Journal of Social and Economics Research
Volume 7, Issue 2, December 2025
P-ISSN: 2715-6117 E-ISSN: 2715-6966
Open Access at: https://idm.or.id/JSER/index.php/JSER

DIGITAL BUSINESS AND PRIVACY RIGHTS: TECHNOLOGY COMPANY ACCOUNTABILITY IN PERSONAL DATA PROTECTION IN INDONESIA

BISNIS DIGITAL DAN HAK PRIVASI: AKUNTABILITAS PERUSAHAAN TEKNOLOGI DALAM PERLINDUNGAN DATA PRIBADI DI INDONESIA

R. Raafi Adhi Rahman
Magister Ilmu Hukum Kampus Jakarta, Fakultas Hukum, Universitas Gadjah Mada
E-mail: rraafiadhirahman@mail.ugm.ac.id

ARTICLE INFO

Correspondent

R. Raafi Adhi Rahman
rraafiadhirahman@mail.ugm.ac.id

Key words:
Privacy, Digital Business, Technology Companies, Data Protection, Human Rights, Accountability.

Website:
https://idm.or.id/JSER/index.php/JSER

Page: 1534 - 1552

ABSTRACT

The rapid expansion of Indonesia's digital economy has increased the volume of personal data processed by technology companies, raising substantial concerns regarding privacy rights and corporate accountability. This study examines the extent to which digital businesses fulfill their human rights responsibilities in protecting personal data, particularly after the enactment of the Personal Data Protection Law (Law No. 27/2022). Using a normative juridical method through statutory, conceptual, and human rights approaches, this research evaluates whether existing corporate practices align with principles of legality, transparency, necessity, and proportionality. The findings reveal persistent gaps in compliance, including inadequate consent mechanisms, opaque data-sharing arrangements, weak cybersecurity safeguards, and limited corporate oversight. These shortcomings expose users to risks of data misuse, surveillance, and discriminatory profiling, indicating that many technology companies have not yet internalized human rights due diligence as part of their operational governance. The study concludes that stronger regulatory enforcement, mandatory human rights impact assessments, and comprehensive accountability mechanisms are required to ensure that digital businesses actively respect and protect the right to privacy as a fundamental human right.

INFO ARTIKEL

Koresponden

R. Raafi Adhi Rahman
rraafiadhirahman@mail.ugm.ac.id

Kata kunci:

Privasi, Bisnis Digital, Perusahaan Teknologi, Perlindungan Data, Hak Asasi Manusia, Akuntabilitas

Website:
https://idm.or.id/JSER/index.php/JSER

Hal: 1534 - 1552

ABSTRAK

Perluasan pesat ekonomi digital Indonesia meningkatkan jumlah data pribadi yang diproses oleh perusahaan teknologi dan menimbulkan kekhawatiran signifikan terhadap hak privasi serta akuntabilitas korporasi. Penelitian ini menelaah sejauh mana pelaku bisnis digital memenuhi tanggung jawab hak asasi manusia dalam melindungi data pribadi, terutama setelah berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dengan menggunakan metode yuridis normatif melalui pendekatan peraturan perundang-undangan, konseptual, dan hak asasi manusia, penelitian ini mengevaluasi apakah praktik korporasi saat ini selaras dengan prinsip legalitas, transparansi, kebutuhan, dan proporsionalitas. Hasil penelitian menunjukkan masih adanya kesenjangan kepatuhan, termasuk mekanisme persetujuan yang tidak memadai, pengaturan berbagi data yang tidak transparan, pengamanan siber yang lemah, serta pengawasan internal perusahaan yang terbatas. Kekurangan tersebut meningkatkan risiko penyalahgunaan data, pengawasan berlebihan, dan profiling yang diskriminatif, sehingga menunjukkan bahwa banyak perusahaan teknologi belum mengintegrasikan human rights due diligence atau uji tuntas hak asasi manusia dalam tata kelola operasional mereka. Penelitian ini menyimpulkan perlunya penegakan regulasi yang lebih kuat, kewajiban penilaian dampak hak asasi manusia, serta mekanisme akuntabilitas yang komprehensif guna memastikan bahwa aktivitas bisnis digital menghormati dan melindungi hak privasi sebagai hak asasi yang fundamental.

PENDAHULUAN

Perkembangan teknologi digital dalam satu dekade terakhir ini telah mengubah secara radikal cara perusahaan beroperasi, berinteraksi dengan konsumen, dan membangun model bisnis yang bergantung pada pemrosesan data pribadi dalam skala luas. Transformasi digital tersebut mendorong munculnya ekosistem ekonomi baru yang ditopang oleh algoritma, kecerdasan buatan, dan otomatisasi, yang memungkinkan pengumpulan data secara *real-time* dari aktivitas daring masyarakat (Mayer-Schönberger et al., 2013). Dalam konteks ini, data pribadi tidak lagi dipahami sekadar sebagai informasi tentang individu, tetapi telah berubah menjadi aset strategis bagi perusahaan, terutama perusahaan teknologi yang mengandalkan analitik dan *behavioural advertising* (Andrejevic, 2020). Data menjadi "komoditas baru" yang menentukan daya saing perusahaan, struktur pasar, hingga perilaku sosial masyarakat (Zuboff, 2019).

Namun perkembangan tersebut menimbulkan paradoks. Di satu sisi, digitalisasi meningkatkan efisiensi layanan dan membuka peluang bisnis yang luas. Di sisi lain, ekspansi pengumpulan data menghadirkan ancaman signifikan terhadap

hak privasi sebagai hak asasi manusia (Solove, 2021). Ketika perusahaan memiliki kemampuan melacak perilaku pengguna secara detail, mulai dari lokasi, riwayat, pencarian, preferensi belanja hingga interaksi media sosial, batas antara layanan komersial dan praktik pengawasan menjadi semakin kabur (Cohen, 2019). Pengguna sering tidak menyadari sejauh mana data mereka dikumpulkan dan diproses, sementara mekanisme transparansi yang dijanjikan perusahaan seringkali tidak sebanding dengan kompleksitas teknologi yang digunakan (Richards & Hartzog, 2015).

Dalam praktiknya, bisnis digital didapati pelanggaran privasi yang tidak hanya terjadi melalui kebocoran data yang masif, tetapi melalui praktik-praktik yang tampak sah secara hukum tetapi melanggar substansi hak privasi. Praktik tersebut mencakup penggunaan *dark patterns* untuk memanipulasi persetujuan pengguna (Marthur et al., 2019), *profiling* dan *microtargeting* yang bersifat invasif (F. Wang, 2016) serta pemrosesan data sensitif tanpa kontrol yang memadai. Situasi ini jelas semakin memperlemah posisi tawar pengguna, yang kerap tidak memiliki pemahaman cukup mengenai konsekuensi jangka panjang dari pemrosesan data pribadi.

Di Indonesia, persoalan ini menjadi semakin mendesak karena menurut survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2025, pengguna internet di Indonesia mencapai 229,43 juta jiwa, jumlah ini setara dengan 80,66% populasi (APJII, 2025). Sementara itu, ekonomi digital Indonesia diperkirakan mencapai USD 90 Miliar pada tahun 2024 yang menjadikan Indonesia sebagai pasar digital terbesar di Asia Tenggara (Google et al., 2024). Proyeksi terbaru menunjukkan pertumbuhan *Gross Merchandise Value* (GMV) digital Indonesia mendekati USD 100 Miliar pada 2025 (Google et al., 2025). Berdasarkan data tersebut, pertumbuhan ekonomi digital Indonesia berlangsung sangat pesat dan diproyeksikan menjadi yang terbesar di Asia Tenggara dalam beberapa tahun mendatang. Namun perkembangan ini tidak selalu diimbangi oleh kesiapan regulasi yang kuat. Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang Perlindungan Data Pribadi), Indonesia hanya mengandalkan pendekatan sektoral yang tersebar, sehingga memberikan keleluasaan besar bagi perusahaan untuk menentukan standar pengelolaan data mereka sendiri (Sutanto, 2020). Akibatnya, berbagai insiden kebocoran data, penyalahgunaan data, dan kurangnya transparansi menjadi fenomena berulang dan sistemik di berbagai sektor, termasuk telekomunikasi, kesehatan, hingga layanan keuangan.

Meski Undang-Undang Perlindungan Data Pribadi merupakan tonggak penting bagi perlindungan privasi, implementasinya tidak sederhana. Perusahaan teknologi kini dihadapkan pada kewajiban persetujuan yang sah, penilaian dampak perlindungan data (*Data Protection Impact Assessment*), pelaporan insiden, serta kewajiban keamanan data. Namun, bagi perusahaan digital yang model bisnisnya sangat bergantung pada monetisasi data, muncul potensi konflik antara kewajiban hukum kepentingan komersial untuk memaksimalkan *data extraction* (Acquisti et al., 2016). Di sinilah isu akuntabilitas perusahaan teknologi semakin relevan.

Pendekatan berbasis hak asasi manusia telah memberikan kerangka yang lebih komprehensif untuk mengevaluasi praktik bisnis digital. Hak privasi merupakan

bagian dari hak sipil yang dijamin dalam berbagai instrumen internasional seperti *International Convenant on Civil and Political Rights* (ICCPR) dan Deklarasi Universal HAM . Kerangka *UN Guiding Principles on Business and Human Rights* (UNGPs) menegaskan bahwa perusahaan memiliki tanggung jawab untuk menghormati hak asasi manusia, termasuk melalui pelaksanaan *human rights due dilligence,* terlepas dari keberadaan hukum nasional (Ruggie, 2011) Artinya, perusahaan tidak dapat semata-mata berlindung di balik kepatuhan formal, melainkan wajib secara substantif memastikan minimnya dampak negatif terhadap pengguna.

Dalam konteks bisnis digital, perusahaan teknologi bukan sekadar pelaku ekonomi, tetapi aktor yang memegang pengaruh besar terhadap struktur informasi dan perilaku masyarakat. Ketika perusahaan gagal menjalankan prinsip akuntabilitas, dampaknya tidak hanya terbatas pada keamanan data, tetapi juga berpotensi menciptakan diskriminasi algoritmik, penyalahgunaan kekuasaan digital, hingga mengganggu integritas proses demokrasi (Eubanks, V., 2018). Selain itu, dalam ekosistem digital yang terhubung, kebocoran data dapat berdampak pada keamanan nasional, kepercayaan publik, serta stabilitas lembaga negara.

Dinamika global memperlihatkan adanya kesenjangan dalam cara negara merespons isu privasi. Uni Eropa dengan *The General Data Protection Regulation* (GDPR) mengambil langkah tegas dengan menjadikan privasi sebagai hak fundamental, sementara beberapa negara lain lebih mengedepankan model berbasis industri. Indonesia kini berada pada fase krusial dalam menentukan standar perlindungan data yang mampu menyeimbangkan inovasi digital dan penghormatan hak asasi manusia (Arrazy, 2023).

Berbeda dengan penelitian terdahulu yang umumnya menempatkan Undang-Undang Perlindungan Data Pribadi sebagai kerangka evaluasi utama perlindungan privasi di Indonesia, artikel ini menawarkan kebaruan dengan menggunakan *United Nations Guiding Principles on Business and Human Rights* (UNGPs) sebagai standar evaluatif normatif untuk menilai kualitas akuntabilitas perusahaan teknologi dalam bisnis digital. Pendekatan ini tidak hanya menguji kepatuhan formal terhadap norma hukum positif, tetapi juga menilai apakah praktik pengelolaan data pribadi telah memenuhi standar akuntabilitas substantif berbasis hak asasi manusia, khususnya melalui penerapan *human rights due diligence*. Dengan menjadikan UNGPs sebagai lensa analitis, penelitian ini memperluas diskursus perlindungan data dari sekedar rezim kepatuhan administratif menuju kerangka tanggung jawab korporasi global, sekaligus mengisi kekosongan kajian yang masih minim membahas integrasi antara hukum perlindungan data, akuntabilitas bisnis digital, dan prinsip hak asasi manusia di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif (*normative legal research*), karena fokus analisis diarahkan pada norma hukum, prinsip hak asasi manusia, doktrin hukum, dan regulasi terkait perlindungan data pribadi dalam konteks bisnis digital. Metode ini lazim digunakan untuk menelaah isu-isu hukum

modern yang berkembang akibat perkembangan teknologi informasi (Soekanto & Mamudji, 2011). Penelitian ini menggunakan 3 (tiga) pendekatan utama:

1. Pendekatan Perundang-undangan (*statute approach*)

   Pendekatan ini dilakukan dengan menelaah ketentuan hukum positif yang mengatur perlindungan data pribadi dan akuntabilitas perusahaan dalam bisnis digital. Analisis berfokus pada Undang-Undang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta prinsip-prinsip hak asasi manusia yang diatur dalam ICCPR yang telah diratifikasi Indonesia. Pendekatan ini penting karena penelitian bertujuan menguji kecukupan kerangka hukum dalam melindungi hak privasi di tengah ekspansi ekonomi digital.

2. Pendekatan Konseptual (*conceptual approach*)

   Pendekatan konseptual digunakan untuk mengkaji konsep-konsep kunci seperti hak privasi sebagai hak asasi manusia, akuntabilitas perusahaan (*corporate accountability*) dalam kerangka hak asasi manusia, dan prinsip-prinsip *data protection* modern seperti *lawfulness, transparency, purpose limitation,* dan *proportionality* yang berkembang melalui praktik global seperti GDPR. Pendekatan ini diperlukan karena isu privasi dalam bisnis digital tidak dapat dipahami hanya melalui teks undang-undang, tetapi perlu ditopang oleh teori dan doktrin hukum.

3. Pendekatan Kasus (*case approach*)

   Pendekatan ini dilakukan melalui penelusuran kasus-kasus relevan terkait pelanggaran data pribadi oleh perusahaan teknologi, baik di Indonesia maupun yurisdiksi lain untuk memberikan ilustrasi konkret mengenai persoalan akuntabilitas korporasi digital. Pendekatan ini sejalan dengan pendapat bahwa yuridis normatif dapat diperkuat dengan telaah kasus untuk memahami penerapan norma dalam praktik.

Adapun jenis dan sumber bahan hukum yang digunakan dalam penelitian ini adalah:

1. Bahan hukum primer, meliputi peraturan perundang-undngan yakin Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya; Instrumen hak asasi manusia internasional seperti ICCPR; serta dokumen resmi PBB seperti *UN Guiding Principles on Business and Human Rights.*
2. Bahan hukum sekunder, meliputi buku, artikel jurnal, laporan riset independen, publikasi ilmiah, laporan penelitian, serta tulisan para ahli yang membahas privasi, surveilans, ekonomi digital, dan regulasi perlindungan data.
3. Bahan hukum tersier, meliputi kamus hukum, ensiklopedia, dan sumber pendukung lain untuk memperkuat pemahaman konseptual.

Seluruh bahan hukum dikumpulkan melalui studi kepustakaan (*library research*) dengan menelusuri peraturan, putusan, dokumen internasional, jurnal ilmah, serta laporan industri terkait bisnis digital dan privasi. Teknik ini merupakan cara utama dalam riset hukum normatif.

Selanjutnya, bahan hukum dianalisis menggunakan analisis deskriptif kualitatif, yaitu menguraikan norma hukum, doktrin, serta teori yang relevan, kemudian menafsirkan untuk menjawab permasalahan penelitian. Analisis dilakukan dengan:

1. Mengidentifikasi kesenjangan antara praktik bisnis dan prinsip perlindungan privasi;
2. Mengaitkan temuan dengan teori hak asasi manusia, akuntabilitas korporasi, serta prinsip perlindungan data modern;
3. Mengevaluasi kecukupan regulasi nasional dalam menghadapi ekosistem digital yang berkembang pesat.

Sehingga seluruh metode tersebut memberikan gambaran komprehensif mengenai bagaimana perusahaan teknologi seharusnya bertanggung jawab terhadap hak privasi pengguna di era ekonomi digital.

HASIL DAN PEMBAHASAN

Paradoks Data dalam Bisnis Digital: Dampak Praktik Korporasi terhadap Hak Privasi Pengguna

Ekonomi digital Indonesia telah mencapai skala signifikan, dengan pertumbuhan berkelanjutan didorong oleh pemrosesan masif data pribadi Menurut laporan e-Conomy SEA 2024, *Gross Merchandise Value (*GMV) digital Indonesia diproyeksikan mencapai sekitar USD 82 Miliar dan diperkirakan akan mendekati USD 100 Miliar pada tahun 2025 (Google et al., 2025). Pertumbuhan ini didukung oleh 229,43 juta pengguna internet, yang menjadikannya pasar yang sangat mengandalkan *data extraction* dan monetisasi.

Dalam paradigma ini, data bukan sekadar input operasional, melainkan telah menjadi aset ekonomi inti dan sumber daya strategis yang memungkinkan pembentukan model bisnis baru yang didominasi oleh perusahaan teknologi raksasa (*big tech*). Ketegangan fundamental muncul ketika upaya maksimisasi keuntungan melalui *data extraction* berhadapan langsung dengan jaminan hak privasi sebagai hak asasi manusia yang universal, yang di Indonesia dilindungi oleh Pasal 28G Undang- UUD NRI 1945 dan Pasal 17 ICCPR. Praktik korporasi digital cenderung mengikis otonomi dan kontrol individu melalui mekanisme yang tampak legal, tetapi secara substantif melanggar hak privasi.

Dampak negatif atas praktik pengendali data pribadi terhadap hak privasi pengguna dapat dianalisis melalui tiga lensa utama: erosi otonomi saat akuisisi data, pemrosesan data invasif dan diskriminatif, serta risiko kegagalan teknis dan keamanan sistemik.

1. Erosi Otonomi Individu pada Titik Akuisisi Data

Undang-Undang Perlindungan Data Pribadi secara eksplisit menempatkan persetujuan (*consent*) sebagai salah satu landasan hukum utama pemrosesan data, dengan syarat persetujuan tersebut harus diberikan secara eksplisit, bebas dan terinformasi, hal ini diatur secara rigid dalam Pasal 20 dan 22 Undang-Undang Perlindungan Data Pribadi. Namun, dalam ekosistem digital, syarat ini seringkali hanya dipenuhi secara formalistik yang mengakibatkan erosi otonomi individu, hal ini sangat berlasan sebab:

a. Manipulasi Persetujuan Melalui *Dark Patterns*

Dark patterns adalah desain antarmuka (UI/UX) pengguna yang sengaja memanipulasi atau menyesatkan pengguna agar mengambil keputusan yang bertentangan dengan kepentingan privasi mereka (Marthur et al., 2019). Dalam praktik bisnis digital di Indonesia, hal ini tampak melalui:

a) Pelanggaran Syarat Kebebasan (*freely given*): Proses penolakan (*opt-out)* dibuat jauh lebih rumit, membutuhkan banyak klik, atau disembunyikan dalam menu berlapis, sementara persetujuan (*opt-in*) disajikan sebagai opsi *default* yang mudah dengan tombol yang menonjol. Perlakuan asimetris ini mendorong *consent fatigue,* di mana pengguna memilih jalan paling sedikit hambatannya, yaitu menyetujui tanpa adanya pertimbangan substantif (Acquisti et al., 2016).

b) Pelanggaran Syarat Informasi (*informed*): Kebijakan privasi disajikan dalam bahasa hukum yang kompleks, sangat panjang, dan tidak sebanding dengan tingkat literasi digital rata-rata. Kesenjangan informasi (*information asymmetry*) ini berarti pengguna tidak dapat memahami konsekuensi penuh dari data yang diserahkan. Persetujuan menjadi ritual kepatuhan hukum perusahaan, bukan manifestasi otonomi pengguna (N. Richards & Hartzog, 2015).

Sebuah studi komprehensif terhadap 11.000 situs belanja daring menemukan bahwa 11% dari situs-situs tersebut menggunakan *dark patterns* (Marthur et al., 2019). Dalam konteks Indonesia, *dark patterns* sering muncul dalam bentuk kotak centang yang sudah terisi (*pre-checked boxes*) untuk persetujuan berbagi data dengan pihak ketiga atau membuat tombol "tolak semua" sulit ditemukan.

b. Ketidaksetaraan Posisi Tawar (*Bargaining Power Imbalance*)

Perusahaan teknologi besar seringkali memegang kendali atas layanan-layanan yang kini dianggap esensial bagi partisipasi sosial dan ekonomi. Terdapat implikasi "*Take it or Leave it*", hal ini terjadi ketika pengguna dihadapkan pada dikotomi di mana penolakan terhadap pemrosesan data tertentu bahkan yang tidak relevan dengan fungsi layanan inti, dapat mengakibatkan hilangnya akses total. Sebuah aplikasi dompet digital atau transportasi seringkali meminta izin akses ke galeri foto, kontak telepon, dan mikrofon sebagai prasyarat wajib untuk menggunakan layanan inti, meskipun izin tersebut tidak proporsional dengan tujuan layanan.

Dalam situasi ini, persetujuan tidak dapat dianggap bebas sebagaimana diatur dalam Pasal 22 Undang-Undang Perlindungan Data Pribadi, sebab individu dipaksa menukarkan hak privasi mereka dengan hak untuk berpartisipasi dalam kehidupan digital (Solove, 2021). Kondisi ini menimbulkan risiko serius bagi kelompok rentan yang bergantung pada layanan digital untuk akses ekonomi atau sosial.

2. Dampak Pemrosesan Data Invasif: *Profiling*, Diskriminasi Algoritmik, dan *Corporate Surveillance*

Setelah data berhasil dikumpulkan, praktik pemrosesan data oleh perusahaan teknologi seringkali melanggar prinsip-prinsip inti Undang-Undang

Perlindungan Data Pribadi, yaitu "Pembatasan Tujuan "sebagaimana diatur dalam Pasal 16, "Kebutuhan dan Proporsionalitas" sebagaimana diatur dalam Pasal 17, dan "Transparansi" sebagaimana diatur dalam Pasal 21 Undang-undang *a quo*.

a. *Function Creep* dan Pelanggaran Prinsip Pembatasan Tujuan

Fenomena *function creep* adalah praktik di mana data yang dikumpulkan untuk satu tujuan spesifik (misalnya, pengiriman barang atau pemrosesan pembayaran) kemudian digunakan untuk tujuan lain yang tidak diantisipasi atau tidak diizinkan oleh subjek data, misalnya analisis prediktif pasar atau *cross-selling*. Hal ini menimbulkan konflik dalam Undang-Undang Perlindungan Data Pribadi. Sebagaimana Pasal 16 mengatur prinsip pembatasan tujuan, secara ketat membatasi pemrosesan pada tujuan yang telah diungkapkan di awal. *Function creep* secara sistemik melanggar prinsip pada Pasal 16 karena motif yang mendasari pemrosesan bergeser dari manfaat layanan (*utility*) menjadi monetisasi data (*profit*), sehingga menunjukkan kegagalan akuntabilitas dalam menjaga integritas tujuan.

b. *Profiling* Invasif dan Diskriminasi Algoritmik

Perusahaan teknologi menggunakan *Machine Learning* dan *Artificial Intelligence* (AI) untuk menganalisis data perilaku yang sangat besar (*big data*), guna menciptakan profil psikografis, finansial, dan sosial yang sangat detail. Sehingga hal tersebut memungkinkan *microtargeting* konten, iklan, atau bahkan penawaran layanan tertentu dengan presisi tinggi. Meskipun menjajikan efisiensi pasar, praktik ini berpotensi manipulatif, memengaruhi keputusan konsumen, dan dalam konteks politik dapat mengancam integritas proses demokrasi (P. Wang, 2016).

Di Amerika Serikat dan Eropa, riset menunjukkan bahwa algoritma penentuan kelayakan kredit dan pemrosesan aplikasi pinjaman seringkali membebankan suku bunga yang lebih tinggi atau menolak pemohon yang berasal dari etnis atau wilayah dengan pendapatan rendah. Meskipun data spesifik Indonesia masih terbatas, sistem *scoring* berbasis AI pada sektor *fintech* dan asuransi berpotensi mengimpor bias serupa.

Dampak hak asasi manusia yang paling krusial adalah potensi *profiling* yang menghasilkan diskriminasi algoritmik. Jika data pelatihan yang dimasukkan ke dalam sistem AI mencerminkan bias sosial atau ketidaksetaraan historis, misalnya bias gender atau geografis dalam data pengajuan pinjaman, maka keputusan otomatis yang dihasilkan oleh algoritma akan memperkuat bias tersebut, bahkan tanpa disadari oleh pengembang sistem (Eubanks & Virginia, 2018)

Diskriminasi algoritmik melanggar hak untuk non-diskriminasi. Di Indonesia, ini dapat membatasi peluang hidup individu, misalnya dalam penentuan kelayakan kredit *fintech,* penawaran asuransi, atau proses rekrutmen otomatis. Keputusan yang tertutup (*opaque*) dan tidak dapat dibantah secara efektif menyulitkan korban untuk menggunakan Hak Akses sebagaimana diatur dalam Pasal 15 dan Hak Koreksi sebagaimana diatur dalam Pasal 11 Undang-Undang Perlindungan Data Pribadi.

Pemrosesan data yang menghasilkan diskriminasi tidak dapat dianggap proporsional karena dampak negatifnya terhadap individu jauh melebihi manfaat komersial yang diperoleh perusahaan.

c. *Corporate Surveillance*

Melalui interkoneksi layanan (*cross-platiform tracking*) dan pengumpulan data *real-time*, perusahaan teknologi menciptakan ekosistem di mana pengguna berada dalam kondisi pengawasan yang permanen. Pengawasan ini bersifat *pervasive,* melacak jejak digital dan fisik pengguna. Motifnya didorong oleh keuntungan, menjadikannya jenis pengawasan yang secara kualitatif lebih invasif daripada pengawasan negara tradisional karena cakupan datanya yang detail, berkelanjutan, dan ditujukan untuk memprediksi serta memengaruhi perilaku (Cohen, 2019). Mayoritas aplikasi dan situs web menggunakan *tracker* pihak ketiga seperti Google Analytics, Facebook Pixel, dll., yang memungkinkan perusahaan teknologi melacak perilaku pengguna di luar platform mereka sendiri. Laporan menunjukkan rata-rata situs web menggunakan 30-40 *tracker*.

Kesadaran bahwa setiap interaksi digital direkam, dianalisis, dan diprofilkan dapat menimbulkan efek mendingin (*chilling effect*) pada kebebasan berekspresi dan eksplorasi informasi. Individu cenderung menyensor diri sendiri, yang merupakan pelanggaran tidak langsung terhadap kebebasan sipil.

3. Kegagalan Akuntabilitas Keamanan dan *Data Breach* Sistemik

Akuntabilitas perusahaan teknologi tidak hanya mencakup aspek legalitas pemrosesan, tetapi juga kewajiban teknis untuk menjaga keamanan data sebagaimana diatur dalam Pasal 35 Undang-Undang Perlindungan Data Pribadi. Kegagalan di bidang ini telah menghasilkan insiden *data breach* yang sistemik di Indonesia. Pada tahun 2020, salah satu *e commerce* besar Indonesia mengalami kebocoran data yang melibatkan 91 juta akun, termasuk nama, email, dan *hash password.* Penyebabnya diduga adalah kerentanan keamanan di sisi server. Pada tahun 2021-2022, dalam sektor layanan publik terjadi beberapa insiden kebocoran data warga yang dikelola oleh lembaga pemerintah dan layanan kesehatan, melibatkan puluhan juta data pribadi, termasuk data sensitif.

Insiden ini mengonfirmasi bahwa banyak pengendali data pribadi, baik sektor swasta maupun publik gagal menerapkan pengamanan yang memadai. Kegagalan ini seringkali disebabkan oleh kurangnya investasi pada *security by design* atau tata kelola siber yang lemah, menunjukkan akuntabilitas yang rendah terhadap perlindungan hak privasi. Setelah insiden, banyak perusahaan cenderung menunda atau meminimalkan pengungkapan, yang melanggar kewajiban pelaporan dalam waktu 3 x 24 jam. Kurangnya transparansi ini mencegah subjek data mengambil langkah mitigasi tepat waktu, seperti mengganti kata sandi atau memblokir kartu kredit, sehingga memperburuk kerugian individu.

Evaluasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai Standar Akuntabilitas Berbasis Hak Asasi Manusia.

Undang-Undang Perlindungan Data Pribadi menandai pergeseran paradigma hukum di Indonesia, dari pendekatan sektoral yang terfragmentasi menjadi kerangka hukum yang komprehensif dan horizontal. Tujuan utama Undang-Undang Perlindungan Data Pribadi adalah memberikan kepastian hukum dan memperkuat perlindungan hak privasi sebagai hak konstitusional dan hak asasi manusia. Evaluasi terhadap Undang-Undang Perlindungan Data Pribadi harus menilai sejauh mana standar akuntabilitas yang ditetapkan dapat selaras dan efektif dalam menjamin hak asasi manusia di tengah ekspansi bisnis digital.

1. **Titik Tumpu Undang-Undang Perlindungan Data Pribadi dalam Mendorong Akuntabilitas Berbasis Hak Asasi Manusia**

   Undang-Undang Perlindungan Data Pribadi mengadopsi prinsip-prinsip perlindungan data global, khusunya yang dicetuskan oleh GDPR di Uni Eropa, yang secara eksplisit mengakui privasi sebagai hak fundamental. Sehingga ada beberapa titik tumpu dalam Undang-Undang Perlindungan Data Pribadi guna mendorong akuntabilitas berbasis hak asasi manusia, yakni:

   a. **Penguatan Prinsip Akuntabilitas (*accountability principle*)**

      Undang-Undang Perlindungan Data Pribadi secara eksplisit mengatur prinsip akuntabilitas dan mengamanatkan kewajiban akuntabilitas yang ketat bagi pengendali data pribadi, sebagaimana termakhtub dalam Pasal 5 Undang-undang *a quo*, yang berbunyi: "*Subjek Data Pribadi berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi*".

      Pasal 53 Undang-Undang Perlindungan Data Pribadi mewajibkan pengendali data pribadi untuk menunjukkan akuntabilitas, yang mencakup penetapan mekanisme tata kelola yang memadai, termasuk menunjuk Pejabat atau Petugas Perlindungan Data Pribadi (*Data Protection Officer*). Kewajiban ini sejalan dengan kerangka *UN Guiding principles on Business and Human Rights* (UNGPs) yang menekankan perlunya mekanisme *governance* internal untuk menghormati hak asasi manusia (Ruggie, 2011).

      Penunjukan *Data Protection Officer* adalah langkah krusial. *Data Protection Officer* bertindak sebagai titik kontak internal dan eksternal untuk isu perlindungan data. Keberadaan *Data Protection Officer,* jika independen dan berwenang, menjamin bahwa risiko privasi dipertimbangkan pada tingkat pengambilan keputusan strategis perusahaan, bergerak melampaui kepatuhan hukum (*legal compliance*) semata.

   b. **Pengakuan Hak Subjek Data sebagai Manifestasi Hak Asasi Manusia**

      Pasal 5 sampai 14 Undang-Undang Perlindungan Data Pribadi memperluas dan memperjelas hak-hak Subjek Data Pribadi, yang merupakan manifestasi konkret dari hak otonomi dan kontrol atas informasi pribadi (Solove, 2021).

Pasal 8 Undang-Undang Perlindungan Data Pribadi berbunyi: "*Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan*". Ketentuan Pasal 8 Undang-undang *a quo* memberikan hak kepada Subjek Data untuk meminta penghapusan dan/atau pemusnahan data pribadi. Hak ini sangat penting dalam era digital karena data dapat hidup selamanya secara *online*. Pengakuan hak ini selaras dengan upaya internasional untuk memulihkan kontrol individu atas jejak digital mereka.

Kemudian, Pasal 6 Undang-Undang Perlindungan Data Pribadi berbunyi: "*Subjek Data Pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi.*" Sementara Pasal 11 Undang-Undang Perlindungan Data Pribadi menerangkan bahwa : "*Subjek Data Pribadi berhak mendunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi.*" Hak tersebut diberikan untuk mengoreksi data yang tidak akurat dan menunda pemrosesan yang menjadi benteng terhadap *profiling* atau diskriminasi algoritmik yang didasarkan pada data yang salah atau telah usang.

c. Mekanisme Pencegahan Proaktif (*Data Protection Impact Assessment*)

Pada Pasal 34 ayat (1) Undang-Undang Perlindungan Data Pribadi menyebutkan: "*Pengendali Data Pribadi wajib melakukan penilaian dampak Perlindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi.*" Sehingga dalam rezim Undang-undang ini mewajibkan untuk melakukan Penilaian Dampak Perlindungan Data (*Data Protection Impact Assessment*) jika pemrosesan data memiliki potensi risiko tinggi.

Data Protection Impact Assessment adalah alat kunci *Human Rights Due Diligence* yang diamanatkan dalam Prinsip 17 UNGPs:

"*In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human right impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Human rights due diligence:*

(a). Should cover adverse human rights impacts that the business enterprises may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationship;

(b). Will vary complexity with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations;

(c). Should be ongoing, recognizing that the human rights risks may change over time as the business enterprise's operations and operating context evolve.

Prinsip-prinsip ini secara komprehensif mendefinisikan paramater terhadap uji tuntas hak asasi manusia. Risiko hak asasi manusia harus dipahami sebagai potensi dampak merugikan badan usaha terhadap hak asasi manusia. Potensi dampak harus diatasi melalui pencegahan atau mitigasi, sementara dampak aktual yang telah terjadi harus menjadi subjek

remediasi. Uji tuntas hak asasi manusia dapat dicakup dalam sistem manajemen perusahaan yang lebih luas, dengan syarat sistem tersebut tidak hanya mengidentifikasikan dan mengelola risiko materiil terhadap perusahaan itu sendiri, tetapi juga mencakup risiko terhadap pemegang hak.

Data Protection Impact Assessment memaksa perusahaan untuk mengidentifikasi dan memitigasi risiko privasi secara proaktif sebelum sistem atau produk baru diluncurkan, Dengan mewajibkan *Data Protection Impact Assessment*, Undang-Undang Nomor Perlindungan Data Pribadi mendorong perusahaan untuk mengadopsi prinsip *Privacy by Design*, dengan mengintegrasikan perlindungan data ke dalam arsitektur sistem sejak awal, yang merupakan tuntutan etis dan teknis dari akuntabilitas modern (Bygrave, 2024).

d. Penegakan Hukum dan Sanksi yang Memberikan Daya Paksa

Undang-Undang Perlindungan Data Pribadi memperkenalkan sanksi administratif, sebagaimana termaktub dalam Pasal 57 ayat (3) yang berbunyi: "*Sanksi adminidtratif berupa denda administratif sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.*" Potensi denda hingga 2% dari pendapatan tahunan adalah daya getar (*deterrent*) yang kuat. Bagi perusahaan teknologi multinasional yang beroperasi di Indonesia, ancaman denda yang besar ini dapat memaksa perubahan perilaku *data governance* secara signifikan, alih-alih hanya menganggap denda sebagai biaya operasional yang kecil (*cost of doing business*).

2. Kesenjangan Implementasi dan Tantangan Akuntabilitas dalam Ekosistem Digital

Meskipun secara tekstual Undang-Undang Perlindungan Data Pribadi sudah kuat, namun Undang-undang ini mengadapi tantangan besar dalam implementasinya, terutama karena sifat dinamis dan *data-greedy* dari bisnis digital.

a. Tantangan Penerapan Prinsip Pembatasan Tuujuan dan Proporsionalitas

Model bisnis berbasis *Big Data* didorong oleh asumsi bahwa "*lebih banyak data selalu lebih baik*" dan "*data yang dikumpulkan hari ini mungkin berguna untuk tujuan yang tak terduga di masa depan*" (Mayer-Schönberger et al., 2013). Paradigma ini bertentangan secara fundamental dengan prinsip Pembatasan Tujuan dan Proporsionalitas, yang menuntut *data minimization* dan pembatasan pemrosesan hanya sebatas tujuan yang diungkapkan.

Banyak perusahaan *fintech* dan *e-commerce* masih berjuang untuk membenarkan pengumpulan data yang berlebihan, misalnya akses ke kontak atau galeri dalam konteks perlindungan data pribadi. Kesenjangan ini menunjukkan bahwa konflik antara kepentingan komersial dan kewajiban hukum belum terselesaikan di tingkat operasional korporasi.

b. Isu Yurisdiksi Ekstrateritorial dan Penegakan Terhadap *Big Tech*

Undang-Undang Perlindungan Data Pribadi memiliki ketentuan yurisdiksi ekstrateritorial sebagaimana diamksud dalam Pasal 2 Undang-undang *a quo*, yang memungkinkan penerapan Undang-undang ini kepada

pengendali data pribadi asing yang memproses data subjek Indonesia. Menurut data dari Otoritas Jasa Keuangan (OJK) pada Oktober 2024, terdapat ratusan perusahaan teknologi finansial termasuk yang didukung modal asing yang beroperasi. Sebagian besar *Big Tech* global juga beroperasi di Indonesia. Penegakan hukum terhadap entitas asing yang melanggar di luar wilayah Indonesia memerlukan (Arrazy, 2023):

(1) Kapasitas teknis otoritas pengawas, otoritas harus memiliki keahlian teknis dan sumber daya yang memadai untuk mengaudit sistem *cloud* dan data lintas batas dari perusahaan global.

(2) Kerja sama internasional, penegakan efektif memerlukan kerja sama hukum yang kuat dengan yurisdiksi lain.

c. Kelemahan Otoritas Pengawas

Efektivitas Undang-Undang Perlindungan Data Pribadi sangat bergantung pada kinerja lembaga pengawas yang independen. Proses pembentukan dan penguatan otoritas pengawas pasca Undang-Undang Perlindungan Data Pribadi membutuhkan waktu dan investasi signifikan. Ketiadaan otoritas yang kuat di masa transisi atau ketiadaan sumber daya yang memadai dapat melumpuhkan daya getar sanksi yang telah ditetapkan. Jika otoritas tidak dapat secara efektif menjatuhkan denda 2% kepada perusahaan global, maka Undang-Undang Perlindungan Data Pribadi akan kehilangan taringnya.

3. Akuntabilitas Substantif sebagai Kebutuhan Integrasi *Human Rights Due Diligence*

Akuntabilitas dalam perspektif hak asasi manusia sebagaimana diatur prinsip-prinsip nya di dalam *UN Guiding Principles on Business and Human Rights,* menuntut lebih dari sekadar kepatuhan formal (*tick-box compliance*), yakni akuntabilitas substantif, dimana perusahaan wajib membuktikan bahwa operasionya tidak melanggar hak asasi manusia, termasuk hak privasi (Ruggie, 2011).

Meskipun Undang-Undang Perlindungan Data Pribadi mewajibkan *Data Protection Impact Assessment* yang dinilai merupakan mekanisme tepat, akan tetapi fokusnya masih sempit pada privasi data. Akuntabilitas hak asasi manusia menuntut *Human Rights Impact Assessment*. *Human Rights Impact Assessment* menilai dampak yang lebih luas, seperti risiko diskriminasi algoritmik, dampak terhadap kebebasan berkespresi, dan manipulasi perilaku yang melampaui lingkup keamanan data dan kerahasiaan. Untuk memastikan akuntabilitas substantif, perusahaan teknologi perlu menginternalisasi *Human Rights Impact Assessment* sebelum implementasi sistem AI atau *profiling* berisiko tinggi.

Tantangan terbesar bagi Undang-Undang Perlindungan Data Pribadi adalah mengatur transparansi dan akuntabilitas algoritma. Dalam kasus *profiling* yang menghasilkan keputusan otomatis yang merugikan, misalnya penolakan kartu kredit, Undang-Undang Perlindungan Data Pribadi belum memiliki mekanisme yang cukup eksplisit untuk menuntut penjelasan yang berarti (*meaningful explanation*) dari pengendali data pribadi, yang esensial untuk menggunakan hak koreksi dan gugatan. Hak subjek data untuk mengetahui

logika di balik keputusan otomatis sangat penting untuk menuntut akuntabilitas korporasi (N. M. Richards & Woodrow Hartzog, 2015).

Teori keadilan algoritmik (O'Neil, 2016) menekankan bahwa sistem AI harus adil, transparan, dan dapat dipertanggunghawabkan. Akuntabilitas korporasi harus mencakup audit rutin oleh pihak independen terhadap bias dalam data pelatihan dan mekanisme keputusan algoriitma, bukan sekadar janji etis internal.

Pilar ketiga UNGPs menekankan perlu adanya akses ke pemulihan yang efektif. Mekanisme pengaduan internal yang disediakan oleh perusahaan teknologi seringkali *opaque*, lambat, dan tidak memenuhi standar efektivitas UNGPs. Masyarakat berpenghasilan rendah atau mereka yang kurang terliterasi digital menghadapi hambatan besar untuk menuntut pemulihan, menjadikan jalur hukum formal menjadi satu-satunya, namun mahal.

Dengan demikian, Undang-Undang Perlindungan Data Pribadi telah menyediakan fondasi hukum yang kuat untuk akuntabilitas. Namun, transisi dari akuntabilitas hukum formal menuju akuntabilitas substantif berbasis hak asasi manusia menuntut penegakan yang ketat, investasi pada otoritas pengawas, dan adopsi *Human Rights Due Diligence* yang komprehensif di sektor digital.

UN Guiding Principles on Business and Human Rights (UNGPs) sebagai Instrumen Evaluatif Akuntabilitas Korporasi Digital

Mengingat keterbatasan hukum nasional, akuntabilitas perusahaan teknologi dalam perlindungan privasi haruslah dievaluasi menggunakan kerangka standar global yang lebih komprehensif. UNGPs menawarkan kerangka normatif yang melampaui kepatuhan hukum semata. UNGPs mendefinisikan tanggung jawab korporasi untuk menghormati hak asasi manusia, termasuk hak privasi, sebagai standar perilaku global yang diharapkan dari seluruh entitas bisnis, terlepas dari keberadaan atau kekuatan hukum domestik.

UNGPs beroperasi di atas 3 (tiga) pilar: (1) Kewajiban negara untul melindungi hak asasi manusia (*duty to protect*); (2) Tanggung jawab korporasi untuk menghormati hak asasi manusia (*responsibility to respect*); dan (3) Akses ke remediasi (Ruggie, 2011). Pilar kedua adalah instrumen evaluatif utama bagi akuntabilitas perusahaan teknologi di Indonesia.

1. **Tanggung Jawab Korporasi untuk Menghormati Hak Asasi Manusia**

   Prinsip 11 UNGPs menegaskan bahwa perusahaan memiliki tanggung jawab independen untuk menghormati hak asasi manusia, yang berarti perusahaan harus bertindak dengan uji tuntas (*due diligence*), untuk memastikan operasinya tidak melanggar hak asasi manusia. Dalam konteks digital, tanggung jawab ini direalisasikan melalui tiga komponen inti, yakni komitmen kebijakan, uji tuntas dan mekanisme pemulihan operasional.

   a. **Kebijakan komitmen dan pengakuan hak privasi sebagai hak asasi manusia**

      Prinsip 16 UNGPs mengharuskan perusahaan memiliki kebijakan publik yang secara jelas menyatakan komitmen untuk menghormati hak asasi manusia. Mayoritas perusahaan teknologi di Indonesia memiliki kebijakan

privasi yang panjang, tetapi jarang yang secara eksplisit mengakui "hak privasi sebagai hak asasi manusia" dalam bahasa kebijakan internal mereka. Kebijakan tersebut cenderung berfokus pada kepatuhan Undang-Undang Perlindungan Data Pribadi atau Undang-Undang Transaksi dan Informasi Elektronik, bukan pada kepatuhan terhadap standar hak asasi manusia yang lebih tinggi. Kurangnya komitmen eksplisit terhadap kerangka hak asasi manusia membuat perlindungan privasi perusahaan berpotensi berubah-ubah, bergantung pada interpretasi hukum nasional yang mungkin bersifat minimalis. Akuntabilitas yang sejati menuntut pengakuan dan integrasi prinsip hak asasi manusia yang universal ke dalam tata kelola perusahaan (*corporate governance*).

b. Uji tuntas hak asasi manusia (*Human Rights Due Diligence*)

Human Rights Due Diligence sebagaimana diatur pada Prinsip 17 sampai dengan 21 UNGPs adalah jantung dari akuntabilitas korporasi, yang didefinisikan sebagai proses berkelanjutan untuk mengidentifikasi, mencegah, memitigasi, dan mempertanggungjawabkan bagaimana perusahaan menangani dampak hak asasi manusia aktual dan potensial dari operasinya.

Dalam bisnis digital, *Human Rights Due Diligence* harus dimanifestasikan melalui *Human Rights Impact Assessment. Human Rights Impact Assessment* melampaui *Data Protection Impact Assessment* yang diwajibkan oleh Undang-Undang Perlindungan Data Pribadi. *Human Rights Impact Assessment* harus menilai dampak produk digital, algoritma, dan *data sharing* terhadap seluruh spektrum hak asasi manusia, termasuk non-diskriminasi, kebebasan berekspresi, dan hak privasi. Penggunaan AI untuk *content moderation* di *platform* media sosial, misalnya, berpotensi melanggar kebebasan berekspresi. *Human Rights Due Diligence* akan mewajibkan perusahaan mengaudit algoritma tersebut untuk memastikan proporsionalitas dan transparansi sebelum diimplementasikan. Tanpa *Human Rights Due Diligence* yang terstruktur, risiko diskriminasi algoritmik dan pengawasan berlebihan akan terus meningkat.

Human Rights Due Diligence menuntut integrasi temuan *Human Rights Due Diligence* ke dalam desain sistem (*privacy by design*). Misalnya, jika *profiling* untuk iklan berisiko tinggi terhadap kelompok rentan, perusahaan harus memilih mekanisme data *minimization* atau *purpose limitation* secara aktif. Perusahaan wajib melacak efektivitas langkah mitigasi mereka dan mengkomunikasikannya secara transparan kepada publik sebagaimana diatur dalam Prinsip 21 UNGPs. Transparansi ini esensial untuk akuntabilitas, namun seringkali menjadi titik lemah bagi perusahaan teknologi yang berdalih melindungi kerahasiaan dagang (*trade secrets*). Di Indonesia, *Human Rights Due Diligence* di sektor teknologi sebagian besar masih bersifat sukarela atau hanya sebatas *check-box compliance* terhadap *Data Protection Impact Assessment* Undang-Undang Perlindungan Data Pribadi. Hingga saat ini belum adanya mandat regulasi yang mengharuskan perusahaan besar secara rutin menerbitkan laporan *Human Rights Due Diligence* yang diaudit secara eksternal.

2. Akses ke Remediasi dalam Konteks Digital

Prinsip 31 UNGPs menetapkan kriteria bagi mekanisme pengaduan operasional yang harus sah, dapat diakses, transparan, prediktif, adil, didasarkan pada dialog, dan menjadi sumber pembelajaran. Ketika *data breach* atau keputusan algoritmik merugikan terjadi, mekanisme pengaduan yang disediakan oleh perusahaan teknologi, misalnya, *help center* atau formulir *customer service* seringkali gagal memenuhi kriteria ini. Pengguna seringkali tidak tahu proses penanganan pengaduan mereka, kerangka waktu penyelesaian, atau kriteria apa yang digunakan untuk menilai kerugian. Bagi pelanggaran privasi serius, misalnya, *identity theft* akibat kebocoran data, pemulihan yang ditawarkan perusahaan seperti mengganti kata sandi atau memberikan kupon seringkali tidak proporsional dengan kerugian yang diderita.

UNGPs sangat relevan untuk mengatasi masalah akuntabilitas perusahaan teknologi multinasional atau *big tech*. UNGPs menekankan bahwa perusahaan induk bertanggung jawab atas dampak hak asasi manusia anak perusahaan dan rantai lainnya, sebagaimana diatur dalam Prinsip 13 dan 19 UNGPs. Hal ini memaksa perusahaan global untuk memastikan bahwa standar perlindungan privasi di Indonesia tidak lebih rendah daripada di yurisdiksi lain.

3. *UN Guiding Principles on Business and Human Rights* sebagai Standar Evaluatif Transformatif

Penerapan UNGPs secara substantif di sektor digital Indonesia adalah kunci untuk transisi dari akuntabilitas formal menuju akuntabilitas etis dan berbasis HAM. UNGPs menyediakan kerangka kerja untuk menilai kualitas akuntabilitas, bukan hanya sekadar kuantitas dokumen kepatuhan. Meskipun Undang-Undang Perlindungan Data Pribadi kuat, UNGPs berfungsi sebagai *benchmark* yang meningkatkan standar implementasi. Misalnya, kewajiban *Data Protection Officer* harus diukur berdasarkan apakah *Data Protection Officer* memiliki wewenang untuk mendorong *Human Rights Due Diligence*, bukan hanya untuk mengurus perizinan semata.

UNGPs juga memberdayakan investor dan konsumen. Investor global semakin menggunkaan kerangka *Environmental, Social, and Governance* (ESG) untuk menilai resiko. Kegagalan perusahaan teknologi memenuhi standar *Human Rights Due Diligence* UNGPs, misalnya insiden *data breach* yang berulang dapat dianggap sebagai risiko ESG yang serius yang dapat mempengaruhi pendanaan dan nilai pasar mereka.

Dengan mengadopsi UNGPs, akuntabilitas korporasi digital di Indonesia dapat dipastikan untuk menjadi proaktif, komprehensif, dan secara mendasar mengormati hak privasi sebagai hak asasi manusia.

SIMPULAN

Kesimpulan

Kesimpulan penelitian ini menjawab tiga pertanyaan utama mengenai hubungan antara bisnis digital, hak privasi, dan akuntabilitas perusahaan di Indonesia.

1. Praktik perusahaan teknologi saat ini merusak hak privasi secara mendasar melalui tiga cara utama, yakni:

(a). Perusahaan menggunakan desain aplikasi yang menipu, dalam hal ini disebut sebagai *dark patterns* untuk mendapatkan persetujuan pengguna secara tidak jujur. Hal Ini merampas hak pengguna untuk memutuskan secara otonom atas data mereka;

(b). Perusahaan mengumpulkan terlalu banyak data yang melebihi kebutuhan layanan dan menggunakannya untuk tujuan lain (*function creep*), seperti *profiling* yang invasif dan melacak perilaku pengguna secara terus menerus.

(c). Pengguna algoritma untuk *profiling* berisiko tinggi menciptakan diskriminasi algoritmik, yang melanggar hak asasi untuk tidak didiskriminasi.

2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah selaras dengan prinsip hak asasi manusia global karena menetapkan hak-hak pengguna yang diperluas, seperti hak untuk dilupakan (*right to be forgotten*) dan menetapkan kewajiban akuntabilitas serta sanksi denda yang besar hingga 2% pendapatan perusahaan. Namun, disisi lain efektivitas Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhambat karena Undang-undang ini menuntut batasan data, sementara perusahaan ingin data sebanyak mungkin. Sementara itu, penerapan sanksi dan pengawasan terhadap perusahaan *big tech* multinasional sangat bergantung pada otoritas pengawas yang harus kuat dan independen.
3. *UN Guiding Principles on Business and Human Rights* (UNGPs) berfungsi sebagai standar etika global yang harus digunakan untuk menilai kualitas akuntabilitas perusahaan, melampaui kepatuhan hukum saja. UNGPs mewajibkan perusahaan melakukan Uji Tuntas Hak Asasi Manusia (*Human Rights Due Diligence*). Hal ini berarti perusahaan harus secara proaktif menilai, mencegah, dan memitigasi risiko hak asasi manusia sebelum produk atau layanan diluncurkan, bukan hanya setelah terjadi masalah. UNGPs juga menuntut adanya mekanisme pemulihan (*remedy*) yang efektif dan adil bagi korban, memastikan bahwa kompensasi atau solusi yang diberikan sepadan dengan kerugian privasi yang diderita.

DAFTAR PUSTAKA

Buku

Andrejevic, M. (2020). *Automated media*. Routledge.

APJII. (2025). *Profil Internet Indonesia 2025*.

Bygrave, L. A. (2024). *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Edward Elgar Publishing.

Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Eubanks, & Virginia. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Mayer-Schönberger, Viktor, & Kenneth Cukier. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

Richards, N., & Hartzog, W. (2015). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

Ruggie, J. (2011). *The UN Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. United Nations.

Soekanto, S., & Mamudji, S. (2011). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat.* RajaGrafindo Persada.

Solove, D. (2021). *Understanding Privacy*. Harvard University Press.

Wang, F. (2016). *Big Data and the Law*. Cambridge University Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Jurnal Ilmiah

Acquisti, Alessandro, Leslie K, & George Loewenstein. (2016). What Is Privacy Worth? *The Journal of Legal Studies*, *45*(S1), 249–270.

Arrazy, F. (2023). Tantangan Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia Pasca-Pengesahan. *Jurnal Hukum Dan Pembangunan*, *53*(1), 1–20.

Marthur, Arunesh, Gunes Acar, Michael J. Backes, Emmanouil Vasilomanolakis, Michael Schlichtkrull, Balachander Krishnamurthy, & Nick Feamster. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 1–32.

Richards, N. M., & Woodrow Hartzog. (2015). The Pathologies of Digital Consent. *New York University Law Review*, *90*(2), 522–596.

Sutanto, A. W. (2020). The Urgency of Personal Data Protection Law in Indonesia: A Comparison with GDPR. *Indonesian Law Review*, *10*(2), 203–225.

Wang, P. (2016). Journal of Management and Sustainability. *Information Systems Journal*, *26*(5), 415–432.

Prosiding Seminar

Google, Tamasek, & Bain & Company. (2024). *e-Conomy Southeast Asia 2024: Southeast Asia's Digital Decade*.

Google, Temasek, & Bain & Company. (2025). *e-Conomy Southeast Asia 2025: Indonesia's Digital Market Approaches US$100 Billion GMV*.

Peraturan Perundang-Undangan dan Konvensi Internasional

Undang-Undang Dasar Negara Republik Indonesia 1945.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Undang-undang (UU) Nomor 12 Tahun 2005 tentang *Pengesahan International Covenant on Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik).

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

UN Guiding Principles on Business and Human Rights.

International Covenant on Civil and Political Rights.

Universal Declaration of Human Rights.

The General Data Protection Regulation.