Berajah Journal
Published by: CV Lafadz Jaya | ISSN: 2797-1805 | E-ISSN: 2797-1882

Volume 6 No. 2 (2026)
Page: 698 – 707
https://ojs.berajah.com/index.php/go/

PENGARUH CYBER LAW TERHADAP KEPERCAYAAN MASYARAKAT DALAM LAYANAN ONLINE

THE IMPACT OF CYBER LAW ON PUBLIC CONFIDENCE IN ONLINE SERVICES

Wisnu Cahyo Apriliyadi, Pandri Zulfikar, Muhammad Fajar Alfahimi, Aditya Putra Setyawan, Ahiruddin
Universitas Islam Syekh-Yusuf Tangerang
Coorespondence : wisnucahyo3232@yahoo.com

Received: 15-03-2026 | **Revised:** 25-03-2026 | **Accepted:** 05-04-2026 | **Published:** 07-05-2026

Abstract

The development of information and communication technology has transformed the paradigm of social and economic interaction through online services. However, the proliferation of cybercrime, personal data breaches, digital fraud, and illegal content has threatened public trust in the digital ecosystem. Cyber Law as a legal instrument governing cyberspace is expected to build and maintain public trust. This study analyzes the influence of Cyber Law on public trust in using online services through a normative juridical and empirical socio-legal approach. The results show that the effectiveness of Cyber Law in building trust depends on several factors: regulatory clarity, consistency of law enforcement, public legal awareness, and balance between protection and innovation. This study recommends regulatory harmonization, strengthening of cyber law enforcement institutions, and development of alternative dispute resolution mechanisms to increase public trust in online services.

Keywords: *Cyber Law, Public Trust, Online Services, Cybersecurity, Digital Consumer Protection.*

PENDAHULUAN

Revolusi digital telah mengubah cara masyarakat berinteraksi, bertransaksi, dan mengakses informasi. Berdasarkan data Asosiasi Penyelenggara Jaringan Telekomunikasi (APJII), penetrasi internet di Indonesia mencapai 77,02 persen pada tahun 2024, dengan jumlah pengguna internet sekitar 215 juta jiwa (APJII, 2024). Pertumbuhan ini didorong oleh kemudahan akses layanan online yang mencakup e-commerce, fintech, layanan pemerintah digital (e-government), media sosial, platform streaming, dan berbagai aplikasi layanan digital lainnya.

Transformasi digital ini membawa manfaat signifikan dalam hal efisiensi, aksesibilitas, dan inovasi. Namun, di sisi lain, ruang siber juga menjadi medan bagi berbagai bentuk kejahatan dan pelanggaran hukum yang mengancam keamanan dan kepercayaan pengguna. Badan Siber dan Sandi Negara (BSSN) mencatat adanya peningkatan insiden keamanan siber yang signifikan, dengan lebih dari 1,4 miliar serangan siber terjadi pada tahun 2023 (BSSN, 2024). Selain itu, laporan Kementerian Komunikasi dan Digital menunjukkan adanya ribuan konten ilegal yang dihapus setiap bulannya, mencakup penipuan online, perjudian, pornografi, dan ujaran kebencian (Kemenkomdigi, 2024).

Kepercayaan masyarakat menjadi faktor krusial dalam adopsi dan keberlanjutan layanan online. Tanpa kepercayaan yang memadai, masyarakat akan enggan menggunakan layanan digital, yang pada akhirnya menghambat pertumbuhan ekonomi digital dan inklusi digital. Cyber Law, sebagai cabang hukum yang mengatur aktivitas di ruang siber, memiliki peran strategis dalam membangun, mempertahankan, dan memulihkan kepercayaan masyarakat.

Di Indonesia, kerangka hukum siber telah mengalami evolusi signifikan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE 2016) merupakan pilar utama regulasi siber. Selain itu, berbagai

DOI: https://doi.org/10.47353/bj.v6i2.451

regulasi turunan telah dikeluarkan, termasuk Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik (PP PSTE), Peraturan Pemerintah Nomor 80 Tahun 2012 tentang Perdagangan Melalui Sistem Elektronik, serta berbagai peraturan di sektor spesifik seperti Peraturan Otoritas Jasa Keuangan (OJK) untuk fintech dan Peraturan Bank Indonesia untuk sistem pembayaran digital.

Meskipun kerangka hukum telah tersedia, efektivitasnya dalam membangun kepercayaan masyarakat masih menjadi pertanyaan. Beberapa kasus menunjukkan adanya kekhawatiran publik terhadap penegakan UU ITE yang dinilai kriminalisasi, ketidakpastian hukum dalam perlindungan data pribadi, dan kelemahan dalam penanganan kejahatan siber lintas batas. Penelitian ini bertujuan untuk menganalisis secara mendalam pengaruh Cyber Law terhadap kepercayaan masyarakat dalam layanan online.

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah: 1) Bagaimana kerangka hukum Cyber Law di Indonesia dalam mengatur layanan online? 2) Apa saja faktor-faktor yang mempengaruhi kepercayaan masyarakat dalam menggunakan layanan online? 3) Bagaimana pengaruh Cyber Law terhadap kepercayaan masyarakat dalam layanan online?

METODE

Penelitian ini menggunakan metode campuran (mixed methods) dengan pendekatan:

Pendekatan Normatif Yuridis: Analisis terhadap peraturan perundang-undangan, putusan pengadilan, dan dokumen hukum terkait Cyber Law.

Pendekatan Empiris Sosio-Legal:Analisis terhadap data statistik, laporan survei, dan studi kasus mengenai kepercayaan masyarakat dan implementasi Cyber Law.

Pendekatan Komparatif: Perbandingan dengan regulasi Cyber Law di yurisdiksi lain untuk mengidentifikasi best practices.

Sumber data meliputi data primer (peraturan perundang-undangan, putusan pengadilan) dan data sekunder (literatur ilmiah, laporan organisasi, data statistik). Analisis data dilakukan dengan metode kualitatif deskriptif-analitis dan kuantitatif sederhana.

HASIL DAN PEMBAHASAN

Kerangka Hukum Cyber Law Di Indonesia

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

UU ITE 2016 merupakan fondasi hukum siber di Indonesia. Undang-undang ini mengatur beberapa aspek fundamental:

- Aspek Validitas Transaksi Elektronik: Pasal 9 UU ITE menegaskan bahwa transaksi elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan tertentu. Ini memberikan legal certainty bagi transaksi online.
- Aspek Tanda Tangan Elektronik: Pasal 11-15 mengatur tentang tanda tangan elektronik dan sertifikat elektronik, memberikan kerangka autentikasi untuk transaksi digital.
- Aspek Domain Name: Pasal 16-19 mengatur tentang nama domain, memberikan perlindungan terhadap hak kekayaan intelektual dalam ruang digital.
- Aspek Perlindungan Privasi: Pasal 15 ayat (3) dan Pasal 26 mengatur tentang perlindungan data pribadi dalam transaksi elektronik.

DOI: https://doi.org/10.47353/bj.v6i2.451

- Aspek Keamanan dan Penyelenggaraan Sistem Elektronik: Pasal 30-35 mengatur tentang kewajiban penyelenggara sistem elektronik dalam hal keamanan, integritas, dan ketersediaan sistem.
- Aspek Tindak Pidana: Pasal 27-37 mengatur berbagai tindak pidana di ruang siber, termasuk penipuan, pencemaran nama baik, pengancaman, pornografi, dan perjudian.
- Aspek Penyelidikan dan Penegakan: Pasal 38-43 mengatur kewenangan penyelidikan, penyidikan, dan penuntutan tindak pidana siber.

Namun, UU ITE juga menghadapi kritik signifikan. Pasal 27 ayat (3) tentang pencemaran nama baik dan Pasal 28 tentang penyebaran berita bohong seringkali dikritik karena multitafsir dan potensial kriminalisasi. Kekhawatiran ini mempengaruhi kepercayaan masyarakat terhadap kebebasan berekspresi di ruang digital.

Peraturan Pemerintah dan Regulasi Sektor

PP PSTE 2019 memberikan detail teknis mengenai penyelenggaraan sistem elektronik dan transaksi elektronik. Regulasi ini mengatur:

- Klasifikasi penyelenggara sistem elektronik (PSE) publik dan privat
- Kewajiban registrasi PSE
- Standar keamanan sistem elektronik
- Penanganan konten yang melanggar hukum
- Kewajiban penyimpanan data dalam negeri (data localization)

Regulasi sektoral yang relevan meliputi:

Peraturan OJK No. 10/POJK.05/2022 tentang Penyelenggaraan Teknologi Finansial yang mengatur aktivitas fintech, peer-to-peer lending, dan layanan keuangan digital lainnya.

Peraturan Bank Indonesia No. 23/6/PBI/2021 tentang Penyelenggaraan Payment System yang mengatur sistem pembayaran digital, e-wallet, dan QRIS.

Peraturan Menteri Perdagangan No. 50 Tahun 2020 tentang Perizinan Berusaha Melalui Sistem Elektronik yang mengatur perizinan usaha di bidang perdagangan melalui sistem elektronik.

Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggaraan Sistem Elektronik Lingkup Privat yang mengatur kewajiban PSE privat dalam hal registrasi, keamanan, dan penanganan konten.

Undang-Undang Perlindungan Data Pribadi (UU PDP)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan perkembangan signifikan dalam kerangka hukum siber Indonesia. UU ini mengadopsi prinsip-prinsip GDPR Uni Eropa dengan penyesuaian konteks nasional. Aspek-aspek fundamental meliputi:

- Prinsip legalitas, keadilan, dan transparansi pengolahan data
- Hak subjek data (hak akses, koreksi, penghapusan, portabilitas)
- Kewajiban pengendali dan pemroses data
- Mekanisme penanganan pelanggaran data
- Sanksi administratif dan pidana

UU PDP diharapkan dapat membangun kepercayaan masyarakat melalui pengendalian yang lebih kuat atas data pribadi. Namun, efektivitasnya bergantung pada implementasi yang konsisten dan pembentukan lembaga pengawas yang independen dan kompeten.

DOI: https://doi.org/10.47353/bj.v6i2.451

Faktor-Faktor Yang Mempengaruhi Kepercayaan Masyarakat

Faktor Teknis dan Keamanan

Faktor teknis merupakan fondasi kepercayaan dalam layanan online. Aspek-aspek ini meliputi:

Keamanan infrastruktur: Keamanan server, enkripsi data, proteksi terhadap serangan DDoS, dan keamanan jaringan. Kerentanan teknis dapat menyebabkan kebocoran data yang merusak kepercayaan secara instan.

Autentikasi dan identifikasi:Sistem autentikasi yang kuat (multi-factor authentication, biometrik) membangun kepercayaan melalui jaminan bahwa hanya pihak berwenang yang dapat mengakses akun.

Integritas sistem: Jaminan bahwa sistem berfungsi sesuai yang diharapkan, data tidak dimanipulasi, dan transaksi diproses dengan benar.

Ketersediaan layanan: Uptime yang konsisten dan recovery yang cepat dari gangguan membangun kepercayaan melalui reliability.

Faktor Hukum dan Regulasi

Faktor hukum berperan sebagai institution-based trust mechanism. Aspek-aspek ini meliputi:

Kepastian hukum: Kejelasan regulasi, prediktabilitas penegakan, dan konsistensi interpretasi. Ketidakpastian hukum, seperti multitafsir dalam UU ITE, dapat mengurangi kepercayaan.

Perlindungan hukum: Keberadaan mekanisme perlindungan yang efektif bagi pengguna, termasuk perlindungan konsumen, perlindungan data, dan hak untuk mendapatkan remedi.

Penegakan hukum: Efektivitas penegakan hukum terhadap pelanggaran, termasuk kecepatan respons, profesionalisme aparat, dan konsistensi sanksi.

Akses keadilan: Ketersediaan mekanisme penyelesaian sengketa yang efisien dan terjangkau, termasuk pengadilan dan alternative dispute resolution.

Faktor Sosial dan Kultural

Faktor sosial dan kultural mempengaruhi disposition to trust dan characteristic-based trust:

Digital literacy: Tingkat pemahaman masyarakat terhadap teknologi, risiko digital, dan mekanisme perlindungan. Literasi digital yang rendah dapat meningkatkan perceived risk dan mengurangi kepercayaan.

Social proof: Rekomendasi dari keluarga, teman, atau komunitas mempengaruhi kepercayaan. Review online dan rating juga berfungsi sebagai social proof.

Cultural factors: Norma budaya terkait privasi, kepercayaan terhadap institusi, dan sikap terhadap teknologi. Di Indonesia, kepercayaan terhadap komunitas dan rekomendasi personal seringkali lebih kuat daripada kepercayaan terhadap institusi formal.

Generational differences: Generasi yang berbeda memiliki tingkat kenyamanan dan kepercayaan yang berbeda terhadap teknologi. Generasi muda (digital natives) cenderung lebih percaya namun juga lebih aware terhadap risiko.

Faktor Ekonomi

Faktor ekonomi mempengaruhi cost-benefit analysis pengguna:

Biaya transaksi: Biaya yang terkait dengan penggunaan layanan online, termasuk biaya langsung dan biaya kepatuhan.Manfaat yang diharapkan nilai yang diperoleh dari layanan, termasuk convenience, akses, dan efisiensi. Risiko finansial Potensi kerugian finansial akibat penipuan, kebocoran data, atau kegagalan

DOI: https://doi.org/10.47353/bj.v6i2.451

sistem. Keberadaan mekanisme perlindungan finansial, seperti escrow services, money-back guarantees, atau asuransi transaksi.

Analisis Pengaruh Cyber Law Terhadap Kepercayaan Masyarakat

Pengaruh Positif Cyber Law

Cyber Law memiliki potensi untuk membangun kepercayaan masyarakat melalui beberapa mekanisme:

Pertama, legal certainty. UU ITE memberikan pengakuan hukum atas transaksi elektronik, tanda tangan elektronik, dan dokumen elektronik. Ini mengurangi uncertainty dan perceived risk dalam bertransaksi online. Pengakuan hukum ini merupakan fondasi bagi kepercayaan institution-based.

Kedua, consumer protection. Regulasi seperti PP PSTE dan peraturan sektoral memberikan perlindungan konsumen digital melalui kewajiban transparansi, hak untuk membatalkan, dan mekanisme pengaduan. Perlindungan ini membangun kepercayaan melalui jaminan bahwa kepentingan konsumen dilindungi.

Ketiga, data protection.UU PDP memberikan pengendalian kepada individu atas data pribadinya. Right to access, correction, deletion, dan portability memberikan empowerment kepada pengguna, yang membangun kepercayaan melalui sense of control.

Keempat, security requirements. Kewajiban keamanan yang diatur dalam PP PSTE dan regulasi sektoral memberikan jaminan teknis. Walaupun kepatuhan tidak selalu sempurna, keberadaan regulasi memberikan baseline expectation.

Kelima, deterrence effect. Sanksi pidana dan administratif dalam UU ITE dan UU PDP memberikan deterrence terhadap pelaku kejahatan siber. Efek deterrence ini, meskipun sulit diukur, berkontribusi pada perceived safety.

Keenam, dispute resolution. Keberadaan mekanisme pengaduan dan penyelesaian sengketa, baik melalui pengadilan maupun lembaga alternatif, memberikan jaminan remedi. Ini membangun kepercayaan melalui assurance bahwa jika terjadi masalah, ada jalur untuk menyelesaikannya.

Pengaruh Negatif atau Tantangan Cyber Law

Namun, Cyber Law juga menghadapi tantangan yang dapat mengurangi atau bahkan merusak kepercayaan:

Pertama, over-criminalization dan chilling effect. Pasal 27 ayat (3) UU ITE tentang pencemaran nama baik dan Pasal 28 tentang berita bohong seringkali dikritik karena multitafsir dan potensial kriminalisasi. Kekhawatiran ini menciptakan chilling effect terhadap kebebasan berekspresi dan partisipasi digital. Masyarakat yang takut berbicara di ruang digital akan mengurangi engagement dan kepercayaan terhadap ekosistem digital.

Kedua, inconsistent enforcement. Penegakan hukum yang tidak konsisten, baik dalam hal selektivitas penuntutan maupun disparitas sanksi, mengurangi predictability dan fairness. Ini merusak institution-based trust.

Ketiga, regulatory fragmentation. Keragaman regulasi yang tumpang tindih menciptakan kebingungan dan beban kepatuhan. Penyelenggara layanan harus mematuhi berbagai set regulasi yang mungkin saling bertentangan.

DOI: https://doi.org/10.47353/bj.v6i2.451

Keempat, capacity constraints. Keterbatasan kapasitas aparat penegak hukum dalam menangani kejahatan siber yang semakin canggih menciptakan gap antara expectation dan reality. Masyarakat yang mengharapkan perlindungan namun tidak mendapatkannya akan kehilangan kepercayaan.

Kelima, slow adaptation. Kecepatan evolusi teknologi jauh melampaui kecepatan evolusi regulasi. Regulasi yang outdated atau tidak relevan dengan teknologi terkini mengurangi efektivitas perlindungan.

Keenam, extraterritorial challenges. Kejahatan siber seringkali bersifat lintas batas, namun kerja sama internasional dalam penegakan hukum masih terbatas. Ini menciptakan impunity bagi pelaku di luar yurisdiksi.

Analisis Empiris: Data dan Tren

Data empiris menunjukkan kompleksitas pengaruh Cyber Law terhadap kepercayaan:

Data penetrasi dan adopsi: Pertumbuhan penetrasi internet dan adopsi layanan online di Indonesia menunjukkan kepercayaan yang meningkat dalam penggunaan teknologi. Namun, ini juga mencerminkan necessity dan lack of alternatives daripada pure trust.

Data kejahatan siber: Peningkatan insiden kejahatan siber, meskipun sebagian disebabkan oleh pertumbuhan basis pengguna, menunjukkan bahwa ancaman tetap signifikan. Respon penegakan hukum terhadap insiden ini mempengaruhi persepsi keamanan.

Data pengaduan konsumen: Laporan pengaduan konsumen ke Badan Perlindungan Konsumen Nasional (BPKN) dan lembaga terkait menunjukkan tingkat kepuasan dan ketidakpuasan. Tren peningkatan pengaduan dapat mencerminkan peningkatan awareness atau peningkatan masalah.

Survei kepercayaan: Survei yang dilakukan oleh berbagai lembaga menunjukkan variasi kepercayaan berdasarkan demografi, jenis layanan, dan pengalaman. Umumnya, kepercayaan lebih tinggi untuk layanan yang telah mapan dan memiliki reputasi.

Studi Kasus

Studi Kasus 1: E-commerce dan Perlindungan Konsumen

Platform e-commerce seperti Tokopedia, Shopee, dan Lazada telah mengimplementasikan berbagai mekanisme perlindungan konsumen, termasuk escrow system, return policy, dan customer service. Regulasi seperti PP PSTE dan peraturan perdagangan elektronik memberikan kerangka hukum. Kepercayaan masyarakat terhadap e-commerce umumnya tinggi, ditunjukkan oleh pertumbuhan transaksi yang signifikan. Namun, kasus-kasus penipuan, produk palsu, dan kesulitan refund masih terjadi, menunjukkan bahwa kepercayaan bersifat conditional dan fragile.

Studi Kasus 2: Fintech dan Regulasi OJK

Industri fintech di Indonesia mengalami pertumbuhan pesat. OJK mengimplementasikan regulatory sandbox dan peraturan yang bertahap. Kepercayaan terhadap fintech umumnya tinggi, namun kasus-kasus gagal bayar pada platform peer-to-peer lending dan penipuan investasi online telah merusak kepercayaan sebagian segmen. Respons regulasi, termasuk penutupan platform yang tidak berizin dan peningkatan supervisi, berperan dalam memulihkan kepercayaan.

Studi Kasus 3: UU ITE dan Kebebasan Berekspresi

Kasus-kasus penegakan Pasal 27 ayat (3) UU ITE terhadap aktivis, jurnalis, dan warga biasa telah menciptakan kontroversi signifikan. Mahkamah Konstitusi telah memberikan putusan yang membatasi interpretasi pasal ini, namun kekhawatiran masih ada. Chilling effect ini mengurangi kepercayaan terhadap ruang digital sebagai medium ekspresi yang aman.

DOI: https://doi.org/10.47353/bj.v6i2.451

Studi Kasus 4: Kebocoran Data dan UU PDP

Kasus kebocoran data yang melibatkan berbagai perusahaan dan institusi telah mengguncang kepercayaan. Implementasi UU PDP diharapkan dapat membangun kembali kepercayaan melalui kewajiban pelaporan, notifikasi korban, dan sanksi yang signifikan. Namun, efektivitasnya masih perlu dibuktikan dalam praktik.

Digital forensics: Penyidikan kejahatan siber memerlukan keahlian teknis yang tinggi dan infrastruktur forensik digital yang memadai. Keterbatasan kapasitas ini menghambat penegakan hukum.

Encryption and privacy: Tension antara kebutuhan law enforcement untuk mengakses data terenkripsi dan hak privasi individu menciptakan dilema hukum dan teknis yang belum terpecahkan.

KESIMPULAN

Cyber Law memiliki pengaruh yang signifikan dan multidimensional terhadap kepercayaan masyarakat dalam layanan online. Pengaruh ini bersifat dual: di satu sisi, Cyber Law memiliki potensi besar untuk membangun dan mempertahankan kepercayaan melalui legal certainty, consumer protection, data protection, security requirements, deterrence effect, dan dispute resolution mechanisms. Di sisi lain, Cyber Law juga menghadapi risiko merusak kepercayaan melalui over-criminalization, inconsistent enforcement, regulatory fragmentation, capacity constraints, slow adaptation, dan extraterritorial challenges.

Efektivitas Cyber Law dalam membangun kepercayaan sangat bergantung pada beberapa faktor kunci:

Pertama, kejelasan dan konsistensi regulasi.Regulasi yang jelas, tidak multitafsir, dan diterapkan secara konsisten membangun predictability dan fairness yang merupakan fondasi kepercayaan institution-based.

Kedua, kapasitas dan profesionalisme penegakan.Penegakan hukum yang efektif, tepat waktu, dan profesional membangun assurance bahwa regulasi memiliki teeth dan akan melindungi kepentingan pengguna.

Ketiga, kesadaran dan pemberdayaan pengguna. Masyarakat yang memahami hak dan kewajibannya dalam ruang digital, serta memiliki akses ke mekanisme perlindungan, akan memiliki kepercayaan yang lebih tinggi.

DAFTAR PUSTAKA

Buku

Brenner, S. W. (2010). Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford University Press.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly. 27(1), 51-90.

Lessig, L. (2006). Code: Version 2.0. Basic Books.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. Academy of Management Review, 20(3), 709-734.

McKnight, D. H., & Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce, 6(2), 35-59.

Murray, A. D. (2016). Information Technology Law: The Law and Society (3rd ed.). Oxford University Press.

Reed, C. (2012). Making Laws for Cyberspace. Oxford University Press.

Rowland, D., Macdonald, E., & Charlesworth, A. (2018). Information Technology Law (5th ed.). Routledge.

Svantesson, D. J. B. (2013). Extraterritoriality in Data Privacy Law. Ex Tuto Publishing.

DOI: https://doi.org/10.47353/bj.v6i2.451

Zucker, L. G. (1986). Production of Trust: Institutional Sources of Economic Structure, 1840-1920. Research in Organizational Behavior, 8, 53-111.

Jurnal Ilmiah

Belli, L., & Zingales, N. (2017). Platform Regulations: How Platforms Are Regulated and How They Regulate Us. Internet Policy Review, 6(4), 1-17.

Buhmann, A., Paßmann, J., & Fieseler, C. (2020). Managing Algorithmic Accountability: Balancing Reputational Concerns, Engagement Strategies, and the Potential of Rational Discourse. Journal of Business Ethics, 163(2), 265-280.

Cinnamon, J. (2017). Technologies of Discretion: Social sorting in Mumbai's slum redevelopment. Environment and Planning A: Economy and Space, 49(5), 1033-1051.

De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? Computer Law & Security Review, 32(2), 179-194.

Edwards, L. (2018). The EU Digital Single Market Strategy: A Critical Analysis. Computer Law & Security Review, 34(4), 762-774.

Floridi, L. (2018). Soft Ethics and the Governance of the Digital. Philosophy & Technology, 31(1), 1-8.

Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.

Hargittai, E., & Marwick, A. (2016). What Can I Really Do? Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, 10, 3737-3757.

Helberger, N., Borgesius, F. Z., & Reyna, A. (2017). The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law.Common Market Law Review, 54(5), 1427-1466.

Klonick, K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. Harvard Law Review, 131(6), 1598-1670.

Koops, B. J. (2011). The Law and Technology of User Identification: Improving the Reliability of Online User Identification. Computer Law & Security Review, 27(1), 73-78.

Laidlaw, E. B. (2015). Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility. Cambridge University Press.

Mantelero, A. (2016). Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. Computer Law & Security Review, 32(2), 238-255.

Mittelstadt, B. D. (2017). From Individual to Group Privacy in Big Data Analytics. Philosophy & Technology, 30(4), 475-494.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57, 1701-1777.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

Sartor, G. (2018). Providers' Liabilities in the New EU Draft Directive on Contracts for the Supply of Digital Content. European Review of Contract Law, 14(3), 231-259.

Schwartz, P. M. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. Harvard Law Review, 126(7), 1966-2009.

Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

Tusikov, N. (2016). Chokepoints: Global Private Regulation on the Internet. University of California Press.

Van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. Surveillance & Society, 12(2), 197-208.

Zarsky, T. Z. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. Philosophy & Technology, 29(4), 409-433.

DOI: https://doi.org/10.47353/bj.v6i2.451

Peraturan Perundang-undangan dan Instrumen Hukum

Bank Indonesia. (2021). Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyelenggaraan Payment System.

Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik.

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Kementerian Komunikasi dan Digital. (2020). Peraturan Menteri Komunikasi dan Digital Nomor 5 Tahun 2020 tentang Penyelenggaraan Sistem Elektronik Lingkup Privat.

Kementerian Perdagangan. (2020). Peraturan Menteri Perdagangan Nomor 50 Tahun 2020 tentang Perizinan Berusaha Melalui Sistem Elektronik.

Otoritas Jasa Keuangan. (2022). Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Penyelenggaraan Teknologi Finansial.

Council of Europe. (2001). Convention on Cybercrime(Budapest Convention). CETS No. 185.

European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

European Parliament and Council. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC* (Digital Services Act). Official Journal of the European Union, L 277, 1-102.

European Parliament and Council. (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). Official Journal of the European Union, L 265, 1-66.

Laporan dan Dokumen Organisasi

Asosiasi Penyelenggara Jaringan Telekomunikasi Indonesia (APJII). (2024). Laporan Survei Internet Indonesia 2024. APJII.

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Keamanan Siber Indonesia 2023. BSSN.

Bank Indonesia. (2024). Laporan Sistem Pembayaran Indonesia 2023. Bank Indonesia.

Kementerian Komunikasi dan Digital. (2024). Laporan Kinerja Penanganan Konten Negatif 2023. Kemenkomdigi.

OECD. (2022). OECD Digital Economy Outlook 2022. OECD Publishing.

Otoritas Jasa Keuangan. (2024). Statistik Perkembangan Fintech 2023. OJK.

United Nations Conference on Trade and Development (UNCTAD). (2023). Digital Economy Report 2023. United Nations.

World Bank. (2023). Digital Development Report 2023. World Bank Group.

World Economic Forum. (2024). Global Cybersecurity Outlook 2024*. WEF.

Sumber Elektronik dan Database

Badan Perlindungan Konsumen Nasional. (2024). Statistik Pengaduan Konsumen. Retrieved from https://www.bpkn.go.id/

European Commission. (2024). Digital Services Act. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Indonesia Investment Coordinating Board. (2024). E-commerce in Indonesia. Retrieved from https://www.indonesia-investments.com/business/industries/e-commerce/item611

Internet Governance Forum. (2023). National and Regional Internet Governance Forums. Retrieved from https://www.intgovforum.org/

DOI: https://doi.org/10.47353/bj.v6i2.451

OECD. (2024). Digital Government Index. Retrieved from https://www.oecd.org/gov/digital-government-index.htm

United Nations. (2023). Global Digital Compact. Retrieved from https://www.un.org/techenvoy/global-digital-compact