

PRIVASI DAN PERLINDUNGAN DATA PRIBADI

Pertemuan 6 — Privasi digital, keamanan data, UU PDP, dan jejak digital

Program Studi Informatika
Fakultas Ilmu Komputer
UPN “Veteran” Jawa Timur

Posisi Pertemuan 6 dalam RPS

Fokus: menerapkan prinsip privasi dan perlindungan data pribadi melalui analisis kasus kebocoran data.

Sub-CPMK 6

Mahasiswa mampu menerapkan prinsip privasi dan perlindungan data pribadi (C3, A3).

Indikator

Memberikan solusi terhadap kasus kebocoran data.

Metode & Penugasan

Analisis studi kasus •
Problem-Based Learning

Tugas: menganalisis satu kasus kebocoran data di Indonesia dan mengidentifikasi penyebab, dampak, serta langkah mitigasinya.

Tujuan Pembelajaran

Setelah pertemuan ini, mahasiswa diharapkan mampu:

Tujuan 1

Menjelaskan konsep privasi digital dan data pribadi.

Tujuan 2

Membedakan privasi, keamanan informasi, dan perlindungan data.

Tujuan 3

Mengidentifikasi risiko terhadap data pribadi dalam aktivitas digital.

Tujuan 4

Memahami peran UU Perlindungan Data Pribadi (UU PDP) dalam konteks perlindungan data.

Tujuan 5

Menganalisis kasus kebocoran data dan merumuskan langkah mitigasi.

Apa Itu Privasi Digital?

Privasi berkaitan dengan kemampuan seseorang mengendalikan informasi tentang dirinya dan bagaimana informasi tersebut digunakan.

Privasi

Dalam konteks digital, privasi mencakup pertanyaan tentang siapa yang mengetahui informasi tentang kita, bagaimana informasi dikumpulkan, digunakan, disimpan, dan dibagikan.

Contoh sederhana

- Profil akun
- Nomor telepon/email
- Lokasi
- Foto dan rekaman
- Riwayat transaksi
- Aktivitas pada platform digital

Pertanyaan etis: “Apakah penggunaan informasi tersebut sesuai konteks dan harapan pemilik data?”

Privasi bukan berarti “tidak boleh ada data yang dikumpulkan”, tetapi data perlu dikelola secara bertanggung jawab.

Data Pribadi dan Mengapa Harus Dilindungi

Data dapat menjadi sensitif ketika dapat mengidentifikasi atau menggambarkan seseorang dan kehidupannya.

Identitas

Nama, identitas resmi, akun, atau informasi yang mengarah pada identifikasi.

Kontak

Nomor telepon, email, alamat, atau sarana komunikasi.

Aktivitas

Riwayat transaksi, penggunaan layanan, aktivitas digital, atau preferensi.

Lokasi

Informasi lokasi atau pola pergerakan yang dapat mengungkap kebiasaan.

Data sensitif

Jenis data tertentu dapat memiliki risiko lebih tinggi jika tersebar atau disalahgunakan.

Data gabungan

Beberapa data yang tampak sederhana dapat menjadi sangat informatif jika digabungkan.

Privasi vs Keamanan Informasi vs Perlindungan Data

Ketiganya berkaitan, tetapi fokusnya berbeda.

Privasi

Fokus: hak, kendali, konteks, dan kepantasan penggunaan informasi tentang individu.

Pertanyaan: “Apakah penggunaan data ini menghormati privasi?”

Keamanan informasi

Fokus: melindungi informasi dari akses, perubahan, pengungkapan, atau gangguan yang tidak semestinya.

Pertanyaan: “Apakah data terlindungi dari ancaman?”

Perlindungan data

Fokus: tata kelola dan praktik pengelolaan data agar pemrosesan dilakukan secara bertanggung jawab dan sesuai ketentuan.

Pertanyaan: “Bagaimana data dikelola sepanjang siklus hidupnya?”

Data bisa aman secara teknis tetapi tetap bermasalah secara privasi jika digunakan di luar konteks yang semestinya.

Siklus Hidup Data

Risiko privasi dan keamanan dapat muncul pada setiap tahap pengelolaan data.

1. Kumpulkan

Apakah data yang dikumpulkan memang diperlukan?

2. Simpan

Bagaimana data disimpan dan siapa yang dapat mengakses?

3. Gunakan

Apakah penggunaan sesuai tujuan dan kewenangan?

4. Bagikan

Dengan siapa data dibagikan dan untuk tujuan apa?

5. Retensi

Berapa lama data perlu disimpan?

6. Hapus

Bagaimana data dihapus atau dimusnahkan secara tepat?

Prinsip Praktis Perlindungan Data

Gunakan prinsip ini sebagai lensa awal ketika menilai bagaimana suatu sistem mengelola data.

Minimasi

Kumpulkan data yang diperlukan untuk tujuan yang jelas.

Tujuan jelas

Penggunaan data harus memiliki tujuan yang dapat dijelaskan.

Transparansi

Pengguna perlu mengetahui informasi penting tentang pemrosesan datanya.

Akses terbatas

Akses diberikan berdasarkan kebutuhan dan kewenangan.

Keamanan

Gunakan kontrol yang sesuai untuk mengurangi risiko.

Akuntabilitas

Organisasi/profesional harus dapat menjelaskan dan mempertanggungjawabkan pengelolaan data.

UU Perlindungan Data Pribadi (UU PDP)

RPS mencantumkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai referensi pendukung.

Mengapa penting dipahami?

Perlindungan data bukan hanya persoalan teknis. Ada aspek hak, kewajiban, tata kelola, tanggung jawab, dan kepatuhan hukum.

Dalam mata kuliah ini, UU PDP digunakan sebagai konteks untuk memahami mengapa pengelolaan data harus dilakukan secara bertanggung jawab.

Cara membaca kasus dengan perspektif UU PDP

- Apa jenis data yang terlibat?
- Siapa yang mengelola/memproses?
- Untuk tujuan apa data digunakan?
- Bagaimana data dilindungi?
- Apa dampak ketika terjadi pelanggaran?
- Apa kewajiban/tindakan yang perlu diperhatikan?

Catatan: pembahasan kelas berfokus pada konteks etika dan pembelajaran, bukan pengganti nasihat hukum.

Jejak Digital

RPS memasukkan jejak digital sebagai bagian materi. Jejak digital dapat memengaruhi privasi, keamanan, dan reputasi.

Jejak aktif

Informasi yang sengaja kita unggah atau bagikan:

- posting
- komentar
- foto/video
- profil
- formulir online

Jejak pasif

Data yang dapat terbentuk dari penggunaan layanan, misalnya aktivitas, perangkat, lokasi, atau log sistem.

Pertanyaan etis

- Apa yang saya bagikan?
- Siapa yang dapat melihat?
- Apakah bisa disalin/disebar?
- Apa dampaknya di masa depan?
- Apakah saya membagikan data orang lain?

Apa Itu Kebocoran Data?

Kebocoran data terjadi ketika informasi keluar, diakses, atau terungkap kepada pihak yang tidak semestinya.

Penyebab teknis

- Kerentanan aplikasi
- Salah konfigurasi
- Kredensial dicuri
- Malware
- Sistem tidak diperbarui

Penyebab teknis bukan satu-satunya faktor.

Penyebab manusia/tata kelola

- Phishing/social engineering
- Salah kirim data
- Hak akses berlebihan
- Kelalaian
- Prosedur lemah
- Kurang pelatihan

Dampak

- Privasi terganggu
- Penipuan/penyalahgunaan
- Kerugian organisasi
- Hilangnya kepercayaan
- Dampak reputasi
- Konsekuensi hukum/regulasi

Mitigasi: Jangan Hanya Menambal Sistem

Solusi perlindungan data perlu melihat teknologi, manusia, dan proses.

Teknis

Kontrol akses • autentikasi
• enkripsi • logging •
backup • patching •
monitoring • pengujian
keamanan

Manusia

Pelatihan • kesadaran
privasi • pengelolaan
kredensial • prosedur
pelaporan • budaya
keamanan

Tata kelola

Kebijakan • klasifikasi
data • minimasi •
penilaian risiko • audit •
incident response •
akuntabilitas

Pertanyaan penting: “Apakah solusi mengurangi kemungkinan kejadian dan mengurangi dampaknya jika kejadian terjadi?”

Ringkasan Pertemuan 6

Privasi dan perlindungan data adalah tanggung jawab etis, teknis, dan tata kelola.

Privasi digital

Berkaitan dengan kendali, konteks, dan kepantasan penggunaan informasi tentang individu.

Data pribadi

Perlu dikelola secara bertanggung jawab karena dapat berdampak pada individu.

Keamanan data

Melindungi informasi dari akses, perubahan, pengungkapan, atau gangguan yang tidak semestinya.

UU PDP

Menjadi konteks hukum penting dalam pembahasan perlindungan data di Indonesia.

Jejak digital

Aktivitas digital dapat meninggalkan informasi yang berdampak pada privasi dan reputasi.

Kebocoran data

Analisis harus mencakup penyebab, dampak, mitigasi, dan pencegahan.

Profesional Informatika harus mampu merancang teknologi yang tidak hanya berfungsi, tetapi juga menghormati data dan privasi.

TERIMA KASIH

“Data adalah aset teknologi,
tetapi bagi seseorang, data juga merupakan bagian dari kehidupan pribadinya.”

Pertemuan berikutnya → Kampanye Etika Digital