TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

# Analisis Etika Profesi IT dalam Kasus Kebocoran Data 91 Juta Pengguna Tokopedia

**Nizar Muharrom[1], Muhammad Wildan U D[2], Rafif Thoriq Wibowo[3], Arfan Prihandika R[4], Annisa Elfina Augustia[5]**

[1-5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1]muharromnizar13@gmail.com, [2]fikarula354@gmail.com, [3]rafifthoriq30@gmail.com, [4]fanprihan@gmail.com, [5]annisa12elfina@gmail.com
(* : coressponding author)

**Abstrak**−Insiden kebocoran data Tokopedia tahun 2020 menjadi perhatian besar dalam sektor teknologi informasi Indonesia. Lebih dari 91 juta data pengguna bocor dan dijual di forum online, mengungkap kelemahan praktik perlindungan data dan keamanan siber di perusahaan digital. Penelitian ini menganalisis pelanggaran etika profesi IT dalam kasus tersebut menggunakan pendekatan studi literatur kualitatif. Data dikumpulkan melalui dokumen resmi, berita kredibel, dan literatur ilmiah terkait etika IT dan keamanan data. Temuan menunjukkan pelanggaran prinsip kerahasiaan, tanggung jawab profesional, dan integritas dalam pengelolaan data pengguna. Dampak kebocoran ini mencakup penurunan kepercayaan publik terhadap Tokopedia sebagai *platform e-commerce* dan meningkatnya urgensi regulasi perlindungan data yang lebih kuat di Indonesia. Studi ini menekankan pentingnya implementasi etika profesi IT untuk menjaga kepercayaan publik dan keamanan *digital* di era ekonomi berbasis data.

**Kata Kunci:** etika profesi IT; kebocoran data; Tokopedia; privasi; keamanan siber

***Abstract***−*The 2020 Tokopedia data breach incident became a major concern in Indonesia's information technology sector. More than 91 million user records were leaked and sold on online forums, exposing weaknesses in data protection practices and cybersecurity within digital companies. This study analyzes violations of IT professional ethics in this case using a qualitative literature review approach. Data was collected through official documents, credible news sources, and scientific literature related to IT ethics and data security. The findings indicate breaches of the principles of confidentiality, professional responsibility, and integrity in managing user data. The impact of this leak includes a decline in public trust towards Tokopedia as an e-commerce platform and an increased urgency for stronger data protection regulations in Indonesia. This study emphasizes the importance of implementing IT professional ethics to maintain public trust and digital security in the data-driven economy era.*

***Keywords****: IT professional ethics; data breach; Tokopedia; privacy; cybersecurity*

## 1. PENDAHULUAN

Perkembangan teknologi informasi di era digital telah membawa kemudahan dalam berbagai aspek kehidupan, mulai dari transaksi ekonomi, layanan publik, hingga aktivitas sosial. Namun, kemajuan tersebut juga menimbulkan tantangan serius terkait keamanan dan privasi data pribadi. Di Indonesia, penggunaan layanan digital semakin meningkat, sehingga potensi risiko kebocoran data menjadi semakin besar dan memerlukan perhatian khusus, terutama dari perspektif etika dan profesionalisme bidang teknologi informasi (TI).

Salah satu insiden terbesar yang pernah terjadi di Indonesia adalah kebocoran sekitar 91 juta data pengguna Tokopedia pada tahun 2020. Informasi penting seperti nama lengkap, alamat email, nomor telepon, hingga password hash diretas dan dijual melalui dark web. Peretasan ini diperkirakan terjadi pada Maret 2020 dan baru terungkap beberapa bulan kemudian setelah data tersebut diperdagangkan di forum daring. Insiden ini tidak hanya meresahkan pengguna karena risiko penyalahgunaan data pribadi, tetapi juga menimbulkan pertanyaan mengenai tanggung jawab etis penyelenggara sistem dalam menjaga keamanan platform digital yang mereka kelola.

Pada saat insiden terjadi, Indonesia belum memiliki regulasi khusus yang mengatur perlindungan data pribadi secara komprehensif. Ketiadaan regulasi yang kuat menyebabkan posisi pengguna menjadi lemah dan menimbulkan tuntutan publik terhadap perlunya standar etika serta tata kelola keamanan yang lebih baik bagi perusahaan teknologi. Dalam konteks profesi TI, kasus Tokopedia menunjukkan perlunya penerapan prinsip etika yang ketat dalam pengelolaan sistem informasi dan data pengguna.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

Profesional TI berkewajiban untuk menjaga kerahasiaan informasi, memastikan integritas sistem, dan meminimalkan risiko yang dapat merugikan masyarakat. Prinsip-prinsip tersebut menekankan pentingnya tanggung jawab moral dan profesional dalam menangani data sensitif. Pelanggaran terhadap prinsip ini dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi, serta merusak kepercayaan publik terhadap layanan digital *(Association for Computing Machinery, 2018).*

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada analisis etika profesi dalam insiden kebocoran data Tokopedia. Permasalahan utama yang dikaji mencakup prinsip etika apa saja yang dilanggar, bagaimana dampak pelanggaran tersebut terhadap pengguna dan reputasi perusahaan, serta rekomendasi yang perlu disusun untuk mencegah terulangnya insiden serupa di masa mendatang.

Penelitian ini juga bertujuan memberikan kontribusi bagi pemahaman akademis dan praktik profesional mengenai pentingnya penerapan etika dalam pengelolaan sistem informasi di era *digital.* Dengan demikian, penelitian ini diharapkan dapat menjadi rujukan dalam mengembangkan kebijakan dan praktik etis yang lebih baik bagi perusahaan teknologi, sehingga keamanan data pengguna dapat terjamin dan kepercayaan masyarakat terhadap layanan digital dapat meningkat.

## 2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk memahami secara mendalam penerapan prinsip etika profesi teknologi informasi dalam kasus kebocoran data 91 juta pengguna Tokopedia pada tahun 2020. Pendekatan kualitatif dipilih karena mampu memberikan penjelasan komprehensif mengenai fenomena sosial yang terjadi, termasuk konteks, nilai moral, dan tanggung jawab profesional yang melatarbelakangi insiden kebocoran data. Melalui pendekatan ini, peneliti berupaya menelaah bagaimana prinsip integritas, kerahasiaan, dan tanggung jawab profesional diterapkan dalam praktik pengelolaan data pribadi pada *platform digital*, serta dampak sosial dan etis yang ditimbulkan akibat pelanggaran etika tersebut.

### 2.1 Jenis dan Sumber Data

Penelitian ini menggunakan data sekunder yang diperoleh dari berbagai literatur ilmiah, dokumen resmi, dan sumber berita kredibel. Sumber data tersebut meliputi jurnal nasional maupun internasional yang terbit antara tahun 2020 hingga 2025, laporan penelitian akademik, serta regulasi dan kebijakan yang berkaitan dengan perlindungan data pribadi di Indonesia, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Pemilihan sumber dilakukan untuk memberikan gambaran terkini mengenai praktik keamanan data dan penerapan etika profesi IT dalam pengelolaan data pengguna.

### 2.2 Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan metode studi pustaka *(library research)*. Peneliti menelusuri referensi yang relevan menggunakan kata kunci seperti Tokopedia data *breach*, etika profesi IT, dan perlindungan data pribadi. Tahapan pengumpulan data meliputi :

a. Menyusun daftar literatur yang kredibel sesuai dengan topik penelitian.
b. Mengumpulkan artikel jurnal, laporan penelitian, dan berita resmi terkait isu kebocoran data.
c. Mengelompokkan data berdasarkan tema etika profesi, keamanan siber, dan dampak sosial.

### 2.3 Teknik Analisis Data

Analisis data dilakukan dengan menggunakan metode analisis isi (*content analysis*) untuk menafsirkan pola dan makna dari berbagai sumber literatur yang dikaji. Tahapan analisis meliputi :

a. Mengidentifikasi permasalahan etika dan pelanggaran prinsip profesional dalam kasus kebocoran data Tokopedia.
b. Mengklasifikasikan temuan berdasarkan prinsip etika, seperti kerahasiaan, tanggung jawab, dan integritas.
c. Membandingkan hasil temuan dengan penelitian terdahulu untuk memperkuat kesimpulan.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

### 2.4 Validitas dan Keabsahan Data

Validitas data dilakukan dengan metode triangulasi sumber, yaitu membandingkan data dari jurnal akademik, berita resmi, dan regulasi pemerintah untuk memastikan keakuratan dan konsistensi informasi. Teknik ini digunakan untuk meningkatkan keabsahan hasil analisis.

## 3. ANALISA DAN PEMBAHASAN

Penelitian ini menganalisis penerapan etika profesi IT dalam konteks kebocoran data 91 juta pengguna Tokopedia tahun 2020. Analisis difokuskan pada identifikasi pelanggaran prinsip etika profesi, evaluasi dampak terhadap berbagai pemangku kepentingan, serta pembelajaran strategis untuk pencegahan insiden serupa di masa depan. Melalui pendekatan studi literatur terhadap berbagai sumber akademis dan laporan resmi, pembahasan ini menyoroti bagaimana kegagalan teknis dalam keamanan data pada dasarnya merupakan manifestasi dari kegagalan penerapan etika profesional.

### 3.1 Identifikasi Pelanggaran Prinsip Etika Profesi

Berdasarkan tinjauan pustaka, etika profesi TI memiliki beberapa pilar utama yang dirumuskan oleh organisasi seperti ACM, mencakup tanggung jawab, penghormatan terhadap privasi, kejujuran, dan kompetensi. Kasus Tokopedia menunjukkan adanya pelanggaran serius terhadap prinsip-prinsip ini.

#### 3.1.1 Pelanggaran Prinsip Kerahasiaan (*Confidentiality*) dan Privasi

Prinsip etika fundamental bagi profesional TI adalah menghormati privasi pengguna dan menjaga kerahasiaan informasi. Prinsip ini juga merupakan bagian inti dari triad keamanan data *(Confidentiality, Integrity, Availability)*. Kebocoran 91 juta data pengguna merupakan bukti kegagalan penerapan prinsip ini. Data sensitif seperti nama lengkap, alamat email, nomor telepon, tanggal lahir dan jenis kelamin, serta *password hash* yang seharusnya dilindungi telah terekspos dan diperjual belikan.

Ini menunjukkan bahwa profesional TI yang bertanggung jawab atas arsitektur dan pemeliharaan sistem di Tokopedia gagal mengimplementasikan mekanisme perlindungan yang memadai untuk menjaga kerahasiaan aset data pengguna. Moric *et al. (2024)* dalam penelitiannya tentang perlindungan data pribadi dalam konteks e-commerce menegaskan bahwa kelemahan sistem keamanan siber dan kurangnya implementasi standar privasi yang memadai menjadi faktor utama terjadinya pelanggaran data pribadi dalam skala besar.

Lebih buruk lagi, setelah data awal bocor, lebih dari 200.000 *password* berhasil di-crack dan dibagikan gratis di forum *hacker*. Ini menunjukkan sistem enkripsi *password* tidak cukup kuat. Ditemukan bahwa kegagalan dalam menerapkan standar enkripsi yang memadai mencerminkan tidak hanya keterbatasan teknis, tetapi juga kurangnya kesadaran etis terhadap tanggung jawab perlindungan data pengguna (Fauzy & Hafizhah, 2023).

#### 3.1.2 Pelanggaran Prinsip Tanggung Jawab Profesional *(Responsibility)*

Profesional TI memiliki tanggung jawab etis terhadap masyarakat untuk memastikan sistem yang mereka bangun dan kelola aman. Kegagalan dalam mencegah peretasan skala besar ini menunjukkan adanya kelalaian dalam memenuhi tanggung jawab tersebut. Aspek tanggung jawab yang dilanggar mencakup beberapa dimensi kritis.

Pertama, dari aspek pencegahan, sistem keamanan tidak cukup tangguh untuk mendeteksi dan mencegah peretasan yang berlangsung dari Maret hingga Mei 2020, selama 2 bulan tanpa deteksi. Kedua, dari aspek deteksi, perusahaan baru mengetahui kebocoran setelah dilaporkan pihak eksternal (*Under the Breach*), bukan dari sistem monitoring internal. Ketiga, respons perusahaan dinilai publik kurang transparan. Tokopedia mengklaim password aman padahal faktanya 200.000 lebih *password* berhasil di-crack. Keempat, tidak ada notifikasi tertulis kepada pengguna yang terdampak sesuai PP No. 71/2019.

Menteri Kominfo *Johnny Plate* harus memanggil Tokopedia untuk investigasi internal, menunjukkan kurangnya inisiatif proaktif dari perusahaan. Keterlambatan deteksi dan respons yang

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

tidak memadai terhadap insiden keamanan merupakan indikator kuat dari lemahnya budaya tanggung jawab profesional dalam organisasi *e-commerce* (Strzelecki & Rizun, 2022).

### 3.1.3 Pelanggaran Prinsip Kompetensi Profesional (*Competence*)

Kode etik ACM menuntut profesional TI untuk terus meningkatkan kompetensi diri dalam praktik profesional. Skala kebocoran data yang masif ini menimbulkan pertanyaan kritis mengenai standar kompetensi keamanan siber yang diterapkan. Indikator kurangnya kompetensi terlihat dari beberapa aspek: sistem enkripsi lemah dimana *password* hash dapat di-*crack* dalam jumlah besar, tidak adanya *multi-factor authentication (MFA)* untuk akses kritis, audit keamanan yang tidak memadai sehingga peretasan tidak terdeteksi selama 2 bulan, tidak adanya sistem monitoring real-time untuk aktivitas mencurigakan, serta *backup* dan *recovery plan* yang tidak efektif.

Profesional TI yang terlibat seharusnya menerapkan standar industri terbaik seperti enkripsi yang kuat, *multi-factor authentication*, dan audit keamanan rutin untuk memitigasi risiko. Fakta bahwa data dapat diekstraksi dan dijual menunjukkan adanya celah keamanan signifikan yang berakar pada kurangnya kompetensi dalam implementasi pertahanan siber. Perkasa dan Saly (2022) menekankan bahwa kegagalan *marketplace* dalam melindungi keamanan data pengguna mencerminkan ketidakmampuan dalam menerapkan standar keamanan teknis yang memadai, yang merupakan tanggung jawab profesional fundamental.

### 3.1.4 Pelanggaran Prinsip Integritas

Integritas mencakup kejujuran dalam berkomunikasi dengan publik. Tokopedia mengklaim *"passwords remain protected through encryption"* padahal faktanya 200.000 lebih *password* berhasil di-crack, data dijual dan disebarkan gratis di berbagai *platform*, serta tidak ada transparansi penuh tentang skala kebocoran. Klaim yang tidak sesuai fakta ini melanggar prinsip integritas profesional. Transparansi dan kejujuran dalam komunikasi pasca-insiden merupakan kewajiban etis yang tidak dapat ditawar, karena berkaitan langsung dengan kepercayaan publik terhadap institusi teknologi (Fauzy & Hafizhah, 2023).

### 3.1.5 Dampak Pelanggaran Etika Profesi

Pelanggaran etika profesi dalam kasus Tokopedia ini tidak hanya bersifat teoretis, tetapi memiliki dampak nyata dan merugikan terhadap berbagai pemangku kepentingan. Dalam penelitian tentang perubahan kepercayaan konsumen pasca-kebocoran data ditemukan bahwa dampak insiden keamanan data meluas ke dimensi ekonomi, psikologis, dan sosial yang kompleks (Strzelecki & Rizun, 2022).

### 3.1.6 Dampak terhadap Pengguna

Dampak langsung terhadap pengguna mencakup beberapa dimensi. Dari aspek risiko keamanan langsung, akun dapat diambil alih oleh pihak tidak berwenang, data pribadi digunakan untuk *phishing* dan penipuan, serta risiko *identity theft* yang meningkat. Dari segi kerugian finansial potensial, pengguna harus mengganti password di berbagai platform jika menggunakan password yang sama, menanggung biaya monitoring kredit dan identitas, serta menghadapi potensi kerugian akibat penipuan berbasis data curian.

Dampak psikologis yang dialami pengguna juga signifikan, meliputi kecemasan tentang privasi, kehilangan kepercayaan terhadap *platform digital*, serta stress akibat harus mengganti berbagai credential. Dampak psikologis dari kebocoran data sering kali diabaikan, padahal dapat mempengaruhi perilaku digital jangka panjang konsumen dan mengurangi partisipasi mereka dalam ekonomi digital (Strzelecki & Rizun, 2022).

### 3.1.7 Dampak Terhadap Perusahaan

Dampak terhadap Tokopedia sebagai perusahaan juga multidimensi. Pertama, terjadi penurunan kepercayaan pengguna. Insiden ini secara langsung mengurangi kepercayaan pengguna. Pengguna yang semula percaya bahwa data pribadi mereka aman menjadi cemas dan ragu terhadap kapabilitas perusahaan dalam melindungi privasi mereka.

Kedua, terjadi perubahan perilaku konsumen. Kehilangan kepercayaan berdampak pada aspek bisnis. secara empiris membuktikan bahwa pelanggaran terhadap privasi data di Tokopedia

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

memiliki dampak yang signifikan terhadap pilihan pembelian konsumen, di mana *perceived behavioral* control berperan utama dalam memengaruhi keinginan belanja pengguna setelah kejadian tersebut. Hal ini menegaskan bahwa etika data lebih dari sekadar masalah kepatuhan, melainkan elemen penting untuk keberlanjutan bisnis digital (Pakpahan et al., 2025).

Ketiga, citra perusahaan terganggu. Reputasi adalah aset penting. Berita mengenai kebocoran data ini berpengaruh signifikan terhadap citra Tokopedia *(Betsy Eliasta Roos et al., n.d.).* Persepsi publik terhadap kredibilitas perusahaan menurun drastis akibat kegagalan dalam menjaga amanah data pengguna.

Keempat, risiko hukum dan regulasi meningkat. Tokopedia dipanggil Kementerian Kominfo untuk investigasi, laporan polisi dibuat meski menargetkan hacker bukan audit internal, serta menghadapi potensi sanksi jika UU PDP sudah berlaku saat itu. Tercatat bahwa *marketplace* sebagai pelaku usaha dapat dikenakan tanggung jawab hukum perdata dan pidana atas kelalaian dalam melindungi data konsumen (Perkasa & Saly, 2022).

Kelima, kerugian finansial yang signifikan meliputi biaya investigasi dan perbaikan sistem, penurunan valuasi perusahaan, serta biaya hukum dan PR *recovery*. Kerugian finansial dari kebocoran data *e-commerce* tidak hanya bersifat jangka pendek, tetapi juga mencakup kerugian jangka panjang dari hilangnya kepercayaan konsumen dan penurunan nilai merek (Morić et al., 2024).

#### 3.1.8 Dampak Sistemik terhadap Ekosistem Digital Indonesi

Dampak insiden Tokopedia meluas ke level ekosistem digital Indonesia secara keseluruhan. Pertama, terjadi erosi kepercayaan publik terhadap *e-commerce* Indonesia. Fauzy dan Hafizhah (2020) menyatakan bahwa kasus-kasus kebocoran data besar seperti Tokopedia menciptakan ketidakpercayaan sistemik terhadap kemampuan industri teknologi Indonesia dalam melindungi data pribadi masyarakat.

Kedua, insiden ini memperlambat adopsi digital di segmen tertentu masyarakat yang menjadi lebih skeptis dan berhati-hati dalam menggunakan layanan digital. Ketiga, meningkatnya tuntutan regulasi yang lebih ketat dari masyarakat dan pemangku kepentingan. Keempat, insiden ini menjadi peringatan serius bagi platform digital lain di Indonesia untuk meningkatkan standar keamanan data mereka.

### 3.2 Analisis Konteks Regulasi

Pada saat insiden terjadi antara Maret hingga Mei 2020, Indonesia belum memiliki Undang-Undang Perlindungan Data Pribadi yang komprehensif. Regulasi yang ada pada saat itu hanya PP No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi. Namun, regulasi ini tidak memiliki sanksi tegas dan enforcement yang kuat.

Kondisi ini menciptakan lingkungan di mana perusahaan tidak merasa urgensi tinggi untuk investasi keamanan data yang memadai. Fauzy dan Hafizhah (2020) mengidentifikasi bahwa kekosongan regulasi yang kuat menjadi salah satu faktor penyebab lemahnya praktik perlindungan data di Indonesia sebelum tahun 2022. Pada saat insiden Tokopedia, Indonesia sedang dalam proses pembahasan RUU Perlindungan Data Pribadi yang stagnan sejak diajukan ke DPR pada Januari 2020.

UU PDP baru disahkan pada Oktober 2022, dua tahun setelah insiden Tokopedia. Hal ini menunjukkan bahwa kasus Tokopedia menjadi salah satu katalis penting untuk mempercepat regulasi perlindungan data di Indonesia. Pengesahan UU PDP mencerminkan kesadaran pemerintah akan urgensi perlindungan data pribadi dalam era ekonomi digital. Perkasa dan Saly (2022) menyatakan bahwa ketiadaan UU PDP pada saat insiden membuat proses hukum menjadi sangat sulit, bahkan gugatan konsumen terhadap Tokopedia ditolak oleh pengadilan karena ketiadaan mekanisme penyelesaian sengketa yang jelas.

### 3.3 Pembelajaran Kunci dan Implikasi Strategis

Pembahasan menyeluruh terhadap kasus Tokopedia ini menguatkan argumen bahwa kegagalan teknis dalam keamanan data pada dasarnya adalah kegagalan etika profesi. Insiden Tokopedia 2020 menjadi studi kasus penting yang menyoroti beberapa pembelajaran kunci.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

Pertama, etika profesi IT bukan hanya pedoman moral, tetapi kebutuhan praktis untuk keberlangsungan bisnis. Secara empiris bahwa pelanggaran etika data berdampak langsung pada keputusan pembelian konsumen, yang pada gilirannya mempengaruhi performa bisnis. Penelitian ini menunjukkan bahwa *perceived behavioral control* menjadi faktor paling dominan mempengaruhi niat pembelian konsumen pasca-kebocoran data (Pakpahan et al., 2025).

Kedua, investasi keamanan data harus dipandang sebagai investasi strategis, bukan biaya operasional. Organisasi *e-commerce* yang memprioritaskan investasi keamanan siber dan implementasi teknologi privacy-enhancing mengalami insiden kebocoran data yang lebih sedikit dan memiliki tingkat kepercayaan konsumen yang lebih tinggi (Morić et al., 2024).

Ketiga, transparansi dan akuntabilitas pasca-insiden sama pentingnya dengan pencegahan. Komunikasi yang jujur dan transparan setelah insiden dapat membantu memulihkan kepercayaan publik lebih cepat dibandingkan dengan sikap defensif atau menyembunyikan informasi. Penelitian ini menunjukkan bahwa konsumen yang menerima komunikasi transparan dari perusahaan cenderung mempertahankan kepercayaan mereka meskipun terjadi kebocoran data (Strzelecki & Rizun, 2022).

Keempat, regulasi yang kuat diperlukan untuk menciptakan *insentif compliance*. Fauzy dan Hafizhah (2020) menyatakan bahwa pengesahan UU PDP memberikan landasan hukum yang lebih kuat untuk penegakan standar perlindungan data dan memberikan efek *deterrence* terhadap kelalaian dalam pengelolaan data pribadi. Namun, efektivitas regulasi sangat bergantung pada mekanisme *enforcement* yang kuat.

Kelima, kompetensi keamanan siber harus menjadi prioritas dalam pendidikan dan pelatihan profesional IT. Perkasa dan Saly (2022) menekankan pentingnya peningkatan kesadaran dan kompetensi keamanan data sebagai bagian integral dari profesionalisme TI, bukan hanya sebagai pengetahuan teknis tambahan.

Keenam, diperlukan perubahan budaya organisasi menuju *security-first mindset*, di mana keamanan data menjadi pertimbangan utama dalam setiap keputusan teknologi, bukan *afterthought.* Moric et al. (2024) menyatakan bahwa organisasi dengan budaya keamanan yang kuat dan penerapan prinsip *privacy by design* cenderung lebih responsif dan efektif dalam mencegah dan menangani insiden keamanan.

Ketujuh, kolaborasi *multi-stakeholder* antara pemerintah, industri, dan akademisi sangat penting untuk menciptakan ekosistem digital yang aman dan terpercaya. Fauzy dan Hafizhah (2020) menekankan bahwa perlindungan data pribadi bukan hanya tanggung jawab perusahaan teknologi, tetapi memerlukan sinergi dari berbagai pihak termasuk pembuat kebijakan, regulator, dan masyarakat.

Analisis komprehensif ini menunjukkan bahwa penerapan etika profesi IT dalam pengelolaan data tidak dapat dipisahkan dari keberhasilan dan keberlanjutan bisnis digital di era *modern*. Kasus Tokopedia menjadi pengingat penting bahwa teknologi tanpa etika adalah resep untuk bencana, dan bahwa kepercayaan adalah aset paling berharga yang harus dijaga oleh setiap profesional dan organisasi teknologi. Lebih dari sekadar isu teknis, kebocoran data Tokopedia mengajarkan bahwa etika profesional IT adalah fondasi dari *trust economy* dalam era *digital*.

## 4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap kasus kebocoran 91 juta data pengguna Tokopedia pada tahun 2020, dapat ditarik kesimpulan sebagai berikut:

a. Telah terjadi pelanggaran serius terhadap prinsip fundamental etika profesi TI, meliputi :
    1. Prinsip Kerahasiaan (*Confidentiality*): Profesional TI gagal melindungi data pribadi pengguna dari akses tidak sah. Lebih dari 91 juta data bocor dan 200.000+ *password* di-*crack*.
    2. Prinsip Tanggung Jawab (*Responsibility*): Kegagalan sistem dalam menjamin keamanan data, deteksi insiden yang lambat (2 bulan tanpa deteksi), dan respons yang dinilai publik kurang transparan.
    3. Prinsip Kompetensi (*Competence*): Ketidakmampuan sistem keamanan dalam memitigasi ancaman siber yang berujung pada peretasan masif, termasuk enkripsi password yang lemah dan tidak adanya MFA.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 469-475

4. Prinsip Integritas: Komunikasi publik yang tidak sepenuhnya transparan tentang skala dan dampak kebocoran.

b. Pelanggaran etika berimplikasi langsung pada erosi kepercayaan public terhadap *platform*, dengan dampak:
    1. Menurunnya kredibilitas Perusahaan
    2. Terpengaruhnya citra merek
    3. Perubahan negatif dalam keputusan pembelian konsumen
    4. Kerugian finansial dan reputasi jangka Panjang
c. Kasus ini menggarisbawahi pentingnya etika profesi TI sebagai landasan moral dan profesional dalam pengelolaan data di era ekonomi digital, serta menyoroti urgensi regulasi perlindungan data yang lebih kuat di Indonesia (yang kemudian terwujud dengan pengesahan UU PDP pada Oktober 2022).

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing mata kuliah Etika Profesi yang telah memberikan arahan dalam penyusunan artikel ini, serta kepada pihak-pihak yang telah menyediakan sumber literatur dan data yang digunakan dalam penelitian ini. Tidak lupa apresiasi kepada rekan-rekan satu tim yang telah bekerja sama dalam penyusunan karya ilmiah ini. Kami harap penelitian ini dapat memberikan manfaat dan kontribusi bagi pengembangan kesadaran etika profesi IT di Indonesia, khususnya dalam penerapan teknologi yang berorientasi pada nilai moral dan tanggung jawab sosial. Penulis menyadari bahwa karya ilmiah ini belum mencapai kesempurnaan, sehingga masukan dan tanggapan yang konstruktif sangat diharapkan untuk perbaikan di masa yang akan datang.

## REFERENCES

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. Https://Www.Acm.Org/Code-of-Ethics.

Betsy Eliasta Roos, A., Setyabudi, D., Nur Suryanto Gono, J., Studi, P. S., & Komunikasi, I. (n.d.). *Pengaruh Terpaan Berita Kebocoran Data Pengguna Tokopedia dan Terpaan E-Word of Mouth Terhadap Citra Tokopedia*. Retrieved November 14, 2025, from https://ejournal3.undip.ac.id/index.php/interaksi-online/article/view/30162

Fauzy, E., & Hafizhah, A. (2023). Legal Analysis of User Personal Data Leak Cases at Tokopedia. In *Mahadi : Indonesia Journal of Law* (Vol. 2, Issue 1). https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. *Journal of Cybersecurity and Privacy*, *4*(3), 731–761. https://doi.org/10.3390/jcp4030034

Pakpahan, F. M., Suratno, T., & Lestari, D. (2025). Pengaruh Pelanggaran Privasi Data Terhadap Keputusan Pembelian Pengguna Tokopedia Menggunakan Theory Of Planned Behavior (TPB). *Infotek: Jurnal Informatika Dan Teknologi*, *8*(2), 686–697. https://doi.org/10.29408/jit.v8i2.30169

Perkasa, J., & Saly, J. N. (2022). *Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020)*.

Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability (Switzerland)*, *14*(10). https://doi.org/10.3390/su14105866