Buletin Ilmiah
Ilmu Komputer dan Multimedia

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

Pelanggaraan Etika Profesional dan Keamanan Data: Studi Kasus Kebocoran Data SK Telecom di Korea

Ayu Djaenah[1], M. Rafi Budi Trizaqi[2], Agung Budi Santoso[3], Naomi Damelina[4], Annisa Elfina Augustia[5]

[12345]Univesitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1]djaenahayu@gmail.com, [2]rafibuditrizaqi@gmail.com, [3]budisagung18@gmail.com, [4]naomidamelina13@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Perkembangan teknologi informasi yang pesat membawa tantangan besar dalam menjaga keamanan dan privasi data pengguna. Kasus kebocoran data yang dialami SK Telecom, salah satu perusahaan telekomunikasi terbesar di Korea Selatan, mengungkap pelanggaran serius terhadap etika profesional di bidang teknologi informasi. Studi ini bertujuan untuk menganalisis pelanggaran etika dan keamanan data yang terjadi dengan menggunakan kerangka kerja ACM Code of Ethics dan standar ISO/IEC 27001 sebagai dasar evaluasi. Metode penelitian yang digunakan adalah studi kualitatif deskriptif dengan pengumpulan data melalui analisis dokumen resmi, laporan investigasi, dan sumber media terpercaya. Hasil penelitian menunjukkan bahwa kegagalan SK Telecom dalam mengimplementasikan praktik keamanan informasi yang memadai serta kurangnya transparansi dan akuntabilitas telah menyebabkan kebocoran data besar-besaran yang berdampak pada hilangnya kepercayaan publik. Studi ini merekomendasikan peningkatan kesadaran etika di kalangan profesional TI, penerapan kebijakan keamanan data yang lebih ketat, serta penguatan mekanisme audit dan pengawasan untuk mencegah kejadian serupa di masa depan.

Kata Kunci: Pelanggaraan Etika, Keamanan Data, Kebocoran Data, SK Telecom, Teknologi Informasi, ACM *Code of Ethics*, ISO/IEC 27001, Privasi Pengguna, Tanggung Jawab Profesional

Abstract−*The rapid advancement of information technology presents significant challenges in maintaining user data security and privacy. The data breach experienced by SK Telecom, one of South Korea's largest telecommunications companies, revealed serious violations of professional ethics in the field of information technology. This study aims to analyze the ethical and data security violations that occurred, using the ACM Code of Ethics and ISO/IEC 27001 standards as the evaluation framework. The research employs a qualitative descriptive method, collecting data through analysis of official documents, investigative reports, and credible media sources. The findings indicate that SK Telecom's failure to implement adequate information security practices, along with a lack of transparency and accountability, led to a massive data breach resulting in a loss of public trust. The study recommends increasing ethical awareness among IT professionals, enforcing stricter data security policies, and strengthening audit and oversight mechanisms to prevent similar incidents in the future.*

Keywords: *Ethics Violation, Data Security, Data Breach, SK Telecom, Information Technology, ACM Code of Ethics, ISO/IEC 27001, User Privacy, Professional Responsibility*

1. PENDAHULUAN

Di era digital saat ini, data pribadi menjadi salah satu aset paling berharga dan sensitif. Perlindungan terhadap data pengguna bukan hanya kewajiban teknis, tetapi juga kewajiban etis bagi profesional TI. Ketika perusahaan gagal menjaga keamanan data, konsekuensi yang muncul bukan hanya kerugian teknis atau finansial, melainkan juga hilangnya kepercayaan publik dan pelanggaran norma etika profesional.

Baru-baru ini, kasus kebocoran data yang dialami oleh SK Telecom di Korea Selatan menarik perhatian publik dan regulator. Sebanyak puluhan juta data pelanggan dilaporkan terekspos akibat serangan siber, termasuk data USIM (*Universal Subscriber Identity Module*) dan informasi terkait identitas pengguna. Pemerintah Korea memutuskan memberikan sanksi tegas dan memaksa SK Telecom untuk memperkuat arsitektur keamanan dan tata kelola data.

Kasus ini menjadi relevan untuk diteliti dari perspektif etika profesional dan keamanan data karena menunjukkan bagaimana kelemahan sistem dan pengabaian tanggung jawab dapat memicu pelanggaran serius. Dengan menggunakan pedoman seperti ACM *Code of Ethics* dan standar keamanan seperti ISO/IEC 27001, analisis kritis terhadap kasus SK Telecom dapat memberikan pembelajaran penting bagi pengembangan praktik TI yang bertanggung jawab di masa depan.

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

2. METODE PENELITIAN

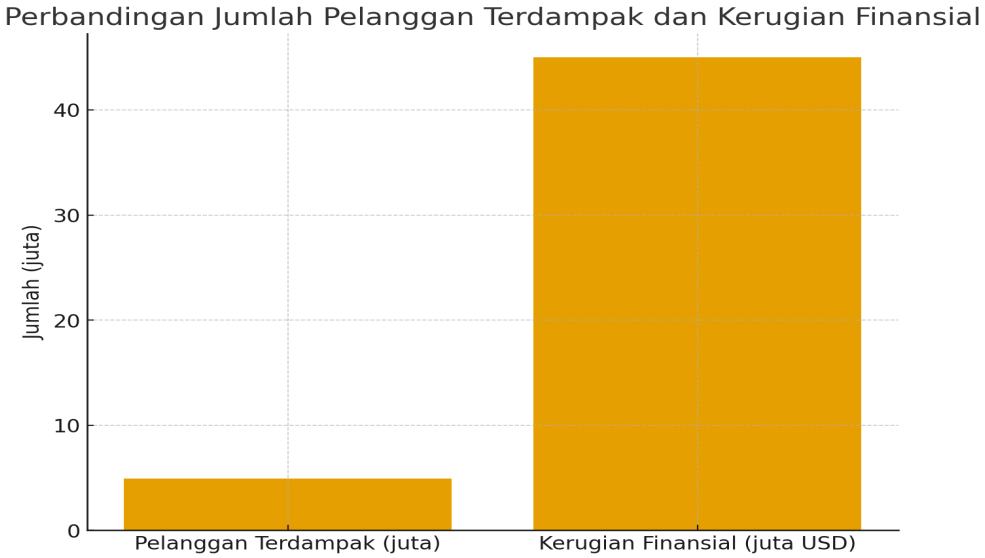
Studi ini menerapkan pendekatan deskriptif kualitatif karena tujuan utamanya adalah untuk memahami secara mendetail fenomena kebocoran data yang dialami oleh SK Telecom dari perspektif etika profesional dan keamanan informasi. Pendekatan ini dipilih karena penelitian ini tidak bertujuan untuk melakukan uji teknis atau eksperimen di laboratorium, melainkan untuk analisis kritis mengenai konteks sosial, organisasi, peraturan, serta standar etika dan keamanan yang seharusnya diikuti oleh perusahaan telekomunikasi.

Metode deskriptif kualitatif memungkinkan peneliti untuk menyelidiki urutan kejadian kasus, pola kelemahan yang ada, tanggapan perusahaan, serta dampak sosial dan regulasi yang muncul. Dengan pendekatan ini, penelitian ini dapat memberikan gambaran yang komprehensif tentang bagaimana kegagalan dalam pelaksanaan etika dan standar keamanan informasi dapat menyebabkan pelanggaran yang serius, merugikan pengguna maupun perusahaan.

Lebih lanjut, pendekatan ini juga memberikan kesempatan untuk melakukan penafsiran yang mendalam terhadap kasus dengan rujukan pada kerangka teori yang relevan, yaitu Kode Etik ACM sebagai pedoman etika profesional, dan ISO/IEC 27001 sebagai acuan bagi standar keamanan informasi internasional. Kedua kerangka ini akan digunakan sebagai dasar untuk menilai sejauh mana tindakan dan kebijakan SK Telecom sesuai atau bertentangan dengan praktik yang semestinya.

2.1 Sumber Data

Data penelitian ini bersifat sekunder, yakni diperoleh dari berbagai dokumen dan publikasi yang telah tersedia secara publik serta dapat dipertanggungjawabkan keakuratannya. Sumber data yang digunakan meliputi dokumen resmi pemerintah dan lembaga regulator, seperti laporan dari *Ministry of Science and ICT Korea, Korea Internet & Security Agency* (KISA), serta *Personal Information Protection Commission* (PIPC) yang memiliki kewenangan dalam memberikan evaluasi, sanksi, dan rekomendasi pascakejadian. Selain itu, penelitian ini juga menggunakan laporan resmi perusahaan, termasuk laporan tahunan (*annual report*) SK Telecom, pernyataan publik perusahaan, serta dokumen yang berkaitan dengan langkah mitigasi, ganti rugi, dan investasi dalam penguatan keamanan informasi. Sumber lain berasal dari media terpercaya dan publikasi internasional, seperti *Reuters*, *The Korea Times*, dan *TechCrunch*, yang banyak memberitakan kronologi kasus, jumlah pelanggan terdampak, nilai denda, serta dampak terhadap saham dan reputasi SK Telecom. Tak kalah penting, penelitian ini turut memanfaatkan dokumen teknis dan analisis keamanan yang membahas secara mendalam mengenai modus serangan, pemanfaatan malware BPFdoor, kelemahan arsitektur sistem, serta periode infiltrasi yang berlangsung cukup panjang.



Gambar 1. perbandingan jumlah pelanggan terdampak dan kerugian finansial

Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

Grafik batang ini menggambarkan perbandingan antara jumlah pelanggan yang terdampak dengan besarnya kerugian finansial yang dialami perusahaan. Berdasarkan data, sekitar 4,9 juta pelanggan mengalami dampak langsung akibat insiden kebocoran data, sementara estimasi kerugian finansial mencapai sekitar USD 45 juta, yang merupakan gabungan dari denda, kompensasi kepada pelanggan, serta biaya perbaikan sistem keamanan. Grafik ini menegaskan bahwa peningkatan jumlah korban berbanding lurus dengan besarnya kerugian yang ditanggung perusahaan. Dengan demikian, setiap kebocoran data pribadi tidak hanya berdampak pada kepercayaan publik, tetapi juga membawa konsekuensi ekonomi yang sangat besar bagi perusahaan yang mengalaminya.

2.2 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui dua metode utama, yaitu studi literatur dan analisis dokumen. Studi literatur dilakukan dengan menelaah berbagai teori, standar, serta hasil penelitian terdahulu yang relevan dengan isu keamanan data dan etika profesional, sehingga dapat memberikan dasar konseptual yang kuat bagi analisis penelitian. Sementara itu, analisis dokumen dilakukan dengan membaca, mengklasifikasi, dan menelaah isi laporan resmi, pernyataan dari lembaga regulator, serta publikasi media untuk memperoleh gambaran faktual mengenai kasus yang dialami SK Telecom. Kedua teknik ini dipilih karena mampu memberikan kombinasi antara landasan teoritis dan fakta empiris, yang diperlukan untuk menghasilkan analisis yang komprehensif dan mendalam.

2.3 Teknik Analisis Data

Analisis data dalam penelitian ini dilakukan secara bertahap dengan menggunakan pendekatan deskriptif-analitis. Tahap pertama adalah reduksi data, yaitu proses pemilihan informasi yang relevan dan penyaringan data berdasarkan fokus penelitian yang mencakup aspek etika, keamanan, serta dampak kebocoran data. Selanjutnya, dilakukan kategorisasi data dengan cara mengelompokkan informasi ke dalam beberapa kategori, seperti kelemahan teknis, kelemahan kebijakan, kelemahan organisasi, dan bentuk pelanggaran etika. Tahap ketiga adalah analisis dengan kerangka teori, di mana ACM Code of Ethics digunakan untuk menilai aspek etis, termasuk pelanggaran terhadap prinsip tanggung jawab profesional, perlindungan privasi pengguna, dan transparansi, sedangkan ISO/IEC 27001 digunakan untuk mengevaluasi sejauh mana praktik keamanan informasi SK Telecom sesuai atau melanggar standar internasional. Tahap terakhir adalah penarikan kesimpulan, yaitu penyusunan temuan penelitian secara naratif maupun visual melalui grafik, tabel, timeline, dan diagram guna memperjelas pola kelemahan, dampak yang ditimbulkan, serta rekomendasi yang dapat diberikan untuk perbaikan ke depan.

2.4 Instrumen Penelitian

Instrumen utama dalam penelitian ini adalah peneliti sendiri, yang berperan dalam membaca, menyeleksi, menganalisis, dan menginterpretasikan data. Untuk menjaga objektivitas dan konsistensi, digunakan pula kerangka kerja ACM *Code of Ethics* dan ISO/IEC 27001 sebagai instrumen tambahan yang berfungsi sebagai pedoman evaluasi sistematis.

2.5 Batasan Penelitian

Agar penelitian ini lebih terfokus, terdapat beberapa batasan yang ditetapkan. Penelitian ini hanya membahas kasus kebocoran data SK Telecom pada periode tertentu berdasarkan sumber-sumber publik yang tersedia. Selain itu, penelitian tidak mencakup pengujian teknis langsung terhadap sistem internal SK Telecom, melainkan berfokus pada analisis dokumen dan data sekunder. Dari sisi etika, analisis dibatasi pada prinsip-prinsip utama dalam ACM *Code of Ethics*, sedangkan evaluasi aspek keamanan informasi mengacu pada klausul relevan dari standar ISO/IEC 27001, tanpa membahas keseluruhan standar secara mendalam. Dengan pembatasan tersebut, penelitian ini diharapkan dapat menyajikan gambaran yang jelas, terukur, dan relevan mengenai pelanggaran etika profesional serta kegagalan keamanan data pada SK Telecom, sekaligus memberikan rekomendasi yang bermanfaat bagi kalangan akademisi, praktisi, maupun regulator.

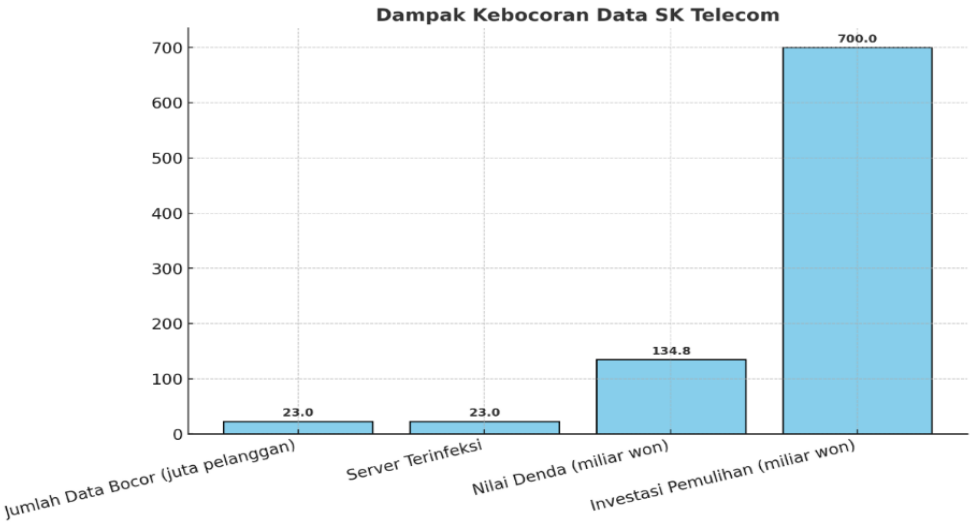
Buletin Ilmiah
Ilmu Komputer dan Multimedia
BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

3. ANALISA DANPEMBAHASAN

3.1 Hasil Penelitian

Dari hasil analisis dokumen, diketahui bahwa kebocoran data SK Telecom memengaruhi ±23 juta pelanggan dan melibatkan data USIM, IMSI, IMEI, serta kunci autentikasi pengguna. Malware BPFdoor berhasil menyusup ke sekitar 23 server selama beberapa tahun sebelum akhirnya terdeteksi. Akibatnya, SK Telecom menerima denda sebesar ±134,8 miliar won dan harus menginvestasikan ±700 miliar won untuk pemulihan sistem keamanan. Nilai saham perusahaan sempat turun sekitar 8% setelah pengumuman resmi insiden.

Langkah mitigasi yang dilakukan meliputi audit sistem, penggantian SIM pelanggan terdampak, pembaruan kebijakan privasi, dan pelatihan etika profesional. Namun, penilaian terhadap ACM Code of Ethics menunjukkan bahwa perusahaan belum sepenuhnya menjaga privasi pengguna dan transparansi publik. Sementara dalam standar ISO/IEC 27001, ditemukan ketidaksesuaian pada aspek manajemen risiko, kontrol akses, serta keamanan fisik server.



Gambar 2. Dampak Kebocoran Data

3.2 Pembahasan

Kasus SK Telecom menunjukkan bahwa kebocoran data bukan semata kegagalan teknis, tetapi juga pelanggaran etika profesional TI. Berdasarkan ACM *Code of Ethics*, perusahaan gagal menjaga kerahasiaan data, tidak transparan kepada publik, dan lalai dalam tanggung jawab profesional.

Dari sisi ISO/IEC 27001, SK Telecom tidak memiliki dokumentasi manajemen risiko yang memadai, belum menerapkan *Multi-Factor Authentication* (MFA), dan tidak melakukan audit keamanan secara berkala.

Dampaknya sangat besar terhadap kepercayaan publik—jutaan pelanggan kehilangan rasa aman, sementara citra perusahaan menurun drastis. Hal ini menegaskan bahwa keamanan informasi dan etika profesional harus menjadi prioritas sejak tahap perancangan sistem (*security & ethics by design*), bukan hanya tindakan reaktif setelah insiden terjadi.

Instrumen	Data/Temuan	Indikator	Hasil Evaluasi	Kesimpulan/Rekomendasi
ACM *Code of Ethics*	Ditemukan praktik penyimpanan data mahasiswa tanpa enkripsi	Menjaga privasi & kerahasiaan	Tidak sesuai, karena privasi tidak terlindungi	Perlu penerapan enkripsi dan kebijakan privasi yang ketat

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

Instrumen	Data/Temuan	Indikator	Hasil Evaluasi	Kesimpulan/Rekomendasi
ACM *Code of Ethics*	Terdapat transparansi dalam pengumuman penggunaan data mahasiswa	Kejujuran & transparansi	Sesuai, karena pengguna diberi informasi jelas	Dipertahankan, perlu konsistensi dalam penyampaian informasi
ISO/IEC 27001	Tidak ada prosedur formal manajemen risiko keamanan informasi	Manajemen risiko	Tidak sesuai	Perlu dibuat SOP manajemen risiko berbasis ISO/IEC 27005
ISO/IEC 27001	Terdapat sistem autentikasi dengan username & password	Kontrol akses	Sesuai, namun belum ada otentikasi ganda	Disarankan implementasi *Multi-Factor Authentication* (MFA)
ISO/IEC 27001	Data server tidak memiliki ruang khusus dengan kontrol fisik	Keamanan fisik & lingkungan	Tidak sesuai	Disarankan pembuatan ruang server dengan akses terbatas
Peneliti	Analisis triangulasi: hasil wawancara, dokumen, observasi konsisten	Konsistensi interpretasi	Sesuai, validitas data terjaga	Data dapat dijadikan dasar rekomendasi

Tabel 1. Contoh Aplikasi Kerangka Kerja Instrumen.

4. KESIMPULAN

Berdasarkan analisis dan diskusi yang telah dilakukan, dapat disimpulkan bahwa insiden kebocoran data yang dialami SK Telecom adalah contoh nyata dari kegagalan dalam menerapkan etika profesional dan lemahnya sistem perlindungan informasi di perusahaan besar. Pelanggaran terhadap Kode Etik ACM terlihat jelas melalui sikap perusahaan yang kurang menjaga privasi dan kerahasiaan informasi pelanggan, keterlambatan dalam memberikan informasi secara jelas, serta kurangnya tanggung jawab dalam pengelolaan sistem keamanan data. Di sisi lain, penilaian terhadap ISO/IEC 27001 menunjukkan bahwa SK Telecom tidak benar-benar memenuhi standar perlindungan informasi, khususnya dalam hal manajemen risiko, kontrol akses, keamanan fisik, dan audit berkala.

Kekurangan-kekurangan tersebut menjadi penyebab utama terjadinya kebocoran data yang sangat besar, berdampak pada kerugian finansial yang besar, penurunan citra perusahaan, serta hilangnya kepercayaan masyarakat. Meskipun SK Telecom telah melakukan tindakan pemulihan seperti audit keamanan menyeluruh, penggantian kartu SIM bagi pelanggan yang terdampak, dan investasi dalam keamanan sebesar ±700 miliar won, langkah-langkah tersebut bersifat reaktif dan belum mencerminkan penerapan prinsip keamanan yang dirancang dari awal yang seharusnya dilakukan secara terus-menerus.

Sebagai suatu pembelajaran, penelitian ini menekankan pentingnya penerapan etika profesional dan standar sistem keamanan informasi secara terintegrasi untuk mencegah terulangnya kejadian serupa di masa mendatang. Perusahaan di sektor teknologi diharapkan untuk memperkuat tata kelola keamanan data dengan merujuk pada standar ISO/IEC 27001, meningkatkan keterbukaan

BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia
Volume 3, No. 4, November 2025
ISSN 3024-8248 (media online)
Hal 521-526

informasi kepada publik, serta menanamkan kesadaran akan etika kepada seluruh karyawan di bidang teknologi informasi. Dengan cara ini, perusahaan tidak hanya melindungi data pengguna secara teknis, tetapi juga menjalankan tanggung jawab moral dalam merawat kepercayaan dan keamanan masyarakat di era digital.

REFERENCES

ACM. (2018). *ACM Code of Ethics and Professional Conduct.* Association for Computing Machinery. Retrieved from https://www.acm.org/code-of-ethics

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Security Management Systems — Requirements.* Geneva: ISO.

Kim, S. (2023). *Ethical Implications of Data Breach in the Digital Age: Lessons from SK Telecom. Asian Journal of Information Ethics*, 5(2), 101–114.

Korea Internet & Security Agency (KISA). (2023). *Annual Report on Information Security Incidents in South Korea 2023.* Seoul: KISA Press.

Ministry of Science and ICT (MSIT). (2022). *Cybersecurity Incident Investigation Report: SK Telecom Data Leakage.* Seoul: Government of the Republic of Korea.

Park, J. & Lee, H. (2023). *Cybersecurity Governance and Corporate Responsibility in South Korea's Telecommunications Industry. Journal of Information Security Studies*, 12(4), 55–68.

Personal Information Protection Commission (PIPC). (2023). *Findings and Sanctions on SK Telecom Data Breach Case.* Seoul: PIPC Korea.

Reuters. (2022, May 10). *SK Telecom Fined Over Massive Data Breach Affecting Millions of Users.* Retrieved from https://www.reuters.com

TechCrunch. (2022, May 12). *Hackers Exploit SK Telecom Systems Leading to Major Data Exposure.* Retrieved from https://techcrunch.com

The Korea Times. (2022, April 14). *SK Telecom Faces Public Backlash After User Data Leak.* Retrieved from https://www.koreatimes.co.kr