

Studi Kasus Kebocoran Data Facebook dan Perlindungan Informasi Pribadi

Reza Irfan Akmal Bonggi^{1*}, Muhammad Rachman², Riski Dwi Ramadhan³, Mukhammad Alifio Fikri⁴, Annisa Elfina Augustia⁵

¹⁻⁵Fakultas Teknik dan Ilmu Komputer Unindra, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia

Email: ^{1*}rezairfanbonggi@gmail.com, ²muhammadrachman20@gmail.com,
³riskidwiramadhan23@gmail.com, ⁴alivio_321@gmail.com, ⁵annisa12elfina@gmail.com

(* : corresponding author)

Abstrak—Kasus kebocoran data pada *Facebook* menjadi salah satu isu besar dalam keamanan informasi digital di era modern. Penelitian ini bertujuan untuk mengkaji dampak kebocoran data *Facebook* terhadap perlindungan informasi pribadi pengguna, serta mengevaluasi strategi yang dapat diterapkan untuk meningkatkan keamanan data pribadi di media sosial. Metode penelitian yang digunakan adalah studi kasus dengan pendekatan kualitatif melalui analisis literatur, laporan investigasi, dan regulasi terkait perlindungan data. Hasil penelitian menunjukkan bahwa kebocoran data menimbulkan kerugian pada aspek privasi, kepercayaan pengguna, serta potensi penyalahgunaan data oleh pihak ketiga. Studi ini juga menekankan pentingnya penerapan regulasi perlindungan data yang lebih ketat serta peningkatan kesadaran pengguna dalam menjaga informasi pribadi.

Kata kunci: *Facebook*, Kebocoran Data, Perlindungan Informasi, Privasi, Keamanan

Abstract—The data breach case involving *Facebook* has become one of the major issues in digital information security in the modern era. This study aims to examine the impact of *Facebook*'s data breach on the protection of users' personal information and to evaluate strategies that can be implemented to enhance data security on social media platforms. The research method employed is a case study with a qualitative approach through the analysis of literature, investigative reports, and regulations related to data protection. The results show that the data breach caused significant harm in terms of privacy, user trust, and the potential misuse of personal information by third parties. This study also emphasizes the importance of stricter implementation of data protection regulations and the need to raise user awareness in safeguarding personal information.

Keywords: *Facebook*, Data Breach, Information Protection, Privacy, Security

1. PENDAHULUAN

Dalam era digital saat ini, data pribadi pengguna menjadi salah satu aset paling berharga bagi perusahaan platform media sosial seperti *Facebook*. Namun, kasus kebocoran data dan penyalahgunaan informasi pribadi kini menjadi sorotan global. Salah satu insiden paling menonjol adalah skandal *Cambridge Analytica* yang diungkap lewat berbagai media, termasuk *The New York Times*. (Confessore, 2018)

Menurut laporan, *Cambridge Analytica* berhasil mengakses data ratusan juta pengguna *Facebook* melalui aplikasi pihak ketiga bernama “*This Is Your Digital Life*”. Data yang dikumpulkan tidak hanya berasal dari pengguna aplikasi itu sendiri, tetapi juga dari daftar teman (*friends*) mereka melalui fitur *API Open Graph Facebook* tanpa persetujuan eksplisit dari semua pihak.

Pihak *Facebook* kemudian mengakui bahwa estimasi awal 50 juta pengguna yang terkena dampak dinaikkan menjadi sekitar 87 juta pengguna di Amerika Serikat dan global. Insiden ini mengundang kritik luas terhadap praktik privasi *Facebook*, regulasi perlindungan data, dan tanggung jawab *platform* terhadap perlindungan informasi pribadi pengguna. (Kozlowska, 2018)

Secara konseptual, kebocoran data seperti ini menimbulkan sejumlah konsekuensi serius: penurunan kepercayaan pengguna terhadap platform, risiko penyalahgunaan data untuk tujuan manipulasi politik atau pemasaran yang agresif, serta potensi pelanggaran hukum privasi yang berlaku di berbagai negara. (Katie Harbath & Collier Fernekes, 2023)

Di Indonesia, persoalan kebocoran data dan perlindungan informasi pribadi juga relevan, sejalan dengan berkembangnya regulasi perlindungan data pribadi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Maka dari itu, studi kasus kebocoran data *Facebook* menjadi

sangat penting untuk dianalisis untuk memahami bagaimana kelemahan dalam sistem, regulasi, dan kesadaran pengguna dapat dimitigasi.

2. METODE PENELITIAN

2.1 Tahapan Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus, yang berfokus pada insiden kebocoran data *Facebook* melalui kasus *Cambridge Analytica*. Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam mengenai mekanisme kebocoran data, dampaknya terhadap perlindungan informasi pribadi, serta upaya mitigasi yang dapat diterapkan oleh pengguna maupun penyedia platform media sosial.

2.2 Sumber Data dan Teknik Analisis Data

Penelitian ini menggunakan dua jenis data, yaitu data primer dan data sekunder, yang dikumpulkan melalui pendekatan studi pustaka.

1. **Data primer:** Diperoleh dari dokumen resmi dan peraturan yang berkaitan langsung dengan perlindungan data pribadi serta etika profesi di bidang teknologi informasi. Sumber utama meliputi *General Data Protection Regulation* (GDPR) sebagai regulasi internasional, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai dasar hukum nasional. Selain itu, kode etik profesi seperti *ACM Code of Ethics* dan *IEEE Code of Ethics* juga dijadikan rujukan dalam menelaah aspek moral dan tanggung jawab profesional penyedia layanan digital.
2. **Data Sekunder:** Diperoleh dari berbagai literatur pendukung seperti artikel ilmiah, jurnal penelitian, serta berita daring dari media terpercaya. Data ini mencakup laporan mengenai kasus kebocoran data *Facebook* oleh *Cambridge Analytica*, hasil investigasi lembaga seperti *Federal Trade Commission* (FTC), serta analisis dari Badan Siber dan Sandi Negara (BSSN). Seluruh data sekunder digunakan untuk memperkuat pemahaman terhadap konteks kasus, dampaknya terhadap pengguna, dan tanggapan publik serta lembaga terkait.

2.3 Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis isi (*content analysis*). Tahapan analisis dilakukan sebagai berikut:

- a. Identifikasi Kasus, yaitu menelusuri kronologi kebocoran data, pihak-pihak yang terlibat, serta dampak yang ditimbulkan bagi pengguna.
- b. Klasifikasi Informasi, dengan mengelompokkan data berdasarkan aspek hukum, etika, dan keamanan informasi.
- c. Analisis dan Penafsiran, yaitu membandingkan temuan dengan teori privasi digital serta prinsip etika profesi dalam pengelolaan data pribadi.
- d. Triangulasi Sumber, dilakukan dengan cara mencocokkan hasil temuan dari berbagai referensi untuk memastikan keabsahan dan konsistensi data.

3. ANALISA DAN PEMBAHASAN

3.1 Kronologi dan Dampak Kasus

Kasus kebocoran data *Facebook* oleh *Cambridge Analytica* menjadi sorotan dunia setelah terungkap pada tahun 2018. Perusahaan *Cambridge Analytica* diketahui mengumpulkan dan memanfaatkan data pribadi sekitar 87 juta pengguna *Facebook* tanpa izin. Data tersebut diperoleh melalui aplikasi pihak ketiga bernama *This Is Your Digital Life* yang awalnya dikembangkan untuk tujuan riset akademik, namun ternyata digunakan untuk keperluan politik. (HASIRAH, 2024)

Melalui aplikasi tersebut, *Cambridge Analytica* tidak hanya mengakses data pengguna yang mengisi survei, tetapi juga data teman-teman pengguna tersebut tanpa persetujuan mereka. Informasi yang dikumpulkan kemudian dianalisis untuk membuat profil kepribadian dan preferensi politik, yang selanjutnya digunakan dalam strategi kampanye politik, termasuk dalam pemilihan Presiden Amerika Serikat tahun 2016.

Dampak dari peristiwa ini sangat besar. Dari sisi pengguna, terjadi pelanggaran terhadap hak privasi dan keamanan data pribadi. Dari sisi *Facebook*, kasus ini menimbulkan krisis kepercayaan publik, sanksi hukum dari berbagai negara, serta penurunan nilai saham yang signifikan. Lebih luas lagi, kasus ini membuka mata masyarakat global tentang pentingnya regulasi dan kesadaran akan perlindungan data pribadi di era digital.

Menurut Konsep *Human security*, keamanan termasuk dalam individu dan komunitas. Padakasus ini terlihat jelas bahwa ancaman yang terjadi akibat *microtargeting* yang dibuat oleh *Cambridge Analytica* dapat mengakibatkan permasalahan dalam kehidupan. Dengan mudahnya informasi-informasi yang diberikan pada target-target sesuai dengan kebutuhan perusahaan dan klien ini memberikan efek yang luas sehingga masyarakat dapat terkelabui. Ketika hal seperti ini tidak diregulasi maka tidak hanya masyarakat satu negara saja yang terancam namun masyarakat internasional juga.(Zaelian & Putranti, 2023)

3.2 Pelanggaran Prinsip Etika Profesi

Jika ditinjau berdasarkan kode etik profesi Teknologi Informasi seperti yang dikeluarkan oleh ACM dan IEEE, kasus kebocoran data *Facebook* menunjukkan adanya pelanggaran terhadap beberapa prinsip mendasar.

- a. **Pelanggaran terhadap prinsip kejujuran dan transparansi (honesty and transparency).** *Facebook* gagal memberi penjelasan terbuka kepada pengguna tentang bagaimana data mereka dikumpulkan dan digunakan oleh pihak ketiga. Kurangnya kejelasan mengenai izin akses dan tujuan penggunaan data menunjukkan tidak diterapkannya prinsip keterbukaan yang seharusnya menjadi tanggung jawab etis perusahaan teknologi.
- b. **Pelanggaran terhadap prinsip menghindari bahaya (avoid harm).** Tindakan penyalahgunaan data menyebabkan kerugian bagi pengguna dalam bentuk manipulasi opini, penyebaran informasi palsu, dan gangguan terhadap kebebasan memilih. Hal ini membuktikan bahwa perusahaan tidak berupaya mencegah dampak negatif dari penggunaan teknologi mereka.
- c. **Pelanggaran terhadap prinsip akuntabilitas (accountability).** Sebagai penyedia platform, *Facebook* memiliki tanggung jawab hukum dan moral untuk memastikan keamanan data pengguna. Namun, lemahnya sistem pengawasan terhadap aplikasi pihak ketiga menunjukkan kurangnya tanggung jawab dalam menjaga integritas dan keamanan data yang dipercayakan oleh pengguna.

3.3 Tanggung Jawab Perlindungan Data Pribadi

Dalam perspektif regulasi, kasus kebocoran data *Facebook* oleh *Cambridge Analytica* menjadi contoh nyata lemahnya penerapan perlindungan data pribadi di era digital. Berdasarkan *General Data Protection Regulation (GDPR)* di Eropa dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) di Indonesia, setiap penyelenggara sistem elektronik wajib menjaga keamanan data pengguna dan memastikan pengumpulan data dilakukan atas dasar persetujuan yang sah. Kegagalan *Facebook* dalam mengendalikan penggunaan data oleh *Cambridge Analytica* menunjukkan pelanggaran terhadap prinsip-prinsip dasar perlindungan data pribadi serta kurangnya pengawasan internal terhadap aktivitas pihak ketiga. Selain berdampak pada privasi individu, kasus ini juga menyoroti pentingnya tanggung jawab moral dan profesional penyedia layanan digital dalam menjaga kepercayaan publik. Perlindungan data pribadi tidak cukup diatur melalui kebijakan semata, tetapi harus diwujudkan melalui sistem keamanan yang kuat, audit berkala, serta transparansi terhadap pengguna agar hak privasi mereka benar-benar terjamin.

3.4 Analisis Berdasarkan Teori Etika

Untuk memperdalam pemahaman terhadap pelanggaran yang terjadi, analisis dapat dikaitkan dengan teori-teori etika normatif yang relevan.

- a. **Teori Deontologi**
Teori ini menekankan bahwa suatu tindakan dinilai benar atau salah berdasarkan kewajiban moral yang melekat, bukan akibatnya. Dalam konteks ini, *Facebook* memiliki kewajiban moral untuk menjaga kerahasiaan dan privasi data pengguna. Pelanggaran terhadap kewajiban

tersebut menunjukkan adanya kegagalan dalam menjalankan tanggung jawab etis, terlepas dari tujuan bisnis atau politik yang ingin dicapai.

b. Teori Utilitarianisme

Menurut teori ini, tindakan dianggap benar bila memberikan manfaat terbesar bagi banyak orang. Dalam kasus ini, tindakan *Facebook* dan *Cambridge Analytica* justru menimbulkan kerugian besar bagi jutaan pengguna, seperti pelanggaran privasi dan manipulasi politik. Oleh karena itu, dari perspektif utilitarian, tindakan tersebut jelas tidak etis karena menimbulkan dampak negatif yang lebih besar daripada manfaatnya.

c. Teori Etika Tanggung Jawab

Teori ini menegaskan bahwa setiap individu atau organisasi harus bertanggung jawab atas akibat dari tindakan atau teknologi yang mereka ciptakan. Dalam kasus *Facebook*, kegagalan mengontrol akses pihak ketiga merupakan bentuk kelalaian terhadap tanggung jawab sosial dan profesional. Etika tanggung jawab mengingatkan bahwa setiap keputusan dalam bidang teknologi membawa konsekuensi bagi masyarakat, sehingga harus diambil dengan penuh kesadaran dan integritas moral.

4. KESIMPULAN

Kasus kebocoran data *Facebook* oleh *Cambridge Analytica* menunjukkan bahwa lemahnya perlindungan data pribadi dapat menimbulkan dampak sosial, politik, dan moral yang sangat luas. Pengumpulan dan pemanfaatan data tanpa izin jelas melanggar hak privasi pengguna serta mencerminkan kelalaian penyedia layanan dalam menerapkan tanggung jawab etika profesi di bidang Teknologi Informasi.

Dari hasil analisis, dapat disimpulkan bahwa telah terjadi pelanggaran terhadap prinsip-prinsip dasar etika profesi, seperti kejujuran, tanggung jawab, transparansi, dan akuntabilitas. Tindakan tersebut juga bertentangan dengan prinsip-prinsip perlindungan data pribadi yang diatur dalam *General Data Protection Regulation (GDPR)* maupun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). (Rahmat, 2023)

Penelitian ini menegaskan bahwa tanggung jawab terhadap data pengguna bukan hanya persoalan hukum, melainkan juga kewajiban moral yang harus dijunjung tinggi oleh setiap profesional di bidang teknologi informasi. Untuk mencegah kasus serupa, perusahaan digital perlu memperkuat sistem keamanan siber, meningkatkan transparansi terhadap pengguna, serta memastikan seluruh aktivitas pengelolaan data mematuhi prinsip etika dan peraturan yang berlaku. Kesadaran etis dan integritas profesional harus menjadi dasar utama dalam pengembangan dan operasional layanan digital agar teknologi tidak menjadi ancaman bagi privasi dan kebebasan individu.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga penelitian dengan judul “Studi Kasus Kebocoran Data *Facebook* oleh *Cambridge Analytica*” dapat diselesaikan dengan baik.

Penulis menyampaikan terima kasih kepada dosen pengampu mata kuliah Etika Profesi yang telah memberikan bimbingan, arahan, serta wawasan yang sangat bermanfaat selama proses penyusunan jurnal ini. Ucapan terima kasih juga disampaikan kepada rekan-rekan mahasiswa yang telah berpartisipasi dalam diskusi dan berbagi referensi yang membantu memperkaya isi tulisan ini.

Tidak lupa, apresiasi diberikan kepada berbagai pihak yang telah menyediakan sumber data, literatur, serta informasi yang menjadi dasar dalam analisis penelitian ini. Penulis menyadari bahwa masih terdapat kekurangan dalam penyusunan jurnal ini, sehingga saran dan kritik yang membangun sangat diharapkan untuk penyempurnaan di masa mendatang. Semoga hasil penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang etika profesi teknologi informasi dan perlindungan data pribadi di era digital.

REFERENCES

- Confessore, N. (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. https://www-nytimes-com.translate.goog/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc
- HASIRAH, S. M. (2024). *Analisis Kebocoran Data Facebook-Cambridge Analytica*. 0411, 1–32.
- Katie Harbath, & Collier Fernekes. (2023). History of the Cambridge Analytica Controversy. *Bipartisan Policy Center*. <https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/>
- Kozlowska, I. (2018). *Facebook and Data Privacy in the Age of Cambridge Analytica*. <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/>
- Rahmat, M. (2023). *Cambridge Analytica*. 1–17.
- Zaelany, F. A., & Putranti, I. R. (2023). Pelanggaran Privasi dan Ancaman Terhadap Keamanan Manusia dalam Kasus Cambridge Analytica. *Journal of International Relations Diponegoro*, 9(1), 125–137. <https://doi.org/10.14710/jirud.v9i1.37259>