



Dampak Kebijakan Perlindungan Data Terhadap Perilaku Konsumen Di Era Digital

Andre Fahreza

andrefahrezaandre89@gmail.com

Universitas Islam Negeri Sumatera Utara

Muhammad Aidil Azman Lubis

azmanaidil35@gmail.com

Universitas Islam Negeri Sumatera Utara

Nurbaiti

commurbaiti@uinsu.ac.id

Universitas Islam Negeri Sumatera Utara

Korespondensi penulis : *andrefahrezaandre89@gmail.com*.

Abstract *This study aims to qualitatively explore how data protection policies affect consumer behavior in Indonesia's digital ecosystem. Through literature studies and in-depth interviews, it was found that consumers are increasingly aware of the importance of privacy as part of digital identity. Uncommunicative data protection policies trigger resistance in the form of application avoidance and self-control over shared information. However, the privacy literacy gap remains a major obstacle in realizing effective and fair data protection. Therefore, personal data protection must be understood not only as a legal framework, but also as an ethical value that shapes the relationship between consumers, platforms, and the state. This study suggests a multi-level approach through regulation, education, and consumer empowerment to build an inclusive and equitable digital ecosystem.*

Keywords: *Privacy Data, Consumer Behavior, Digital Literacy, Data Protection*

Abstrak Penelitian ini bertujuan untuk mengeksplorasi secara kualitatif bagaimana kebijakan perlindungan data memengaruhi perilaku konsumen dalam ekosistem digital Indonesia. Melalui studi literatur dan wawancara mendalam, ditemukan bahwa konsumen semakin menyadari pentingnya privasi sebagai bagian dari identitas digital. Kebijakan perlindungan data yang tidak komunikatif memicu resistensi dalam bentuk penghindaran aplikasi dan kontrol mandiri atas informasi yang dibagikan. Namun, kesenjangan literasi privasi masih menjadi hambatan utama dalam mewujudkan perlindungan data yang efektif dan adil. Oleh karena itu, perlindungan data pribadi harus dipahami tidak hanya sebagai kerangka hukum, tetapi juga sebagai nilai etis yang membentuk hubungan antara konsumen, platform, dan negara. Penelitian ini menyarankan pendekatan multi-level melalui regulasi, edukasi, dan pemberdayaan konsumen untuk membangun ekosistem digital yang inklusif dan berkeadilan.

Kata kunci: *Data Privasi, Perilaku Konsumen, Literasi Digital, Perlindungan Data*

PENDAHULUAN

Era digital telah mengubah secara fundamental cara konsumen berinteraksi dengan perusahaan dan merek. Setiap aktivitas daring konsumen, mulai dari pencarian informasi, interaksi di media sosial, hingga transaksi e-commerce, meninggalkan jejak digital yang kemudian menjadi sumber data berharga bagi perusahaan. Data konsumen ini dimanfaatkan untuk berbagai kepentingan bisnis seperti personalisasi pengalaman pengguna, pengembangan produk, dan strategi pemasaran yang lebih tepat sasaran. Namun, seiring dengan meningkatnya volume pengumpulan dan pengolahan data konsumen, tumbuh pula kekhawatiran mengenai privasi dan keamanan data

pribadi. Berbagai skandal kebocoran data berskala besar seperti kasus Cambridge Analytica telah membangkitkan kesadaran publik terhadap risiko penyalahgunaan data pribadi. Menanggapi kekhawatiran tersebut, berbagai otoritas regulasi di seluruh dunia telah mengembangkan kebijakan perlindungan data yang bertujuan melindungi hak privasi konsumen. Regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa, California Consumer Privacy Act (CCPA) di Amerika Serikat, dan Undang-Undang Perlindungan Data Pribadi (PDP) di Indonesia menetapkan standar yang lebih ketat mengenai bagaimana perusahaan dapat mengumpulkan, menyimpan, memproses, dan membagikan data konsumen. Kebijakan-kebijakan ini memberikan konsumen kontrol yang lebih besar atas data pribadi mereka melalui hak-hak seperti persetujuan eksplisit (explicit consent), hak untuk mengetahui (right to know), hak untuk dilupakan (right to be forgotten), dan hak untuk meminta penghapusan data (right to erasure). Implementasi kebijakan perlindungan data ini telah menciptakan paradigma baru dalam hubungan antara konsumen dan perusahaan di ekosistem digital. Di satu sisi, perusahaan harus beradaptasi dengan persyaratan regulasi yang lebih ketat, yang seringkali memerlukan investasi signifikan dalam infrastruktur teknologi, proses bisnis, dan sumber daya manusia. Di sisi lain, konsumen kini dihadapkan pada keputusan yang lebih kompleks mengenai siapa yang dapat mengakses data mereka dan untuk tujuan apa. Fenomena ini menimbulkan pertanyaan penting tentang bagaimana kebijakan perlindungan data mempengaruhi perilaku konsumen dalam lingkungan digital, serta implikasinya terhadap strategi bisnis perusahaan.

TINJAUAN TEORITIS

Konsep Perlindungan Data dan Privasi Digital.

Privasi digital merujuk pada hak individu untuk mengendalikan informasi pribadi mereka dalam ekosistem digital. Konsep ini telah berevolusi secara signifikan dari gagasan tradisional tentang "hak untuk dibiarkan sendiri" yang dikemukakan oleh Warren dan Brandeis (1890) menjadi konstruksi multidimensi yang mencakup berbagai aspek pengendalian, transparansi, dan kewenangan atas data pribadi dalam konteks digital (Nissenbaum, 2010). Westin (1967) mendefinisikan privasi sebagai "klaim individu, kelompok, atau institusi untuk menentukan kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain," definisi yang tetap relevan dalam era digital meskipun tantangan implementasinya telah berubah drastis.

Dalam lanskap digital kontemporer, Solove (2008) mengusulkan taksonomi privasi yang mengidentifikasi empat kategori utama aktivitas yang berpotensi problematik: pengumpulan informasi, pemrosesan informasi, diseminasi informasi, dan invasi. Kerangka kerja ini membantu mengkonseptualisasikan berbagai cara di mana privasi digital dapat dilanggar dan menggarisbawahi kompleksitas dalam merancang kebijakan perlindungan data yang efektif. Penelitian yang lebih baru oleh Acquisti et al. (2015) menunjukkan bahwa privasi digital tidak hanya menyangkut perlindungan informasi tetapi juga berkaitan dengan kontrol atas representasi diri dan interaksi sosial dalam ruang digital.

Perkembangan teknologi analitik big data dan kecerdasan buatan telah memperumit lebih lanjut konsep privasi digital. Seperti yang diargumentasikan oleh Zuboff (2019) dalam karyanya tentang "kapitalisme pengawasan," model bisnis dominan di ekonomi digital saat ini bergantung pada ekstraksi, analisis, dan monetisasi data perilaku pengguna dalam skala besar, sering kali dengan sedikit transparansi atau persetujuan bermakna. Praktik-praktik ini menantang paradigma tradisional privasi berbasis persetujuan dan menggarisbawahi kebutuhan akan pendekatan perlindungan data yang lebih nuansa dan kontekstual (Barocas & Nissenbaum, 2014).

Evolusi Kebijakan Perlindungan Data Global

Kebijakan perlindungan data telah mengalami evolusi signifikan selama beberapa dekade terakhir, mencerminkan perubahan dalam teknologi, model bisnis digital, dan kekhawatiran publik. Direktif Perlindungan Data Uni Eropa 1995 menjadi salah satu kerangka hukum perlindungan data komprehensif pertama yang mengatur pemrosesan data pribadi. Namun, kerangka ini menjadi semakin tidak memadai ketika internet berkembang dan praktik pengumpulan data menjadi lebih canggih dan invasif.

GDPR, yang diberlakukan pada Mei 2018, menandai titik balik dalam regulasi perlindungan data global. Dengan cakupan ekstrateritorial, persyaratan persetujuan yang lebih ketat, dan denda yang substansial untuk ketidakpatuhan, GDPR secara fundamental mengubah cara perusahaan mendekati privasi data. Golia dan Stamelou (2020) mengamati bahwa GDPR telah menciptakan efek riak global, mendorong yurisdiksi di luar Uni Eropa untuk memperbarui atau memperkuat kerangka perlindungan data mereka sendiri.

Di Amerika Serikat, pendekatan terhadap perlindungan data historis telah bersifat sektoral dan terfragmentasi. Namun, pemberlakuan CCPA pada 2020 menandai pergeseran ke arah perlindungan konsumen yang lebih komprehensif, meskipun masih dengan perbedaan filosofis dan implementasi yang signifikan dari model Eropa (Chander et al., 2019). Peraturan negara bagian lainnya seperti Virginia Consumer Data Protection Act dan Colorado Privacy Act telah mengikuti, menciptakan mosaik regulasi yang kompleks bagi bisnis yang beroperasi secara nasional.

Di Asia, lanskap perlindungan data juga telah berevolusi secara signifikan. Jepang memperbarui Undang-Undang Perlindungan Informasi Pribadi pada 2020 untuk menyelaraskan lebih dekat dengan GDPR, sementara keputusan kecukupan privasi data antara Jepang dan Uni Eropa menetapkan preseden penting untuk harmonisasi regulasi lintas batas. Korea Selatan, Singapura, dan Thailand telah memperkuat kerangka perlindungan data mereka juga, sementara Indonesia sedang dalam proses akhir pengesahan UU Perlindungan Data Pribadi yang komprehensif. Greenleaf (2019) mencatat bahwa meskipun ada perbedaan regional yang signifikan, tren global mengarah pada konvergensi yang lebih besar dalam prinsip-prinsip dasar perlindungan data, dengan GDPR sering berfungsi sebagai model referensi.

Perilaku Konsumen dan Privasi Digital

Hubungan antara kebijakan privasi dan perilaku konsumen digital telah menjadi fokus penelitian yang berkembang. Norberg et al. (2007) mengidentifikasi fenomena yang disebut "privacy paradox," di mana konsumen mengekspresikan kekhawatiran tinggi tentang privasi namun sering bertindak dengan cara yang tidak konsisten dengan kekhawatiran tersebut, secara sukarela membagikan informasi pribadi untuk keuntungan yang relatif kecil. Studi selanjutnya oleh Kokolakis (2017) menunjukkan bahwa paradoks ini terus berlanjut dalam era big data, meskipun konsumen semakin sadar tentang risiko privasi.

Barth dan de Jong (2017) mengusulkan model pengambilan keputusan privasi yang menjelaskan paradoks ini melalui lensa pertukaran sosial dan teori prospek. Menurut model mereka, konsumen sering membuat keputusan privasi berdasarkan pertimbangan manfaat langsung versus risiko yang tampak jauh dan abstrak. Namun, Athey et al. (2017) menemukan bahwa ketika konsumen diberi informasi yang jelas tentang risiko privasi dan pilihan yang bermakna, perilaku mereka cenderung lebih selaras dengan preferensi privasi yang dinyatakan.

Implementasi GDPR telah memberikan kesempatan unik untuk meneliti bagaimana perubahan kebijakan berdampak pada perilaku konsumen. Aridor et al. (2020) menemukan bahwa setelah GDPR, situs web di UE mengalami penurunan pengunjung sebesar 10% tetapi peningkatan dalam

tingkat konversi, menunjukkan bahwa sementara beberapa konsumen memilih keluar dari pengumpulan data, mereka yang tetap menunjukkan keterlibatan yang lebih kuat. Demikian pula, Goldberg et al. (2021) mengidentifikasi perubahan dalam pola penelusuran web setelah implementasi GDPR, dengan pengguna menjadi lebih selektif tentang situs web mana yang mereka kunjungi.

Di kawasan Asia, Shin dan Park (2019) menemukan bahwa konsumen Korea menunjukkan kesadaran privasi yang lebih tinggi setelah penguatan Undang-Undang Perlindungan Informasi Pribadi negara tersebut, dengan dampak yang terutama terlihat pada preferensi mereka untuk layanan lokal yang dianggap lebih sesuai dengan regulasi nasional. Di Indonesia, studi terbatas oleh Widagdo dan Susanto (2021) mengindikasikan bahwa kesadaran dan kepedulian terhadap privasi di kalangan konsumen digital Indonesia sedang meningkat, meskipun masih tertinggal dibandingkan dengan rekan-rekan mereka di negara dengan kerangka perlindungan data yang lebih mapan.

Kepercayaan Merek dan Transparansi Data

Kepercayaan telah lama diakui sebagai komponen kritis dalam hubungan konsumen-merek, dan dimensi ini menjadi semakin penting dalam konteks keputusan berbagi data. Martin et al. (2017) menunjukkan bahwa kepercayaan terhadap merek secara signifikan mempengaruhi kesediaan konsumen untuk berbagi data pribadi, dengan transparansi menjadi anteseden kunci dari kepercayaan tersebut. Studi oleh Morey et al. (2015) menemukan bahwa perusahaan yang transparan tentang bagaimana mereka mengumpulkan, menggunakan, dan melindungi data konsumen dapat menikmati keunggulan kompetitif yang signifikan, dengan konsumen menunjukkan kesediaan yang lebih besar untuk berbagi data dengan merek tersebut.

Dalam penelitian komparatif mereka, Okazaki et al. (2020) menemukan bahwa kekhawatiran privasi membentuk kepercayaan merek secara berbeda di berbagai konteks budaya, dengan konsumen di negaranegara dengan orientasi kolektif yang kuat (seperti beberapa negara Asia) dan derajat penghindaran ketidakpastian yang tinggi menunjukkan sensitivitas yang lebih besar terhadap bagaimana data mereka dikelola. Temuan ini menyarankan bahwa perusahaan multinasional perlu menyesuaikan strategi transparansi data mereka berdasarkan norma budaya lokal.

Penelitian terbaru oleh Liu et al. (2022) menunjukkan bahwa transparansi dalam kebijakan privasi bukanlah sekedar masalah kepatuhan hukum tetapi juga alat strategis untuk membangun hubungan konsumen yang kuat. Studi mereka mengidentifikasi tiga tingkat transparansi data yang mempengaruhi kepercayaan konsumen: informasi tentang data apa yang dikumpulkan, bagaimana data digunakan, dan kontrol yang diberikan kepada konsumen atas data mereka. Perusahaan yang unggul dalam semua dimensi ini menunjukkan tingkat kepercayaan konsumen dan nilai seumur hidup pelanggan yang secara signifikan lebih tinggi.

Strategi Adaptasi Bisnis dalam Rezim Perlindungan Data Baru

Implementasi kebijakan perlindungan data yang lebih ketat telah mendorong perusahaan untuk mengadopsi strategi adaptasi yang beragam. Malgieri dan Custers (2018) mengategorikan respons perusahaan terhadap GDPR menjadi tiga pendekatan: minimalis (fokus pada kepatuhan dasar), strategis (mengggunakan kepatuhan sebagai diferensiasi kompetitif), dan transformatif (mengadopsi privasi sebagai nilai inti). Martin dan Murphy (2017) berpendapat bahwa perusahaan yang mengadopsi pendekatan transformatif lebih mungkin untuk mendapatkan kepercayaan konsumen jangka panjang dan keunggulan kompetitif.

Salah satu tantangan utama bagi perusahaan adalah menyeimbangkan personalisasi dengan kekhawatiran privasi. Aguirre et al. (2016) menemukan bahwa personalisasi dapat meningkatkan

respons konsumen positif ketika konsumen merasa memiliki kendali atas data mereka, tetapi dapat membangkitkan "kengerian personalisasi" ketika konsumen merasa dibombardir atau diawasi. Dalam studi yang lebih baru, Karwatzki et al. (2022) menunjukkan bahwa perusahaan dapat mengurangi respons negatif terhadap personalisasi melalui transparansi tentang bagaimana rekomendasi dibuat dan memberikan kontrol yang bermakna kepada konsumen.

Implementasi GDPR juga telah mendorong banyak perusahaan untuk memfokuskan kembali strategi data mereka. Johnson dan Shriver (2021) menemukan bahwa setelah GDPR, sebagian besar perusahaan mengurangi jumlah data yang mereka kumpulkan tetapi meningkatkan upaya untuk mendapatkan nilai dari data yang mereka miliki, menghasilkan strategi "less but better" dalam pemanfaatan data konsumen. Demikian pula, Jia et al. (2019) mengobservasi pergeseran dari strategi pengumpulan data "just in case" menjadi pendekatan yang lebih bertarget dan berorientasi tujuan.

Dalam konteks Indonesia, studi oleh Maulana dan Fitrianto (2020) menunjukkan bahwa perusahaan teknologi lokal mengadopsi pendekatan bertahap terhadap kepatuhan perlindungan data, dengan banyak yang melihat peningkatan praktik pengelolaan data sebagai kesempatan untuk meningkatkan kepercayaan dalam layanan digital yang masih berkembang. Namun, kendala sumber daya dan ketidakjelasan dalam implementasi regulasi tetap menjadi tantangan signifikan, terutama bagi perusahaan kecil dan menengah.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk memahami secara mendalam bagaimana kebijakan perlindungan data mempengaruhi perilaku konsumen di era digital. Pendekatan kualitatif dipilih karena mampu menggambarkan persepsi, sikap, serta pengalaman individu secara kontekstual dan holistik terhadap isu perlindungan data pribadi dalam kehidupan digital sehari-hari (Liu Chen & Ye 2022).

1. Jenis Penelitian

Jenis penelitian ini bersifat kualitatif interpretatif, yang menekankan pada eksplorasi makna dan dinamika sosial yang muncul akibat interaksi konsumen dengan kebijakan privasi digital. Dalam konteks ini, konsumen diposisikan sebagai subjek aktif yang memaknai kebijakan perlindungan data berdasarkan pengalaman, tingkat kesadaran, serta kepercayaan terhadap platform digital. (Widagdo & Susanto 2021)

2. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui wawancara mendalam dan observasi partisipatif terhadap konsumen digital yang aktif menggunakan layanan berbasis internet seperti e-commerce, media sosial, dan layanan keuangan digital. Informan dipilih menggunakan teknik purposive sampling dengan kriteria: Berusia minimal 18 tahun; Aktif menggunakan internet untuk transaksi digital dalam 6 bulan terakhir; Memahami atau pernah membaca kebijakan privasi digital pada platform yang digunakan. Selain itu, dokumentasi kebijakan privasi dari beberapa platform populer juga dikumpulkan untuk dianalisis sebagai pelengkap data lapangan. Data dikumpulkan dalam bentuk rekaman audio dan transkrip tertulis yang kemudian dianalisis secara sistematis. (Okazaki & Hirose 2020)

3. Teknik Analisis Data

Analisis data dilakukan dengan pendekatan analisis tematik (thematic analysis) yang terdiri dari beberapa tahapan, yaitu: familiarisasi terhadap data transkrip, pengkodean data secara terbuka, identifikasi tema utama, interpretasi makna di balik tema, dan penarikan kesimpulan interpretatif berdasarkan konteks sosial dan digitalisasi.

Validitas data dijaga melalui teknik triangulasi sumber dan metode, serta konfirmasi informan (member checking) untuk memastikan bahwa interpretasi peneliti sesuai dengan pengalaman informan. (Golia & Stamelou 2020)

4. Etika Penelitian

Seluruh partisipan diberikan informasi yang jelas dan persetujuan tertulis sebelum wawancara dilakukan. Peneliti menjamin kerahasiaan identitas informan dan menggunakan data semata-mata untuk keperluan akademik. Prinsip etis seperti transparansi, anonimitas, dan informed consent dijalankan secara ketat sesuai standar penelitian sosial modern. (Martin & Murphy 2019)

HASIL DAN PEMBAHASAN

Penelitian ini menggali secara mendalam bagaimana kebijakan perlindungan data pribadi membentuk, mengubah, dan mempengaruhi perilaku konsumen dalam ekosistem digital Indonesia. Melalui pendekatan kualitatif berbasis studi literatur dan wawancara terhadap pengguna digital lintas generasi, ditemukan bahwa persepsi konsumen terhadap data pribadi kini tidak lagi bersifat pasif, melainkan telah berkembang menjadi arena negosiasi yang aktif dan kritis. Pembahasan berikut dibagi ke dalam lima subtema utama.

1. Privasi sebagai Reaksi terhadap Ketidakpastian Digital

Dalam konteks masyarakat digital, privasi tidak lagi dimaknai sebatas “hak untuk tidak diganggu,” melainkan telah bertransformasi menjadi bentuk resistensi terhadap ketidakpastian struktural yang menyelimuti praktik pengumpulan data. Para responden dalam penelitian ini mengungkapkan bahwa mereka merasakan ambiguitas dan kekhawatiran saat menggunakan platform digital, terutama yang tidak secara eksplisit menjelaskan bagaimana data mereka dikelola dan untuk tujuan apa informasi itu digunakan.

Kekhawatiran ini diperkuat oleh maraknya praktik profiling konsumen, pelacakan lokasi secara real-time, serta integrasi lintas platform yang membuat konsumen merasa kehilangan kendali atas informasi pribadinya. Sebagaimana diteorikan oleh Helen Nissenbaum dalam konsep contextual integrity, pelanggaran privasi terjadi bukan hanya karena data dikumpulkan, tetapi karena data digunakan di luar konteks sosial yang diharapkan oleh pemiliknya. (Affandi, Dasuha & Parapat 2025)

Dalam praktiknya, pengguna menanggapi ketidakpastian ini dengan mulai membatasi aktivitas daring yang bersifat terbuka, seperti menyembunyikan tanggal lahir, menonaktifkan geolokasi, hingga membuat akun alternatif. Artinya, privasi bukan sekadar hak, tetapi juga reaksi adaptif terhadap ketidakjelasan relasi antara individu dan sistem digital yang semakin invasif.

2. Kebijakan Perlindungan Data sebagai Indikator Kepercayaan

Penelitian ini menemukan bahwa keberadaan dan kualitas kebijakan perlindungan data sangat memengaruhi tingkat kepercayaan konsumen terhadap platform digital. Dalam wawancara, banyak informan menyatakan bahwa mereka lebih memilih menggunakan aplikasi atau layanan yang secara eksplisit mencantumkan komitmen terhadap pengelolaan data pribadi, termasuk fitur penghapusan akun permanen, pengaturan granular atas izin data, dan kebijakan penghapusan otomatis data tidak aktif. (Wati & Widodo 2024)

Sebaliknya, platform yang menyajikan kebijakan privasi dalam bahasa legalistik dan tanpa pemahaman praktis justru menimbulkan keraguan dan ketidaknyamanan. Konsumen cenderung merasa bahwa perusahaan yang tidak terbuka dalam praktik privasinya adalah pihak yang tidak menghormati otonomi digital mereka.

Penelitian Liu et al. (2022) memperkuat temuan ini dengan menyatakan bahwa transparansi dan kontrol yang diberikan kepada konsumen secara langsung membentuk loyalitas dan keterikatan emosional terhadap suatu merek digital, bahkan lebih dari fitur produk itu sendiri. Dengan demikian, kebijakan perlindungan data telah berevolusi dari sekadar instrumen regulatif menjadi elemen pembentuk hubungan emosional dan sosial antara perusahaan dan konsumennya.

3. Perilaku Konsumen: Antara Adaptasi, Resistensi, dan Ambivalensi

Wawancara dengan informan memperlihatkan adanya tiga bentuk utama respons perilaku terhadap risiko privasi:

a. Adaptasi Proaktif

Konsumen yang memiliki literasi digital memadai menunjukkan perilaku adaptif seperti menggunakan browser dengan fitur pelindung privasi, VPN, serta aplikasi pengelola izin (permission manager). Mereka secara sadar mengatur jenis data apa yang dibagikan dan ke platform mana. (Zuboff, 2019)

b. Resistensi Selektif

Kelompok ini menolak menggunakan layanan yang dianggap melanggar prinsip privasi. Contohnya, menolak aplikasi pinjaman online yang meminta akses kontak, atau menolak menggunakan layanan cloud asing karena takut data disalahgunakan. Tindakan ini dilakukan sebagai bentuk perlindungan diri dari kemungkinan penyalahgunaan data.

c. Ambivalensi Fungsional

Namun, ada pula kelompok yang menyadari risiko privasi tetapi tetap menggunakan aplikasi invasif karena alasan fungsional—misalnya transportasi, layanan keuangan, atau pembelajaran daring. Konsumen ini mengalami konflik antara kebutuhan praktis dan kesadaran etis, yang dalam teori disebut sebagai *privacy paradox*. Paradoks ini mencerminkan realitas kompleks di mana konsumen terjebak dalam sistem digital yang tidak sepenuhnya memberi alternatif etis, sehingga membuat pilihan berdasarkan pertimbangan kompromistis.

4. Literasi Privasi dan Kesenjangan Akses Pengetahuan

Literasi privasi muncul sebagai determinan utama dalam perilaku konsumen digital. Penelitian ini mencatat bahwa tingkat pemahaman terhadap hak-hak data sangat variatif, tergantung pada usia, tingkat pendidikan, serta eksposur terhadap isu teknologi.

Konsumen muda (18–25 tahun) memiliki kemampuan teknis, tetapi sering kali mengabaikan aspek regulatif dan etika. Sebaliknya, konsumen berusia 40 tahun ke atas cenderung lebih berhati-hati, tetapi lemah dalam pemahaman teknis seperti enkripsi, cookie, dan pelacakan data. Kondisi ini menunjukkan kesenjangan literasi privasi sebagai tantangan besar dalam pelaksanaan efektif kebijakan perlindungan data pribadi. Edukasi yang hanya bersifat formal tidak cukup; diperlukan pendekatan kontekstual dan berbasis pengalaman agar konsumen dapat menavigasi lingkungan digital secara kritis. Program edukatif yang dikembangkan pemerintah dan LSM harus mempertimbangkan diversitas sosial-budaya konsumen Indonesia, agar tidak mengulang model literasi yang eksklusif dan elitis.

5. Privasi sebagai Nilai Strategis dan Etika Bisnis Digital

Temuan terakhir dari penelitian ini menyoroti pentingnya privasi sebagai nilai strategis dalam lanskap bisnis digital. Di era di mana reputasi perusahaan dapat jatuh karena satu pelanggaran data, banyak platform mulai menyadari bahwa etika data menjadi komoditas reputasional. Hal ini mendorong munculnya inisiatif-inisiatif seperti “privacy-first marketing,” audit privasi independen, dan sertifikasi “trust platform” oleh lembaga eksternal. Beberapa perusahaan rintisan lokal bahkan secara sadar memosisikan diri sebagai “platform etis” dengan menampilkan sertifikasi keamanan dan kebijakan data yang mudah dipahami. Konsumen pun mulai menyadari dan menghargai komitmen ini dengan memilih platform yang menunjukkan empati dan keterbukaan. Seperti dikemukakan Martin & Murphy (2019), privasi bukan lagi sekadar risiko hukum, tetapi merupakan bagian dari keunggulan kompetitif perusahaan dalam membangun loyalitas dan hubungan jangka panjang dengan konsumen.

KESIMPULAN DAN SARAN

Penelitian ini menegaskan bahwa kebijakan perlindungan data pribadi memainkan peran yang semakin sentral dalam membentuk perilaku dan kesadaran konsumen digital di Indonesia. Konsumen tidak lagi pasif dalam menyikapi pengumpulan data oleh platform digital, melainkan mulai memperlihatkan sikap kritis, adaptif, dan selektif terhadap layanan yang mereka gunakan. Kebijakan perlindungan data yang transparan, komunikatif, dan ramah pengguna berkontribusi langsung pada pembentukan kepercayaan konsumen, sedangkan kebijakan yang ambigu atau disusun dalam bahasa teknis justru memicu keraguan dan resistensi. Temuan lapangan menunjukkan bahwa sebagian besar konsumen telah mengidentifikasi data pribadi sebagai representasi digital dari identitas mereka—sehingga pengelolannya tidak dapat dipisahkan dari hak atas privasi dan kendali diri. Dalam konteks ini, kebijakan perlindungan data harus dipandang tidak hanya sebagai kewajiban hukum, tetapi sebagai komitmen etis dan instrumen membangun loyalitas konsumen. Namun demikian, penelitian ini juga mengungkap masih adanya tantangan signifikan berupa ketimpangan literasi digital, rendahnya pemahaman terhadap hak data, serta minimnya keterlibatan publik dalam desain dan pengawasan kebijakan privasi.

Maka dari itu, perlu disampaikan beberapa saran sebagai implikasi praktis dari penelitian ini. Pertama, negara dan regulator harus memperluas cakupan implementasi kebijakan perlindungan data tidak hanya di ranah hukum formal, tetapi juga melalui pendekatan edukatif dan partisipatif, termasuk pelatihan privasi berbasis komunitas dan integrasi kurikulum hak digital dalam pendidikan formal. Kedua, perusahaan teknologi harus memposisikan diri bukan sekadar sebagai pelaku bisnis, tetapi juga sebagai penjaga kepercayaan publik. Transparansi kebijakan, audit privasi berkala, dan fitur kontrol data oleh pengguna harus dijadikan standar etika baru dalam lanskap digital. Ketiga, penting bagi masyarakat sipil, akademisi, dan media untuk memperkuat kolaborasi dalam menyebarkan kesadaran akan pentingnya perlindungan data pribadi. Ini tidak hanya penting dalam mencegah penyalahgunaan data, tetapi juga untuk mewujudkan ekosistem digital yang adil, setara, dan manusiawi. Terakhir, penelitian selanjutnya dapat memperluas cakupan studi ini dengan pendekatan komparatif lintas negara atau fokus pada kelompok rentan yang paling terdampak oleh rendahnya standar perlindungan data. Dengan menyatukan kebijakan, literasi, teknologi, dan partisipasi publik, perlindungan data pribadi dapat menjadi landasan etis dan strategis bagi masa depan ekonomi digital Indonesia yang lebih berkeadilan dan berkelanjutan.

DAFTAR PUSTAKA

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514.
- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2016). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness.
- Aridor, G., Che, Y.-K., & Salz, T. (2020). The economic consequences of data privacy regulation: Empirical evidence from GDPR. NBER Working Paper No. 26900
- Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: Small money, small costs, small talk. NBER Working Paper No. 23488.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*.
- Liu, L., Chen, J., & Ye, Y. (2022). Consumer trust and transparency in data privacy: A qualitative approach. *Journal of Consumer Behaviour*, 21(4), 987–1003.
- Widagdo, P., & Susanto, T. D. (2021). Understanding digital privacy awareness among Indonesian millennials: A qualitative study. *Jurnal Ilmu Komunikasi*, 19(1), 15–28.
- Okazaki, S., Li, H., & Hirose, M. (2020). Consumer privacy concerns and trust in digital environments: A cultural comparison. *Journal of Interactive Marketing*, 52, 58–73.
- Tufekci, Z. (2015). *Algorithmic harms beyond Facebook and Google*.
- Isaak, J., & Hanna, M. J. (2018). *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*.

- Golia, A., & Stamelou, A. (2020). The impact of GDPR on consumer behavior: A qualitative perspective. *European Journal of Law and Technology*, 11(1), 1–20.
- Martin, K., & Murphy, P. E. (2019). The role of data privacy regulation in marketing and ethical consumer behavior. *Journal of Public Policy & Marketing*, 38(1), 80–85.
- Affandi, M. R., Dasuha, B. L. P., & Parapat, D. S. (2025). Dinamika digitalisasi dan manajemen keuangan UMKM. *JUMPER*, 3(2).
- Wati, S. K., & Widodo, E. K. (2024). Analisis literasi digital pada konsumen usia produktif. *Jurnal EKOBIL*, 3(2), 7–13.
- Widagdo, P., & Susanto, T. D. (2021). Privacy paradox among Indonesian millennials. *Jurnal Ilmu Komunikasi*, 19(1), 15–28.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- Nissenbaum, H. (2010). *Privacy in Context*. Stanford University Press