Semester GENAP - 2024/2025

PRAKTIK PROFESIONAL GLOBAL

Minggu 2 :

- PRIVASI DAN KEAMANAN DATA

Dosen pengampu:

Suamanda Ika N, S.Kom., M.Kom.

PRODI TEKNOLOGI INFORMASI
JURUSAN TEKNIK ELEKTRO, MEKATRONIKA, DAN INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS TIDAR

Jl. Kapten Suparman No.39, Tuguran, Potrobangsan, Kec. Magelang Utara, Kota Magelang, Jawa Tengah 56116

PRIVASI

Sub bab ini membahas Konsep dan Dimensi Privasi

KONSEP PRIVASI

Privasi secara umum dapat diartikan sebagai hak individu atau organisasi untuk mengendalikan informasi tentang diri mereka dan menentukan sejauh mana informasi tersebut dapat diakses oleh pihak lain.

- "**Menurut Westin (1967),** privasi adalah klaim seseorang untuk menentukan kapan, bagaimana, dan sejauh mana informasi tentang dirinya dikomunikasikan kepada orang lain.
- Sedangkan dalam konteks hukum, **Warren & Brandeis (1890)** mendefinisikan privasi sebagai ***the right to be let alone***, yaitu hak untuk tidak diganggu atau hak untuk mengendalikan informasi pribadi kita."

DIMENSI PRIVASI

Privasi memiliki beberapa dimensi yang penting untuk dipahami. Schofield dalam Barak (2008) mengelompokkan privasi menjadi tiga dimensi utama, yaitu:

- **"Privasi Informasi (Informational Privacy)“**
  - Dimensi ini berkaitan dengan bagaimana, kapan, dan sejauh mana informasi pribadi seseorang disebarluaskan. Contohnya adalah data keuangan, rekam medis, atau informasi pribadi yang hanya boleh diakses oleh pihak tertentu.
- **"Privasi Fisik (Accessibility Privacy)“**
  - Ini berhubungan dengan sejauh mana seseorang bisa diakses secara fisik oleh orang lain. Misalnya, seseorang memiliki hak untuk menentukan siapa saja yang dapat memasuki rumah atau ruang pribadinya.
- **"Privasi Ekspresif (Expressive Privacy)“**
  - Dimensi ini mencakup perlindungan dalam mengekspresikan identitas dan pendapat seseorang tanpa tekanan atau gangguan. Contohnya adalah kebebasan berbicara di internet tanpa takut intimidasi atau pembatasan dari pihak lain."

PRIVASI DALAM KEHIDUPAN DIGITAL

Dalam **kehidupan sehari-hari**, kita sering kali dengan **mudah menjaga privasi**, seperti menutup pintu saat ingin sendiri atau merahasiakan informasi pribadi dari orang asing.

Namun, di **dunia digital**, **menjaga privasi tidak semudah itu**. Saat kita **berselancar** di internet, menggunakan **media sosial**, atau bahkan **berbelanja online**, kita **tanpa sadar** meninggalkan ***jejak digital*** yang **dapat diakses oleh pihak lain**.

Contoh Kasus:

- Kebocoran data melalui platform media sosial,
- *Hacking* yang mengungkap data pribadi tokoh publik.

Ancaman terhadap Privasi Online

1. Penyalahgunaan Data Pribadi“

   Contoh Kasus:

   Skandal Cambridge Analytica, di mana data jutaan pengguna Facebook digunakan tanpa izin untuk kepentingan politik

2. Pelacakan Digital dan Jejak Online

   Misalnya, pernahkah Anda mencari suatu produk di Google, lalu tiba-tiba melihat iklan produk tersebut di berbagai platform media sosial? Itu adalah hasil dari pelacakan digital.

3. Serangan Siber dan Peretasan (Hacking)

   Contoh Kasus:

   Kasus peretasan data pernah menimpa banyak perusahaan besar, seperti Yahoo dan LinkedIn, di mana jutaan akun pengguna diretas dan dijual di pasar gelap.

4. Kebocoran Data dan Identitas Palsu

   Terjadi karena kelalaian atau sistem keamanan yang lemah.

   Terjadi pada perusahaan layanan digital, lembaga keuangan, dan bahkan pemerintahan.

Kebebasan Informasi vs. Perlindungan Privasi

Sub bab ini membahas Kebebasan Informasi vs. Perlindungan Privasi

1. Pengertian Kebebasan Informasi

Kebebasan informasi adalah **hak individu** untuk mengakses dan **menyebarluaskan** informasi **tanpa batasan** yang berlebihan. Konsep ini sangat penting dalam **demokrasi**, karena memungkinkan **transparansi**, kebebasan berekspresi, dan **akuntabilitas**.

✓ **Contoh Kebebasan Informasi:**

- Akses publik terhadap data pemerintah melalui kebijakan *Open Data*.
- Kebebasan jurnalis dalam menyampaikan berita tanpa sensor.
- Kemudahan berbagi informasi melalui media sosial dan platform digital.

☞ ***Namun, apakah kebebasan informasi selalu berdampak positif?***

2. Dampak Negatif Kebebasan Informasi terhadap Privasi

"Meski kebebasan informasi memberikan banyak manfaat, jika tidak dibatasi dengan bijak, hal ini bisa berisiko terhadap privasi. Beberapa dampak negatifnya antara lain:"

❌ **Penyalahgunaan Data Pribadi**

Informasi pribadi bisa tersebar dan dimanfaatkan untuk kepentingan yang tidak diinginkan, seperti peretasan, pencurian identitas, atau bahkan kejahatan siber.

❌ **Kurangnya Kontrol terhadap Informasi yang Beredar**

Data yang kita bagikan di internet sulit dikendalikan. Sekali tersebar, informasi tersebut bisa diakses oleh banyak pihak tanpa izin.

❌ **Penyebaran Hoaks dan Disinformasi**

Kebebasan berbagi informasi tanpa regulasi yang jelas juga bisa menyebabkan maraknya berita palsu (*fake news*) yang berpotensi menyesatkan masyarakat.

3. Perlindungan Privasi sebagai Hak Asasi

"Sementara kebebasan informasi penting, perlindungan privasi juga harus dijaga. **Privasi adalah hak asasi manusia** yang harus dihormati dan dilindungi oleh setiap individu, organisasi, maupun pemerintah."

✓ **Regulasi tentang Privasi di Dunia**

- **Uni Eropa** memiliki kebijakan ketat seperti **General Data Protection Regulation (GDPR)** yang mengatur perlindungan data pengguna.
- **Indonesia** memiliki UU ITE dan RUU PDP (Perlindungan Data Pribadi) yang berupaya mengamankan privasi warganya.
- **Amerika Serikat** masih menghadapi perdebatan mengenai perlindungan privasi, terutama dalam pengawasan internet oleh pemerintah.

☞ ***Jadi, bagaimana cara menyeimbangkan antara kebebasan informasi dan privasi?***

4. Menemukan Keseimbangan

"Untuk memastikan kebebasan informasi tidak melanggar privasi, diperlukan keseimbangan melalui berbagai cara:"

✓ **Regulasi yang Jelas**

Pemerintah harus menetapkan aturan yang memastikan transparansi informasi tanpa mengorbankan privasi individu.

✓ **Peningkatan Kesadaran Masyarakat**

Pengguna internet perlu lebih memahami hak dan tanggung jawab mereka dalam berbagi serta mengelola informasi pribadi.

✓ **Teknologi Keamanan Data**

Perusahaan teknologi perlu mengembangkan fitur keamanan seperti enkripsi, kontrol akses, dan kebijakan privasi yang lebih transparan.

✓ **Tanggung Jawab Perusahaan dan Media**

Platform digital harus memiliki kebijakan privasi yang kuat dan melindungi data pengguna dari penyalahgunaan.

Strategi Perlindungan Privasi dan Keamanan Data

Sub bab ini membahas Strategi Perlindungan Privasi dan Keamanan Data

1. Gunakan Kata Sandi yang Kuat dan Unik

"Kata sandi adalah pertahanan pertama dalam menjaga keamanan akun kita. Namun, **banyak orang** masih menggunakan **kata sandi yang lemah**, seperti '123456' atau 'password'. Ini sangat berbahaya karena peretas dapat dengan mudah menebaknya."

✓ Tips:

- Gunakan kombinasi huruf besar, kecil, angka, dan simbol.
- Jangan gunakan kata sandi yang sama untuk banyak akun.
- Gunakan aplikasi *password manager* untuk menyimpan kata sandi dengan aman.

2. Aktifkan Autentikasi Dua Faktor (2FA)

"Autentikasi dua faktor (2FA) menambahkan lapisan keamanan ekstra dengan mengharuskan pengguna memasukkan kode verifikasi yang dikirim melalui SMS atau aplikasi khusus."

✓ Keuntungan 2FA:

- Jika seseorang mencuri kata sandi Anda, mereka tetap tidak bisa mengakses akun tanpa kode verifikasi tambahan.
- Mencegah akses tidak sah ke akun penting, seperti email dan media sosial.

3. Batasi Informasi Pribadi yang Dibagikan Online

"Banyak orang secara tidak sadar membagikan terlalu banyak informasi pribadi di media sosial, seperti lokasi, nomor telepon, atau data pribadi lainnya yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab."

✓ Langkah yang bisa dilakukan:

- Periksa dan sesuaikan **pengaturan privasi** di akun media sosial.
- Hindari membagikan data sensitif, seperti alamat rumah atau nomor kartu identitas.
- Hati-hati saat menerima permintaan pertemanan dari orang yang tidak dikenal.

4. Gunakan VPN saat Mengakses Internet Publik

"Jika Anda sering menggunakan Wi-Fi publik di kafe, bandara, atau tempat umum lainnya, data Anda bisa dengan mudah disadap oleh pihak lain."

✓ Solusi:

- Gunakan **Virtual Private Network (VPN)** untuk mengenkripsi koneksi internet Anda.
- Hindari mengakses layanan perbankan atau akun penting melalui Wi-Fi publik.

5. Periksa Izin Aplikasi dan Situs Web

"Banyak aplikasi dan situs web meminta akses ke informasi pribadi, seperti lokasi, kontak, dan bahkan kamera atau mikrofon tanpa alasan yang jelas."

✓ Apa yang harus dilakukan?

- Hanya berikan izin yang benar-benar diperlukan.
- Periksa kembali pengaturan privasi pada perangkat Anda.
- Hindari menginstal aplikasi dari sumber yang tidak terpercaya.

6. Waspada terhadap Phishing dan Penipuan Online

"*Phishing* adalah salah satu metode yang sering digunakan peretas untuk mencuri informasi pribadi dengan mengirim email atau pesan palsu yang terlihat resmi."

✓ Cara menghindarinya:

- Jangan mengklik tautan mencurigakan dalam email atau pesan tak dikenal.
- Periksa alamat email pengirim sebelum merespons.
- Jika ragu, langsung akses situs resmi melalui browser, bukan dari tautan dalam email.

7. Rutin Memeriksa Jejak Digital Anda

"Pernahkah Anda mencoba mencari nama Anda di Google? Ini bisa menjadi cara untuk mengetahui informasi apa saja yang tersedia secara publik tentang Anda."

✓ Langkah yang bisa dilakukan:

- Gunakan mesin pencari untuk melihat informasi tentang diri Anda.
- Hapus atau ubah informasi yang tidak ingin dipublikasikan.
- Jika memungkinkan, gunakan mode **incognito** saat berselancar di internet.

KESIMPULAN

✓ **1. Privasi online adalah hak yang harus dilindungi.**

Privasi bukan hanya sekadar pilihan, tetapi juga hak asasi yang memungkinkan kita menjaga informasi pribadi agar tidak disalahgunakan.

✓ **2. Ancaman terhadap privasi semakin meningkat.**

Mulai dari penyalahgunaan data pribadi, pelacakan digital, hingga serangan siber, semua ini dapat membahayakan individu maupun organisasi jika tidak diantisipasi.

✓ **3. Kebebasan informasi perlu diimbangi dengan perlindungan privasi.**

Meski akses informasi sangat penting, tanpa regulasi yang tepat, kebebasan ini bisa berisiko dan mengancam privasi individu.

✓ **4. Strategi perlindungan privasi sangat penting untuk diterapkan.**

Penggunaan kata sandi yang kuat, autentikasi dua faktor, pengaturan privasi di media sosial, serta kewaspadaan terhadap serangan siber adalah langkah utama dalam menjaga keamanan data kita.

REKOMENDASI

✓ 1. Tingkatkan Kesadaran Digital

Kita harus lebih memahami bagaimana data kita digunakan dan bagaimana cara melindunginya.

✓ 2. Gunakan Teknologi Keamanan dengan Bijak

Menggunakan VPN, mengaktifkan autentikasi dua faktor, serta menghindari tautan mencurigakan bisa membantu menjaga keamanan informasi pribadi.

✓ 3. Periksa dan Sesuaikan Pengaturan Privasi

Pastikan pengaturan privasi di media sosial dan aplikasi lainnya selalu diperbarui agar hanya informasi yang diperlukan yang bisa diakses oleh pihak lain.

✓ 4. Selalu Berpikir Kritis dalam Berbagi Informasi Online

Sebelum membagikan informasi pribadi, tanyakan pada diri sendiri: *Apakah ini aman? Apakah ini perlu? Apakah saya siap jika informasi ini disalahgunakan?*

TERIMAKASIH

PRAKTIK PROFESIONAL GLOBAL