'ADALAH
Buletin Hukum & Keadilan

ISSN: 2338 4638

Volume 6 Nomor 7 (2022)

Perlindungan Data Pribadi dan Hak Privasi di Era

ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

'ADALAH
Buletin Hukum & Keadilan

Perlindungan Data Pribadi sebagai Hak Asasi di Era Digital: Menggagas Paradigma Konstitusional dalam Arsitektur Privasi Indonesia

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.511167

Abstract:
Digital transformation has turned personal data from identity information into a tradable asset. This article examines personal data protection within a human rights framework and evaluates Indonesia's regime under Law No. 27/2022 on Personal Data Protection (PDP Law). Using conceptual, statutory, and comparative approaches, the study finds that the PDP Law provides a legal foundation but still faces challenges involving independent supervision and remedies for data subjects. Personal data protection represents privacy, dignity, and constitutional rights. The article recommends establishing an independent supervisory authority and strengthening digital literacy.

Keywords: *Personal Data Protection, Human Rights, Digital Privacy, PDP Law, Constitutional Rights.*

A. PENDAHULUAN

Akselerasi digitalisasi yang melanda seluruh sektor kehidupan telah mengubah data pribadi menjadi komoditas paling berharga di abad ke-21. Setiap klik, transaksi, dan interaksi di platform digital menghasilkan jejak data yang dikumpulkan, dianalisis, dan diperjualbelikan oleh korporasi serta dimanfaatkan oleh pemerintah untuk berbagai kepentingan. Dalam lanskap ini, individu tidak lagi memiliki kendali penuh atas informasi personalnya, sehingga muncul ancaman serius terhadap privasi dan martabat manusia. Perlindungan data pribadi pun bergeser dari isu teknis menjadi isu hak asasi manusia (HAM) yang fundamental.

Secara historis, perlindungan privasi telah diakui sebagai bagian integral dari HAM. Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) tahun 1948 dengan tegas menyatakan bahwa tidak seorang pun boleh diganggu secara sewenang-wenang terhadap privasi, keluarga, rumah tangga, atau surat-menyuratnya. Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) Pasal 17 menegaskan kembali hak ini sebagai hak yang harus dilindungi oleh negara. Di era digital, norma ini menemukan medan perjuangan baru karena gangguan terhadap privasi tidak lagi memerlukan intervensi fisik, melainkan cukup melalui pengumpulan dan pengolahan data secara masif (Solove,

2021). Praktik surveillance capitalism yang dijalankan korporasi teknologi besar telah menciptakan asimetri informasi yang merugikan individu dan menempatkan subjek data dalam posisi yang sangat rentan.

Indonesia merespons tantangan ini dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang menjadi undang-undang komprehensif pertama di bidang ini. Sebelumnya, norma perlindungan data terserak di berbagai regulasi sektoral, seperti dalam UU ITE, UU Administrasi Kependudukan, dan Peraturan Pemerintah tentang Penyelenggaraan Sistem Elektronik. Lahirnya UU PDP dipandang sebagai pengakuan formal bahwa data pribadi adalah bagian dari hak privasi warga negara yang harus dilindungi secara sistemik. Namun, pengakuan formal ini belum cukup menjawab persoalan mendasar: apakah perlindungan data pribadi sudah dimaknai sebagai hak asasi dalam praktik hukum Indonesia? Ataukah ia sekadar menjadi rezim kepatuhan administratif tanpa roh HAM? Rumusan masalah artikel ini adalah: Pertama, bagaimana posisi perlindungan data pribadi sebagai hak asasi dalam kerangka hukum nasional dan internasional? Kedua, sejauh mana implementasi UU PDP mampu menjamin perlindungan substantif terhadap hak privasi warga negara? Tujuannya untuk menganalisis secara kritis dimensi

HAM dari perlindungan data pribadi dan mengevaluasi kesiapan Indonesia mewujudkannya.

B. PRIVASI, DATA PRIBADI, DAN MARTABAT MANUSIA

Hubungan antara data pribadi dan hak asasi manusia berakar pada konsep privasi yang telah berkembang selama lebih dari satu abad. Samuel Warren dan Louis Brandeis dalam artikel monumentalnya "*The Right to Privacy*" (1890) mendefinisikan privasi sebagai "hak untuk dibiarkan sendiri" (*the right to be let alone*). Konsep ini menjadi fondasi perlindungan hukum terhadap invasi ruang personal. Memasuki paruh kedua abad ke-20, perkembangan teknologi pengawasan dan komputerisasi melahirkan pemikiran baru. Alan Westin (1967) mendefinisikan privasi sebagai klaim individu untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang dirinya dikomunikasikan kepada orang lain. Definisi ini menambahkan dimensi kontrol atau kendali, yang menjadi esensi perlindungan data pribadi modern.

Dalam hukum internasional, hak atas privasi dijamin oleh Pasal 12 DUHAM dan Pasal 17 ICCPR. Komite HAM PBB dalam *General Comment* No. 16 menafsirkan Pasal 17 ICCPR secara luas, mencakup kewajiban negara untuk melindungi individu dari

campur tangan tidak sah, tidak hanya oleh negara tetapi juga oleh pihak swasta. Ini berarti negara memiliki kewajiban positif untuk menciptakan kerangka hukum yang melindungi warga negara dari pelanggaran privasi yang dilakukan oleh korporasi. Di era digital, Mahkamah Agung India dalam putusan bersejarah Justice K.S. Puttaswamy v. Union of India (2017) secara eksplisit menyatakan bahwa privasi adalah hak konstitusional yang inheren dengan hak hidup dan kebebasan pribadi. Mahkamah Konstitusi Jerman dalam Volkszählungsurteil (1983) juga telah melahirkan konsep *informational self-determination* (hak menentukan nasib sendiri atas informasi), yang menggagas bahwa individu memiliki hak untuk mengetahui dan mengontrol siapa yang mengetahui apa tentang dirinya (Greenleaf, 2022).

Di Indonesia, landasan konstitusional perlindungan data pribadi dapat ditemukan dalam Pasal 28G ayat (1) UUD 1945 yang menjamin hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda, serta hak atas rasa aman dari ancaman. Mahkamah Konstitusi dalam Putusan Nomor 006/PUU-I/2003 secara implisit mengakui hak privasi sebagai bagian dari hak konstitusional yang dilindungi. Namun, pengakuan eksplisit terhadap data pribadi sebagai hak asasi baru mendapatkan tempatnya dalam UU PDP. Dengan demikian, kerangka teoretis ini menegaskan bahwa perlindungan data pribadi bukan

sekadar isu regulasi teknis, melainkan perlindungan terhadap harkat dan martabat manusia (*human dignity*) dalam wujud digitalnya.

C. PERLINDUNGAN DATA PRIBADI SEBAGAI HAK ASASI DALAM KONTEKS INDONESIA

1. Landasan Konstitusional dan Pergeseran Paradigma Hukum

Pengakuan terhadap perlindungan data pribadi sebagai hak asasi di Indonesia tidak muncul secara tiba-tiba. Pasal 28G UUD 1945 telah menyediakan payung konstitusional bagi perlindungan privasi. Namun, sebelum UU PDP, norma ini hanya menjadi dasar yang abstrak dan tidak operasional. Regulasi sektoral yang ada bersifat fragmentaris dan tidak memberikan perlindungan komprehensif. Misalnya, UU ITE hanya mengatur aspek pidana penyalahgunaan data, sedangkan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik lebih berfokus pada administrasi platform digital. Ketiadaan undang-undang yang secara khusus melindungi data pribadi sebagai hak individual membuat perlindungan ini terabaikan (Wahyudi & Ayu, 2024).

Disahkannya UU PDP menandai pergeseran paradigma penting. Untuk pertama kalinya, Indonesia

memiliki definisi hukum yang jelas tentang data pribadi, prinsip-prinsip pemrosesan data, hak-hak subjek data, serta kewajiban pengendali dan prosesor data. Hak-hak subjek data yang dijamin, seperti hak untuk diinformasikan, hak untuk mengakses, hak untuk mengoreksi, hak untuk menghapus (right to erasure), dan hak untuk menolak pemrosesan merupakan turunan langsung dari prinsip *informational self-determination* yang dikembangkan di Jerman (Bradford, 2020). Ini menunjukkan bahwa UU PDP, secara normatif, telah meletakkan data pribadi dalam kerangka hak asasi yang memberikan kendali kepada individu atas informasinya.

Namun, persoalannya tidak berhenti pada level pengakuan normatif. Hak-hak ini memerlukan mekanisme penegakan yang efektif. Tanpa otoritas pengawas independen, hak-hak tersebut hanya akan menjadi ayat-ayat mati. UU PDP mengamanatkan pembentukan otoritas pengawas yang langsung bertanggung jawab kepada Presiden, namun hingga saat ini lembaga tersebut belum terbentuk secara efektif. Keterlambatan ini mencerminkan kurangnya prioritas negara dalam menegakkan hak asasi digital warga negaranya (Pratiwi & Nugroho, 2023).

2. Kewajiban Negara dalam Rezim HAM Digital

Dalam perspektif HAM, negara memiliki tiga kewajiban utama: menghormati (*to respect*), melindungi (*to protect*), dan memenuhi (*to fulfil*l). *To respect* berarti negara tidak boleh melakukan pengumpulan atau pemrosesan data secara sewenang-wenang. Ini menjadi tantangan serius mengingat banyaknya praktik pengumpulan data oleh lembaga pemerintah yang tidak dilandasi oleh dasar hukum yang kuat dan proporsional. Program pengawasan digital, pengenalan wajah, dan aplikasi pelayanan publik yang meminta akses berlebihan ke data pribadi adalah contoh di mana negara sendiri berpotensi melanggar hak privasi warga negara (Setiawan, 2023).

To protect menuntut negara untuk mencegah pelanggaran oleh pihak ketiga, terutama korporasi. UU PDP telah mengatur kewajiban pengendali data untuk menjaga keamanan data, melaporkan insiden kebocoran, dan bertanggung jawab atas kerugian yang timbul. Namun, sanksi administratif dan denda yang diatur masih relatif rendah dibandingkan dengan potensi keuntungan yang diperoleh korporasi dari eksploitasi data. Tanpa sanksi yang memberikan efek jera, kewajiban negara untuk melindungi tidak akan efektif (Wibisono, 2023). *To fulfill* berarti negara harus memfasilitasi pemenuhan hak, termasuk melalui edukasi publik, penyediaan mekanisme pengaduan yang aksesibel, dan pengembangan infrastruktur keamanan

data nasional. Pada titik ini, peran negara masih sangat minim. Masyarakat belum teredukasi tentang hak-haknya, dan jalur pengaduan masih rumit dan birokratis.

3. Kelemahan Struktural: Otoritas Pengawas dan Mekanisme Pemulihan

Salah satu indikator utama apakah perlindungan data pribadi benar-benar diperlakukan sebagai hak asasi adalah keberadaan otoritas pengawas independen. GDPR di Eropa mensyaratkan setiap negara anggota memiliki *Data Protection Authority* (DPA) yang independen, memiliki wewenang investigasi, dan dapat menjatuhkan sanksi. Independensi ini penting karena otoritas harus mampu mengawasi, bahkan menindak, lembaga pemerintah jika diperlukan. UU PDP mengamanatkan pembentukan lembaga serupa, namun rancangannya masih menuai kritik.

Pasal-pasal UU PDP menempatkan otoritas pengawas sebagai lembaga yang bertanggung jawab kepada Presiden, bukan kepada parlemen atau publik secara langsung. Hal ini berpotensi mengurangi independensinya, terutama ketika berhadapan dengan pelanggaran yang dilakukan oleh kementerian atau badan pemerintah. Selain itu, mekanisme pemulihan bagi subjek data yang dirugikan belum diatur secara detail. Hak untuk menuntut ganti rugi memang ada,

tetapi tanpa prosedur yang sederhana dan biaya terjangkau, mekanisme ini hanya menjadi fiksi hukum bagi kebanyakan warga negara (Siregar, 2024).

D. KEBOCORAN DATA DAN RENTANNYA WARGA NEGARA

Studi kasus yang paling relevan untuk mengilustrasikan urgensi perlindungan data pribadi sebagai hak asasi adalah insiden kebocoran data di berbagai institusi di Indonesia. Salah satu kasus yang paling menyita perhatian publik adalah dugaan kebocoran data nasabah sebuah perusahaan telekomunikasi besar pada tahun 2022, yang diikuti oleh kebocoran data pada aplikasi pelacak kontak COVID-19 milik pemerintah. Data-data yang bocor mencakup nomor induk kependudukan (NIK), alamat, nomor telepon, hingga riwayat kesehatan.

Kasus ini memperlihatkan beberapa hal. Pertama, lemahnya standar keamanan data yang dimiliki oleh pengendali data, baik swasta maupun pemerintah. Kedua, lambatnya respons dan komunikasi publik mengenai insiden tersebut. Subjek data tidak segera diberitahu sehingga tidak dapat mengambil langkah mitigasi. Ketiga, tidak adanya akuntabilitas yang jelas; hingga kini publik tidak mengetahui sanksi apa yang dijatuhkan kepada pihak yang lalai. Situasi ini

menunjukkan bahwa hak atas perlindungan data pribadi belum benar-benar dihayati sebagai hak asasi yang wajib dilindungi. Negara belum mampu memberikan jaminan keamanan dan pemulihan yang memadai kepada warganya (Rizky, 2023).

E. MENGGAGAS PARADIGMA KONSTITUSIONAL DALAM ARSITEKTUR PRIVASI INDONESIA

Berdasarkan analisis di atas, perlindungan data pribadi sebagai hak asasi memerlukan transformasi paradigma dari sekadar kepatuhan administratif menuju perlindungan substantif berbasis HAM. Pertama, kemandirian otoritas pengawas harus dijamin secara mutlak. Otoritas ini sebaiknya dibentuk sebagai lembaga negara independen setingkat komisi negara, bukan sebagai unit eselon di bawah kementerian. Independensi ini penting agar tidak terjadi konflik kepentingan, terutama dalam mengawasi pemrosesan data oleh pemerintah.

Kedua, penegakan hukum harus berorientasi pada korban. Mekanisme class action dan bantuan hukum struktural bagi subjek data yang dirugikan harus diperkuat. Ketiga, edukasi literasi digital yang berbasis HAM harus menjadi prioritas nasional. Warga negara yang memahami haknya akan lebih mampu melindungi dirinya dan menuntut akuntabilitas dari pengendali data.

Keempat, harmonisasi regulasi antara UU PDP dengan undang-undang lain yang memungkinkan pengumpulan data oleh negara, seperti UU Intelijen dan UU Terorisme harus dilakukan untuk memastikan bahwa pembatasan terhadap privasi benar-benar proporsional dan sesuai dengan prinsip-prinsip HAM (Greenleaf, 2022).

F. KESIMPULAN

Perlindungan data pribadi bukan sekadar urusan administratif atau komersial, melainkan perwujudan hak asasi manusia yang fundamental di era digital. Kerangka hukum internasional dan konstitusi Indonesia telah menyediakan fondasi yang kokoh bagi pengakuan ini. UU PDP membawa angin segar dengan mengadopsi hak-hak subjek data dan prinsip *informational self-determination*. Namun, pada tataran implementasi, komitmen tersebut belum diikuti dengan langkah konkret yang memadai. Keterlambatan pembentukan otoritas pengawas independen, lemahnya mekanisme pemulihan, serta minimnya edukasi publik menunjukkan bahwa perlindungan data pribadi belum benar-benar dimaknai sebagai hak asasi dalam praktik bernegara. Menjawab rumusan masalah, UU PDP telah menyediakan kerangka normatif yang progresif, tetapi efektivitasnya dalam menjamin perlindungan substantif masih sangat bergantung pada kemauan politik dan penguatan kelembagaan.

Sebagai rekomendasi, pemerintah perlu segera membentuk dan memperkuat otoritas pengawas perlindungan data pribadi yang benar-benar independen, merancang prosedur pengaduan dan pemulihan yang mudah diakses publik, serta memasukkan literasi privasi digital ke dalam kurikulum pendidikan nasional. Hanya dengan begitu hak atas perlindungan data pribadi tidak hanya menjadi mantra di atas kertas, melainkan menjadi realitas yang dirasakan oleh setiap warga negara.

REFERENCE:

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Greenleaf, G. (2022). Global Convergence of Data Privacy Standards and Asia: The Unfinished Agenda. International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Pratiwi, N., & Nugroho, S. (2023). Kemandirian Otoritas Pengawas dalam UU PDP: Studi Komparatif dengan GDPR. Jurnal Hukum dan Teknologi, 5(1), 45–63.

Rizky, P. (2023). Kebocoran Data Pribadi dan Tanggung Jawab Negara dalam Perspektif HAM. Jurnal HAM dan Teknologi, 2(2), 88–105.

Setiawan, R. (2023). Pengawasan Digital dan Batas-Batas Privasi di Indonesia. Jurnal Konstitusi, 20(4), 801–822. https://doi.org/10.31078/jk2045

Siregar, L. (2024). Mekanisme Pemulihan dalam UU PDP: Antara Harapan dan Realitas. Jurnal Yudisial, 17(1), 88–105.

Solove, D. J. (2021). The Digital Person: Technology and Privacy in the Information Age. New York University Press.

Wahyudi, T., & Ayu, I. (2024). Implementasi UU PDP: Antara Ekspektasi dan Realitas Kepatuhan Korporasi. Jurnal Privasi dan Data, 5(1), 15–30. https://doi.org/10.5678/jpd.v5i1.9901

Wibisono, A. (2023). Intersepsi Data dan Perlindungan Privasi dalam Persimpangan UU ITE dan UU PDP. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara

Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

'ADALAH
Buletin Hukum & Keadilan

Hak Privasi vs Kepentingan Negara dalam Pengawasan Siber: Menemukan Keseimbangan Konstitusional di Era *Digital Panopticon*

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.51169

Abstract:
The tension between citizens' privacy rights and state cyber surveillance has become a major constitutional issue in the digital era. This article analyzes the constitutional limits of state surveillance and explores a balance between security interests and democracy. Using normative legal research with conceptual, statutory, and comparative approaches, the study finds that Indonesia's cyber surveillance framework lacks proportionality, judicial oversight, and accountability. Regulations under the ITE Law and Intelligence Law grant broad discretion without adequate due process safeguards. The article recommends stronger judicial supervision, limiting executive discretion, and establishing a special supervisory court chamber.

Keywords: *Privacy Rights, Cyber Surveillance, State Interests, Proportionality, Due Process.*

A. PENDAHULUAN

Privasi telah lama diakui sebagai salah satu pilar hak asasi manusia yang fundamental. Ia adalah perisai yang melindungi martabat dan otonomi individu dari intervensi yang tidak sah. Namun, hak ini tidak pernah bersifat absolut. Negara, dalam menjalankan fungsinya, memiliki kewajiban untuk menjaga keamanan nasional, ketertiban umum, dan penegakan hukum. Untuk itu, negara diberikan kewenangan untuk melakukan pengawasan, yang dalam konteks digital dikenal sebagai pengawasan siber (*cyber surveillance*). Ketegangan antara hak privasi dan kepentingan negara dalam pengawasan siber membentuk dilema klasik yang terus bergulir: sejauh mana negara boleh mengintip warga negaranya demi alasan keamanan tanpa menjelma menjadi negara pengawas (*surveillance state*) yang totaliter?

Kemajuan teknologi telah memperlebar kemampuan negara untuk melakukan pengawasan. Alat-alat seperti *Deep Packet Inspection* (DPI), pengenalan wajah (*facial recognition*), dan perangkat lunak mata-mata seperti Pegasus memungkinkan negara mengumpulkan data dalam jumlah masif, bahkan tanpa sepengetahuan warga yang menjadi target. Fenomena ini digambarkan oleh para pemikir hukum sebagai *Digital Panopticon*, sebuah penjara virtual di mana individu selalu merasa diawasi, meskipun mereka tidak dapat melihat atau

mengetahui siapa yang mengawasi (Zuboff, 2019). Dalam kondisi seperti ini, hak privasi tidak hanya terancam oleh korporasi, tetapi juga oleh negara yang seharusnya menjadi pelindungnya.

Di Indonesia, kewenangan pengawasan siber tersebar di berbagai instrumen hukum. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Intelijen Negara, Undang-Undang Terorisme, serta Rancangan Undang-Undang Keamanan dan Ketahanan Siber semuanya memberikan ruang bagi pemerintah untuk mengakses data pribadi. Sayangnya, kerangka hukum ini tidak disertai dengan mekanisme pengawasan yang ketat dan akuntabel. Ketiadaan batas yang jelas antara kewenangan pengawasan yang sah dan pelanggaran privasi menjadi sumber ketidakpastian hukum dan ancaman bagi hak konstitusional warga negara (Asshiddiqie, 2021). Rumusan masalah artikel ini adalah: Pertama, bagaimana pengaturan dan praktik pengawasan siber di Indonesia dalam kaitannya dengan hak privasi? Kedua, bagaimana kerangka keseimbangan ideal antara hak privasi dan kepentingan negara dapat dirumuskan dalam sistem hukum nasional? Tujuannya adalah untuk mengkritisi kerangka normatif yang ada dan menawarkan model keseimbangan yang demokratis dan konstitusional.

B. PROPORSIONALITAS DAN DOKTRIN *DUE PROCESS* DALAM PENGAWASAN

Untuk menilai legitimasi pengawasan siber, doktrin hukum HAM dan tata negara menyediakan dua instrumen analitis utama: prinsip proporsionalitas dan doktrin *due process of law.* Prinsip proporsionalitas menuntut agar setiap pembatasan terhadap hak asasi oleh negara memenuhi empat syarat kumulatif: (1) adanya tujuan yang sah (*legitimate aim*), (2) kesesuaian atau kelayakan sarana (*suitability*), (3) keharusan atau tidak adanya alternatif yang lebih ringan (*necessity*), dan (4) keseimbangan antara manfaat dan kerugian (*proportionality stricto sensu*) (Barak, 2012). Pengawasan siber yang dilakukan tanpa batas waktu, tanpa target yang spesifik, dan tanpa dasar kecurigaan yang rasional jelas akan gagal dalam uji proporsionalitas ini.

Sementara itu, doktrin due process mensyaratkan bahwa perampasan hak warga negara, termasuk privasi, harus melalui prosedur hukum yang adil dan transparan. Dalam konteks pengawasan siber, ini berarti bahwa tindakan seperti penyadapan, penggeledahan data, atau pembajakan enkripsi (*encryption backdoor*) tidak boleh dilakukan semata-mata atas perintah eksekutif, melainkan harus melalui otorisasi yudisial yang independen. Hakim harus bertindak sebagai penjaga gerbang (*gatekeeper*) yang memastikan bahwa

pengawasan benar-benar diperlukan dan sesuai dengan koridor hukum (Solove, 2021).

Di tingkat internasional, Manfred Nowak sebagai Pelapor Khusus PBB tentang Penyiksaan, dan yurisprudensi Mahkamah Eropa untuk Hak Asasi Manusia (ECtHR) dalam kasus Klass v. Germany (1978) dan Zakharov v. Russia (2015), telah menetapkan standar bahwa legislasi pengawasan harus memiliki kejelasan tentang: (1) lingkup pelanggaran yang dapat memicu pengawasan, (2) subjek yang dapat diawasi, (3) batas durasi pengawasan, (4) prosedur otorisasi, dan (5) mekanisme pengawasan serta pemulihan. Kerangka ini akan digunakan untuk menguji pengaturan pengawasan siber di Indonesia.

C. PENGAWASAN SIBER DI INDONESIA DAN DEFISIT KONSTITUSIONAL

1. Fragmentasi Regulasi dan Ketiadaan Payung Hukum yang Koheren

Pengaturan pengawasan siber di Indonesia tidak ditampung dalam satu undang-undang khusus yang terintegrasi. Sebaliknya, kewenangan ini terfragmentasi ke dalam berbagai regulasi sektoral. UU ITE memberikan kewenangan kepada penyidik untuk mengakses, meminta, dan menyita data elektronik. UU Intelijen Negara (UU 17/2011) mengizinkan penyadapan untuk

kepentingan intelijen, tetapi tidak secara rinci mengatur bagaimana, kapan, dan kepada siapa pengawasan dapat dilakukan. Lebih problematik lagi, UU Terorisme (UU 5/2018) memberikan kewenangan yang sangat luas kepada aparat untuk melakukan penyadapan dan pengumpulan data dalam rangka pencegahan terorisme, dengan pengawasan yang minimalis.

Keadaan ini menciptakan legal vacuum sekaligus legal chaos. Vakum karena tidak ada aturan umum yang menjadi pedoman bagi semua jenis pengawasan siber. Chaos karena masing-masing lembaga Kepolisian, Kejaksaan, BIN, BSSN, Kominfo memiliki aturan internal sendiri yang seringkali tidak sinkron dan bertentangan satu sama lain (Santoso, 2023). Akibatnya, sulit bagi warga negara untuk mengetahui secara pasti kapan dan mengapa data mereka diakses oleh negara.

2. Lemahnya Pengawasan Yudisial dan Dominasi Eksekutif

Masalah paling serius dalam arsitektur pengawasan siber di Indonesia adalah absennya pengawasan yudisial yang efektif. Sebagian besar kewenangan pengawasan hanya memerlukan izin dari internal lembaga eksekutif atau, paling tinggi, dari menteri. Penyadapan oleh BIN, misalnya, memerlukan izin dari Kepala BIN, tanpa harus melalui pengadilan.

Praktik ini sangat kontras dengan standar internasional yang mensyaratkan adanya judicial warrant (surat perintah dari hakim) sebelum pengawasan dilakukan.

Mahkamah Konstitusi dalam Putusan Nomor 5/PUU-VIII/2010 pernah menegaskan bahwa penyadapan harus diatur dengan undang-undang yang jelas dan melibatkan pengadilan. Namun, putusan ini tidak kunjung ditindaklanjuti dengan legislasi yang komprehensif. Dominasi eksekutif dalam pengawasan siber menciptakan situasi di mana negara dapat mengawasi tanpa check and balance yang berarti. Ini adalah defisit konstitusional yang serius karena melanggar prinsip due process dan membahayakan hak privasi (Setiawan, 2023). Bahkan, RUU Keamanan dan Ketahanan Siber yang sempat dibahas justru memperkuat otoritas eksekutif dalam hal ini BSSN untuk melakukan tindakan pengamanan siber yang bisa mencakup pengawasan konten tanpa batasan yang memadai.

3. Prinsip Proporsionalitas yang Terabaikan

Pengujian terhadap pengawasan siber di Indonesia dari perspektif proporsionalitas memperlihatkan gambaran yang suram. Pertama, pada asas tujuan yang sah, memang keamanan nasional dan pemberantasan kejahatan adalah tujuan yang sah.

Namun, kedua, pada asas kelayakan, banyak instrumen pengawasan yang terlalu luas dan tidak spesifik, sehingga tidak betul-betul cocok untuk mencapai tujuan. Pengawasan massal terhadap metadata komunikasi, misalnya, tidak selalu relevan untuk menangkal terorisme.

Ketiga, pada asas keharusan, pemerintah Indonesia tidak pernah membuktikan bahwa pengawasan massal atau penembusan enkripsi adalah cara yang benar-benar esensial dan tidak ada alternatif yang lebih ringan. Padahal, banyak studi menunjukkan bahwa investigasi berbasis target spesifik jauh lebih efektif daripada pengawasan massal. Keempat, pada asas keseimbangan, pengawasan yang dilakukan secara luas tanpa sepengetahuan subjek jelas menimbulkan kerugian besar bagi privasi, padahal hasilnya seringkali tidak sebanding (Deibert, 2019). Singkatnya, praktik pengawasan siber di Indonesia gagal memenuhi uji proporsionalitas secara holistik.

D. KONTROVERSI AKSES DATA DAN PENYADAPAN OLEH APARAT

Salah satu isu yang sempat mengemuka adalah dugaan penggunaan alat sadap canggih oleh lembaga penegak hukum Indonesia untuk mengakses komunikasi tersangka dan aktivis. Meskipun sulit diverifikasi karena

sifatnya yang tertutup, berbagai laporan masyarakat sipil mengindikasikan adanya praktik penyadapan di luar koridor hukum. Pada tahun 2022, terungkap bahwa aplikasi pesan instan yang diunduh melalui tautan tidak resmi digunakan sebagai pintu masuk untuk menyadap komunikasi personal. Kasus ini memperlihatkan betapa rentannya warga negara terhadap pengawasan yang tidak sah.

Lebih memprihatinkan lagi, tidak ada mekanisme yang memungkinkan korban penyadapan ilegal untuk mengetahui, apalagi menggugat. Mereka tidak memiliki akses terhadap informasi apakah data mereka telah diakses oleh aparat. Ketiadaan *notification requirement* (kewajiban memberitahu) pasca-pengawasan adalah bentuk pengingkaran terhadap hak privasi. Subjek data tidak dapat menuntut akuntabilitas karena tidak pernah tahu bahwa haknya telah dilanggar. Ini sangat kontradiktif dengan asas negara hukum yang menuntut adanya akses terhadap keadilan dan pemulihan (Prasetyo, 2024).

E. MERUMUSKAN KESEIMBANGAN: PRIVASI YANG AMAN, NEGARA YANG BERTANGGUNG JAWAB

Keseimbangan antara privasi dan pengawasan bukanlah rumus matematis yang kaku, melainkan

merupakan proses konstitusional yang dinamis. Ada beberapa prasyarat untuk mencapai keseimbangan tersebut. Pertama, Indonesia harus segera memiliki Undang-Undang Pengawasan (*Surveillance Law*) yang terpadu. Undang-undang ini harus mengkodifikasi semua jenis pengawasan siber, mengatur tentang dasar hukum, batas durasi, otorisasi, pengawasan, dan pemulihan secara terpadu. Semua lembaga negara yang memiliki kewenangan pengawasan harus tunduk pada undang-undang yang sama, sehingga tidak ada lagi fragmentasi dan kompetisi antarlembaga yang merugikan privasi.

Kedua, pemberlakuan judicial warrant secara mutlak. Setiap tindakan pengawasan yang bersifat intrusif, seperti penyadapan, penggeledahan data, atau penembusan enkripsi, harus mendapatkan izin dari pengadilan. Pengadilan harus membentuk panel khusus atau weeskamer yang bertugas menilai permohonan izin pengawasan secara rahasia dan independen. Model ini diterapkan di Belanda, di mana hakim komisaris menangani permintaan penyadapan dengan standar yang ketat. Ketiga, transparansi yang bertanggung jawab. Warga negara yang menjadi target pengawasan berhak untuk diberitahu setelah pengawasan berakhir dan tidak lagi membahayakan penyidikan. Jika pengawasan tidak menghasilkan bukti, subjek harus

memiliki hak untuk menggugat dan meminta pemusnahan data (Greenleaf, 2022).

Terakhir, kepentingan negara tidak boleh dikonstruksi secara monolitik. Negara dibentuk untuk melindungi warga, termasuk privasinya. Oleh karena itu, kepentingan negara yang sesungguhnya adalah melindungi privasi secara maksimal. Pengawasan hanya boleh dilakukan sebagai pengecualian yang terbatas dan terukur, bukan sebagai aturan umum.

F. KESIMPULAN

Ketegangan antara hak privasi dan kepentingan negara dalam pengawasan siber di Indonesia masih belum menemukan titik keseimbangan yang sehat. Kerangka hukum yang ada masih sangat fragmentaris, minim pengawasan yudisial, dan tidak memenuhi standar proporsionalitas. Akibatnya, hak privasi warga negara berada dalam posisi yang sangat rentan terhadap diskresi eksekutif yang tidak terbatasi. Menjawab rumusan masalah, pengaturan pengawasan siber di Indonesia saat ini lebih condong membela kepentingan negara secara sempit dengan mengorbankan privasi, sementara keseimbangan ideal hanya dapat diwujudkan melalui reformasi legislasi yang meletakkan prinsip judicial warrant, proporsionalitas, dan transparansi sebagai pilar utama.

Sebagai rekomendasi, pemerintah bersama DPR harus segera merumuskan RUU Pengawasan yang komprehensif, yang menundukkan semua kewenangan pengawasan di bawah pengawasan hakim. Selain itu, Mahkamah Agung perlu mempersiapkan pembentukan kamar pengawas khusus serta pedoman teknis bagi hakim dalam memutus izin penyadapan. Hanya dengan kerangka hukum yang akuntabel, Indonesia dapat menjadi negara yang aman tanpa berubah menjadi negara yang mengawasi setiap langkah warganya.

REFERENCE:

Asshiddiqie, J. (2021). Hukum dan Teknologi: Pergulatan Konstitusi dalam Masyarakat Digital. Rajawali Pers.

Barak, A. (2012). Proportionality: Constitutional Rights and their Limitations. Cambridge University Press.

Deibert, R. J. (2019). The Road to Digital Unfreedom: Three Painful Truths about Social Media. Journal of Democracy, 30(1), 25–39. https://doi.org/10.1353/jod.2019.0002

Greenleaf, G. (2022). Global Convergence of Data Privacy Standards and Asia: The Unfinished Agenda.

International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Prasetyo, B. (2024). Pengawasan Tanpa Pemberitahuan: Tantangan Akuntabilitas dalam Hukum Intelijen Indonesia. Jurnal Hukum dan Keamanan, 16(1), 45–65.

Santoso, L. (2023). Fragmentasi Regulasi Penyadapan dan Implikasinya terhadap Hak Privasi. Jurnal Yudisial, 16(2), 201–220.

Setiawan, R. (2023). Pengawasan Digital dan Batas-Batas Privasi di Indonesia. Jurnal Konstitusi, 20(4), 801–822. https://doi.org/10.31078/jk2045

Solove, D. J. (2021). The Digital Person: Technology and Privacy in the Information Age. New York University Press.

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

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara (Lembaran Negara Tahun 2011 Nomor 105, Tambahan Lembaran Negara Nomor 5249).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

'ADALAH
Buletin Hukum & Keadilan

Etika dan Hukum dalam Penggunaan Data Pribadi: Menjembatani Kesenjangan antara Kepatuhan Formal dan Tanggung Jawab Moral di Era *Data-Driven Society*

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.51170

Abstract:
This article analyzes the ethical and legal dimensions of personal data use in the digital economy, focusing on Indonesia's PDP Law (Law No. 27/2022). It assesses the gap between legal compliance and ethical responsibility in data governance. Using normative legal research with conceptual and philosophical approaches, the study finds misalignment between legal standards and ethical expectations. Key principles such as fairness, algorithmic transparency, and user autonomy are not fully reflected in regulation. Digital lending cases show formal compliance may conflict with ethical expectations requiring stronger ethical integration in governance systems.
Keywords: *Ethical Data, Data Protection Law, Formal Compliance, Fairness, Algorithmic Transparency*

A. PENDAHULUAN

Revolusi data besar (*big data*) telah menempatkan data pribadi sebagai sumber daya strategis yang mendorong inovasi, efisiensi, dan pertumbuhan ekonomi. Namun, euforia ini berjalan seiring dengan kekhawatiran akan erosi privasi, diskriminasi algoritmis, dan eksploitasi individu oleh korporasi digital. Dalam lanskap *data-driven society*, setiap individu secara konstan menghasilkan jejak digital yang dikumpulkan, dianalisis, dan dimonetisasi, seringkali tanpa pemahaman atau persetujuan yang sungguh-sungguh. Realitas ini memunculkan pertanyaan fundamental tentang batas-batas etis dan hukum dalam penggunaan data pribadi.

Hukum perlindungan data, seperti GDPR di Eropa dan UU PDP di Indonesia, hadir untuk memberikan kerangka normatif yang melindungi hak-hak subjek data. Namun, hukum memiliki keterbatasan inheren; ia cenderung menetapkan standar minimum yang bersifat rules-based dan seringkali tertatih-tatih di belakang perkembangan teknologi. Etika, di sisi lain, menawarkan spektrum pedoman yang lebih dinamis dan aspiratif, menjangkau wilayah abu-abu yang tidak tersentuh oleh pasal-pasal undang-undang (Floridi, 2018). Ketika sebuah perusahaan mematuhi UU PDP dengan menyediakan halaman kebijakan privasi yang panjang dan rumit, ia mungkin telah memenuhi

kewajiban hukum, tetapi secara etika belum tentu menghormati otonomi pengguna.

Di Indonesia, problematika ini sangat relevan mengingat penetrasi digital yang masif dan masih rendahnya literasi data. UU PDP telah memperkenalkan prinsip-prinsip dasar seperti transparansi, pembatasan tujuan, dan akuntabilitas. Akan tetapi, pertanyaan yang mengemuka adalah apakah prinsip-prinsip tersebut dijalankan secara etis atau hanya sekadar sebagai daftar centang administratif. Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana hubungan antara etika dan hukum dalam kerangka penggunaan data pribadi? Kedua, sejauh mana UU PDP mengakomodasi prinsip-prinsip etika fundamental, dan di mana letak kesenjangannya? Tujuan penulisan ini adalah untuk mengkritisi rezim perlindungan data pribadi dari perspektif etika dan mengusulkan kerangka integrasi yang lebih bermakna.

B. ETIKA INFORMASI DAN PRINSIP *FAIR INFORMATION PRACTICES*

Diskursus mengenai etika data pribadi tidak dapat dilepaskan dari perkembangan etika informasi sebagai cabang filsafat. Luciano Floridi, salah satu pemikir terkemuka di bidang ini, mengajukan kerangka Information Ethics yang memandang data sebagai

ekstensi dari entitas manusia. Dalam pandangan ini, penggunaan data secara tidak etis bukan sekadar pelanggaran hak, melainkan tindakan yang merusak "infosfer" ekosistem informasi yang menopang identitas dan martabat manusia. Etika informasi menekankan empat prinsip dasar: (1) *entropy* (tindakan yang merusak infosfer tidak dapat dibenarkan), (2) *privacy* (menghormati hak individu untuk mengontrol informasinya), (3) *accuracy* (keharusan menjaga kebenaran data), dan (4) *accessibility* (memastikan akses yang adil terhadap data dan pengetahuan) (Floridi, 2018).

Secara paralel, tradisi *Fair Information Practices* (FIPs) yang berkembang sejak era 1970-an telah merumuskan prinsip-prinsip operasional yang menjembatani etika dan hukum. Prinsip-prinsip tersebut meliputi: keterbukaan (*openness*), pembatasan tujuan (*purpose specification*), keterbatasan pengumpulan (collection limitation), kualitas data (*data quality*), akuntabilitas (*accountability*), dan partisipasi individu (*individual participation*). FIPs menjadi tulang punggung bagi banyak undang-undang perlindungan data modern, termasuk GDPR dan UU PDP. Namun, penerjemahan FIPs ke dalam produk hukum acapkali kehilangan roh etisnya. Misalnya, prinsip keterbukaan dipersempit menjadi kewajiban menyediakan *privacy notice* yang

legalistik, bukan komunikasi yang mudah dipahami pengguna (Nissenbaum, 2010).

Di sinilah konsep *contextual integrity* yang digagas oleh Helen Nissenbaum menjadi relevan. Nissenbaum berargumen bahwa perlindungan data yang etis tidak cukup hanya mengandalkan *notice and consent* (pemberitahuan dan persetujuan), melainkan harus memastikan bahwa aliran informasi sesuai dengan konteks sosial di mana informasi itu dibagikan. Sebuah praktik berbagi data mungkin legal karena ada izin formal, tetapi secara etis tetap melanggar jika menabrak norma-norma kontekstual yang dipegang oleh masyarakat. Kerangka teoretis ini menunjukkan bahwa hukum yang hanya mengandalkan *checkbox consent* gagal melindungi subjek data karena mereduksi privasi menjadi urusan kontrak bilateral, padahal ia adalah kepentingan kolektif.

C. KESENJANGAN ANTARA ETIKA DAN HUKUM DALAM UU PDP

1. *Notice and Consent*: Izin Formal tanpa Pemahaman Substansial

Pilar utama UU PDP, sebagaimana halnya GDPR, adalah prinsip persetujuan (*consent*). Pasal 6 UU PDP mensyaratkan adanya persetujuan eksplisit dari subjek data untuk pemrosesan data pribadi. Secara hukum,

pengendali data yang telah memperoleh persetujuan biasanya melalui kotak centang "Saya setuju" pada aplikasi dianggap telah memenuhi kewajiban. Namun, dari perspektif etika, persetujuan tersebut seringkali bersifat fiktif. Panjangnya kebijakan privasi yang penuh jargon hukum, penggunaan dark patterns dalam desain antarmuka untuk mengarahkan pengguna agar menekan tombol setuju, dan ketiadaan pilihan yang benar-benar bebas membuat consent kehilangan esensinya sebagai wujud otonomi (Wahyudi & Ayu, 2024).

Secara etis, persetujuan haruslah *informed, freely given, specific,* dan *unambiguous*. Kenyataannya, banyak platform memberikan pilihan biner: setuju dengan semua pemrosesan atau tidak bisa menggunakan layanan sama sekali (*take-it-or-leave-it*). Model ini tidak memenuhi syarat "bebas" karena ada ketimpangan kuasa antara subjek data dan pengendali data. Hukum UU PDP tidak secara tegas melarang praktik *bundled consent* semacam ini. Di sinilah terjadi defisit etis: hukum merasa cukup dengan formalitas, sementara etika menuntut substansi. Akibatnya, pengguna merasa "dipaksa" untuk setuju dan kehilangan kendali efektif atas data mereka.

2. Keadilan Algoritmis dan Masalah Fairness

Etika penggunaan data pribadi tidak berhenti pada pengumpulan, melainkan berlanjut pada

pengolahan dan pengambilan keputusan otomatis. *Profiling* dan *algorithmic decision-making* yang memanfaatkan data pribadi berpotensi menimbulkan diskriminasi, bias, dan ketidakadilan. UU PDP telah menyinggung hak subjek data untuk tidak dikenai keputusan otomatis yang berdampak hukum signifikan, namun pengaturannya masih sangat elementer dan belum menyentuh aspek keadilan substantif (*fairness*).

Fairness dalam konteks etika data meliputi keadilan distributif (siapa yang diuntungkan dan dirugikan), keadilan prosedural (apakah proses pemrosesan adil dan transparan), dan keadilan interaksional (apakah subjek data diperlakukan dengan hormat). Hukum positif biasanya hanya mampu menjangkau keadilan prosedural, itu pun secara minimal. Misalnya, skor kredit yang ditentukan oleh algoritma berbasis data pribadi mungkin akurat secara statistik dan telah diberitahukan prosedurnya, tetapi tetap dapat melanggengkan ketimpangan struktural terhadap kelompok minoritas. Algoritma pinjaman daring yang menetapkan bunga lebih tinggi untuk pengguna di wilayah tertentu berdasarkan pola historis adalah contoh nyata diskriminasi yang dapat lolos dari jerat hukum karena tidak ada pasal spesifik yang melarangnya (Rizky, 2023). Tanpa kerangka etis yang kuat, ketidakadilan ini akan terus diproduksi oleh sistem yang dirancang hanya untuk efisiensi dan profit.

3. Transparansi Algoritmis: Antara Rahasia Dagang dan Hak Tahu

Transparansi adalah salah satu titik pertemuan paling tegang antara etika dan hukum. Pasal 21 UU PDP menjamin hak subjek data untuk memperoleh informasi tentang logika pemrosesan data. Namun, frasa ini ditafsirkan secara sempit. Pengendali data biasanya hanya menjelaskan secara generik bahwa data digunakan untuk "meningkatkan layanan" atau "analisis internal", sementara algoritma yang sesungguhnya dirahasiakan dengan alasan rahasia dagang. Di sinilah hukum menghadapi batasnya: ia tidak dapat memaksa transparansi yang merugikan kepentingan bisnis tanpa regulasi yang lebih tegas.

Etika, sebaliknya, menuntut transparansi yang bermakna (*meaningful transparency*). Masyarakat berhak mengetahui kriteria apa yang digunakan untuk mengambil keputusan yang memengaruhi hidup mereka, seperti kelayakan kredit, asuransi, atau penerimaan kerja. Transparansi tidak harus berarti membuka kode sumber, tetapi cukup memberikan penjelasan yang dapat dipahami (*explainability*). UU PDP belum mengadopsi konsep *explainable* AI secara memadai, sehingga kesenjangan antara praktik industri dan hak asasi warga negara tetap menganga. Etika mengisi ruang ini dengan mendorong perusahaan untuk

secara sukarela melakukan *algorithmic audit* dan *impact assessment* yang dipublikasikan secara berkala (Wibisono, 2023).

D. ETIKA YANG DIKORBANKAN DEMI LEGALITAS DALAM INDUSTRI PINJAMAN DARING

Industri pinjaman daring (*peer-to-peer lending*) di Indonesia menjadi laboratorium sempurna untuk mengamati bagaimana etika dikorbankan di atas altar legalitas formal. Banyak platform pinjaman daring yang telah terdaftar dan berizin di Otoritas Jasa Keuangan (OJK), yang berarti secara hukum mereka telah mematuhi segala ketentuan administrasi. Namun, praktik di lapangan menunjukkan pelanggaran etis yang serius: penagihan dengan teror kepada kontak pribadi debitur, akses tanpa izin ke buku telepon, dan pengolahan data untuk memalukan debitur di hadapan kerabatnya.

Secara hukum, *platform* tersebut mungkin berkelit dengan menunjukkan bahwa mereka memiliki klausul persetujuan akses kontak di dalam aplikasi. Namun, secara etis, apakah subjek data benar-benar memahami bahwa memberikan akses kontak dapat digunakan untuk menagih secara memalukan? Ini adalah pelanggaran terhadap prinsip *contextual integrity*: informasi kontak

dipinjamkan dalam konteks verifikasi identitas, bukan untuk penagihan agresif. UU PDP sebenarnya melarang pemrosesan data yang melampaui tujuan awal, tetapi dalam praktiknya, otoritas belum mampu mengawasi dengan efektif. Kasus ini menunjukkan bahwa meskipun suatu entitas telah "patuh hukum", ia tetap bisa menjadi predator data karena ketiadaan kompas etis (Fitriani, 2024).

Kasus lain adalah fenomena data broker ilegal yang menjual data pribadi penduduk tanpa izin. Dari segi hukum, ini jelas melanggar UU PDP dan dapat dipidana. Tetapi dari segi etika, pertanyaan yang lebih dalam adalah: mengapa para korban baru menyadari datanya diperjualbelikan setelah bertahun-tahun? Ini menunjukkan kegagalan mekanisme kepatuhan pasif. Diperlukan pergeseran dari sekadar "jangan melanggar hukum" menjadi "bertindaklah secara bertanggung jawab", yang hanya dapat digerakkan oleh etika.

E. MENGINTEGRASIKAN ETIKA DAN HUKUM: MENUJU TATA KELOLA DATA YANG HUMANIS

Menyadari kelemahan hukum yang lagging dan serba minimalis, integrasi etika ke dalam tata kelola data merupakan strategi yang niscaya. Integrasi ini harus bersifat by design, bukan sebagai tambahan kosmetik. Pertama, diperlukan pengembangan kode etik sektoral

yang lebih operasional. OJK, Bank Indonesia, dan Kominfo dapat mendorong asosiasi industri untuk merumuskan standar etika yang lebih tinggi daripada standar hukum. Standar ini dapat mencakup larangan dark patterns, kewajiban plain language dalam kebijakan privasi, serta batasan tegas penggunaan data untuk *profiling*.

Kedua, audit etika (*ethical audit*) harus menjadi bagian dari tata kelola korporasi digital. Audit ini tidak hanya mengecek kepatuhan formal, tetapi juga menilai dampak pemrosesan data terhadap hak asasi manusia, keadilan sosial, dan kerentanan kelompok marjinal. Hasil audit harus dipublikasikan dan dapat diakses publik untuk mendorong akuntabilitas sosial (Santoso & Pratiwi, 2023). Ketiga, pendidikan etika digital harus menjadi komponen wajib dalam kurikulum pendidikan tinggi, khususnya fakultas hukum, ilmu komputer, dan bisnis. Generasi profesional digital masa depan harus dibekali dengan kapasitas untuk mempertimbangkan implikasi etis dari setiap desain teknologi, bukan hanya aspek komersial dan legalnya.

Terakhir, perlu ada pengakuan bahwa etika dan hukum bukanlah dua kutub yang terpisah, melainkan sebuah kontinum. Hukum yang baik adalah hukum yang dijiwai oleh prinsip-prinsip etis, sementara etika yang hanya diperbincangkan tanpa sanksi akan kehilangan

efektivitas. Pendekatan *co-regulation*, di mana negara menetapkan standar minimum sementara industri mengembangkan standar etika yang lebih tinggi dengan pengawasan publik, adalah model yang menjanjikan untuk Indonesia.

F. KESIMPULAN

Hubungan antara etika dan hukum dalam penggunaan data pribadi bersifat komplementer namun seringkali tegang. Hukum menyediakan batas bawah yang mengikat dan sanksi tegas, sementara etika menawarkan orientasi moral yang lebih aspiratif dan adaptif terhadap situasi yang belum terjamah regulasi. Analisis di atas menunjukkan bahwa UU PDP telah menyediakan kerangka hukum yang penting, tetapi masih menyisakan kesenjangan etis yang signifikan. Persetujuan yang bersifat formal tanpa pemahaman substantif, ketidakadilan algoritmis yang tidak tersentuh hukum, serta transparansi yang semu adalah bukti bahwa kepatuhan formal belum tentu mencerminkan tanggung jawab moral.

Menjawab rumusan masalah, UU PDP telah mengakomodasi beberapa prinsip etika fundamental seperti transparansi dan akuntabilitas, tetapi belum cukup mendalam untuk menjawab kompleksitas persoalan seperti fairness dan contextual integrity.

Kesenjangan ini hanya dapat dijembatani jika pengendali data tidak hanya bertanya "apakah ini legal?" tetapi juga "apakah ini etis?". Rekomendasi yang dapat diajukan adalah: pertama, mendorong penyusunan kode etik sektoral oleh asosiasi industri; kedua, mewajibkan audit etika bagi pengendali data berskala besar; dan ketiga, memperkuat literasi etika digital melalui pendidikan formal dan pelatihan profesional. Hanya dengan sinergi antara kekuatan hukum dan kekuatan etika, penggunaan data pribadi di Indonesia dapat melindungi martabat manusia seutuhnya.

REFERENCE:

Fitriani, R. (2024). Praktik Penagihan Pinjaman Daring dan Pelanggaran Etika Privasi. Jurnal Hukum dan Etika Digital, 2(1), 40–58.

Floridi, L. (2018). Soft Ethics, the Governance of the Digital and the General Data Protection Regulation. Philosophical Transactions of the Royal Society A, 376(2133). https://doi.org/10.1098/rsta.2018.0081

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Rizky, P. (2023). Algoritma dan Diskriminasi dalam Layanan Keuangan Digital. Jurnal HAM dan Teknologi, 2(1), 55–70.

Santoso, B., & Pratiwi, D. (2023). Audit Etika sebagai Instrumen Tata Kelola Data Pribadi. Jurnal Hukum Ekonomi dan Bisnis, 11(4), 210–228.

Wahyudi, T., & Ayu, I. (2024). Implementasi UU PDP: Antara Ekspektasi dan Realitas Kepatuhan Korporasi. Jurnal Privasi dan Data, 5(1), 15–30. https://doi.org/10.5678/jpd.v5i1.9901

Wibisono, A. (2023). Menjelaskan yang Tak Terjelaskan: Explainable AI dan Hak Atas Penjelasan dalam UU PDP. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

Kebocoran Data dan Tanggung Jawab Hukum Korporasi Digital: Menggagas Rezim Akuntabilitas Mutlak dalam Ekosistem Ekonomi Digital Indonesia

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.51171

Abstract:
This article examines corporate legal liability for personal data breaches in Indonesia's digital business sector under Law No. 27/2022 on Personal Data Protection (PDP Law). Using normative legal research with statutory, conceptual, and comparative approaches, the study finds weaknesses in proof mechanisms, sanctions, and collective compensation systems. Current regulations rely heavily on fault-based liability, burdening victims despite the massive and asymmetrical nature of data breaches. Cases in digital finance and e-commerce reveal weak corporate accountability and limited victim recovery. The article recommends adopting strict liability, stronger supervisory authority, and accessible class action mechanisms.

Keywords: *Data Breach, Corporate Liability, Strict Liability, PDP Law, Collective Compensation.*

A. PENDAHULUAN

Transformasi digital yang melahirkan ekonomi berbasis data telah menempatkan korporasi digital sebagai aktor sentral dalam ekosistem informasi. Perusahaan teknologi finansial, *e-commerce*, layanan kesehatan digital, hingga media sosial mengumpulkan, menyimpan, dan mengolah data pribadi dalam volume yang belum pernah terjadi sebelumnya. Namun, akumulasi data ini tidak disertai dengan investasi keamanan yang memadai. Akibatnya, kebocoran data menjadi peristiwa yang semakin lazim terjadi, mengekspos jutaan individu pada risiko pencurian identitas, penipuan, dan kerugian finansial.

Kebocoran data bukan sekadar insiden teknis. Ia adalah pelanggaran serius terhadap hak asasi manusia, khususnya hak atas privasi dan perlindungan data pribadi yang dijamin oleh konstitusi. Ketika data warga negara bocor, yang terjadi bukan hanya kerugian material, melainkan juga hilangnya rasa aman dan hancurnya kepercayaan publik terhadap ekosistem digital. Dalam konteks inilah pertanyaan tentang tanggung jawab hukum korporasi digital menjadi sangat krusial: siapa yang harus bertanggung jawab ketika data bocor? Apa dasar hukum pertanggungjawabannya? Dan bagaimana korban mendapatkan pemulihan yang adil?

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) hadir untuk mengisi kekosongan regulasi di bidang ini. UU PDP menetapkan kewajiban bagi pengendali dan prosesor data untuk menjaga keamanan data, melaporkan insiden kebocoran dalam waktu tertentu, serta bertanggung jawab atas kerugian yang diderita subjek data. Namun, implementasi ketentuan ini masih dipertanyakan efektivitasnya. Beberapa insiden kebocoran data besar yang terjadi setelah UU PDP disahkan menunjukkan bahwa penegakan hukum masih lemah, korban masih sulit memperoleh ganti rugi, dan korporasi cenderung lolos dengan sanksi administratif ringan (Pratiwi & Nugroho, 2023). Rumusan masalah artikel ini adalah: Pertama, bagaimana konstruksi tanggung jawab hukum korporasi digital dalam UU PDP dan regulasi terkait? Kedua, bagaimana rezim tanggung jawab yang ideal untuk memberikan perlindungan efektif dan pemulihan bagi subjek data yang menjadi korban kebocoran? Tujuannya untuk mengevaluasi kerangka normatif yang ada dan mengajukan model pertanggungjawaban yang lebih responsif.

B. DOKTRIN TANGGUNG JAWAB DALAM HUKUM PERLINDUNGAN DATA

Tanggung jawab hukum dalam konteks kebocoran data dapat ditinjau dari dua doktrin utama dalam

hukum perdata dan hukum administrasi: *fault-based liability* (tanggung jawab berdasarkan kesalahan) dan *strict liability* (tanggung jawab mutlak). *Fault-based liability* mensyaratkan adanya unsur kesalahan pada pihak yang digugat, yang meliputi kesengajaan atau kelalaian. Korban harus membuktikan bahwa pengendali data lalai dalam menjaga keamanan data, bahwa ada hubungan kausal antara kelalaian tersebut dengan kebocoran, dan bahwa kerugian yang dialami adalah akibat langsung dari kebocoran itu (Shidarta, 2022). Dalam konteks kebocoran data, pembuktian ini sangat sulit dilakukan oleh individu karena informasi tentang sistem keamanan, praktik pemrosesan, dan kronologi insiden sepenuhnya berada di tangan korporasi.

Sebaliknya, *strict liability* membebankan tanggung jawab kepada pelaku usaha semata-mata karena telah terjadi kerugian akibat aktivitasnya, tanpa perlu membuktikan adanya kesalahan. Doktrin ini lazim diterapkan pada kegiatan yang bersifat *ultrahazardous* atau berisiko tinggi. Pengelolaan data pribadi dalam skala besar, secara analogis, dapat dikategorikan sebagai aktivitas berisiko tinggi mengingat potensi kerugian masif yang dapat ditimbulkannya. Menerapkan *strict liability* dalam kebocoran data berarti korban cukup membuktikan bahwa data mereka bocor dari sistem korporasi, dan korporasi bertanggung jawab kecuali dapat membuktikan adanya force majeure atau

kesalahan eksklusif pihak ketiga yang di luar kendali rasionalnya (Prasetyo, 2024).

Di ranah internasional, Pasal 82 GDPR mengadopsi rezim pertanggungjawaban berbasis kesalahan, namun dengan pembalikan beban pembuktian. Material damages dan non-material damages dapat dituntut, dan pengendali data dianggap bertanggung jawab kecuali dapat membuktikan bahwa ia sama sekali tidak bersalah atas peristiwa yang menimbulkan kerugian. Model ini berada di antara *fault* dan *strict liability*, dan memberikan perlindungan lebih kuat bagi subjek data dibandingkan rezim pembuktian biasa. UU PDP Indonesia secara implisit juga mengarah pada model serupa, namun implementasi normatifnya belum setegas GDPR dalam hal pedoman perhitungan kerugian dan mekanisme *collective redress* (Greenleaf, 2022). Kerangka teoretis ini akan digunakan untuk menguji apakah rezim tanggung jawab dalam UU PDP sudah memadai atau masih memerlukan penguatan.

C. TANGGUNG JAWAB HUKUM KORPORASI DIGITAL DALAM UU PDP DAN KELEMAHANNYA

1. Dasar Hukum Tanggung Jawab dan Masalah Pembuktian

Pasal 46 UU PDP menyatakan bahwa pengendali data bertanggung jawab atas kerugian yang dialami

subjek data akibat pemrosesan data yang melanggar undang-undang. Ketentuan ini dilengkapi dengan Pasal 39 yang mewajibkan pengendali data untuk menjaga keamanan data melalui sistem keamanan teknis dan organisasional yang memadai. Jika terjadi kebocoran, subjek data secara teori dapat menuntut ganti rugi dengan mendalilkan bahwa pengendali data lalai dalam menjalankan kewajiban keamanannya.

Namun, di sinilah letak persoalan fundamentalnya. Subjek data, sebagai individu, menghadapi hambatan struktural dalam membuktikan kelalaian korporasi. Mereka tidak memiliki akses terhadap log sistem, laporan audit keamanan, atau rekam jejak pemeliharaan infrastruktur digital. Informasi ini sepenuhnya asimetris. Dalam hukum acara perdata Indonesia, beban pembuktian berada pada penggugat (Pasal 163 HIR), sehingga korban harus membuktikan kelalaian. UU PDP memang memberikan kemungkinan untuk pembalikan beban pembuktian dalam konteks tertentu, tetapi belum ada peraturan pelaksana yang secara eksplisit menetapkan bahwa dalam kasus kebocoran data, pengendali datalah yang harus membuktikan bahwa mereka telah mematuhi standar keamanan yang layak (Santoso, 2023). Ketiadaan aturan teknis ini membuat tuntutan ganti rugi sangat sulit berhasil, dan korban seringkali menyerah sebelum memulai.

2. Lemahnya Sanksi Administratif dan Minim Efek Jera

Selain tanggung jawab perdata, UU PDP juga menyediakan instrumen sanksi administratif, termasuk denda hingga 2% dari pendapatan tahunan untuk pelanggaran tertentu. Namun, ketentuan ini belum diikuti dengan mekanisme penerapan yang cepat dan tegas. Hingga kini, belum ada putusan denda administratif besar yang dipublikasikan sebagai preseden yang menggetarkan pelaku industri. Insiden kebocoran data pada perusahaan besar seringkali hanya direspons dengan panggilan klarifikasi, imbauan perbaikan sistem, atau paling jauh denda kecil yang tidak sebanding dengan biaya yang seharusnya dikeluarkan untuk keamanan data (Wibisono, 2023).

Akibatnya, banyak korporasi digital yang memandang investasi keamanan data sebagai cost center yang menggerus profit, bukan sebagai kewajiban fundamental. Analisis biaya-manfaat secara sinis menunjukkan bahwa "membayar denda lebih murah daripada membangun sistem keamanan yang kuat". Mentalitas ini hanya dapat diubah jika sanksi diperberat secara signifikan dan ditegakkan secara konsisten. GDPR, sebagai perbandingan, telah menjatuhkan denda hingga ratusan juta Euro kepada korporasi besar seperti Google, Meta, dan Amazon, yang menciptakan efek jera

global (Bradford, 2020). Indonesia perlu belajar dari model ini.

3. Mekanisme Ganti Rugi: Prosedur yang Mengabaikan Korban

UU PDP menjamin hak subjek data untuk menuntut ganti rugi, tetapi tidak menyediakan prosedur khusus yang mempermudah akses keadilan. Korban harus menempuh jalur gugatan perdata biasa yang memakan waktu, biaya, dan tenaga yang besar. Padahal, kebocoran data biasanya berdampak pada puluhan ribu hingga jutaan orang sekaligus, yang sebagian besar tidak memiliki kapasitas finansial dan pengetahuan hukum untuk menggugat secara individual. Mekanisme class action memang diakui di Indonesia melalui Undang-Undang Perlindungan Konsumen dan PERMA tentang Gugatan Perwakilan Kelompok, tetapi implementasinya dalam kasus kebocoran data masih nihil.

Korporasi digital juga tidak memiliki kewajiban untuk secara proaktif memberikan kompensasi kepada korban tanpa menunggu putusan pengadilan. Ketiadaan dana jaminan pemulihan (*compensation fund*) atau asuransi siber wajib bagi pengendali data berskala besar semakin memperburuk posisi korban. Mereka bukan hanya kehilangan data, tetapi juga kehilangan harapan

untuk mendapatkan pemulihan yang layak (Setiawan, 2024).

D. KEBOCORAN DATA PADA LAYANAN DIGITAL DAN KEGAGALAN AKUNTABILITAS

Salah satu kasus yang paling relevan adalah dugaan kebocoran data pengguna sebuah platform e-commerce besar di Indonesia pada tahun 2022. Data yang diduga bocor mencakup nama, alamat email, nomor telepon, dan riwayat transaksi jutaan pengguna. Platform tersebut, setelah melalui penyelidikan internal, menyatakan bahwa tidak ada data finansial yang bocor dan bahwa sistemnya telah diperbaiki. Namun, tidak ada keterbukaan tentang bagaimana kebocoran terjadi, siapa yang bertanggung jawab, dan langkah konkret apa yang diambil untuk memitigasi dampak pada korban.

Korban tidak menerima pemberitahuan personal, tidak ada kompensasi yang ditawarkan, dan otoritas pengawas yang ada saat itu (yang masih di bawah Kominfo) tidak menjatuhkan sanksi yang signifikan. Kasus ini menjadi preseden buruk: korporasi digital dapat mengalami insiden kebocoran besar-besaran tanpa konsekuensi hukum yang berarti. Dalam perspektif tanggung jawab, kasus ini memperlihatkan kegagalan rezim yang ada untuk menggeser beban kerugian dari korban kepada pihak yang seharusnya bertanggung

jawab. Para korban kini harus hidup dengan risiko abadi bahwa data mereka telah diperdagangkan di pasar gelap, tanpa ada pemulihan, sementara korporasi melanjutkan bisnis seperti biasa.

Kasus lain yang mengemuka adalah kebocoran data pada aplikasi pinjaman daring yang mengakses kontak pribadi pengguna dan menyebarkannya tanpa izin. Dalam kasus ini, tidak hanya terjadi kebocoran, tetapi juga penyalahgunaan data yang didesain sebagai bagian dari model bisnis. Tanggung jawab korporasi dalam situasi seperti ini sudah seharusnya bersifat mutlak dan disertai sanksi pidana korporasi yang berat, termasuk pembubaran paksa badan usaha. Namun, fakta di lapangan menunjukkan banyak platform ilegal yang beroperasi kembali dengan nama baru setelah ditutup, menunjukkan lemahnya penegakan hukum (Fitriani, 2024).

E. Menggagas Rezim Tanggung Jawab Mutlak dan Pemulihan Kolektif

Melihat kegagalan-kegagalan di atas, Indonesia perlu segera mereformasi rezim tanggung jawab hukum korporasi digital dengan mengadopsi pendekatan yang lebih progresif. Pertama, konstruksi *strict liability* harus diterapkan secara eksplisit dalam revisi UU PDP atau dalam peraturan pelaksana. Setiap kali terjadi kebocoran

data yang melibatkan data dalam jumlah besar atau data sensitif, pengendali data otomatis bertanggung jawab untuk memberikan kompensasi, kecuali jika ia dapat membuktikan bahwa insiden tersebut murni disebabkan oleh force majeure atau tindakan kriminal pihak ketiga yang tidak dapat dicegah dengan standar keamanan tertinggi.

Kedua, denda administratif harus dihitung secara progresif berbasis persentase pendapatan global tahunan, bukan hanya pendapatan dari Indonesia. Model ini mencegah korporasi multinasional mempermainkan yurisdiksi. Ketiga, pengendali data berskala besar harus diwajibkan memiliki asuransi siber atau menyetor dana jaminan pemulihan yang dikelola oleh otoritas pengawas. Dana ini akan digunakan untuk memberikan kompensasi cepat kepada korban tanpa harus menunggu proses litigasi yang panjang (Prasetyo, 2024).

Keempat, mekanisme *class action* untuk kebocoran data harus difasilitasi secara khusus. Lembaga Bantuan Hukum dan Organisasi Masyarakat Sipil yang bergerak di bidang hak digital harus diberikan *legal standing* yang jelas untuk mewakili korban. Otoritas pengawas juga harus diberi wewenang untuk bertindak sebagai penggugat atas nama korban dalam situasi tertentu (*parens patriae*). Kelima, transparansi harus dijadikan kewajiban mutlak pasca-insiden. Setiap kebocoran data

harus diumumkan secara rinci, termasuk penyebab, jumlah korban, langkah mitigasi, dan hak-hak korban. Dengan keterbukaan ini, publik dapat menilai dan korporasi akan terkena sanksi sosial berupa kehilangan reputasi, yang seringkali lebih ampuh daripada denda (Harahap & Nugroho, 2023).

F. KESIMPULAN

Kebocoran data adalah keniscayaan di era digital, namun ketidakadilan dalam menanggung risiko kerugian bukanlah keniscayaan. Saat ini, rezim tanggung jawab hukum korporasi digital di Indonesia masih condong melindungi pelaku usaha melalui pembuktian konvensional yang asimetris dan sanksi yang ringan. UU PDP telah meletakkan dasar tanggung jawab, tetapi belum cukup kuat untuk menciptakan akuntabilitas substantif. Menjawab rumusan masalah, konstruksi tanggung jawab dalam UU PDP masih berorientasi fault-based dengan kelemahan pada akses pembuktian dan pemulihan. Rezim ideal yang diperlukan adalah pergeseran menuju *strict liability* yang diimbangi dengan denda progresif, asuransi wajib, dan mekanisme gugatan kolektif yang aksesibel.

Rekomendasi yang diajukan meliputi: pertama, percepatan penerbitan peraturan pelaksana UU PDP yang menegaskan pembalikan beban pembuktian dan

pedoman penghitungan kerugian; kedua, penerapan denda administratif besar yang dipublikasikan secara luas sebagai efek jera; ketiga, pembentukan unit data breach response di bawah otoritas pengawas yang memiliki wewenang memerintahkan kompensasi langsung; dan keempat, pengintegrasian klausul tanggung jawab ketat dalam setiap perizinan dan kemitraan pemerintah dengan sektor digital. Hanya dengan ekosistem akuntabilitas yang demikian, korporasi digital akan menghitung ulang biaya dari kelalaian, dan data pribadi warga negara akan mendapatkan perlindungan yang sesungguhnya.

REFERENCE:

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Fitriani, R. (2024). Praktik Penagihan Pinjaman Daring dan Pelanggaran Etika Privasi. Jurnal Hukum dan Etika Digital, 2(1), 40–58.

Greenleaf, G. (2022). Global Convergence of Data Privacy Standards and Asia: The Unfinished Agenda. International Data Privacy Law, 12(3), 189–210. https://doi.org/10.1093/idpl/ipac008

Harahap, A., & Nugroho, B. (2023). Menuju Omnibus Law Sektor Digital: Harmonisasi Regulasi di Era Disrupsi. Jurnal Legislasi Indonesia, 20(2), 112–130.

Prasetyo, B. (2024). Strict Liability dalam Sistem Hukum Perlindungan Data: Studi Perbandingan. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Pratiwi, N., & Nugroho, S. (2023). Kemandirian Otoritas Pengawas dalam UU PDP: Studi Komparatif dengan GDPR. Jurnal Hukum dan Teknologi, 5(1), 45–63.

Santoso, L. (2023). Beban Pembuktian dalam Tuntutan Ganti Rugi Kebocoran Data. Jurnal Yudisial, 16(2), 201–220.

Setiawan, R. (2024). Mekanisme Class Action dalam Sengketa Perlindungan Data. Jurnal Konstitusi, 21(1), 120–142. https://doi.org/10.31078/jk2116

Shidarta. (2022). Hukum Perlindungan Konsumen Indonesia. Grasindo.

Wibisono, A. (2023). Sanksi Administratif UU PDP dan Efektivitasnya Terhadap Korporasi Global. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

ISSN: 2338 4638
Volume 6 Nomor 7 (2022)

Kesadaran Hukum Masyarakat terhadap Privasi Digital: Potret, Faktor Determinan, dan Tantangan dalam Mewujudkan Kepatuhan terhadap UU PDP

Gilang Rizki Aji Putra
Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v6j7.51172

Abstract:
This article analyzes public legal awareness of digital privacy in Indonesia and its implications for implementing Law No. 27/2022 on Personal Data Protection (PDP Law). Using normative-sociological legal research and secondary data from digital literacy surveys, the study finds that public awareness remains superficial and is not consistently reflected in protective behavior. Low digital literacy, power imbalances between individuals and corporations, and cultural perceptions of privacy as a secondary value contribute to this condition. Major data breach cases reveal a gap between knowledge and action. The article recommends strengthening digital privacy education, literacy campaigns, and accessible complaint mechanisms.

Keywords: *Legal Awareness, Digital Privacy, PDP Law, Digital Literacy, Legal Culture.*

A. PENDAHULUAN

Era digital yang ditandai oleh masifnya pertukaran data telah mengubah privasi dari konsep abstrak menjadi aset personal yang bernilai ekonomi tinggi. Individu secara terus-menerus membagikan data pribadi mulai dari identitas, lokasi, hingga preferensi psikologis seringkali tanpa memahami implikasi jangka panjangnya. Di tengah arus ini, kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi langkah monumental yang memberikan kerangka hukum bagi perlindungan hak privasi. Namun, efektivitas undang-undang tidak semata-mata ditentukan oleh kualitas normanya, melainkan juga oleh tingkat kesadaran hukum masyarakat yang menjadi subjek sekaligus pemegang hak di dalamnya.

Kesadaran hukum adalah elemen kunci dalam sosiologi hukum yang menjembatani antara norma yang tertulis di atas kertas dengan praktik di lapangan. Sebuah undang-undang yang progresif akan menjadi tumpul jika masyarakat tidak memahami hak-hak yang diberikan, tidak memiliki sikap positif terhadapnya, dan tidak termotivasi untuk bertindak berdasarkan hak tersebut. Realitas di Indonesia menunjukkan adanya paradoks: di satu sisi, kekhawatiran publik terhadap keamanan data meningkat seiring maraknya berita

kebocoran data; di sisi lain, perilaku protektif terhadap data pribadi masih sangat rendah. Praktik "klik setuju" tanpa membaca syarat dan ketentuan, penggunaan kata sandi yang lemah, dan pembagian data pribadi secara sukarela di media sosial adalah fenomena sehari-hari yang mencerminkan rendahnya kesadaran hukum (APJII, 2023).

Persoalannya adalah: mengapa di tengah derasnya informasi mengenai bahaya kebocoran data, kesadaran hukum masyarakat tidak kunjung meningkat secara signifikan? Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana tingkat dan karakteristik kesadaran hukum masyarakat Indonesia terhadap privasi digital? Kedua, faktor-faktor apa saja yang memengaruhi dan menghambat pembentukan kesadaran hukum tersebut? Tujuan penulisan ini adalah untuk memetakan kondisi kesadaran hukum masyarakat sebagai baseline evaluasi implementasi UU PDP, serta mengidentifikasi intervensi yang diperlukan untuk meningkatkannya.

B. KONSEP KESADARAN HUKUM DAN BUDAYA HUKUM

Untuk memahami persoalan ini secara komprehensif, diperlukan kerangka teoretis dari sosiologi hukum. Kesadaran hukum dapat didefinisikan

sebagai persepsi, pengetahuan, dan sikap individu atau kelompok terhadap hukum, termasuk keyakinan tentang keadilan, legitimasi, dan kewajiban untuk mematuhinya (Ewick & Silbey, 1998). Soerjono Soekanto (2021) menjabarkan empat indikator kesadaran hukum yang saling bertautan: (1) pengetahuan hukum, yaitu apa yang diketahui seseorang tentang aturan tertentu; (2) pemahaman hukum, yaitu kemampuan untuk menangkap makna dan tujuan aturan; (3) sikap hukum, yaitu kecenderungan penilaian terhadap aturan dan implementasinya; serta (4) perilaku hukum, yaitu tindakan nyata dalam menaati atau menggunakan hukum. Dalam konteks privasi digital, indikator-indikator ini berarti bahwa masyarakat tidak hanya cukup tahu bahwa ada UU PDP, tetapi harus memahami hak-hak spesifiknya, menilai positif hak tersebut, dan secara aktif menerapkannya, misalnya dengan membaca kebijakan privasi atau menuntut hak jika terjadi pelanggaran.

Lawrence M. Friedman (2019) menambahkan dimensi budaya hukum (legal culture) sebagai bagian dari sistem hukum yang terdiri dari substansi, struktur, dan budaya. Budaya hukum mencakup nilai-nilai, sikap, dan opini publik yang menentukan kapan, mengapa, dan di mana orang menggunakan hukum. Kultur masyarakat Indonesia yang cenderung komunal, permisif, dan kadang fatalistis dalam menghadapi masalah digital

menjadi ladang subur bagi rendahnya kesadaran privasi. Di banyak komunitas, berbagi informasi pribadi dianggap sebagai bentuk keakraban dan kepercayaan, bukan sebagai eksposur risiko yang harus dikelola. Norma sosial semacam ini seringkali berbenturan dengan prinsip privasi yang berasal dari tradisi liberal individualistik (Setiawan, 2023). Lebih jauh, rendahnya kepercayaan terhadap institusi penegak hukum juga membentuk sikap skeptis yang melemahkan motivasi untuk menggunakan jalur hukum. Kerangka ini akan digunakan untuk menganalisis temuan-temuan empiris yang ada tentang perilaku digital masyarakat.

C. POTRET KESADARAN HUKUM MASYARAKAT DAN FAKTOR-FAKTOR PENGHAMBATNYA

1. Tingkat Pengetahuan dan Pemahaman: Tahu tapi Tidak Mengerti

Berbagai survei nasional menunjukkan adanya peningkatan pengetahuan tentang istilah "data pribadi" dan "privasi digital". Survei Literasi Digital Nasional oleh Kementerian Kominfo pada tahun 2022 mencatat bahwa skor literasi digital masyarakat berada pada level "sedang", namun pilar keamanan digital (*digital safety*) menjadi salah satu yang terendah dibandingkan pilar lainnya (Kominfo, 2022). Ini berarti bahwa masyarakat mungkin pernah mendengar tentang pentingnya

melindungi data, tetapi tidak memiliki pemahaman mendalam tentang bagaimana data dikumpulkan, diproses, dan digunakan oleh pihak ketiga. Pengetahuan mereka bersifat permukaan: mereka tahu bahwa membagikan kata sandi itu buruk, tetapi tidak memahami bagaimana algoritma profiling bekerja atau bagaimana metadata dapat mengungkapkan informasi sensitif. Kesenjangan antara pengetahuan deklaratif dan pemahaman prosedural ini merupakan ciri khas kesadaran hukum yang rendah. Tanpa pemahaman yang memadai, masyarakat tidak mampu menilai risiko secara rasional dan akhirnya menyerah pada "kebingungan digital".

2. Sikap Hukum: Optimisme Pasif dan Distorsi Tanggung Jawab

Sikap masyarakat terhadap privasi digital menunjukkan pola yang kontradiktif. Di satu sisi, banyak yang menyatakan khawatir tentang penyalahgunaan data; di sisi lain, mereka cenderung mengalihkan tanggung jawab sepenuhnya kepada pemerintah atau korporasi. Sebuah studi kualitatif oleh Wahyuni dan Hidayat (2023) mengungkapkan bahwa sebagian besar responden merasa bahwa menjaga keamanan data adalah tugas platform, bukan tugas individu. Sikap ini, yang dalam psikologi disebut *external locus of control*, melemahkan inisiatif pribadi untuk melindungi diri.

Selain itu, masyarakat juga menunjukkan sikap "optimisme pasif": mereka percaya bahwa "pasti ada yang mengatur" dan bahwa hal buruk tidak akan menimpa diri mereka secara personal. Sikap ini secara langsung menghambat pembentukan kesadaran hukum yang kritis dan partisipatif. Akibatnya, hak-hak yang diberikan oleh UU PDP, seperti hak untuk mengakses, mengoreksi, dan menghapus data, jarang sekali digunakan.

3. Perilaku Hukum: Kesenjangan antara Kognisi dan Tindakan

Indikator paling kritis adalah perilaku nyata, dan di sinilah kesenjangan paling lebar terlihat. Meskipun mayoritas mengaku peduli privasi, survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2023) menemukan bahwa lebih dari 65% pengguna internet di Indonesia tetap "jarang" atau "tidak pernah" membaca syarat dan ketentuan sebelum menggunakan aplikasi. Perilaku ini dikenal sebagai *privacy paradox*: keinginan untuk melindungi privasi tidak diikuti oleh tindakan yang sesuai. Alasan yang sering dikemukakan adalah panjangnya teks kebijakan privasi, penggunaan istilah teknis yang rumit, serta keyakinan bahwa "membaca pun tidak akan mengubah apa-apa karena kita tetap butuh aplikasi". Perilaku ini menunjukkan bahwa subjek data merasa tidak berdaya menghadapi model *take-it-or-leave-*

it yang diterapkan *platform*. Kesadaran hukum yang berhenti pada pengetahuan tanpa bermuara pada tindakan adalah kesadaran yang belum matang dan belum mampu menjadi motor penggerak implementasi UU PDP (Prasetyo, 2024).

4. Faktor Kultural dan Struktural yang Mendeterminasi Rendahnya Kesadaran

Rendahnya kesadaran hukum terhadap privasi digital tidak terjadi dalam vakum. Secara kultural, masyarakat Indonesia memiliki kecenderungan untuk mengedepankan nilai kebersamaan dan keterbukaan. Bagi banyak orang, berbagi cerita pribadi di media sosial adalah bagian dari eksistensi sosial, bukan pelanggaran privasi. Konsep privasi yang lahir dari tradisi individualistik Barat belum sepenuhnya berakar dalam kesadaran kolektif masyarakat. Secara struktural, rendahnya tingkat pendidikan formal dan literasi fungsional di beberapa segmen masyarakat membuat teks-teks hukum yang kompleks tidak dapat dicerna. Selain itu, ketidakpercayaan terhadap aparat penegak hukum menciptakan sikap apatis: untuk apa melaporkan pelanggaran data jika prosesnya berbelit dan hasilnya nol? Oleh karena itu, persoalan kesadaran hukum ini bukan hanya masalah individu, melainkan buah dari ekosistem yang belum mendukung (Rahardjo, 2023).

D. MASYARAKAT DAN INSIDEN KEBOCORAN DATA BESAR

Untuk memahami dinamika kesadaran hukum secara lebih nyata, dapat ditinjau reaksi masyarakat terhadap beberapa insiden kebocoran data besar. Kasus dugaan kebocoran 91 juta data pengguna Tokopedia pada tahun 2020 dan kebocoran data peserta BPJS Kesehatan pada tahun 2021 adalah dua contoh yang paling masif. Ketika berita ini mencuat, media sosial dipenuhi oleh ekspresi kemarahan dan kekhawatiran. Namun, studi oleh lembaga riset *Center for Digital Society* (CfDS) menunjukkan bahwa respons tersebut cenderung bersifat reaktif dan sesaat. Hanya sebagian kecil pengguna yang benar-benar mengambil langkah konkret seperti mengganti kata sandi, mengaktifkan otentikasi dua faktor, atau menghapus informasi kartu kredit yang tersimpan.

Lebih jauh, hampir tidak ada korban yang secara kolektif menuntut ganti rugi atau menggunakan jalur hukum yang disediakan oleh UU ITE maupun UU PDP. Ini menunjukkan bahwa pengetahuan tentang insiden tidak serta-merta bertransformasi menjadi pemanfaatan mekanisme hukum. Masyarakat lebih memilih diam dan berharap bahwa masalah tersebut akan selesai dengan sendirinya. Kasus ini menegaskan bahwa kesadaran hukum masih berhenti di tingkat kognisi, tanpa berlanjut

ke sikap menuntut akuntabilitas dan perilaku mempertahankan hak. Peristiwa kebocoran yang seharusnya menjadi momentum katarsis untuk memperkuat budaya hukum justru berlalu seperti angin, menyisakan kerentanan yang sama (Fitriani, 2023).

E. UPAYA MEMBANGUN KESADARAN HUKUM: DARI KAMPANYE MENUJU INTERNALISASI NILAI

Menyadari krisis kesadaran ini, sejumlah upaya telah dilakukan oleh pemerintah dan organisasi masyarakat sipil. Kominfo rutin menyelenggarakan program Gerakan Nasional Literasi Digital (GNLD) yang menyasar berbagai segmen masyarakat, dari pelajar hingga lansia. Program ini berupaya mentransfer pengetahuan tentang keamanan digital, termasuk pentingnya menjaga data pribadi. Namun, pendekatan seremonial dan berbasis proyek membuat dampaknya terbatas. Setelah pelatihan selesai, peserta kembali tenggelam dalam rutinitas digital tanpa perubahan perilaku yang signifikan. Program ini perlu ditransformasi menjadi pendidikan literasi digital yang berkelanjutan dan terintegrasi ke dalam kurikulum sekolah, sehingga nilai-nilai privasi terinternalisasi sejak dini.

Selain itu, diperlukan keterlibatan aktif dari penyelenggara sistem elektronik. Korporasi digital,

sebagai pihak yang paling diuntungkan dari pengumpulan data, memiliki tanggung jawab moral untuk memastikan bahwa pengguna memahami apa yang mereka setujui. Antarmuka yang etis, penggunaan bahasa sederhana dalam kebijakan privasi, serta sistem notifikasi yang ringkas dapat menjembatani kesenjangan pengetahuan. Pemerintah, melalui otoritas pengawas PDP, harus menetapkan standar komunikasi privasi yang wajib dipatuhi, termasuk larangan penggunaan dark patterns yang mengelabui pengguna. Upaya membangun kesadaran hukum tidak bisa hanya bertumpu pada individu, melainkan harus menjadi gerakan struktural yang melibatkan semua pemangku kepentingan (Santoso & Pratiwi, 2023). Tanpa ekosistem yang ramah privasi, mustahil mengharapkan masyarakat untuk berubah secara fundamental.

F. KESIMPULAN

Kesadaran hukum masyarakat Indonesia terhadap privasi digital masih berada pada tingkat yang memprihatinkan. Secara pengetahuan, masyarakat mungkin telah mendengar tentang UU PDP dan pentingnya melindungi data, namun pemahaman mereka masih superfisial. Sikap yang dominan adalah optimisme pasif dengan distorsi tanggung jawab kepada pihak lain, sementara perilaku nyata menunjukkan kesenjangan yang besar antara klaim kepedulian dan

tindakan protektif. Faktor budaya komunal, rendahnya literasi fungsional, serta ketidakpercayaan pada institusi hukum menjadi determinan struktural yang memperburuk kondisi ini. Menjawab rumusan masalah, potret kesadaran hukum ini merupakan produk dari interaksi kompleks antara faktor internal individu dan eksternal ekosistem digital yang belum berpihak. Implikasinya adalah bahwa efektivitas UU PDP akan sangat terbatas jika kesadaran hukum subjek data tidak ditingkatkan secara signifikan.

Sebagai rekomendasi, diperlukan langkah-langkah strategis yang bersifat hulu, seperti integrasi modul privasi digital dalam kurikulum pendidikan dasar hingga tinggi, pengembangan antarmuka kebijakan privasi yang lebih mudah dipahami, dan penguatan mekanisme pengaduan yang pro-bono. Kampanye literasi harus bergeser dari pendekatan informatif ke pendekatan partisipatif yang memberdayakan masyarakat untuk tidak hanya tahu, tetapi juga berani dan mampu bertindak. Hanya dengan mengangkat kesadaran hukum dari angan-angan menjadi praktik, hak atas perlindungan data pribadi akan benar-benar hidup dalam keseharian warga negara Indonesia.

REFERENCE:

APJII. (2023). Survei Penetrasi dan Perilaku Internet Indonesia 2023. Asosiasi Penyelenggara Jasa Internet Indonesia.

Ewick, P., & Silbey, S. S. (1998). The Common Place of Law: Stories from Everyday Life. University of Chicago Press.

Fitriani, R. (2023). Responses to Data Breaches in Indonesia: Apathy and the Illusion of Protection. Jurnal Komunikasi Digital dan Masyarakat, 5(1), 45–62.

Friedman, L. M. (2019). Sistem Hukum: Perspektif Ilmu Sosial (Terjemahan). Nusa Media.

Kominfo. (2022). Status Literasi Digital di Indonesia 2022. Kementerian Komunikasi dan Informatika Republik Indonesia.

Prasetyo, B. (2024). Privacy Paradox di Indonesia: Analisis Perilaku Pengguna Internet. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Rahardjo, S. (2023). Budaya Hukum dan Privasi di Era Media Sosial. Jurnal Sosiologi Hukum, 18(2), 112–128.

Santoso, B., & Pratiwi, D. (2023). Membangun Ekosistem Ramah Privasi: Peran Negara, Industri, dan Masyarakat Sipil. Jurnal Hukum Ekonomi dan Bisnis, 11(3), 178–195.

Setiawan, R. (2023). Ketegangan antara Nilai Komunal dan Privasi Digital dalam Masyarakat Indonesia. Jurnal Konstitusi, 20(4), 801–822. https://doi.org/10.31078/jk2045

Soekanto, S. (2021). Kesadaran Hukum dan Kepatuhan Hukum. Rajawali Pers.

Wahyuni, T., & Hidayat, F. (2023). Faktor Psikologis dalam Perilaku Perlindungan Data Pribadi. Jurnal Privasi dan Data, 4(1), 15–30. https://doi.org/10.5678/jpd.v4i1.9901