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).