KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 3: Perlindungan Data & Etika Digital

Subtopik 3.4: Jejak Digital & Keamanan Privasi Online

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 hingga membahas subtopik penting mengenai Jejak Digital dan Keamanan Privasi Online. Di era digital saat ini, setiap aktivitas kita di internet, baik berupa unggahan, komentar, maupun pencarian, meninggalkan jejak yang dapat ditelusuri. Jejak digital dapat menjadi aset yang memperkuat reputasi pribadi dan lembaga, namun juga bisa menjadi ancaman bila tidak dikelola dengan bijak.

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung mampu memahami pentingnya menjaga privasi daring serta mengelola rekam jejak digital dengan tanggung jawab. ASN diharapkan dapat menjadi teladan dalam menjaga etika dan keamanan informasi di ruang siber, sementara masyarakat mampu melindungi diri dari risiko penyalahgunaan data dan reputasi di dunia maya. 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-jenis jejak digital (aktif dan pasif).
2. Mengidentifikasi risiko dari jejak digital yang tidak dikelola dengan baik.
3. Menerapkan langkah praktis untuk menjaga keamanan privasi daring.
4. Membedakan antara aktivitas daring yang etis dan yang berpotensi melanggar privasi.
5. Membangun reputasi digital positif sebagai ASN dan warga digital Kabupaten Klungkung.

Sasaran Peserta

1. ASN: agar memahami tanggung jawab dan etika dalam penggunaan media digital, serta mampu mengelola jejak digital dengan bijak untuk menjaga profesionalisme dan citra positif instansi pemerintah.
2. Masyarakat: agar lebih memahami pentingnya privasi digital, mampu mengenali risiko pencurian data, dan menerapkan kebiasaan aman di media sosial serta platform daring lainnya.

A. Konsep Jejak Digital (Digital Footprint)

Bayangkan setiap langkah Anda di dunia maya meninggalkan bekas, seperti jejak kaki di pasir. Bedanya, **jejak digital tidak mudah hilang,** ia bisa disimpan, dianalisis, bahkan disebarkan oleh banyak pihak tanpa sepengetahuan kita.

Setiap kali Anda:

a. Mengirim email atau pesan WhatsApp,
b. Mengunggah foto di Instagram,
c. Mengisi formulir daring, atau
d. Sekadar mencari sesuatu di Google

Semuanya **meninggalkan data** di server internet. Inilah yang disebut **jejak digital (digital footprint)**, yaitu kumpulan data tentang aktivitas daring seseorang yang terekam secara permanen di dunia maya.

Ada dua jenis utama jejak digital:

a. **Jejak Digital Aktif**

   👉 Jejak yang kita buat secara sadar.

   Contohnya: memposting status, berkomentar di media sosial, mengisi survei online, atau mendaftar di situs web.
   Jejak ini biasanya tampak publik dan bisa dengan mudah dilacak kembali ke pemiliknya.

b. **Jejak Digital Pasif**

   👉 Jejak yang tercipta tanpa disadari.

   Contohnya: alamat IP yang direkam situs web, lokasi GPS dari foto, cookie browser, atau histori pencarian yang disimpan otomatis.
   Meskipun tak terlihat, jejak ini justru lebih berisiko karena sering dikumpulkan tanpa izin jelas.

📍 *Contoh nyata:*

Seorang ASN yang mengunggah foto kegiatan kantor di media sosial tanpa

menonaktifkan “lokasi otomatis”, secara tidak sengaja menampilkan koordinat gedung pemerintahan. Data itu bisa dipakai untuk pemetaan digital oleh pihak luar.

🎯 **Mengapa Penting Dipahami?**

Karena **jejak digital adalah identitas diri di dunia maya**. Bagi ASN, ia mencerminkan integritas dan profesionalitas lembaga. Bagi masyarakat, ia menjadi cerminan karakter pribadi dan sumber reputasi digital. Jejak yang baik bisa meningkatkan kepercayaan dan peluang; tetapi jejak yang buruk, seperti komentar kasar, unggahan palsu, atau data pribadi yang bocor, bisa menimbulkan kerugian jangka panjang, bahkan bertahun-tahun setelahnya.

💡 **Ingat:**

“Apa pun yang Anda unggah di internet, bisa menjadi publik selamanya.”

Menjaga jejak digital berarti menjaga nama baik, privasi, dan keamanan diri di dunia maya yang tak pernah benar-benar terhapus.

B. Mengapa Jejak Digital Perlu Dikelola?

Jejak digital bukan hanya rekaman aktivitas, tetapi **cermin kepribadian dan kredibilitas** seseorang di dunia maya. Apa pun yang kita bagikan, sukai, atau komentari, akan membentuk persepsi publik terhadap diri kita, terutama bagi **Aparatur Sipil Negara (ASN)** yang mewakili wajah pemerintah di ruang digital.

1. Untuk Melindungi Reputasi Pribadi dan Instansi

Setiap unggahan bisa menjadi bahan penilaian. Bagi ASN, satu komentar emosional atau unggahan yang mengandung ujaran kebencian dapat merusak citra instansi. Bagi masyarakat, unggahan berlebihan atau informasi pribadi yang terbuka bisa dimanfaatkan oleh pihak tidak bertanggung jawab.

📍 *Contoh nyata:*

Sebuah tangkapan layar percakapan lama dapat muncul kembali dan digunakan untuk menjatuhkan reputasi seseorang, meskipun sudah dihapus.

“Jejak digital tidak mengenal masa lalu. Apa yang pernah dibagikan, bisa muncul kembali

kapan saja."

2. Untuk Mencegah Penyalahgunaan Data Pribadi

Banyak pelaku kejahatan siber mengumpulkan data dari jejak digital. Dari nama lengkap, lokasi, hingga foto, semua bisa dipakai untuk penipuan, pemalsuan identitas, atau peretasan akun.

💡 **Tips singkat:**

a. Jangan membagikan foto dokumen resmi atau kartu identitas.
b. Nonaktifkan fitur lokasi saat mengunggah foto.
c. Hindari menulis informasi pribadi seperti alamat atau nomor HP di kolom komentar publik.

3. Untuk Menunjukkan Etika dan Tanggung Jawab Digital

Bagi ASN, jejak digital adalah bagian dari **etika profesi dan tanggung jawab publik**. Komentar di media sosial, unggahan, hingga tanda suka ("like") dapat dimaknai sebagai sikap resmi. Sementara bagi masyarakat, jejak digital menunjukkan tingkat literasi dan kecerdasan digital seseorang. Di era digital, setiap klik adalah pernyataan, dan setiap unggahan adalah jejak sejarah Anda.

4. Untuk Menghindari Dampak Jangka Panjang

Sekali data tersebar, sulit dikendalikan kembali. Banyak kasus pelamar kerja, ASN, atau tokoh publik ditolak karena unggahan lama yang tidak pantas, bahkan yang dibuat bertahun-tahun lalu. Jejak digital bisa menjadi aset atau bumerang. Maka, **mengelolanya secara sadar** adalah bentuk tanggung jawab pribadi dan sosial di era digital.

C. Jenis-Jenis Jejak Digital dan Contoh Kasus Nyata

Setiap aktivitas online meninggalkan jejak. Namun, tidak semua jejak terlihat jelas. Ada yang tampak di layar, ada pula yang tersimpan diam-diam di sistem digital. Memahami jenisnya membantu kita **menyadari apa yang sebenarnya terekam tentang diri kita di dunia maya**.

1. Jejak Digital Aktif

Ini adalah semua hal yang *sengaja* kita bagikan atau lakukan di internet. Contoh:

a. Unggahan status di Facebook, Instagram, atau X (Twitter).
b. Komentar di berita online.
c. Mengisi formulir daring atau mendaftar akun baru.
d. Mengirim email, mengunggah dokumen ke Google Drive atau e-Office.

📍 **Risikonya:**

Unggahan yang bersifat pribadi bisa disalahgunakan atau disebarluaskan tanpa konteks. Komentar yang emosional dapat direkam sebagai bukti pelanggaran etika, terutama bagi ASN.

🧩 **Contoh Kasus:**

Pada 2024, seorang ASN di daerah Jawa Tengah mendapat sanksi disiplin karena komentar bernada provokatif di media sosial pribadinya. Meskipun dilakukan di luar jam kerja, unggahan tersebut dianggap mencederai netralitas ASN karena masih terkait dengan jabatan publiknya.

2. Jejak Digital Pasif

Jejak ini terekam **tanpa disadari** oleh pengguna. Contoh:

a. Lokasi GPS saat menggunakan aplikasi.
b. Cookies dan riwayat pencarian internet.
c. Metadata dari foto dan video (waktu, lokasi, perangkat).
d. Aktivitas login yang tercatat di server.

📍 **Risikonya:**

Data lokasi dan kebiasaan online bisa dipakai untuk profiling oleh pihak ketiga misalnya perusahaan iklan, peretas, atau bahkan kampanye politik digital.

💡 **Tips Aman:**

a. Bersihkan riwayat pencarian dan cookies secara berkala.
b. Nonaktifkan izin lokasi kecuali saat dibutuhkan.
c. Gunakan mode “incognito” untuk menghindari penyimpanan otomatis riwayat browsing.

3. Jejak Digital Profesional

Jejak ini mencakup aktivitas yang berkaitan dengan pekerjaan atau lembaga tempat kita bekerja.

Bagi ASN, termasuk:

a. Email dinas dengan domain .go.id
b. Dokumen kerja yang diunggah di platform e-Office
c. Aktivitas daring yang mencantumkan jabatan atau instansi

Risikonya:

Data kerja yang tersebar tanpa izin bisa menjadi celah keamanan instansi. Selain itu, perilaku pribadi yang kurang pantas di media sosial dapat merusak citra profesional ASN atau lembaga.

Contoh Kasus:

Beberapa akun palsu di media sosial pernah menggunakan nama instansi pemerintah untuk menipu masyarakat dengan modus “bantuan sosial”. Jejak digital resmi ASN yang mudah ditemukan tanpa pengaturan privasi turut dimanfaatkan pelaku untuk memperkuat kredibilitas palsu.

4. Jejak Digital Sosial

Jejak sosial berasal dari interaksi kita dengan orang lain secara daring. Contoh:

a. Tanda “suka” (like), komentar, dan berbagi (share).
b. Riwayat percakapan di grup WhatsApp atau Telegram.
c. Aktivitas di forum komunitas online.

Risikonya:

Apa yang kita sukai atau bagikan bisa mencerminkan pandangan politik, agama, atau

preferensi pribadi yang mungkin disalahartikan. Bagi ASN, tindakan sederhana seperti "menyukai" unggahan politik bisa dianggap pelanggaran netralitas.

💬 *Ingat:*

"Tidak semua yang menarik untuk dikomentari harus dikomentari. Kadang, diam adalah bentuk kehati-hatian digital."

5. Jejak Digital yang Dihapus (Tapi Tetap Ada)

Banyak orang mengira bahwa menghapus unggahan berarti menghapus jejaknya. Padahal, **data digital tidak benar-benar hilang**. Server platform, mesin pencari, atau pihak ketiga bisa saja masih menyimpan salinannya.

🧩 *Contoh:*

Unggahan foto pribadi di media sosial yang sudah dihapus bisa tetap muncul di hasil pencarian Google selama beberapa minggu, atau bahkan bertahun-tahun.

💡 *Solusi:*

Gunakan fitur "hapus permanen" (*permanent delete*) jika tersedia, dan ajukan permintaan penghapusan ke platform bila diperlukan (misalnya, fitur "*Right to be Forgotten*" di Google).

Setiap klik, unggahan, dan komentar
adalah bagian dari cerita digital kita.
Maka, bijaklah menulis, berhati-hatilah membagikan,
dan sadarlah meninggalkan jejak.

D. Cara Mengelola Jejak Digital dan Melindungi Privasi Online

Mengelola jejak digital bukan berarti menghapus semua aktivitas daring, tetapi **menjaga keseimbangan antara keterbukaan dan keamanan**. Setiap orang berhak tampil aktif di ruang digital, asal tahu cara melindungi diri dan menjaga reputasi.

Berikut panduan langkah-langkah yang dapat diterapkan:

1. Kendalikan Informasi Pribadi yang Dibagikan

Sebelum memposting sesuatu, tanyakan pada diri sendiri:

"Apakah informasi ini aman jika dilihat oleh atasan, rekan kerja, atau publik?"

🧩 *Tips:*

a. Hindari membagikan data pribadi seperti alamat, nomor telepon, atau detail keluarga.
b. Jangan unggah foto dokumen resmi (KTP, KK, SK ASN, tiket perjalanan).
c. Pisahkan akun pribadi dan akun profesional (khusus ASN, gunakan akun resmi .go.id untuk urusan kedinasan).

📍 *Contoh:*

Unggahan foto seragam dinas dengan lokasi kantor aktif bisa dimanfaatkan pihak tak bertanggung jawab untuk keperluan penipuan atau doxing (pengungkapan data pribadi tanpa izin).

2. Atur Privasi Akun Media Sosial

Gunakan fitur keamanan yang sudah disediakan platform:

a. Ubah pengaturan profil menjadi **"private"** atau ***"friends only."***
b. Nonaktifkan fitur *tagging otomatis* untuk menghindari foto tidak pantas muncul di profil.
c. Periksa izin aplikasi yang terhubung ke akun media sosial, hapus yang mencurigakan.

💡 *Ingat:* Privasi bukan berarti menutup diri, melainkan **mengatur siapa yang boleh tahu tentang diri Anda**.

3. Gunakan Identitas Digital Secara Profesional (Terutama ASN)

ASN adalah representasi pemerintah, bahkan di media sosial pribadi. Gunakan bahasa sopan, hindari komentar provokatif, dan pastikan informasi yang dibagikan faktual.

🧩 *Tips:*

a. Jangan menanggapi isu politik atau SARA di akun publik.
b. Gunakan email resmi instansi untuk urusan kedinasan.
c. Jika membagikan informasi instansi, pastikan sumbernya valid dan sudah mendapat izin publikasi.

📍 *Contoh:*

ASN yang tidak sengaja membagikan dokumen internal tanpa izin dapat dikenai sanksi karena dianggap melanggar kerahasiaan data publik.

4. Pantau Jejak Digital Anda Secara Berkala

Cari nama Anda di Google atau mesin pencari lain setidaknya sebulan sekali. Langkah sederhana ini bisa membantu mendeteksi apakah ada informasi pribadi yang bocor atau disalahgunakan.

💡 *Langkah praktis:*

a. Gunakan fitur **"Google Alert"** untuk memantau bila nama Anda muncul di situs baru.
b. Hapus akun lama yang sudah tidak digunakan.
c. Mintalah penghapusan konten ke platform jika mengandung data pribadi.

5. Gunakan Alat Keamanan Tambahan

a. Gunakan teknologi untuk melindungi diri, bukan sekadar sebagai pengguna pasif.
b. Aktifkan **Two-Factor Authentication (2FA)** di semua akun penting.
c. Gunakan **password manager** agar tidak lupa atau menggunakan kata sandi yang sama.
d. Instal **VPN** saat mengakses jaringan publik.
e. Gunakan browser dengan fitur anti-tracking seperti Brave atau Mozilla Firefox.

6. Bijak dalam Membagikan Informasi Orang Lain

Etika digital bukan hanya tentang melindungi diri sendiri, tetapi juga menghormati privasi orang lain.

📍 *Jangan lakukan hal berikut:*

a. Mengunggah foto orang lain tanpa izin.

b. Menyebarkan tangkapan layar percakapan pribadi.
c. Meneruskan informasi pribadi (nomor HP, alamat, data kesehatan) ke grup publik.

🧩 *Ingat:* Sekali data tersebar, tidak ada jaminan bisa ditarik kembali.

7. Pahami Hak Anda atas Privasi Digital

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi memberi hak kepada setiap warga negara untuk:

a. Mengetahui data apa yang dikumpulkan oleh pihak tertentu.
b. Meminta perbaikan atau penghapusan data pribadi.
c. Menolak pemrosesan data tanpa izin.

8. Bangun Jejak Digital Positif

Tidak semua jejak digital harus dihindari. Gunakan internet untuk **meningkatkan citra positif**:

a. Bagikan prestasi kerja, kegiatan sosial, atau kontribusi di instansi.
b. Berpartisipasi dalam diskusi publik dengan sopan dan berbasis data.
c. Gunakan media sosial untuk edukasi, bukan provokasi.
d. Jejak digital yang positif akan menjadi portofolio Anda di masa depan.

📊 **Fakta 2025 – Kominfo & BSSN:**

62% ASN aktif di media sosial profesional (LinkedIn, Facebook for Work).
78% masyarakat menggunakan media sosial lebih dari 3 jam per hari.
Namun, hanya 35% yang rutin memeriksa pengaturan privasi akunnya.

E. Prinsip Etika Digital dan Tanggung Jawab ASN & Masyarakat

Etika digital adalah pedoman moral dan perilaku ketika kita berinteraksi di dunia maya. Jika dunia nyata mengenal sopan santun dan aturan hukum, maka dunia digital pun memiliki prinsip serupa, hanya saja wujudnya berupa **tanggung jawab, kehati-hatian, dan kesadaran digital.** Baik ASN maupun masyarakat, sama-sama memiliki peran penting dalam menciptakan ekosistem digital yang **aman, beradab, dan saling**

menghormati.

1. Berpikir Sebelum Berbagi

Sebuah unggahan sederhana bisa berdampak besar. Sebelum menekan tombol "kirim" atau "bagikan", tanyakan tiga hal:

✅ Apakah informasi ini benar?

✅ Apakah pantas untuk dibagikan?

✅ Apakah akan berdampak positif bagi orang lain?

📍 *Bagi ASN:*

Unggahan di media sosial mencerminkan citra instansi. Hindari menyebarkan opini pribadi yang bisa dianggap mewakili lembaga, terutama soal isu politik, agama, dan kebijakan publik.

📍 *Bagi masyarakat:*

Periksa kembali kebenaran berita sebelum membagikannya. Jangan mudah terprovokasi oleh informasi yang belum tentu benar.

2. Hormati Privasi Diri dan Orang Lain

Etika digital tidak hanya soal "apa yang kita katakan", tapi juga **apa yang kita jaga untuk tidak diungkap.**

🧩 *Prinsip utama:*

a. Jangan mengambil atau membagikan foto, video, atau data pribadi tanpa izin.
b. Hargai privasi rekan kerja dan keluarga di ruang digital.
c. Hindari mengomentari hal pribadi di media sosial yang bersifat publik.

💡 *Contoh sederhana:*

Mengunggah foto rapat internal atau dokumen instansi ke grup WhatsApp publik tanpa izin bisa dianggap pelanggaran etika dan keamanan data.

3. Bangun Citra Profesional di Dunia Digital (Terutama untuk ASN)

ASN merupakan wajah pemerintah, bahkan ketika sedang tidak bekerja. Oleh karena itu, jaga perilaku digital agar tetap profesional dan berintegritas.

📌 *Praktik baik ASN di media digital:*

a. Menggunakan bahasa yang sopan dan netral dalam komentar publik.
b. Menghindari menyukai (*like*) atau membagikan unggahan yang bersifat ujaran kebencian.
c. Membangun profil digital yang mencerminkan nilai ASN: **berakhlak, melayani, dan netral.**
d. Tidak menggunakan media sosial untuk menyerang, menjelekkan, atau membocorkan informasi internal.

🧭 *Ingat:* Jejak digital ASN adalah representasi etika birokrasi modern.

4. Jaga Netiket (Network Etiquette) di Dunia Maya

Netiket adalah tata krama berkomunikasi di dunia digital. Ia menjadi panduan agar interaksi daring tetap santun dan tidak menimbulkan konflik.

📋 *Aturan sederhana netiket:*

a. Gunakan bahasa sopan dalam percakapan digital.
b. Jangan menulis huruf kapital seluruhnya (dianggap berteriak).
c. Gunakan emoji atau tanda baca secukupnya.
d. Hargai perbedaan pendapat tanpa menyerang pribadi.
e. Hindari menyebarkan konten provokatif, vulgar, atau diskriminatif.

💬 *Netiket bukan aturan tertulis, tapi mencerminkan kedewasaan digital seseorang.*

5. Hindari Ujaran Kebencian dan Hoaks

Di tahun 2025, ujaran kebencian dan penyebaran hoaks masih menjadi ancaman terbesar bagi keamanan digital dan kerukunan sosial. Berdasarkan laporan Kominfo (2024), terdapat lebih dari **600.000 unggahan bermuatan hoaks** di Indonesia dalam setahun terakhir.

📍 *Untuk ASN:*

Wajib menjaga netralitas dan tidak ikut menyebarkan hoaks atau opini politik. Jika menemukan berita mencurigakan, periksa di situs resmi seperti

https://cekhoaks.kominfo.go.id.

📍 *Untuk masyarakat:*

Laporkan akun penyebar hoaks ke platform (Facebook, X/Twitter, Instagram). Gunakan fitur "Laporkan" dan hindari memperpanjang penyebaran dengan komentar.

🧠 "Di dunia digital, jari kita bisa jadi sumber kebaikan, atau sumber masalah."

6. Gunakan Teknologi dengan Tujuan Positif

Etika digital tidak hanya menghindari hal buruk, tapi juga **menggunakan teknologi untuk hal baik**:

a. ASN dapat menggunakan media sosial untuk berbagi inovasi pelayanan publik, transparansi data, dan kegiatan sosial.
b. Masyarakat dapat memanfaatkannya untuk edukasi, promosi usaha lokal, dan literasi digital keluarga.

💡 *Contoh positif:*

ASN Klungkung yang membuat konten edukatif tentang keamanan data pribadi di Instagram berhasil meningkatkan kesadaran digital masyarakat sekitar.

7. Sadari Bahwa Dunia Digital Tidak Anonim

Banyak orang merasa aman di balik layar, tetapi kenyataannya:

a. Setiap komentar, unggahan, dan klik meninggalkan jejak digital yang bisa dilacak.
b. Hukum ITE dan UU PDP berlaku penuh untuk aktivitas daring.

Maka, setiap individu, baik ASN maupun masyarakat, harus menyadari konsekuensi dari tindakan digitalnya.

📍 *Ingat:*

Jejak digital yang bijak adalah aset reputasi. Jejak digital yang buruk adalah beban yang sulit dihapus.

8. Kolaborasi ASN dan Masyarakat dalam Menjaga Ekosistem Digital Sehat

Keamanan digital tidak bisa dicapai sendiri. Diperlukan kolaborasi dan tanggung jawab bersama:

a. ASN berperan sebagai panutan etika digital.
b. Masyarakat berperan sebagai pengguna cerdas dan pengawas sosial.
c. Pemerintah daerah, sekolah, dan komunitas digital dapat bekerja sama dalam kampanye literasi dan privasi online.

🤝 *Contoh praktik baik:*

Gerakan "#BijakDigitalKlungkung" yang diluncurkan tahun 2024 berhasil menurunkan penyebaran hoaks lokal hingga 40% dengan kolaborasi antara ASN muda, komunitas IT, dan tokoh masyarakat.

F. Studi Kasus dan Praktik Baik Etika & Privasi Digital (2023–2025)

Agar pemahaman tentang jejak digital dan privasi online tidak sekadar teori, mari kita pelajari beberapa **contoh nyata** dari kasus dan praktik baik yang terjadi di Indonesia, termasuk di lingkungan ASN dan masyarakat.

1. Kasus Pelanggaran Etika Digital ASN (Indonesia, 2024)

Pada tahun 2024, seorang ASN di salah satu pemerintah daerah diberhentikan karena unggahannya di media sosial yang bernada provokatif terkait isu politik. Unggahan tersebut viral dan dianggap melanggar prinsip **netralitas ASN** serta kode etik digital pemerintah.

📍 *Hasil investigasi:*

a. ASN tersebut menggunakan akun pribadinya, tetapi mencantumkan jabatan resmi pada profil.
b. Komentar yang ia tulis dianggap mewakili pandangan instansinya.
c. Jejak digitalnya digunakan sebagai bukti pelanggaran dalam pemeriksaan etik.

💬 *Pelajaran penting:*

Dunia digital tidak memisahkan antara "pribadi" dan "profesional". ASN tetap terikat etika birokrasi di ruang maya.

2. Kasus Kebocoran Data Akibat Unggahan Pribadi (2023)

Seorang masyarakat pengguna media sosial mengunggah foto KTP dan kartu keluarga untuk keperluan lomba daring. Beberapa hari kemudian, ia menerima puluhan panggilan penipuan dan tagihan pinjaman online atas namanya.

📍 *Analisis:*

a. Informasi pribadi yang dibagikan secara terbuka digunakan oleh pihak tidak bertanggung jawab.
b. Pelaku memanfaatkan data tersebut untuk registrasi akun pinjaman.

💡 *Pelajaran penting:*

Data pribadi bukan untuk konsumsi publik. Sekali diunggah, sulit dikendalikan kembali, karena jejak digital bersifat permanen.

3. Praktik Baik ASN Klungkung: "Digital Smart ASN" (2024)

Pemerintah Kabupaten Klungkung melalui program **Digital Smart ASN** berhasil meningkatkan kesadaran keamanan digital di kalangan pegawai. Setiap ASN mengikuti pelatihan tentang:

a. Pengamanan akun kerja (password & 2FA),
b. Etika bermedia sosial,
c. Penghapusan jejak digital yang berisiko,
d. Penerapan privasi dalam komunikasi dinas.

📈 *Dampak positif:*

a. Setelah satu tahun program berjalan:
b. Kasus penyalahgunaan akun dinas turun hingga 60%,
c. ASN lebih berhati-hati dalam menyampaikan opini di media sosial,
d. Muncul budaya saling mengingatkan soal etika digital di tempat kerja.

💬 *Pesan utama:*

ASN bukan hanya pelayan publik, tapi juga teladan etika digital bagi masyarakat.

4. Praktik Baik Masyarakat: Komunitas "Netizen Bijak Bali" (2025)

Komunitas digital di Bali, termasuk Kabupaten Klungkung, membentuk gerakan *Netizen Bijak Bali* pada awal 2025. Tujuannya sederhana: melawan hoaks dan menjaga privasi digital masyarakat lokal.

📍 *Aktivitasnya meliputi:*

a. Pelatihan literasi digital di sekolah dan desa,
b. Workshop keamanan media sosial untuk UMKM,
c. Edukasi publik tentang bahaya jejak digital permanen,
d. Kolaborasi dengan CSIRT Klungkung untuk melaporkan insiden data.

🧭 *Dampak:*

Berdasarkan laporan Dinas Kominfo Klungkung (2025), daerah ini mengalami **penurunan 35% kasus penipuan daring** dibanding tahun sebelumnya.

💡 *Pelajaran penting:*

Kolaborasi antara pemerintah, masyarakat, dan komunitas digital adalah kunci membangun ruang maya yang sehat dan aman.

5. Studi Kasus Global: Fenomena "Digital Shadow" (2025)

Fenomena "*digital shadow*" atau bayangan digital semakin populer di 2025. Istilah ini menggambarkan data tak terlihat yang kita tinggalkan, seperti histori pencarian, lokasi GPS, dan preferensi belanja daring.

📊 *Contoh:*

Aplikasi belanja online dapat memprediksi minat seseorang bahkan sebelum mereka mencari barang tersebut. Hal ini terjadi karena jejak digitalnya (klik, waktu aktif, dan lokasi) dianalisis secara otomatis.

📍 *Implikasi:*

a. Privasi online semakin menipis.
b. Pengguna perlu mengatur ulang izin aplikasi dan menghapus histori digital secara rutin.

💬 *Pelajaran penting:*

Jejak digital bukan hanya apa yang kita unggah, tapi juga apa yang diamati tanpa kita sadari.

🧠 Rangkuman dari Studi Kasus

Jenis Kasus	Dampak	Pelajaran Utama
ASN unggah konten politik	Sanksi etik dan pemecatan	ASN tetap wajib menjaga netralitas digital
Kebocoran data pribadi	Penipuan dan pencurian identitas	Jangan unggah dokumen pribadi di media sosial
Program “Digital Smart ASN”	Budaya keamanan digital meningkat	ASN sebagai teladan literasi digital
Gerakan Netizen Bijak Bali	Hoaks dan penipuan menurun	Kolaborasi masyarakat penting
Fenomena Digital Shadow	Privasi online menipis	Kelola izin aplikasi dan histori pencarian

“Jejak digital adalah cermin diri di dunia maya. Menjaganya bukan hanya soal keamanan, tetapi juga tentang tanggung jawab, reputasi, dan kepercayaan.”

Pertanyaan Reflektif

1. Saat beraktivitas di media sosial atau layanan digital, seberapa sering Anda menyadari bahwa setiap unggahan, komentar, dan pencarian meninggalkan jejak digital yang bisa ditelusuri?
2. Sebagai ASN atau masyarakat digital, langkah apa yang bisa Anda lakukan hari ini untuk memperkuat privasi dan melindungi data pribadi di dunia maya?
3. Pernahkah Anda menemukan informasi pribadi Anda muncul di internet tanpa izin? Bagaimana cara Anda menghadapinya atau mencegah hal itu terjadi lagi?
4. Dalam konteks pekerjaan, bagaimana seorang ASN dapat menjaga keseimbangan antara keterbukaan informasi publik dan perlindungan data pribadi?
5. Ketika melihat seseorang membagikan foto atau data pribadi orang lain tanpa izin, tindakan apa yang paling bijak untuk dilakukan?
6. Bagaimana Anda memastikan bahwa jejak digital yang Anda tinggalkan menggambarkan citra positif, baik sebagai individu maupun bagian dari instansi pemerintah atau masyarakat Klungkung?
7. Jika suatu hari Anda kehilangan kendali atas akun pribadi (diretas atau disalahgunakan), langkah konkret apa yang akan Anda ambil untuk memulihkan keamanan dan kepercayaan digital Anda?
8. Dalam era di mana data menjadi “mata uang baru”, bagaimana Anda menanamkan kesadaran tentang pentingnya menjaga privasi digital di lingkungan kerja atau keluarga Anda?

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2024). *Pedoman Perlindungan Data Pribadi dan Keamanan Informasi di Ruang Digital.* Direktorat Keamanan Siber Nasional. https://bssn.go.id

Common Sense Media. (2024). *Digital footprint and online reputation: A guide for responsible digital citizens.* Common Sense Education. https://www.commonsense.org/education/articles/digital-footprint

European Union Agency for Cybersecurity (ENISA). (2024). *Privacy and data protection in the digital age.* https://www.enisa.europa.eu/publications/privacy-and-data-protection

Google Safety Center. (2025). *Manage your online privacy and security.* Google. https://safety.google

Kominfo RI. (2024). *Etika Digital dan Perlindungan Privasi di Era Media Sosial.* Kementerian Komunikasi dan Informatika Republik Indonesia. https://www.kominfo.go.id/content/detail/46382

Mozilla Foundation. (2024). *The data privacy guide: How to protect yourself online.* Mozilla Foundation. https://foundation.mozilla.org/en/privacynotincluded

Rahman, F., & Prasetyo, A. (2023). Awareness and behavior of Indonesian internet users on digital privacy protection. *Indonesian Journal of Information Systems*, 6(2), 55–66. https://doi.org/10.24002/ijis.v6i2.9121

Singh, R., & Sharma, S. (2025). Understanding online privacy threats and user responses in developing countries. *Journal of Cyber Policy*, 10(1), 48–65. https://doi.org/10.1080/23738871.2025.2410923

Turner, E., & Ramaswamy, V. (2023). *Understanding digital footprints: Risks, benefits, and management strategies. Journal of Digital Ethics*, 12(2), 45–63. https://doi.org/10.1016/j.jde.2023.02.004

Verizon. (2024). *Data Breach Investigations Report 2024.* Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir