Jurnal Riset Ekonomi Syariah (JRES)
e-ISSN 2798-5253 | p-ISSN 2808-1242
https://journals.unisba.ac.id/index.php/JRES

Tersedia secara online di
Unisba Press
https://publikasi.unisba.ac.id/

Pengaruh Pelanggaran Etika dalam Perkembangan Teknologi Informasi terhadap Kerahasiaan Data Pribadi

Qonita Faizulhyrza Tabayyana*, Nyi Raden Mutiara Rai Purwhanata

Prodi Magister Manajemen, Konsentrasi Manajemen Rumah Sakit, Fakultas Ekonomi dan Bisnis, Universitas Islam Bandung, Indonesia

A R T I C L E I N F O

Article history :

Received : 4/7/2024
Revised : 20/12/2024
Published : 29/12/2024

Volume : 4
No. : 2
Halaman : 145 - 152
Terbitan : **Desember 2024**

Terakreditasi Sinta Peringkat 4 berdasarkan Ristekdikti No. 72/E/KPT/2024

A B S T R A K

Perkembangan teknologi informasi membawa perubahan signifikan dalam berbagai aspek kehidupan, namun juga menimbulkan tantangan terkait keamanan dan privasi data pribadi. Volume dan nilai data pribadi yang tersimpan secara digital rentan terhadap penyalahgunaan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis berbagai bentuk pelanggaran etika dalam perkembangan dan penerapan teknologi informasi. Metodologi yang digunakan adalah pendekatan kualitatif dengan metode *literature review* sistematis, menggunakan teknik purposive sampling untuk menganalisis artikel ilmiah dan buku yang relevan dari database akademik seperti Google Scholar dan Scopus. Hasil penelitian mengidentifikasi berbagai pelanggaran etika, termasuk pengumpulan data berlebihan, penyalahgunaan data, kebocoran data, serta kurangnya transparansi dan kontrol pengguna. Dampak dari pelanggaran ini meliputi kerugian finansial dan emosional, penurunan kepercayaan publik terhadap institusi digital, serta potensi perubahan fundamental dalam struktur sosial dan proses demokrasi. Penelitian ini menghasilkan rekomendasi konkret untuk memperkuat perlindungan data pribadi, termasuk perbaikan kerangka regulasi, peningkatan standar etika dalam pengembangan teknologi, serta strategi untuk memberdayakan pengguna dalam mengelola dan melindungi data pribadi mereka.

Kata Kunci: Etika Teknologi Informasi; Privasi Data; Perlindungan Data Pribadi.

A B S T R A C T

The development of information technology has brought significant changes in various aspects of life but challenges the security and privacy of personal data. The volume and value of digitally stored personal data has made it vulnerable to misuse. This research aims to identify and analyze forms of ethical violations in the development and application of information technology. The methodology used is a qualitative approach with a systematic literature review method, using purposive sampling techniques to analyze relevant scientific articles and books from academic databases namely Google Scholar and Scopus. This research identified forms of ethical violations, including excessive data collection, misuse of data, data leaks, lack of transparency and user control. The impact of this breach includes financial and emotional harm, the public distrust in digital institutions, and the potential for fundamental changes in social structures and democratic processes. This research produces concrete recommendations to strengthen personal data protection, including improvements to the regulatory framework, increased ethical standards in technology development, and strategies to empower users to manage and protect their personal data.

Keywords: Information Technology Ethics; Data Privacy; Personal Data Protection.

Corresponding Author : *tabayyana@gmail.com
Indexed : Garuda, Crossref, Google Scholar
DOI : https://doi.org/10.29313/jres.v4i2.4355

A. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat dalam beberapa dekade terakhir telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Kemudahan akses informasi, efisiensi komunikasi, dan peningkatan produktivitas merupakan beberapa manfaat positif yang dirasakan masyarakat. Di sisi lain, perkembangan teknologi informasi turut banyak digunakan untuk hal-hal yang kurang bermanfaat, seperti bermain game dan media sosial yang berkaitan dengan muncul tantangan baru terkait keamanan dan privasi data pribadi pengguna (Mubarokah, 2023). Jumlah pengguna internet di Indonesia meningkat setiap tahunnya dengan kontribusi hampir sama antara pria dan wanita. Hal ini menunjukkan bahwa kebutuhan akan teknologi internet telah menjadi kebutuhan umum bagi banyak orang (Suryaningsih, Rojak, & Himayasari, 2023). Meningkatnya volume dan nilai data pribadi yang tersimpan secara digital telah menjadikannya sebagai aset yang sangat berharga sekaligus rentan terhadap penyalahgunaan. Berbagai kasus pelanggaran data berskala besar yang terjadi dalam beberapa tahun terakhir, seperti skandal Facebook-*Cambridge Analytica* pada 2018 yang melibatkan penyalahgunaan data 87 juta pengguna (Hamilton et al., 2018), serta peretasan *Equifax* pada 2017 yang mengekspos data pribadi dan keuangan 147 juta warga Amerika (Kuhn, 2018), telah menunjukkan betapa seriusnya ancaman terhadap kerahasiaan informasi pribadi di era digital. Peristiwa-peristiwa tersebut tidak hanya menimbulkan kerugian finansial yang besar, tetapi juga mengikis kepercayaan publik terhadap kemampuan perusahaan dan institusi dalam menjaga keamanan data sensitif yang dipercayakan kepada mereka.

Salah satu akar permasalahan yang menyebabkan terjadinya berbagai pelanggaran data tersebut adalah kurangnya penerapan prinsip-prinsip etika dalam pengembangan dan penggunaan teknologi informasi (De George, 2008). Kemajuan teknologi yang begitu cepat seringkali tidak diimbangi dengan pertimbangan etis yang memadai, sehingga aspek keamanan dan privasi cenderung terabaikan demi mengejar inovasi atau keuntungan bisnis. Praktik pengumpulan data yang berlebihan (*data maximization*) tanpa persetujuan yang jelas dari pengguna, penggunaan algoritma yang bias dalam pengambilan keputusan otomatis, serta kurangnya transparansi dalam pengelolaan data merupakan beberapa contoh pelanggaran etika yang umum terjadi (Stoyanovich et al., 2020). Selain itu, ketidakseimbangan kekuatan (*power asymmetry*) antara perusahaan teknologi raksasa dengan pengguna individual juga menciptakan situasi di mana konsumen seringkali tidak memiliki pilihan selain menyerahkan data pribadi mereka sebagai "harga" untuk mengakses layanan digital yang telah menjadi kebutuhan sehari-hari (Cohen, 2019). Kondisi ini diperparah oleh kerangka hukum dan regulasi yang seringkali tertinggal dalam mengikuti laju perkembangan teknologi, sehingga menciptakan celah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk mengeksploitasi data pribadi demi kepentingan mereka sendiri.

Tulisan ini bertujuan untuk mengidentifikasi dan menganalisis berbagai bentuk pelanggaran etika yang terjadi dalam perkembangan dan penerapan teknologi informasi, dengan fokus khusus pada praktik-praktik yang berpotensi mengancam kerahasiaan data pribadi pengguna. Hal ini mencakup evaluasi terhadap kebijakan pengumpulan dan pengelolaan data oleh perusahaan teknologi, penggunaan algoritma dalam pemrosesan informasi pribadi, serta implementasi sistem keamanan data yang tidak memadai. Kedua, penelitian ini berupaya untuk mengeksplorasi dampak jangka pendek dan jangka panjang dari pelanggaran etika tersebut terhadap privasi individu, kepercayaan publik, serta implikasinya yang lebih luas terhadap struktur sosial dan proses demokrasi. Analisis ini akan meliputi studi kasus tentang insiden pelanggaran data besar-besaran, penggunaan data pribadi untuk manipulasi perilaku, serta potensi penyalahgunaan teknologi *surveillance*. Ketiga, tulisan ini bertujuan untuk merumuskan rekomendasi konkret guna memperkuat perlindungan data pribadi dalam konteks perkembangan teknologi informasi yang pesat. Rekomendasi ini akan mencakup usulan perbaikan kerangka regulasi, peningkatan standar etika dalam pengembangan teknologi, serta strategi untuk memberdayakan pengguna dalam mengelola dan melindungi data pribadi mereka

B. Metode Penelitian

Penelitian ini mengadopsi paradigma interpretivisme dengan pendekatan kualitatif, menggunakan metode *literature review* sistematis untuk mengkaji pengaruh pelanggaran etika dalam perkembangan teknologi informasi terhadap kerahasiaan data pribadi. Metode *literature review* dipilih karena memungkinkan

sintesis komprehensif dari pengetahuan yang ada dan identifikasi kesenjangan dalam literatur terkini. Populasi penelitian mencakup semua artikel ilmiah dan buku membahas tentang etika teknologi informasi, keamanan data, dan privasi digital. Sampel diambil menggunakan teknik purposive sampling dengan kriteria inklusi: (1) diterbitkan dalam jurnal *peer-reviewed* atau oleh penerbit akademik terkemuka, (2) ditulis dalam bahasa Inggris atau Indonesia, (3) memiliki fokus utama pada aspek etika dalam teknologi informasi dan implikasinya terhadap privasi data. Pencarian dilakukan pada database akademik seperti Google Scholar dan Scopus dengan minimal referensi 6 buku dan 20 jurnal. Analisis data menggunakan pendekatan sintesis narasi, yang memungkinkan integrasi temuan dari berbagai sumber dan metodologi. Untuk menjamin kualitas dan objektivitas, proses seleksi dan analisis dilakukan oleh dua peneliti independen, dengan diskusi untuk menyelesaikan perbedaan pendapat. Validitas penelitian ditingkatkan melalui triangulasi sumber data, yang mencakup artikel jurnal, buku teks.

C. Hasil dan Pembahasan

Identifikasi dan Analisis Pelanggaran Etika dalam Teknologi Informasi

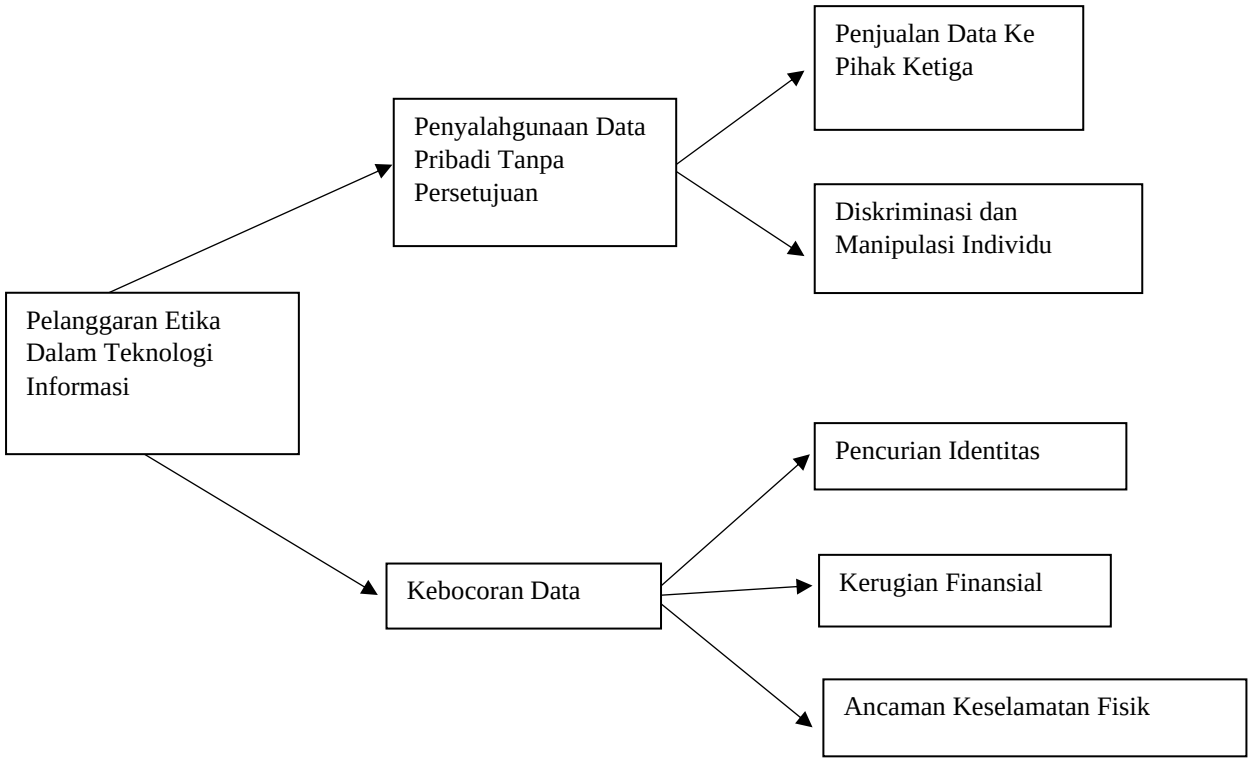
Perkembangan teknologi informasi yang pesat telah membawa berbagai kemudahan dan manfaat bagi kehidupan manusia. Namun, di balik kemajuan tersebut, muncul juga berbagai permasalahan etika yang perlu mendapat perhatian serius. Salah satu isu etika yang paling menonjol dalam konteks teknologi informasi adalah pelanggaran terhadap kerahasiaan data pribadi. Menurut Wisniewski & Page (2022), privasi data merupakan hak fundamental yang harus dilindungi dalam era digital. Namun, realitasnya, banyak perusahaan teknologi dan platform digital yang mengumpulkan, menyimpan, dan menggunakan data pribadi pengguna tanpa izin atau pengetahuan yang memadai dari pemilik data. Praktik ini tidak hanya melanggar prinsip-prinsip etika, tetapi juga berpotensi merugikan individu maupun masyarakat secara luas. Pelanggaran etika semacam ini dapat terjadi dalam berbagai bentuk, mulai dari pengumpulan data yang berlebihan, penyalahgunaan data untuk kepentingan komersial, hingga kebocoran data akibat kelalaian atau serangan siber (Wisniewski & Page, 2022). Masalah ini semakin diperparah dengan fakta bahwa banyak pengguna tidak sepenuhnya memahami bagaimana data mereka dikumpulkan dan digunakan, serta tidak menyadari potensi risiko yang mungkin timbul dari penyalahgunaan data tersebut.

Salah satu bentuk pelanggaran etika dalam konteks teknologi informasi adalah penyalahgunaan data untuk kepentingan komersial tanpa persetujuan yang jelas dari pengguna. Praktik ini sering kali melibatkan penggunaan data pribadi untuk targeting iklan atau penjualan data ke pihak ketiga. Menurut studi yang dilakukan oleh Zuboff (2023), banyak perusahaan teknologi besar mengadopsi model bisnis yang disebut "*surveillance capitalism*", di mana data pribadi pengguna menjadi komoditas utama yang diperdagangkan. Dalam model ini, perusahaan tidak hanya menggunakan data untuk meningkatkan layanan mereka, tetapi juga untuk memprediksi dan mempengaruhi perilaku pengguna demi keuntungan komersial (Zuboff, 2023). Praktik ini berkaitan serius terhadap *ethical concerns*, terutama ketika dilakukan tanpa transparansi dan persetujuan yang memadai dari pengguna. Selain itu, penggunaan algoritma *machine learning* untuk menganalisis data pribadi dapat menghasilkan wawasan yang sangat mendalam tentang individu, yang kemudian dapat digunakan untuk manipulasi psikologis atau diskriminasi (Tay et al., 2022). Misalnya, data tentang riwayat pencarian online atau riwayat pembelian seseorang dapat digunakan untuk menyajikan iklan yang sangat ditargetkan, yang mungkin memanfaatkan kerentanan psikologis atau finansial individu tersebut.

Masalah kebocoran data juga merupakan pelanggaran etika yang serius dan semakin meningkat frekuensinya seiring dengan semakin banyaknya data yang dikumpulkan dan disimpan secara digital. Menurut laporan dari Bisogni & Ashgari, (2020), jumlah insiden kebocoran data terus meningkat dari tahun ke tahun, dengan konsekuensi yang semakin parah bagi korban. Kebocoran data dapat terjadi karena berbagai faktor, mulai dari serangan siber yang disengaja hingga kelalaian dalam pengelolaan keamanan data. Terlepas dari penyebabnya, kebocoran data selalu merupakan pelanggaran serius terhadap privasi dan kepercayaan pengguna. Dampak dari kebocoran data dapat sangat luas dan jangka panjang, termasuk pencurian identitas, kerugian finansial, dan bahkan ancaman terhadap keselamatan fisik dalam kasus-kasus tertentu. Lebih dari itu, kebocoran data dalam skala besar dapat memiliki implikasi sosial yang luas, seperti merusak kepercayaan publik

terhadap institusi digital dan pemerintah (Bisogni & Ashgari, 2020). Hal ini pada gilirannya dapat menghambat adopsi teknologi yang bermanfaat dan inovasi digital yang penting untuk kemajuan sosial dan ekonomi.

Pelanggaran etika dalam teknologi informasi juga sering terjadi dalam bentuk kurangnya transparansi dan kontrol pengguna atas data mereka. Banyak perusahaan teknologi menggunakan kebijakan privasi yang panjang dan sulit dipahami, yang efektif menyembunyikan praktik pengumpulan dan penggunaan data mereka dari pengguna. Menurut penelitian yang dilakukan oleh Schaub et al., (2015), jika pengguna benar-benar membaca setiap kebijakan privasi untuk setiap situs web yang mereka kunjungi, itu akan memakan waktu sekitar 244 jam per tahun. Situasi ini menciptakan asimetri informasi yang signifikan antara perusahaan dan pengguna, di mana pengguna sering kali tidak menyadari sejauh mana data mereka dikumpulkan, digunakan, dan dibagikan. Bahkan, ketika pengguna diberikan opsi untuk mengontrol penggunaan data mereka, opsi tersebut sering kali dirancang dengan cara yang mendorong pengguna untuk memberikan lebih banyak akses data daripada yang mungkin mereka inginkan jika mereka sepenuhnya memahami implikasinya. Praktik ini, yang kadang-kadang disebut sebagai "*dark patterns*" dalam desain antarmuka, merupakan bentuk manipulasi yang melanggar prinsip-prinsip etika tentang otonomi dan *informed consent* (Langner, 2023). Pelanggaran etika dalam teknologi informasi memiliki implikasi yang jauh melampaui tingkat individu. Pada skala yang lebih luas, pelanggaran-pelanggaran ini dapat mengancam fondasi masyarakat demokratis dan terbuka. Seperti yang diargumentasikan oleh Wacks (2015), privasi data bukan hanya masalah perlindungan individu, tetapi juga tentang menjaga ruang untuk perkembangan ide, kreativitas, dan dissent dalam masyarakat. Ketika individu merasa bahwa setiap aspek kehidupan mereka dipantau dan dianalisis, mereka mungkin menjadi lebih berhati-hati dalam mengekspresikan diri atau mengeksplorasi ide-ide baru, yang pada gilirannya dapat menghambat inovasi dan kemajuan sosial (Wacks, 2015).



Gambar 1: Pelanggaran Etika dalam Teknologi Informasi

Berbagai penelitian terdahulu mengindentifikasikan berbagai masalah lain dalam dunia teknologi informasi seperti penyebaran rumor/berita palsu, di mana penelitian oleh Vosoughi et al. (2018) menemukan bahwa berita palsu menyebar lebih cepat dan luas dibandingkan berita yang benar di platform Twitter. Hal ini

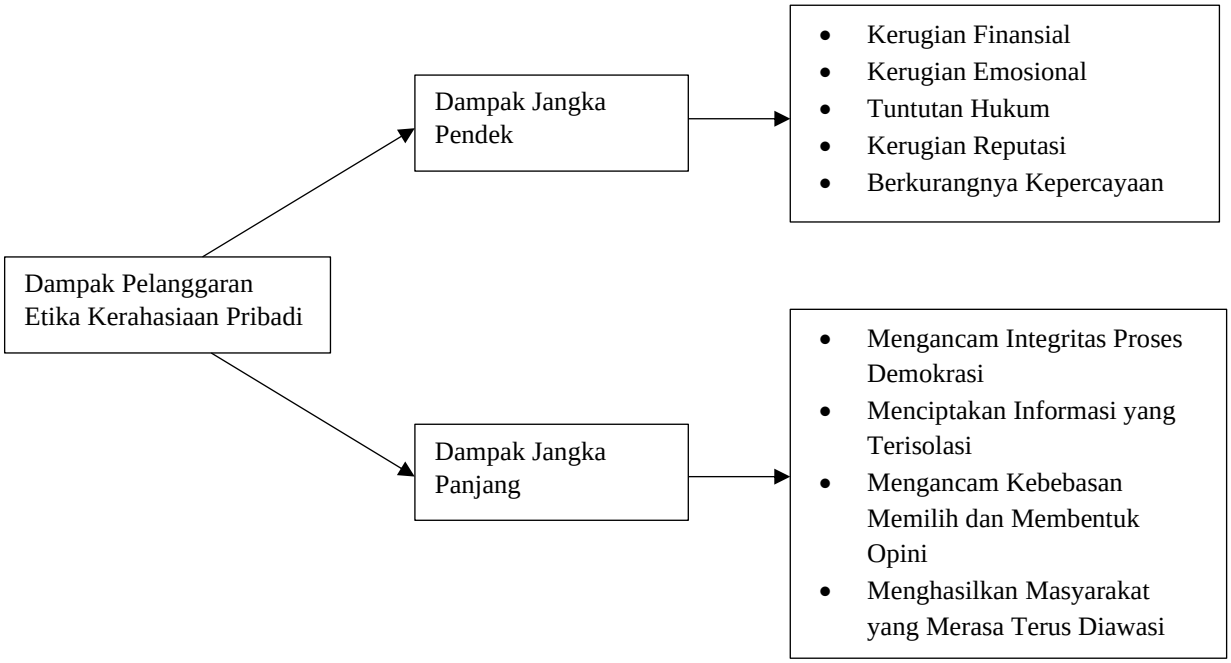
menimbulkan pertanyaan serius tentang tanggung jawab etis platform teknologi dalam memoderasi konten dan melindungi integritas informasi publik. Sementara itu, masalah kecanduan jejaring sosial dan dampaknya terhadap perilaku juga dikonfirmasi oleh studi Twenge et al. (2018) yang menemukan korelasi signifikan antara penggunaan media sosial yang intens dengan peningkatan gejala depresi di kalangan remaja.

Dampak Pelanggaran Etika terhadap Kerahasiaan Data Pribadi

Pelanggaran etika terkait privasi dan data pribadi telah menjadi isu yang semakin krusial di era digital ini. Dalam jangka pendek, insiden pelanggaran data dapat menyebabkan kerugian finansial dan emosional yang signifikan bagi individu yang terdampak. Misalnya, kasus peretasan Equifax pada 2017 yang mengekspos data pribadi dan finansial sekitar 143 juta orang Amerika mengakibatkan risiko pencurian identitas dan penipuan kartu kredit bagi para korban (Gaglione, 2019). Selain itu, perasaan rentan dan hilangnya rasa aman dapat menimbulkan stres psikologis jangka panjang. Dari sisi bisnis, perusahaan yang mengalami kebocoran data seringkali menghadapi konsekuensi serius berupa penurunan kepercayaan pelanggan, kerugian finansial akibat tuntutan hukum, serta kerusakan reputasi yang dapat berlangsung bertahun-tahun. Sebagai contoh, skandal *Cambridge Analytica* yang melibatkan penyalahgunaan data Facebook menyebabkan penurunan drastis nilai saham perusahaan tersebut dan memicu boikot dari pengguna (Natamiharja, 2018). Dalam konteks yang lebih luas, serangkaian pelanggaran etika semacam ini dapat mengikis kepercayaan publik terhadap institusi dan perusahaan teknologi, mendorong skeptisisme terhadap inovasi digital, serta potensial menghambat adopsi teknologi yang sebenarnya bermanfaat bagi masyarakat.

Dampak jangka panjang dari pelanggaran etika terkait privasi dan data lebih kompleks dan berpotensi mengubah struktur sosial secara fundamental. Penggunaan data pribadi untuk manipulasi perilaku, seperti yang terungkap dalam kasus *Cambridge Analytica*, menimbulkan pertanyaan serius tentang integritas proses demokrasi di era digital. Kemampuan untuk menargetkan pesan politik secara presisi berdasarkan profil psikografis individu dapat memperdalam polarisasi politik, menciptakan "*bubble*" informasi yang terisolasi, serta potensial mempengaruhi hasil pemilihan (Hankey et al., 2018). Hal ini menantang asumsi dasar tentang kebebasan memilih dan pembentukan opini publik dalam masyarakat demokratis. Di sisi lain, normalisasi pengawasan massal melalui teknologi *surveillance* canggih seperti pengenalan wajah dan pelacakan lokasi dapat mengubah dinamika kekuasaan antara negara dan warganya (Fontes et al., 2022). Meskipun teknologi ini menjanjikan peningkatan keamanan publik, penggunaannya yang tidak terkontrol berpotensi menciptakan "masyarakat panoptikon" di mana individu merasa terus-menerus diawasi, yang pada gilirannya dapat menekan kebebasan berekspresi dan berserikat. Lebih jauh lagi, akumulasi data personal dalam skala besar oleh perusahaan teknologi telah melahirkan bentuk kapitalisme baru yang disebut "*surveillance capitalism*", di mana pengalaman manusia menjadi bahan baku untuk prediksi dan modifikasi perilaku demi keuntungan komersial (Zuboff, 2015). Fenomena ini berpotensi mengubah hubungan antara bisnis dan konsumen, serta mempertanyakan konsep otonomi individual dalam konteks ekonomi digital.

Studi kasus tentang insiden pelanggaran data tentang pelanggaran data Marriott International pada 2018, yang mengekspos informasi sensitif termasuk nomor paspor dan detail kartu kredit dari sekitar 500 juta tamu hotel (Sanger et al., 2018). Insiden ini mengilustrasikan bagaimana data yang dikumpulkan untuk tujuan bisnis yang sah dapat menjadi target berharga bagi aktor jahat, serta menyoroti tanggung jawab etis perusahaan dalam melindungi informasi pelanggan. Sementara itu, penggunaan data pribadi untuk manipulasi perilaku terlihat jelas dalam kasus Eksperimen Emosi Facebook 2014, di mana platform tersebut memanipulasi umpan berita hampir 700.000 pengguna untuk mempelajari penularan emosi secara online tanpa persetujuan eksplisit (Kramer et al., 2014). Eksperimen ini memicu perdebatan etis tentang batas-batas penelitian perilaku online dan potensi penyalahgunaan kekuatan algoritma media sosial. Dalam konteks *surveillance*, penerapan sistem pengenalan wajah skala besar di Cina untuk tujuan keamanan dan kontrol sosial menyajikan studi kasus yang menggambarkan potensi dan risiko teknologi ini (Fusey & Murray, 2019). Sementara pemerintah Cina mengklaim sistem ini efektif dalam mengurangi kejahatan, kritikus memperingatkan tentang implikasinya terhadap privasi, kebebasan sipil, dan potensi penyalahgunaan kekuasaan. Kasus-kasus ini secara kolektif menggambarkan kompleksitas tantangan etis yang dihadapi masyarakat di era big data dan surveillance digital.



Gambar 2: Dampak Pelanggaran Etika Kerahasiaan Data Pribadi

Strategi Perlindungan Data Pribadi di Era Digital

Dalam era digital yang ditandai dengan pesatnya perkembangan teknologi informasi dan komunikasi, perlindungan data pribadi menjadi semakin krusial dan menantang. Untuk memperkuat perlindungan data pribadi, diperlukan pendekatan multifaset yang melibatkan perbaikan kerangka regulasi, peningkatan standar etika dalam pengembangan teknologi, serta pemberdayaan pengguna. Dari segi regulasi, perlu adanya pembaruan dan harmonisasi undang-undang perlindungan data di tingkat nasional dan internasional untuk mengakomodasi kompleksitas lanskap digital kontemporer. Ini dapat mencakup penerapan prinsip "*privacy by design*" dalam regulasi, yang mengharuskan pertimbangan privasi sejak tahap awal pengembangan produk atau layanan (Levin, 2018). Selain itu, penguatan mekanisme penegakan hukum dan peningkatan sanksi bagi pelanggaran data dapat berfungsi sebagai pencegah yang efektif. Dalam konteks etika pengembangan teknologi, industri perlu mengadopsi dan menginternalisasi prinsip-prinsip etika data yang lebih ketat. Perusahaan teknologi juga perlu didorong untuk menerapkan proses audit etika yang ketat dan transparan dalam siklus pengembangan produk mereka. Sementara itu, pemberdayaan pengguna dapat dicapai melalui peningkatan literasi digital dan privasi di kalangan masyarakat umum. Ini melibatkan kampanye edukasi yang komprehensif tentang risiko privasi online dan strategi perlindungan diri, serta pengembangan alat yang user-friendly untuk memungkinkan individu mengelola preferensi privasi mereka dengan lebih efektif (Acquisti et al., 2015). Lebih lanjut, implementasi sistem persetujuan yang lebih granular dan bermakna dapat memberi pengguna kontrol yang lebih besar atas data mereka. Misalnya, mengadopsi model "*dynamic consent*" di mana individu dapat mengubah preferensi privasi mereka seiring waktu berdasarkan konteks dan kebutuhan yang berubah (Kaye et al., 2015). Selain itu, mendorong pengembangan teknologi yang meningkatkan privasi, seperti *enkripsi end-to-end* dan sistem identitas terdesentralisasi, dapat memberikan lapisan perlindungan tambahan bagi data pengguna. Kolaborasi antara pemerintah, industri, akademisi, dan masyarakat sipil juga penting untuk mengembangkan solusi yang holistik dan efektif dalam menghadapi tantangan privasi di era digital.

Pendekatan untuk merumuskan rekomendasi perlindungan data pribadi ini dapat didasarkan pada beberapa landasan teori dan kerangka konseptual. Teori *Privacy Calculus* menyediakan lensa untuk memahami bagaimana individu membuat keputusan tentang pengungkapan informasi pribadi mereka, menyeimbangkan antara manfaat yang dirasakan dan risiko potensial (Wisniewski & Page, 2022). Berdasarkan teori ini, rekomendasi dapat diarahkan untuk meningkatkan transparansi tentang penggunaan data dan potensi risiko, sehingga memungkinkan pengguna membuat keputusan yang lebih informasi. Sementara itu,

Contextual Integrity Framework yang dikembangkan oleh Shaffer, (2021) menekankan pentingnya mempertimbangkan konteks sosial dalam mengevaluasi praktik informasi. Pendekatan ini mendukung pengembangan kebijakan privasi yang lebih nuansad dan sensitif terhadap norma-norma sosial yang berlaku dalam berbagai domain kehidupan. (Shaffer, 2021) Dari perspektif etika, teori *Capability Approach* dapat diterapkan untuk memahami privasi sebagai aspek penting dari kebebasan dan pembangunan manusia. Ini mendorong fokus pada pemberdayaan individu untuk secara efektif mengelola privasi mereka sendiri, alih-alih hanya mengandalkan perlindungan *top-down* (Gonzales et al., 2019).

D. Kesimpulan

Kesimpulan dari penelitian ini menunjukkan bahwa pelanggaran etika dalam perkembangan teknologi informasi telah mengakibatkan ancaman serius terhadap kerahasiaan data pribadi pengguna. Praktik pengumpulan data berlebihan, penyalahgunaan data untuk kepentingan komersial, serta kebocoran data akibat kelalaian atau serangan siber telah mengikis kepercayaan publik dan berpotensi mengubah struktur sosial secara fundamental. Untuk mengatasi masalah ini, diperlukan pendekatan multifaset yang melibatkan perbaikan kerangka regulasi, peningkatan standar etika dalam pengembangan teknologi, serta pemberdayaan pengguna melalui peningkatan literasi digital. Penting bagi semua pemangku kepentingan - pemerintah, industri, akademisi, dan masyarakat sipil - untuk berkolaborasi dalam mengembangkan solusi holistik guna melindungi privasi di era digital. Dengan menerapkan rekomendasi yang diusulkan, seperti prinsip "privacy by design", model persetujuan yang lebih dinamis, serta pengembangan teknologi yang meningkatkan privasi, diharapkan dapat tercipta ekosistem digital yang lebih aman, etis, dan menghormati hak-hak individu.

Daftar Pustaka

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Bisogni, F., & Asghari, H. (2020). More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. *Journal of Information Policy*, *10*, 45-82. https://doi.org/10.5325/jinfopoli.10.2020.0045

Cohen, J. E. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *Surveillance & Society*, *17*(1/2), 240-245.

De George, R. T. (2008). *The ethics of information technology and business*. John Wiley & Sons.

Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, *71*, 102137. https://doi.org/10.1016/j.techsoc.2022.102137

Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. University of Essex

Gaglione Jr, G. S. (2019). The equifax data breach: an opportunity to improve consumer protection and cybersecurity efforts in America. *Buff. L. Rev.*, *67*, 1133.

González-Cantón, C., Boulos, S., & Sánchez-Garrido, P. (2019). Exploring the link between human rights, the capability approach and corporate responsibility. *Journal of Business Ethics*, *160*(4), 865-879.

Hamilton, L., Robb, E., Fitzpatrick, A., Goel, A., & Nandigam, R. (2018). Generating Text Summaries for the Facebook Data Breach with Prototyping on the 2017 Solar Eclipse. http://hdl.handle.net/10919/86395

Hankey, S., Marrison, J. K., & Naik, R. (2018). *Data and democracy in the digital age*. The Constitution Society, 1-56.

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *European journal of human genetics*, *23*(2), 141-146.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788-8790. https://doi.org/10.1073/pnas.1320040111

Kuhn, M. L. (2018). 147 million social security numbers for sale: Developing data protection legislation after mass cybersecurity breaches. *Iowa L. Rev.*, *104*, 417.

Langner, V. L. (2023). *Influence and ethical impact of design of technology on user behavior* (Doctoral dissertation, Technische Hochschule Ingolstadt). https://nbn-resolving.org/urn:nbn:de:bvb:573-40469

Levin, A. (2018). Privacy by design by regulation: The case study of Ontario. *Can. J. Comp. & Contemp. L.*, *4*, 115.

Mubarokah, A. (2023). View of Market Religion and Religion Marketplace in Digital World. https://doi.org/10.29313/jres.v3i1.1724

Natamiharja, R. (2018). A Case Study on Facebook Data Theft in Indonesia. *Fiat Justisia: Jurnal Ilmu Hukum*, *12*(3), 206-223. https://doi.org/10.25041/fiatjustisia.v12no3.1312

Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018). Marriott Data Breach Traced to Chinese Hackers. *The New York Times*, A1-L.

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 1-17).

Shaffer, G. (2021). Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy*, *11*, 222-265. https://doi.org/10.5325/jinfopoli.11.2021.0222

Stoyanovich, J., Howe, B., & Jagadish, H. V. (2020). Responsible data management. *Proceedings of the VLDB Endowment*, *13*(12).

Suryaningsih, S. S., Rojak, E. A., & Himayasari, N. D. (2023). Analisis Fiqh Muamalah dan Pasal 1320 Kuhperdata terhadap Perjanjian Endorsement Melalui Direct Message. *Jurnal Riset Ekonomi Syariah*, *3*(2), 91–98. https://doi.org/10.29313/jres.v3i2.2790

Tay, L., Woo, S. E., Hickman, L., Booth, B. M., & D'Mello, S. (2022). A conceptual framework for investigating and mitigating machine-learning measurement bias (MLMB) in psychological assessment. *Advances in Methods and Practices in Psychological Science*, *5*(1), 25152459211061337. https://doi.org/10.1177/25152459211061337

Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2018). Increases in depressive symptoms, suicide-related outcomes, and suicide rates among US adolescents after 2010 and links to increased new media screen time. *Clinical psychological science*, *6*(1), 3-17. https://doi.org/10.1177/2167702617723376

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *science*, *359*(6380), 1146-1151. https://doi.org/10.1126/science.aap9559

Wacks, R. (2015). *Privacy: A very short introduction*. OUP Oxford.

Wisniewski, P. J., & Page, X. (2022). *Privacy theories and frameworks. In Modern socio-technical perspectives on privacy* (pp. 15-41). Cham: Springer International Publishing.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75-89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2023). *The age of surveillance capitalism. In Social theory re-wired (pp. 203-213)*. Routledge.