

🧠 *Ingat: Ransomware* dan *malware* sering masuk melalui file lampiran palsu dengan nama yang terlihat resmi seperti *"Surat Edaran ASN 2025.pdf"*.

c. Batasi Akses Berdasarkan Tugas

- Tidak semua pegawai harus memiliki akses penuh ke seluruh data.
- Gunakan sistem **Role-Based Access Control (RBAC)**: akses dibatasi sesuai jabatan atau tanggung jawab.
- Nonaktifkan segera akun pegawai yang sudah mutasi atau pensiun.

🔐 *Tujuan:* Mencegah kebocoran dari pihak dalam (*internal leakage*).

d. Pastikan Backup dan Audit Sistem Rutin

- Lakukan pencadangan data *(backup*) secara berkala, harian atau mingguan.
- Simpan salinan data penting di tempat terpisah dari sistem utama.
- Audit keamanan digital minimal dua kali setahun bersama Dinas Kominfo atau CSIRT daerah.

💾 *Prinsip 3-2-1 Backup:* 3 salinan data, 2 media berbeda, 1 di lokasi berbeda.

e. Ikuti Pelatihan Keamanan Data Secara Berkala

- ASN wajib memahami dasar-dasar keamanan siber sesuai arahan **BSSN dan Kominfo**.
- Pemerintah daerah perlu mengadakan simulasi kebocoran data minimal satu kali dalam setahun.

📣 *Tujuan:* Meningkatkan kesadaran dan kemampuan ASN menghadapi ancaman siber aktual.

2. Upaya Pencegahan untuk Masyarakat

Masyarakat juga memiliki peran besar dalam menjaga keamanan data pribadi. Kebanyakan kebocoran data individu terjadi karena **kurangnya kehati-hatian saat berinteraksi di dunia digital.** Berikut langkah sederhana namun penting yang bisa diterapkan:

a. Jaga Kerahasiaan Data Pribadi

- Jangan pernah membagikan **NIK, KK, nomor rekening, atau OTP (kode verifikasi)** kepada siapa pun melalui pesan, telepon, atau media sosial.
- Hindari mengunggah foto KTP atau dokumen pribadi di internet tanpa keperluan resmi.

🔒 *Ingat:* Data pribadi yang tersebar sulit dihapus dan bisa disalahgunakan untuk penipuan.

b. Gunakan Situs dan Aplikasi Resmi

- Pastikan situs tempat mengisi data memiliki tanda gembok (🔒) di bilah alamat dan domain yang jelas, misalnya **.go.id** untuk pemerintah.
- Hindari mengunduh aplikasi dari sumber tidak dikenal atau situs bajakan.
- Waspadai pesan yang mengarahkan ke tautan aneh seperti “klik di sini untuk hadiah”.

📱 *Tip:* Ketik langsung alamat situs resmi di browser, jangan lewat tautan dari pesan.

c. Perbarui Perangkat dan Gunakan Antivirus

- Aktifkan pembaruan otomatis pada HP dan komputer.
- Gunakan antivirus yang terpercaya, dan hindari mengabaikan peringatan keamanan.
- Jika menggunakan Wi-Fi publik, hindari membuka situs keuangan atau layanan penting.

💡 *Alasan:* Banyak peretasan terjadi karena sistem yang belum diperbarui masih memiliki celah lama.

d. Laporkan Jika Terjadi Indikasi Kebocoran

- Jika merasa data pribadi disalahgunakan (misalnya menerima pesan pinjol atau tagihan palsu), segera laporkan ke **CSIRT Klungkung** atau **Dinas Kominfo.**
- Simpan bukti percakapan, tangkapan layar, dan nomor pengirim.

📢 *Tujuan:* Pelaporan cepat membantu mencegah penyebaran lebih luas.

3. Upaya Pencegahan untuk Pemerintah Daerah

Pemerintah daerah bertanggung jawab membangun sistem keamanan yang kuat serta melindungi data masyarakat. Langkah-langkah berikut perlu dijadikan standar kebijakan operasional di seluruh instansi:

a. Audit Keamanan dan Penilaian Risiko
    - Lakukan audit sistem informasi minimal dua kali setahun.
    - Identifikasi titik rawan kebocoran seperti server publik, API, atau sistem lama.
    - Gunakan standar keamanan **ISO/IEC 27001** atau pedoman BSSN terbaru.

b. Bentuk dan Fungsikan CSIRT Daerah
    - CSIRT (*Computer Security Incident Response Team*) menjadi garda depan dalam menanggapi insiden siber.
    - Tim ini harus aktif melakukan:
        - monitoring keamanan 24 jam,
        - investigasi insiden kebocoran, dan
        - sosialisasi keamanan digital ke OPD dan masyarakat.

    CSIRT Klungkung sudah dibentuk tinggal memastikan seluruh ASN tahu prosedur pelaporannya.

c. Tingkatkan Literasi Keamanan Digital ASN dan Warga
    - Buat modul edukasi, poster, dan video pendek yang mudah dipahami masyarakat.
    - Lakukan kampanye berkala seperti *"Jaga Datamu, Lindungi Klungkung Digital"*.
    - Gandeng sekolah, UMKM, dan organisasi masyarakat untuk memperluas jangkauan edukasi.

d. Terapkan Kebijakan dan SOP Perlindungan Data
    - Setiap OPD harus memiliki SOP penanganan data pribadi.

- Pegawai yang melanggar prosedur harus mendapat pembinaan atau sanksi tegas.
- Gunakan peraturan terbaru seperti **Surat Edaran Bersama Mendagri–BSSN 2025** sebagai acuan.

F. Kebijakan dan Dasar Hukum Terkait Kebocoran Data

Kebocoran data bukan sekadar masalah teknis, tetapi juga **isu hukum dan tata kelola pemerintahan.** Oleh karena itu, setiap ASN dan masyarakat perlu memahami **aturan yang melindungi data pribadi dan mengatur penanganan insiden siber**. Pemahaman hukum ini bukan hanya untuk menegakkan aturan, tetapi juga untuk membangun **rasa tanggung jawab dan kepatuhan digital**.

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

UU ini menjadi tonggak utama perlindungan data di Indonesia. Mulai berlaku penuh sejak **Oktober 2024**, setelah masa transisi dua tahun, sehingga **tahun 2025 adalah masa penerapan aktifnya.**

Pokok penting yang perlu dipahami:

a. **Pasal 2** menegaskan bahwa data pribadi adalah bagian dari hak privasi setiap warga negara.
b. **Pasal 20–30** mengatur kewajiban pengendali data (seperti instansi pemerintah dan perusahaan) untuk menjaga keamanan data pribadi dari kebocoran, penyalahgunaan, dan akses ilegal.
c. **Pasal 55–58** memuat sanksi administratif dan pidana bagi pihak yang lalai atau dengan sengaja membocorkan data.

📌 *Artinya:* ASN yang lalai dalam melindungi data masyarakat bisa dikenakan sanksi sesuai UU PDP, sementara masyarakat berhak menuntut perlindungan dan ganti rugi.

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

Peraturan ini membentuk **BSSN sebagai lembaga resmi negara** yang bertanggung jawab terhadap keamanan siber nasional. Dalam konteks kebocoran data, BSSN berperan sebagai **koordinator utama** dalam penanganan insiden siber di instansi pemerintah dan sektor publik.

Fungsi BSSN terkait kebocoran data:

a. Menyusun pedoman keamanan siber nasional.
b. Melakukan pemantauan dan investigasi insiden kebocoran data.
c. Memberikan asistensi teknis kepada pemerintah daerah dan lembaga publik.
d. Mengembangkan *Computer Security Incident Response Team* (CSIRT) di setiap daerah.

📍 *Contoh aktual:* Kabupaten Klungkung telah memiliki **CSIRT Daerah** yang berkoordinasi langsung dengan BSSN untuk melaporkan dan menangani insiden siber lokal.

3. Surat Edaran Bersama (SEB) Menteri Dalam Negeri dan Kepala BSSN Tahun 2025

Surat edaran ini dikeluarkan untuk memperkuat penerapan keamanan siber di lingkungan pemerintahan daerah. Walaupun bersifat administratif, SEB ini menjadi **acuan operasional bagi ASN dan instansi daerah.**

Isi utama SEB Mendagri–BSSN 2025:

a. Setiap pemerintah daerah wajib memiliki **rencana keamanan siber daerah (Local Cybersecurity Plan).**
b. ASN yang mengelola sistem informasi wajib mengikuti **pelatihan keamanan data minimal dua kali setahun.**
c. Dinas Kominfo daerah wajib melaporkan setiap insiden kebocoran data ke BSSN paling lambat **24 jam setelah kejadian.**

📢 *Manfaat bagi ASN:* Memastikan keamanan sistem tidak hanya tanggung jawab teknis, tapi juga bagian dari kinerja dan integritas pelayanan publik.

📢 *Manfaat bagi masyarakat:* Menjamin hak atas perlindungan data dalam layanan publik digital.

4. Peraturan Kepala BSSN Nomor 4 Tahun 2024 tentang Tata Kelola Keamanan Data Pemerintah Daerah

Peraturan ini menjadi **panduan teknis bagi instansi daerah** untuk mengelola dan melindungi data elektronik. Aturan ini menyesuaikan perkembangan serangan siber dan kebocoran data yang meningkat tajam selama 2020–2024.

Poin penting dalam Perka BSSN 4/2024:

a. Setiap OPD wajib memiliki **Data Protection Officer (DPO)** atau pejabat yang ditunjuk khusus untuk pengawasan keamanan data.
b. Diperlukan penerapan sistem keamanan berbasis prinsip **CIA Triad**:
    - **Confidentiality** (kerahasiaan),
    - **Integrity** (keutuhan), dan
    - **Availability** (ketersediaan).
c. Penerapan **Sistem Manajemen Keamanan Informasi (SMKI)** yang sesuai standar **ISO/IEC 27001:2022**.

🔐 *Makna bagi ASN:* Keamanan data bukan sekadar alat, tetapi bagian dari tata kelola pemerintahan yang transparan dan akuntabel.

5. Pedoman Nasional Penanganan Insiden Siber oleh BSSN (2025 Update)

Dokumen pedoman ini diperbarui setiap tahun dan menjadi **referensi nasional** dalam menangani kebocoran data dan insiden siber di berbagai sektor.

Fokus pedoman edisi 2025:

a. Penguatan sistem pelaporan insiden secara digital melalui *Cyber Security Incident Management System (C-SIMS)*.
b. Penggunaan teknologi deteksi dini berbasis **AI dan machine learning** untuk mencegah kebocoran data.
c. Kewajiban pemerintah daerah melaporkan hasil audit keamanan tahunan ke BSSN.

🧩 *Tujuannya:* Meningkatkan respons cepat terhadap kebocoran data, serta mendorong kolaborasi antara pusat dan daerah dalam keamanan digital nasional.

6. Peraturan Daerah dan Inisiatif Lokal

Beberapa pemerintah daerah, termasuk **Kabupaten Klungkung**, mulai merancang kebijakan turunan dari SEB dan Perka BSSN. Klungkung misalnya, tengah mengembangkan:

a. **SOP Penanganan Data Pribadi Layanan Publik Daerah (SOP PDP-LPD 2025).**
b. **Kebijakan Backup Terpusat untuk Sistem Pelayanan Online.**
c. **Program Edukasi "Waspada Data Bocor" untuk ASN dan Masyarakat.**

🌐 *Makna lokal:* Keamanan siber tidak berhenti pada aturan nasional, tetapi diterjemahkan dalam tindakan nyata di tingkat daerah agar masyarakat merasakan langsung manfaatnya.

7. Kolaborasi antara Pemerintah, Dunia Usaha, dan Masyarakat

Kebocoran data sering terjadi karena **rantai ekosistem digital yang saling terhubung.** Oleh sebab itu, pemerintah daerah didorong untuk bekerja sama dengan sektor swasta dan masyarakat sipil.

Kolaborasi penting:

a. Dunia usaha: wajib menerapkan keamanan data pelanggan sesuai UU PDP.
b. Lembaga pendidikan: membantu meningkatkan literasi digital masyarakat.
c. Masyarakat: berperan aktif melapor dan ikut menjaga data pribadi dalam aktivitas daring.

🤝 *Kunci sukses:* Ekosistem digital yang aman hanya dapat terbentuk bila semua pihak saling percaya dan saling menjaga.

Pertanyaan Reflektif

1. Sebagai ASN atau masyarakat, pernahkah Anda menyadari data pribadi Anda tersimpan dalam sistem digital tertentu (misalnya, layanan kesehatan, administrasi kependudukan, atau aplikasi perizinan)? Menurut Anda, sejauh mana data tersebut aman dari risiko kebocoran?
2. Jika suatu instansi pemerintah mengalami kebocoran data, siapa saja yang akan terdampak dan bagaimana pengaruhnya terhadap kepercayaan publik terhadap pemerintah daerah?
3. Menurut Anda, apakah kebocoran data lebih banyak disebabkan oleh faktor teknis (sistem) atau faktor manusia (kelalaian pengguna)? Jelaskan alasan Anda.
4. Bagaimana seharusnya sikap ASN ketika mengetahui ada kemungkinan kebocoran data pada sistem di instansinya? Apakah cukup melapor, atau perlu langkah konkret lainnya?
5. Sebagai masyarakat digital, langkah apa yang bisa Anda lakukan agar tidak ikut memperburuk dampak kebocoran data (misalnya, tidak menyebarkan data yang bocor di media sosial)?
6. Setelah memahami adanya UU Perlindungan Data Pribadi dan peraturan BSSN, apakah Anda merasa sudah terlindungi secara hukum? Mengapa demikian?
7. Bagaimana cara sederhana membangun kolaborasi antara ASN dan masyarakat untuk mencegah kebocoran data di tingkat daerah, khususnya di Kabupaten Klungkung?

DAFTAR PUSTAKA

Cindy Sabrina. (2025). Krisis Keamanan Data Publik Dan Urgensi Kedaulatan Data Di Era Governansi Digital. *Jurnal Transformasi Administrasi*, *15*(01), 3–6. https://doi.org/10.56196/jta.v15i01.500

Dinata, A. C., & Syafaat, A. (2025). *Peran BSSN dalam Menangani Ancaman Siber di Indonesia*. *01*(01).

Handayani, A. A., Izzati, B. N., Nur'azzah, D., Khoirunnisa, & Prawira, I. F. A. (2025). Strategi Mengatasi Data Breaches di Era Industri 4.0: Kasus Data Breaches Bank Rakyat Indonesia. *Jurnal Manajemen Dan Bisnis Ekonomi*, *3*(2), 161–175. https://doi.org/10.54066/jmbe-itb.v3i2.3170

Hisyam, F. R., & Sekti Kartika Dini. (2023). Persespsi Aparatur Sipil Negara (ASN) Kabupaten Sleman Terhadap Keamanan Data Pribadi dengan Metode Statistika Deskriptif. *Emerging Statistics and Data Science Journal*, *1*(3), 263–277. https://doi.org/10.20885/esds.vol1.iss.3.art34

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. *Jurnal Studi Komunikasi Dan Media*, *24*(1), 37. https://doi.org/10.31445/jskm.2020.2945

Lesmana, R., & Nasution, M. I. P. (2025). Kebocoran Data di Media Sosial : Analisis Pola dan Strategi Pencegahannya. *Socius: Jurnal Administrasi Publik*, *2*(10), 123–128. https://doi.org/10.5281/zenodo.15388529

Nuruzzaman, M. T., Wirawan, A., Muslimah, U. S., & Setyono, Y. (2025). Kesiapan Aparatur Sipil Negara (ASN) Terhadap Implementasi UU Pelindungan Data Pribadi (UU PDP). *Cyber Security Dan Forensik Digital*, *8*(1), 63–71. https://doi.org/10.14421/csecurity.2025.8.1.4999

Putra, R. K., Agustin, Y., Nurul Ihsan, L., & Ahmad Dafiqi, Z. (2025). Institutional Dysfunction in Personal Data Protection: A Legal-Political Analysis Based on New

Institutional Theory. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *3*(2), 938–949. https://doi.org/10.51903/bkktey52

Ramadhani, E. H., Enriko, I. K. A., & Sari, E. L. I. P. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *6*(1), 570–580. https://doi.org/10.35870/jimik.v6i1.1210

Sembiring, F., & Pattihahuan, F. M. (2024). *PERAN BADAN SIBER DAN SANDI NEGARA DALAM KASUS SERANGAN SIBER YANG MENGAKIBATKAN KEBOCORAN DATA PRIBADI PUSAT DATA NASIONAL SEMENTARA 2 (PDNS2)*. *2*, 116–134.

Soleh, M., & Tjenreng, Z. (2024). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics*, *11*(1), 1–10. https://doi.org/10.25299/jkp.2025.vol11(1).20524

Sorisa, C., & Kiareni, C. L. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *Jurnal Sains Student Research*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996