

RINGKASAN MATERI PRIVASI DAN PELANGGARANNYA

1. Pengertian Privasi

Privasi secara umum adalah hak seseorang untuk hidup sendiri, bebas dari gangguan pihak lain. Dalam konteks **privasi informasi**, ini adalah hak individu, kelompok, atau institusi untuk menentukan:

- Informasi pribadi apa yang bisa dibagikan.
- Kapan dan kepada siapa informasi tersebut dikomunikasikan.

2. Informasi yang Dikumpulkan dan Dibagikan oleh Google

Menurut [Kebijakan Privasi Google](#), informasi yang mereka kumpulkan meliputi:

a. Informasi yang Diberikan Pengguna

- Nama, email, nomor telepon.
- Informasi pembayaran jika menggunakan layanan berbayar.

b. Informasi dari Penggunaan Layanan

- **Perangkat:** Informasi tentang model, OS, pengenalan perangkat.
- **Log Aktivitas:** Alamat IP, istilah pencarian, aktivitas situs, waktu permintaan.
- **Lokasi:** GPS, alamat IP, sensor perangkat.
- **Cookie & Teknologi Serupa:** Melacak interaksi pengguna dengan layanan Google.

c. Bagaimana Informasi Digunakan

- Untuk menyediakan layanan.
- Personalisasi iklan dan konten.
- Analisis dan pengembangan layanan.
- Keamanan dan pencegahan penipuan.

d. Pembagian Data

- Mitra terpercaya (penyedia layanan Google).
- Penegakan hukum jika diwajibkan.
- Pengguna lain, sesuai pengaturan privasi.

3. Informasi yang Dikumpulkan dan Dibagikan oleh Facebook

Berdasarkan [Kebijakan Privasi Facebook](#), data yang dikumpulkan meliputi:

a. Informasi Pengguna

- Data pendaftaran (nama, email, nomor telepon).

- Konten yang diunggah (status, foto, video).
- Koneksi sosial (teman, grup, halaman).

b. Penggunaan dan Aktivitas

- Interaksi di platform (like, komentar, share).
- Data transaksi (pembelian, donasi).
- Data perangkat (jenis, lokasi, IP).

c. Bagaimana Informasi Digunakan

- Memberikan pengalaman yang dipersonalisasi.
- Keamanan akun dan pencegahan penipuan.
- Menampilkan iklan yang relevan.
- Penelitian dan pengembangan produk.

d. Pembagian Data

- Dengan mitra iklan.
- Penegakan hukum jika diperlukan.
- Pengguna lain (tergantung pengaturan privasi).

4. Jenis-Jenis Pelanggaran Privasi

Pelanggaran privasi diklasifikasikan dalam 4 jenis utama:

a. Invasion of Privacy (Invasi Privasi)

- Pelanggaran wilayah pribadi tanpa izin.
- Contoh: CCTV di ruang publik, penyadapan, memotret tanpa izin.
- **Kasus Terkait:**
[Kontroversi Kampanye Celup](#)
[Fakta Mengejutkan tentang Penggagas Celup](#)
[Foto Pribadi Penggagas Celup Bocor](#)

b. Profiling

- Pengumpulan data untuk membuat asumsi/spekulasi mengenai seseorang.
- Sering kali data digunakan untuk iklan atau penilaian kredit.
- Risiko: Kesimpulan yang diambil belum tentu akurat.

c. Identity Theft (Pencurian Identitas)

- Pengambilan informasi pribadi seperti nomor KTP, kartu kredit, dll.
- Contoh: **Skimming ATM**, pencurian data untuk kejahatan keuangan.

d. Stalking

- Pelacakan terus-menerus terhadap seseorang tanpa izin.
- Bisa mencakup pengumpulan data lokasi, aktivitas online, bahkan interaksi sosial.

5. Privasi dalam Aktivitas Daring

Informasi pribadi di era digital jauh lebih rentan, seperti:

- Data transaksi online (kartu kredit, perbankan).
- Data kesehatan dari aplikasi.
- Foto/wajah di media sosial.
- Lokasi (GPS, Foursquare, Gojek, Grab).
- IP Address, hingga kata kunci pencarian.

Penggunaan ponsel dan internet memunculkan tantangan baru:

- Pengumpulan data dalam bentuk baru.
- Analisis perilaku pengguna.
- Potensi eksploitasi data oleh pemerintah dan perusahaan.
- Tantangan dalam regulasi privasi karena sifat internet yang lintas batas.

Privasi dalam Aktivitas Daring (Online)

Di era digital, informasi pribadi yang bisa dikumpulkan bukan cuma yang sifatnya standar seperti nomor telepon atau alamat rumah. Bahkan **kata kunci** yang kita ketik di mesin pencari pun termasuk data pribadi yang bisa direkam dan dianalisis.



Ilustrasi dalam gambar menunjukkan bagaimana data pribadi, termasuk **sidik jari** (fingerprints), bisa menjadi "komoditas" yang diperjualbelikan. Hal ini mencerminkan situasi di mana data pribadi sangat rentan disalahgunakan, terutama oleh pihak-pihak yang berkepentingan seperti perusahaan atau lembaga pemerintah.

Ancaman Privasi di Era Digital

Ponsel pintar (smartphone) adalah salah satu alat komunikasi yang:

- **Sangat pribadi** dan melekat dengan pemiliknya.
- Mudah dipantau dan dieksploitasi karena selalu aktif dan terkoneksi.

Keberadaan internet yang terhubung langsung dengan ponsel memungkinkan berbagai aktivitas pengumpulan data, seperti:

1. **Mengumpulkan informasi pribadi dalam bentuk baru**
 Contoh: Data perilaku, lokasi, bahkan kebiasaan harian.
2. **Menjembatani dan mendorong pengumpulan serta penentuan lokasi/informasi pribadi**
 Misalnya: Aplikasi yang melacak lokasi pengguna tanpa sepengetahuan mereka.

3. **Memberikan akses tanpa batas bagi pemerintah dan pihak swasta untuk mengakses informasi pribadi**
➡ Contoh: Permintaan data pengguna oleh lembaga penegak hukum.
4. **Melahirkan peluang komersial baru untuk mengumpulkan dan mengelola informasi pribadi pengguna**
➡ Contoh: Iklan yang sangat personal berdasarkan riwayat pencarian atau lokasi.
5. **Mengakibatkan tantangan regulasi yang besar karena karakteristik internet yang lintas batas geografis**
➡ Misalnya: Data yang dikumpulkan di satu negara bisa disimpan atau dianalisis di negara lain dengan aturan privasi berbeda.

Kebocoran Informasi (Data Breach)

Kasus Kebocoran Data di Filipina

- **Kasus:** Data pribadi **70 juta warga Filipina** dibocorkan oleh peretas **sebulan sebelum pemilihan umum**.
- **Informasi yang bocor:** Data pribadi, termasuk **sidik jari dan paspor** dari sekitar **70 juta orang**.
- **Pihak yang diserang: Komisi Pemilihan Umum Filipina (COMELEC).** Situsnya diretas dan isinya diunggah ke internet pada bulan Maret.

Kelompok peretas **Anonymous Philippines** mengklaim bertanggung jawab, dengan alasan menyoroti kurangnya keamanan situs tersebut. Setelah itu, kelompok **LulzSec Philippines** memublikasikan basis data dari situs COMELEC, berisi **data sensitif** warga Filipina.

Meskipun begitu, perusahaan keamanan **Trend Micro** menyatakan bahwa **insiden ini adalah kebocoran data terbesar dalam sejarah Filipina** dan salah satu yang terbesar di dunia.

Tautan berita lengkap:

🔗 [BBC Indonesia - Dunia Filipina Pemilu](#)

Pertanyaan Diskusi:

1. **Kemungkinan apa saja yang bisa terjadi jika ada pihak yang memiliki sebanyak itu data?**
 - Penyalahgunaan data untuk pencurian identitas (identity theft).
 - Phishing, penipuan finansial, hingga pemerasan.
 - Pemanfaatan data untuk manipulasi politik atau kampanye hitam.
 - Potensi kerugian ekonomi dan kehilangan kepercayaan masyarakat.
2. **Apa yang kira-kira bisa dilakukan oleh pihak tersebut?**
 - Menjual data ke pihak ketiga atau pasar gelap (dark web).
 - Menggunakannya untuk targeted phishing atau serangan siber lainnya.
 - Menciptakan ancaman keamanan nasional, terutama menjelang pemilu.
3. **Apa yang seharusnya dilakukan oleh pemerintah Filipina?**

- Meningkatkan sistem keamanan siber, termasuk audit reguler.
- Mengedukasi publik tentang risiko penyalahgunaan data pribadi.
- Memperketat regulasi privasi data dan memperbaiki infrastruktur IT pemerintah.
- Memberikan dukungan hukum dan perlindungan kepada korban kebocoran data.