MAKALAH

Infringements of Privacy

Disusun Untuk Memenuhi Tugas Mata Kuliah Etika Profesi

Dosen Pengampu

Hairil Kurniadi Siradjuddin S.kom., M.kom.

Oleh :

Ajuan Sahmir (07352311078)

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS KHAIRUN

2025

Link Blog/Web Materi Makalah:

https://alifatullah.github.io/Profil-Website/#blog

KATA PENGANTAR

Segala puji dan syukur saya panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga makalah tentang *Infringements of Privacy* ini dapat saya selesaikan dengan baik. Makalah ini disusun sebagai wujud tanggung jawab saya sebagai mahasiswa dalam memenuhi tugas yang diberikan.

Saya menyadari bahwa makalah ini masih jauh dari kesempurnaan, oleh sebab itu saya sangat mengharapkan kritik dan saran yang membangun guna penyempurnaan di masa mendatang.

Saya mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan, dukungan, dan bimbingan selama proses pembuatan makalah ini.

Ternate, 07 mei 2025

Penulis

DAFTAR ISI

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, informasi pribadi menjadi sangat mudah diakses dan disebarluaskan. Kemajuan teknologi yang pesat, seperti media sosial, aplikasi berbasis lokasi, dan layanan berbasis cloud, telah membawa dampak besar terhadap cara individu berinteraksi dan berbagi informasi. Namun, perkembangan ini juga meningkatkan risiko terjadinya *infringements of privacy* atau pelanggaran privasi. Tanpa disadari, data pribadi seperti identitas, kebiasaan, lokasi, hingga preferensi seseorang dapat dikumpulkan dan digunakan tanpa izin.

Pelanggaran privasi tidak hanya terjadi karena kelalaian pengguna, tetapi juga karena penyalahgunaan data oleh pihak ketiga seperti perusahaan teknologi, pengiklan, bahkan pelaku kejahatan siber. Kasus-kasus seperti penyebaran data pengguna secara ilegal, pengintaian digital (*surveillance*), dan pencurian identitas menunjukkan bahwa privasi kini menjadi isu serius yang perlu mendapat perhatian lebih.

Selain itu, belum meratanya pemahaman masyarakat mengenai pentingnya menjaga privasi serta lemahnya regulasi di beberapa negara turut memperparah situasi ini. Banyak individu yang tidak menyadari bahwa data mereka telah dikompromikan atau dimanfaatkan untuk tujuan yang melanggar hukum dan etika.

Oleh karena itu, penting untuk membahas secara mendalam tentang bentuk-bentuk pelanggaran privasi, penyebabnya, serta dampaknya terhadap individu dan masyarakat. Dengan memahami hal tersebut, diharapkan dapat tercipta kesadaran yang lebih tinggi terhadap pentingnya perlindungan privasi serta dorongan untuk memperkuat regulasi dan edukasi publik.

1.2 Rumusan Masalah

a. Apa yang dimaksud dengan *Infringements of Privacy* atau pelanggaran privasi?

b. Bagaimana bentuk-bentuk pelanggaran privasi yang terjadi di era digital saat ini?
c. Apa saja teori cybercrime dan cyberlaw yang berkaitan dengan pelanggaran privasi?
d. Apa saja motif dan penyebab terjadinya pelanggaran privasi?
e. Bagaimana upaya atau langkah-langkah penanggulangan terhadap pelanggaran privasi?

1.3 Tujuan Penulisan

a. Untuk memahami pengertian dan konsep *Infringements of Privacy* atau pelanggaran privasi.
b. Untuk mengidentifikasi bentuk-bentuk pelanggaran privasi yang umum terjadi di era digital.
c. Untuk menjelaskan teori-teori cybercrime dan cyberlaw yang relevan dengan isu pelanggaran privasi.
d. Untuk menganalisis motif dan penyebab terjadinya pelanggaran privasi dalam dunia maya.
e. Untuk memberikan gambaran mengenai langkah-langkah penanggulangan dan pencegahan pelanggaran privasi secara efektif.

BAB II
LANDASAN TEORI

2.1 Pengertian Kejahatan Siber (Cybercrime)

Cybercrime adalah segala bentuk aktivitas kejahatan yang dilakukan melalui jaringan komputer dan internet. Kejahatan ini mencakup tindakan yang merugikan individu, organisasi, maupun negara, dengan memanfaatkan teknologi informasi. Salah satu bentuk cybercrime yang semakin marak adalah pelanggaran privasi (*infringement of privacy*), di mana informasi pribadi seseorang diakses, digunakan, atau disebarkan tanpa izin.

Menurut The United Nations Office on Drugs and Crime (UNODC), cybercrime diklasifikasikan ke dalam dua kategori utama:

a. Cyber-dependent crime, yaitu kejahatan yang hanya bisa terjadi melalui teknologi digital (contoh: hacking, DDoS).
b. Cyber-enabled crime, yaitu kejahatan konvensional yang diperluas melalui teknologi (contoh: penipuan online, penyebaran data pribadi).

2.2 Pengertian Pelanggaran Privasi (*Infringements of Privacy*)

Pelanggaran privasi adalah tindakan mengakses, mengumpulkan, menggunakan, atau menyebarkan informasi pribadi seseorang tanpa persetujuan atau wewenang yang sah. Di era digital, data pribadi seperti nama, alamat, nomor identitas, riwayat pencarian, hingga kebiasaan belanja menjadi aset yang berharga namun rawan disalahgunakan.

Contoh pelanggaran privasi:

a. Pengambilan data tanpa izin melalui cookies atau aplikasi.
b. Penyebaran foto/video pribadi tanpa sepengetahuan pemilik.
c. Phishing dan pencurian identitas.

2.3 Teori Hukum Siber (Cyberlaw)

Cyberlaw adalah seperangkat aturan hukum yang mengatur aktivitas di dunia digital, termasuk perlindungan data pribadi dan privasi pengguna internet.

Tujuan dari cyberlaw adalah memberikan dasar hukum agar pelaku pelanggaran di dunia maya bisa ditindak secara adil.

Beberapa undang-undang yang relevan:

a. UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya pada UU No. 19 Tahun 2016.
b. Pasal 26: Perlindungan data pribadi.
c. Pasal 30: Larangan mengakses sistem elektronik milik orang lain tanpa izin.
d. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).
e. GDPR (General Data Protection Regulation) – regulasi privasi data di Uni Eropa, sebagai standar global perlindungan data pribadi.

2.4 Teori Terkait Kejahatan dan Privasi

a. Routine Activity Theory: Kejahatan terjadi ketika ada pelaku, target, dan tidak adanya pengawasan. Dalam konteks digital, pelanggaran privasi terjadi ketika pelaku menemukan celah dari korban yang kurang waspada dan sistem yang lemah.
b. Deterrence Theory: Kejahatan bisa dicegah jika ada hukuman yang tegas. Regulasi dan penegakan hukum menjadi faktor penting dalam menekan pelanggaran privasi.
c. Theory of Reasoned Action: Pelaku kejahatan digital seringkali sadar akan tindakan mereka. Pelanggaran privasi terjadi karena ada niat dan keyakinan bahwa mereka tidak akan tertangkap atau dihukum.

BAB III

PEMBAHASAN

3.1 Studi Kasus: *Kebocoran Data Pengguna Tokopedia (2020)*

Pada Mei 2020, terjadi kebocoran data besar-besaran dari platform e-commerce Tokopedia. Sekitar 91 juta data pengguna dilaporkan bocor dan dijual di forum gelap (*dark web*). Data yang bocor mencakup nama lengkap, alamat email, nomor telepon, tanggal lahir, dan hash password.

3.2 Motif Pelaku

Motif dari pelaku pelanggaran privasi ini bisa dijelaskan sebagai berikut:

a. Ekonomi: Data pribadi sangat berharga di pasar gelap karena bisa digunakan untuk penipuan, spam, dan pencurian identitas.
b. Unjuk Kekuatan: Dalam beberapa kasus, peretas hanya ingin menunjukkan bahwa mereka bisa menembus sistem keamanan dari perusahaan besar.
c. Politik atau Sosial: Beberapa pelanggaran privasi dilakukan oleh kelompok hacktivist yang ingin menyampaikan pesan tertentu.

3.3 Penyebab Terjadinya Pelanggaran Privasi

Beberapa faktor penyebab kebocoran data tersebut antara lain:

a. Sistem keamanan yang lemah, seperti enkripsi yang tidak diperbarui atau kerentanan pada API.
b. Kurangnya audit keamanan secara berkala.
c. Kelalaian dalam pengelolaan data pengguna.
d. Kurangnya edukasi pengguna tentang keamanan data pribadi, sehingga mereka menggunakan password yang lemah dan berulang.

3.4 Dampak dari Pelanggaran Privasi

Pelanggaran privasi seperti ini dapat menimbulkan dampak serius, antara lain:

a. Kerugian bagi pengguna, seperti penyalahgunaan data, penipuan, bahkan potensi kerugian finansial.

b. Kerugian reputasi bagi perusahaan, karena kehilangan kepercayaan dari pelanggan.
c. Dampak hukum, baik bagi perusahaan maupun pelaku pelanggaran.

3.5 Upaya Penanggulangan

Beberapa solusi untuk menanggulangi dan mencegah pelanggaran privasi antara lain:

1. Dari Sisi Teknologi:
    a. Meningkatkan sistem keamanan siber seperti firewall, enkripsi data, dan otentikasi dua faktor.
    b. Melakukan audit dan pengujian keamanan (penetration test) secara berkala.
    c. Mengadopsi standar internasional seperti ISO 27001 untuk keamanan informasi.
2. Dari Sisi Hukum:
    a. Penegakan hukum terhadap pelaku sesuai UU ITE dan peraturan perlindungan data.
    b. Peningkatan regulasi mengenai pengelolaan dan perlindungan data pribadi.
3. Dari Sisi Edukasi:
    a. Memberikan edukasi kepada masyarakat tentang pentingnya menjaga data pribadi.
    b. Kampanye digital safety seperti penggunaan password yang kuat, waspada terhadap phishing, dan menjaga privasi di media sosial.

BAB IV
PENUTUP

4.1 Kesimpulan

Pelanggaran privasi (*Infringements of Privacy*) merupakan salah satu bentuk kejahatan siber yang semakin sering terjadi di era digital saat ini. Kasus seperti kebocoran data pengguna Tokopedia menunjukkan bahwa data pribadi sangat rentan disalahgunakan jika tidak dilindungi dengan baik. Motif pelaku biasanya berkaitan dengan keuntungan ekonomi, kepuasan pribadi, atau bahkan ideologi.

Pelanggaran ini disebabkan oleh berbagai faktor, mulai dari lemahnya sistem keamanan, kelalaian pengelola sistem, hingga kurangnya kesadaran pengguna terhadap pentingnya perlindungan data. Oleh karena itu, diperlukan langkah-langkah penanggulangan yang melibatkan teknologi, hukum, dan edukasi agar pelanggaran privasi dapat dicegah dan diminimalkan.

4.2 Saran

Untuk menekan terjadinya pelanggaran privasi, maka disarankan:

1. Setiap penyedia layanan digital harus meningkatkan keamanan sistem dan rutin melakukan audit keamanan.
2. Pemerintah perlu memperketat regulasi perlindungan data pribadi dan memastikan penegakan hukum terhadap pelanggaran privasi.
3. Masyarakat harus meningkatkan literasi digital dan lebih waspada dalam membagikan data pribadi secara online.

DAFTAR PUSTAKA

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).
2. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE.
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).
4. European Union. (2018). *General Data Protection Regulation (GDPR)*. Retrieved from https://gdpr.eu/
5. Kominfo. (2020). *Penjelasan Resmi Tentang Kebocoran Data Tokopedia*. Retrieved from https://kominfo.go.id
6. United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*.
7. Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems* (16th ed.). Pearson Education.
8. Raharjo, B. (2021). *Cybercrime dan Perlindungan Data Pribadi di Indonesia*. Jakarta: Prenadamedia Group.
9. Tirto.id. (2020). *Kebocoran Data Tokopedia: Apa yang Harus Dilakukan Pengguna?* Retrieved from https://tirto.id
10. TechCrunch. (2020). *Hacker leaks 91 million Tokopedia user records*. Retrieved from https://techcrunch.com