JURNAL FUNDAMENTAL JUSTICE
Volume 7, Nomor 1, Maret 2026, hlm. 127–146
E-ISSN: 2721-7671, DOI: https://doi.org/10.30812/fundamental.v7i1.6237

Pertanggungjawaban Pidana Korporasi Atas Kebocoran Data Pribadi di Indonesia: Studi Komparatif dengan Amerika Serikat dan Uni Eropa

Devany Anggriani, Emiliya Febriyani*, Ampuan Situmeang

Universitas Internasional Batam, Batam, Indonesia

Informasi Artikel

Riwayat Artikel:

Diterima : 9 Maret 2026
Direvisi : 17 Maret 2026
Disetujui : 28 Maret 2026

Kata Kunci:

Pertanggungjawaban Pidana Korporasi;
Perlindungan Data Pribadi;
Studi Komparatif Hukum.

Abstrak

Kebocoran data pribadi oleh entitas korporasi digital di Indonesia terus meningkat. Mekanisme pertanggungjawaban pidana korporasi belum berjalan efektif sehingga menimbulkan kekhawatiran terhadap perlindungan hak privasi warga negara di era digital. Penelitian ini bertujuan menganalisis pengaturan dan penerapan pertanggungjawaban pidana korporasi terhadap kebocoran data pribadi di Indonesia serta membandingkannya dengan praktik di Uni Eropa dan Amerika Serikat. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perbandingan hukum dan studi kasus. Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, putusan hukum, dan dokumen terkait yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa di Uni Eropa, korporasi dapat dimintai pertanggungjawaban pidana maupun administratif melalui *General Data Protection Regulation*, dengan sanksi administratif sebesar 10–20 juta Euro atau 2–4% dari omzet global, sementara penentuan sanksi pidana diatur oleh negara anggota. Di Amerika Serikat, korporasi dapat dimintai pertanggungjawaban pidana berdasarkan *Federal Trade Commission Act* dan aturan pidana federal, yang memberikan dasar hukum kuat untuk menindak perusahaan yang lalai melindungi data pribadi. Sebaliknya, di Indonesia, meskipun telah memiliki Undang-Undang Perlindungan Data Pribadi dan KUHP baru, mekanisme pertanggungjawaban pidana korporasi belum efektif karena ketiadaan lembaga pengawas independen dan penegakannya cenderung simbolik. Kondisi ini menegaskan urgensi penguatan mekanisme pertanggungjawaban pidana korporasi serta pembentukan otoritas pengawas independen guna memperkuat perlindungan data pribadi di Indonesia.

***Penulis Korespondensi**

Tel. : -
E-mail : emiliya@uib.ac.id

How to Cite:

Anggriani, D., E. Febriyani, dan A. Situmeang, "Pertanggungjawaban Pidana Korporasi Atas Kebocoran Data Pribadi di Indonesia: Studi Komparatif dengan Amerika Serikat dan Uni Eropa", *Jurnal Fundamental Justice* 7, no. 1 (Maret, 2026): 127–146.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital mendorong pertumbuhan signifikan jumlah pengguna internet yang diperkirakan melebihi 5,5 miliar pada awal 2024.[1] Namun, kemajuan ini juga meningkatkan risiko kebocoran data, di mana pada kuartal III 2022 tercatat lebih dari 108,9 juta akun terdampak secara global.[2] Laporan *Cyber Crime Statistic* mencatat Indonesia menempati peringkat ketiga dunia dengan sekitar 13,2 juta akun terdampak hingga kuartal III 2022.[3] Fakta ini menunjukkan bahwa kebocoran data pribadi merupakan ancaman serius yang membutuhkan regulasi dan pertanggungjawaban hukum untuk melindungi hak privasi masyarakat di tengah transformasi digital. Data pribadi seperti nama, alamat *email*, nomor telepon, hingga informasi finansial kini menjadi aset berharga yang dimanfaatkan untuk layanan digital dan bisnis, namun semakin rentan disalahgunakan, termasuk untuk pencurian identitas dan penipuan.[4] Urgensi perlindungan data ini semakin nyata dengan munculnya fenomena *digital dossier*, yakni kumpulan data pribadi yang dihimpun dan disimpan perusahaan teknologi tanpa sepengetahuan langsung dari pengguna.[5]

Sejumlah kasus besar menunjukkan dampak serius kebocoran data. Di Amerika Serikat, Uber mengalami kebocoran data 57 juta pengguna pada 2016 yang ditutup-tutupi dengan pembayaran tebusan, hingga berujung pada hukuman pidana bagi *Chief Security Officer* dan denda 148 juta dolar AS bagi perusahaan.[6] Di Uni Eropa, kasus Vastaamo di Finlandia pada 2018–2019 melibatkan kebocoran data pasien sekitar 30,000 orang, berujung pada denda administratif dan hukuman pidana, serta menegaskan peran *General Data Protection Regulation* sebagai instrumen utama perlindungan data.[7] Sementara itu, di Indonesia, kasus Tokopedia tahun 2020 dengan 91 juta akun terdampak menunjukkan lemahnya penegakan hukum, karena data pribadi dijual di *dark web* dan disalahgunakan untuk penipuan serta pencurian identitas.[8] Kebocoran data tersebut telah menyebabkan penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab, seperti praktik penipuan, pencurian identitas, atau akses tidak sah terhadap akun pengguna.[9] Dampak kebocoran data sangat luas, mulai dari kejahatan digital seperti pencurian identitas dan *phishing*, hingga menimbulkan kecemasan psikologis serta melemahkan kepercayaan masyarakat

[1] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2024*, 2024, https://www.itu.int:443/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx.

[2] A. Mascellino, *Data Breaches Rise By 70% Globally in Q3 2022*, Infosecurity Magazine, Oktober 25, 2022, https://www.infosecurity-magazine.com/news/data-breaches-rise-by-70-q3-2022/.

[3] Otoritas Jasa Keuangan (OJK), *Roadmap Penguatan Bank Pembangunan Daerah 2024-2027* (Jakarta, 2024), https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Roadmap%20Penguatan%20Bank%20Pembangunan%20Daerah%202024-2027.pdf.

[4] O. T. Joel, dan V. U. Oguanobi, "Data-Driven Strategies for Business Expansion: Utilizing Predictive Analytics for Enhanced Profitability and Opportunity Identification", *International Journal of Frontiers in Engineering and Technology Research* 6, no. 2 (Mei 30, 2024): 071–081, https://doi.org/10.53294/ijfetr.2024.6.2.0035.

[5] C. B. Davison dkk. "Data Privacy in the Age of Big Data Analytics", *Issues In Information Systems* 22, no. 2 (2021): 177–186, https://doi.org/10.48009/2_iis_2021_185-195.

[6] AP News, *Ex-Uber Security Chief Sentenced for Data-Breach Cover-Up*, Mei 5, 2023, https://apnews.com/article/uber-data-breach-coverup-sentenced-san-francisco-05b2ded36daf55012f03651cf2c7c931.

[7] H. Ghanbari, dan K. Koskinen, "When Data Breach Hits a Psychotherapy Clinic: The Vastaamo Case", *Journal of Information Technology Teaching Cases*, Juni 7, 2024, 20438869241258235, https://doi.org/10.1177/20438869241258235.

[8] CNN Indonesia, *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*, 2020, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

[9] E. Budi, D. Wira, dan A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0", *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3 (Desember 21, 2021): 223–234, https://doi.org/10.54706/senastindo.v3.2021.141.

terhadap layanan digital. Kondisi ini berpotensi menghambat pertumbuhan ekonomi digital di Indonesia dan menurunkan kepercayaan publik terhadap platform *e-commerce*.[10]

Dalam konteks hukum, perusahaan sebagai pengendali data pribadi (*data controller*) berdasarkan Pasal 1 angka 4 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) berkewajiban mencegah akses dan penyebarluasan data tanpa dasar hukum yang sah. Pasal 58 UU PDP menegaskan kewajiban pengendali data untuk melindungi data pribadi dari pemrosesan yang bertentangan dengan hukum, sedangkan Pasal 67 ayat (1) menyebutkan secara tegas bahwa "*Setiap orang yang dengan sengaja dan tanpa hak mengungkapkan data pribadi bukan miliknya dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp5,000,000,000.00 (lima miliar rupiah)*".[11] Apabila kelalaian perusahaan mengakibatkan kebocoran data, korporasi dapat dimintai pertanggungjawaban pidana sesuai Pasal 118–124 KUHP 2023, termasuk pidana denda, perampasan keuntungan, hingga pembubaran badan hukum. Kewajiban ini juga diperkuat oleh Pasal 28G ayat (1) UUD 1945 yang menyatakan bahwa "*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*"[12] Dengan demikian, kebocoran data bukan sekadar persoalan administratif, melainkan bentuk pengingkaran terhadap jaminan konstitusional.

Ketiadaan penegakan hukum atas kebocoran data di Indonesia menunjukkan lemahnya penerapan prinsip *corporate criminal liability*, sehingga korporasi digital seolah bebas dari sanksi meski merugikan jutaan warga.[13] Berbeda dengan Indonesia, Amerika Serikat melalui *Federal Trade Commission Act* (*FTC Act*) memberi kewenangan kepada *FTC* untuk menindak praktik bisnis tidak adil atau menipu, sementara ketentuan pidana seperti *Obstruction of Proceedings Before Departments, Agencies, and Committees* (18 U.S.C. § 1505) dan *Misprision of Felony Act* (18 U.S.C. § 4) memungkinkan pemidanaan atas penghalangan penyelidikan pelanggaran data (Baker M, 2022). Di Uni Eropa, *General Data Protection Regulation* sejak 2018 mengatur prinsip transparansi, minimalisasi data, batasan tujuan, akuntabilitas, serta hak individu atas data pribadi dengan ancaman denda 10–20 juta euro atau 2–4% dari omzet global perusahaan. Sementara itu, di Indonesia, meskipun UU Pelindungan Data Pribadi (UU PDP) sudah mengatur sanksi administratif dan pidana, implementasinya masih lemah karena belum ada lembaga independen yang mengawasi secara penuh, sehingga urgensi pembentukan badan khusus menjadi penting untuk efektivitas perlindungan data pribadi.

Beberapa penelitian sebelumnya telah membahas tanggung jawab penyedia layanan digital terhadap kebocoran data pribadi, namun masih terdapat celah penelitian yang belum dikaji secara mendalam. Penelitian yang dilakukan oleh Rochman dkk. menelaah tanggung jawab *marketplace* atas kebocoran data di Indonesia,

[10] D. Rahmawati, M. D. A. Aksana, dan S. Mukaromah, "Privasi Dan Keamanan Data Di Media Sosial: Dampak Negatif Dan Strategi Pencegahan", *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* 3, no. 1 (November 11, 2023): 571–580, https://doi.org/10.33005/sitasi.v3i1.354.

[11] *Undang-Undang (UU) Nomor 27 Tahun 2022: Pelindungan Data Pribadi*, Database Peraturan BPK, 2022, http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

[12] *UUD 1945 Dan Amandemen*, Database Peraturan BPK, 1945, http://peraturan.bpk.go.id/Details/101646/uud-no--.

[13] J. Perkasa, dan J. N. Saly, "Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020):" 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021) (Jakarta, Indonesia, 2022), https://doi.org/10.2991/assehr.k.220404.096.

tetapi tidak membahas perbandingan dengan regulasi negara lain.[14] Panjaitan mengkaji pertanggungjawaban pidana korporasi berbasis *web* dan aplikasi, namun tidak secara spesifik menyinggung penyalahgunaan data akibat kebocoran.[15] Arsjad dkk. fokus pada tanggung jawab penyedia layanan *cloud computing*[16], sedangkan Primanta lebih menyoroti aspek penyalahgunaan data pribadi tanpa menekankan peran platform penyedia layanan.[17] Putra Azhar dan Mahyani meneliti pertanggungjawaban pidana korporasi atas penyebaran data pribadi, tetapi belum menyoroti efektivitas regulasi lintas negara.[18] Sementara itu, Muzakkie dan Juarsa membahas perlindungan hukum terhadap data pribadi pada aplikasi pinjaman online ilegal, namun tidak mengulas aspek kebocoran data akibat kelalaian perusahaan teknologi.[19]

Berbeda dengan penelitian sebelumnya, penelitian ini menghadirkan kebaruan dengan menitikberatkan pada pertanggungjawaban pidana korporasi atas kebocoran data pribadi serta membandingkan regulasi Indonesia dengan Amerika Serikat dan Uni Eropa. Penelitian ini memperkaya literatur hukum pidana korporasi dengan menyoroti tantangan penegakan UU PDP, kelemahan implementasi sanksi, serta urgensi pembentukan badan pengawas independen. Meskipun demikian, penelitian ini tetap memberikan kontribusi penting dalam memahami tantangan dan peluang penguatan kebijakan perlindungan data di Indonesia dalam konteks hukum pidana korporasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan hukum normatif, yaitu metode yang menelaah hukum sebagai sistem norma melalui kajian peraturan perundang-undangan, asas, doktrin, dan putusan pengadilan terkait perlindungan data pribadi serta pertanggungjawaban pidana korporasi di Indonesia, yang kemudian dibandingkan dengan sistem hukum di Uni Eropa dan Amerika Serikat.[20] Menurut Tan, penelitian hukum normatif berfungsi untuk memahami konsep hukum secara konseptual dan menguji konsistensi antara norma dan praktiknya.[21] Sementara itu, Disemadi (2022) menegaskan bahwa pendekatan ini mengevaluasi hubungan antara *das Sollen* dan *das Sein* melalui studi

[14] H. N. Rochman, B. K. Heriawanto, dan I. K. Ayu, "Tanggung Gugat Penyedia Platform Marketplace Terhadap Kebocoran Data Pribadi Konsumen Pengguna Platform Marketplace Di Indonesia", *Dinamika* 27, no. 2 (Januari 19, 2021): 237–250, https://jim.unisma.ac.id/index.php/jdh/article/view/9392.

[15] R. M. Panjaitan, "Pertanggungjawaban Pidana Korporasi Sebagai Penyelenggara Sistem Elektronik Dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik", *Jurnal Hukum Adigama* 4, no. 2 (2021): 2624–2643, https://doi.org/10.24912/adigama.v4i2.17761.

[16] J. Arsjad, S. D. Rosadi, dan R. R. Permata, "Pengaturan Dan Tanggung Jawab Penyedia Jasa Layanan Komputasi Awan (Cloud Computing) Atas Penyimpanan Data Pribadi Pengguna Dari Kebocoran Data Elektronik", *JIHK* 2, no. 1 (Juli 30, 2020): 97–106, https://doi.org/10.46924/jihk.v2i1.136.

[17] A. I. Primanta, "Pertanggungjawaban Pidana Pada Penyalahgunaan Data Pribadi", *Jurist-Diction* 3, no. 4 (Juni 28, 2020): 1431, https://doi.org/10.20473/jd.v3i4.20214.

[18] D. P. Azhar, dan A. Mahyani, "Pertanggungjawaban Pidana Korporasi sebagai Pelaku Tindak Pidana Penyebaran Data Pribadi", *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 540–558, https://doi.org/10.53363/bureau.v3i1.200.

[19] S. A. Muzakkie, dan E. Juarsa, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi", *Bandung Conference Series: Law Studies* 3, no. 2 (Agustus 1, 2023): 984–987, https://doi.org/10.29313/bcsls.v3i2.7284.

[20] M. H. Yanova, P. Komarudin, dan H. Hadi, "Metode Penelitian Hukum: Analisis Problematika Hukum dengan Metode Penelitian Normatif dan Empiris", *Badamai Law Journal* 8, no. 2 (September 11, 2023): 394–408, https://doi.org/10.32801/damai.v8i2.17423.

[21] D. Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum", *NUSANTARA : Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (Desember 28, 2021): 2463–2478, https://doi.org/10.31604/jips.v8i8.2021.2463-2478.

literatur tanpa memerlukan data primer.[22]

Penelitian ini menyoroti kesenjangan antara pengaturan dalam UU No. 1 Tahun 2023 (KUHP) dan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dengan realitas pertanggungjawaban pidana korporasi di Indonesia, serta membandingkannya dengan *General Data Protection Regulation* di Uni Eropa dan ketentuan *Federal Trade Commission Act*, 18 U.S.C. § 1505, dan 18 U.S.C. § 4 di Amerika Serikat. Pendekatan yang digunakan mencakup pendekatan perundang-undangan (*statute approach*) untuk menganalisis regulasi nasional dan pendekatan perbandingan hukum (*comparative approach*) untuk menilai efektivitas serta kelemahan sistem hukum Indonesia. Data yang digunakan berupa bahan hukum primer, sekunder, dan tersier yang dikumpulkan melalui studi kepustakaan dan dianalisis secara deskriptif serta evaluatif guna menilai efektivitas norma hukum dalam melindungi data pribadi dan mencegah kebocoran oleh korporasi.

HASIL PENELITIAN

1. Pengaturan Hukum Mengenai Pertanggungjawaban Pidana Korporasi Atas Kebocoran Data Pribadi Menurut Sistem Hukum di Indonesia, Amerika Serikat, dan Uni Eropa

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang secara efektif mulai diberlakukan pada tanggal 17 Oktober 2024, merupakan sebuah pilar penting dalam perkembangan sistem hukum perlindungan data pribadi di Indonesia.[23] Secara normatif, undang-undang ini membentuk kerangka regulasi yang bersifat menyeluruh dengan ruang lingkup mencakup definisi yuridis data pribadi, pengaturan hak-hak subjek data, kewajiban pengendali dan prosesor data, serta prinsip-prinsip dasar pemrosesan data pribadi.[24] UU PDP secara tegas memuat ketentuan pidana terhadap pelanggaran yang dilakukan oleh korporasi, sebagaimana diatur dalam Pasal 67 ayat (2) yang menyatakan: *"Dalam hal tindak pidana sebagaimana dimaksud pada ayat (1) dilakukan oleh Korporasi, pidana yang dapat dijatuhkan hanya pidana denda paling banyak sepuluh kali dari pidana denda sebagaimana dimaksud pada ayat (1)."*[25] Selain itu, UU PDP juga mengatur sanksi pidana penjara bagi pengurus korporasi yang secara sengaja atau lalai menyebabkan pelanggaran, yang dalam Pasal 70 ayat (1) dinyatakan: *"Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi, dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5,000,000,000.00 (lima miliar rupiah)."*[26] Ketentuan ini memperlihatkan bahwa UU PDP tidak hanya memberikan perlindungan administratif, tetapi juga menegaskan sanksi pidana yang tegas bagi pelaku korporasi.

Selain diatur secara khusus dalam UU PDP, pertanggungjawaban pidana korporasi di Indonesia mendapat legitimasi yuridis dalam KUHP Tahun 2023, khususnya Bab II Bagian Ketiga tentang Tindak Pidana oleh Korporasi yang tertuang dalam Pasal 118 hingga Pasal 124. Pasal 118 ayat (1) KUHP Tahun 2023 menyatakan: *"Korporasi dapat dipidana jika tindak pidana dilakukan untuk dan/atau atas nama korporasi, demi kepentingan korporasi,*

[22] H. S. Disemadi, "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property", *Jurisdictie: Jurnal Hukum dan Syariah* 13, no. 2 (2022): 188–209, https://doi.org/10.18860/j.v13i2.17384.
[23] *Ibid.*
[24] S. A. Kusnadi, "Perlindungan Hukum Data Pribadi sebagai Hak Privasi", *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (April 21, 2021): 9–16, https://doi.org/10.47776/alwasath.v2i1.127.
[25] *Ibid.*
[26] *Ibid.*

atau terjadi karena pembiaran oleh pengurus maupun pengendali korporasi."[27] Selanjutnya, Pasal 119 KUHP Tahun 2023 menegaskan bahwa penuntutan terhadap korporasi tidak menghapuskan pertanggungjawaban pidana individu yang terlibat. Sementara Pasal 121 sampai Pasal 123 KUHP Tahun 2023 mengatur jenis pidana yang dapat dijatuhkan, termasuk pidana denda utama, pidana tambahan berupa perampasan keuntungan, pencabutan izin usaha, atau pembubaran korporasi.[28] Dengan demikian, KUHP Tahun 2023 memberikan landasan umum yang memperkuat penerapan sanksi pidana terhadap pelanggaran UU PDP oleh korporasi, dan kedua instrumen hukum ini saling melengkapi dalam membentuk rezim hukum pidana korporasi di bidang perlindungan data pribadi.

Bila dilihat dari konstruksi hukumnya, sanksi pidana dalam UU PDP dan KUHP bersifat saling menguatkan. UU PDP berfungsi sebagai *lex specialis* yang secara rinci mengatur perbuatan pidana terkait data pribadi, sedangkan KUHP memberikan legitimasi umum dan prinsip dasar pertanggungjawaban pidana korporasi.[29] Sebagai contoh, Pasal 67 ayat (1) UU PDP menentukan bahwa: *"Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5,000,000,000.00 (lima miliar rupiah)."*[30] Jika pelakunya adalah korporasi, maka Pasal 67 ayat (2) menaikkan pidana denda maksimal hingga sepuluh kali lipat. Sementara itu, Pasal 123 KUHP Tahun 2023 mengatur pidana tambahan seperti *"perampasan barang tertentu dan/atau keuntungan yang diperoleh dari tindak pidana, perbaikan akibat tindak pidana, kewajiban mengumumkan putusan hakim, pencabutan izin usaha, atau pembubaran korporasi."*[31] Dengan kombinasi tersebut, hukum pidana Indonesia sebenarnya memiliki instrumen yang memadai untuk menjerat korporasi pelanggar data pribadi secara efektif.

Namun, meskipun instrumen hukumnya telah lengkap, implementasinya tidak dapat dilepaskan dari keberadaan lembaga pengawas yang berfungsi memastikan penegakan aturan berjalan. Pasal 58 UU PDP mengatur pembentukan lembaga independen yang bertugas melakukan pengawasan, meskipun fungsi ini bukanlah inti dari pengaturan pertanggungjawaban pidana, melainkan sarana untuk memastikan penegakan hukum yang optimal.[32] Lembaga tersebut diharapkan mampu mendeteksi, menyelidiki, dan merekomendasikan penindakan terhadap pelanggaran. Tanpa keberadaannya, ancaman pidana yang tegas dalam Pasal 67 sampai Pasal 73 UU PDP dan Pasal 118 sampai Pasal 124 KUHP berisiko tidak dapat diterapkan secara efektif, sehingga melemahkan tujuan perlindungan data pribadi di Indonesia. Dengan kata lain, pengaturan pertanggungjawaban pidana korporasi sudah tegas secara normatif, namun efektivitasnya sangat dipengaruhi oleh dukungan penegakan hukum yang memadai.[33]

Situasi pelik yang dihadapi Indonesia dalam membangun sistem perlindungan data pribadi menjadi semakin terlihat jelas ketika dibandingkan dengan kemapanan sistem yang dimiliki oleh Uni Eropa. *General Data Protection Regulation*, yang mulai berlaku efektif pada 25 Mei 2018, telah diakui secara luas sebagai *gold standard* dalam perlindungan data pribadi di tingkat global. Regulasi ini bukan hanya mengatur secara umum, melainkan membentuk

[27] *UU No. 1 Tahun 2023*, Database Peraturan BPK, 2023, http://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023.
[28] *Ibid.*
[29] J. Isaak, dan M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", *Computer* 51, no. 8 (Agustus 2018): 56–59, https://doi.org/10.1109/MC.2018.3191268.
[30] *Ibid.*
[31] *Ibid.*
[32] *Ibid.*
[33] E. Budi, dkk.

E-ISSN: 2721-7671, DOI: https://doi.org/10.30812/fundamental.v7i1.6237

kerangka hukum substantif dan prosedural yang lengkap, termasuk pengaturan pertanggungjawaban pidana dan sanksi terhadap pelanggaran yang dilakukan oleh korporasi.[34] Salah satu aspek yang menjadi keunggulan utama adalah keberlakuannya yang bersifat *extraterritorial*, sebagaimana ditegaskan dalam *Article 3(2) General Data Protection Regulation*. Ketentuan ini memastikan bahwa subjek hukum di luar Uni Eropa tetap dapat dimintai pertanggungjawaban pidana atau administratif bila memproses data subjek di wilayah Uni Eropa, yang merupakan perluasan yurisdiksi yang tidak ditemukan secara rinci dalam UU PDP Indonesia.[35]

Dari sisi prinsip dasar, *General Data Protection Regulation* memuat ketentuan substantif yang ketat dalam *Article 5(1)* yang menyatakan: *"Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation); (d) accurate and, where necessary, kept up to date; (e) kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation); (f) processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality)."*[36] Prinsip-prinsip ini menjadi dasar untuk menentukan kesalahan korporasi dalam proses pidana. Selanjutnya, mekanisme penjatuhan sanksi diatur secara tegas dalam *Article 83(4)–(6)*, yang menetapkan bahwa pelanggaran tertentu dapat dikenai *"administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover . . . and for certain infringements up to 20,000,000 EUR, or up to 4% of the total worldwide annual turnover, whichever is higher."*[37]

Pengaturan *General Data Protection Regulation* juga memberikan ruang bagi negara anggota untuk mengatur sanksi pidana secara spesifik terhadap pelanggaran perlindungan data pribadi oleh korporasi, sebagaimana tercermin dalam *Article 84(1)* yang menyatakan: *"Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented."*[38] Ketentuan ini berarti bahwa selain sanksi administratif yang berlaku secara seragam di seluruh Uni Eropa, masing-masing negara anggota wajib membentuk aturan pidana yang dapat menjerat korporasi.

Meski fokus utama *General Data Protection Regulation* adalah pada kekuatan pengaturannya yang bersifat komprehensif dan harmonis di seluruh negara anggota, efektivitas penerapannya sangat dipengaruhi oleh keberadaan otoritas pengawas yang berfungsi aktif. Penegakan *General Data Protection Regulation* dilakukan oleh *Data Protection Authorities* (DPAs) di masing-masing negara anggota Uni Eropa, yang keseluruhannya dikoordinasikan oleh *European Data Protection Board*.[39] Lembaga-lembaga ini tidak bersifat pasif, melainkan aktif melakukan pengawasan, investigasi, dan memberikan rekomendasi penindakan, serta memiliki kewenangan penuh untuk menjatuhkan sanksi administratif dalam bentuk denda yang signifikan, yakni sebesar 10 juta hingga 20 juta Euro atau 2% hingga 4% dari omzet global tahunan perusahaan, bergantung pada jenis dan tingkat keparahan

[34] L. Halawi, dan A. Makwana, "The GDPR and U GDPR and Its Impact on US Academic Institutions", *Issues In Information Systems* 24, no. 2 (2023): 232–241, https://doi.org/10.48009/2_iis_2023_120.
[35] G. Greenleaf, dan B. Cottier, "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis", *Computer Law & Security Review* 44 (April 1, 2022): 105638, https://doi.org/10.1016/j.clsr.2021.105638.
[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*
[39] *Ibid.*

pelanggaran.[40] Dengan kata lain, meskipun keunggulan utama Uni Eropa terletak pada substansi pengaturannya, kekuatan pengawasan yang dimilikinya menjadi faktor penentu yang memperkuat posisi *General Data Protection Regulation* sebagai standar global dalam perlindungan data pribadi.

Berbeda dengan Uni Eropa, Amerika Serikat menganut model perlindungan data pribadi sektoral yang berbasis pada penegakan hukum melalui ketentuan pidana dan kewenangan regulator. Hingga kini belum ada undang-undang federal tunggal yang mengatur data secara komprehensif, namun sejumlah ketentuan memberikan dasar hukum bagi pemidanaan korporasi maupun individu. *Federal Trade Commission Act* pada 15 U.S.C. § 45(a)(1) menjadi dasar bagi *Federal Trade Commission* menindak pelanggaran privasi data.[41] Dalam ranah pidana, 18 U.S.C. § 1505 menetapkan pemidanaan bagi pihak yang menghalangi penyelidikan pelanggaran data.[42] Selain itu, 18 U.S.C. § 4 atau *Misprision of Felony* dapat diterapkan pada individu dalam korporasi yang menyembunyikan pelanggaran data.[43]

Bahwa dalam praktik hukum Amerika Serikat, bahkan jika pelanggaran terjadi tanpa niat jahat (*without malicious intent*), pihak yang lalai secara serius (*gross negligence*) atau menunjukkan ketidakpedulian yang sembrono (*reckless disregard*) terhadap kewajiban hukum tetap dapat dimintai pertanggungjawaban pidana.[44] Landasan hukumnya dapat ditemukan, misalnya, pada 18 U.S.C. § 1030(a)(5)(A)–(C) atau *Computer Fraud and Abuse Act*, yang pada huruf (C) secara eksplisit mempidanakan setiap orang, termasuk apabila kerusakan tersebut terjadi *"recklessly"* atau *"negligently"* sebagaimana dijelaskan pada bagian (B) dan (C).[45] Ketentuan ini menunjukkan bahwa *mens rea* yang dipersyaratkan tidak selalu berupa niat jahat, melainkan dapat berupa kelalaian yang signifikan atau tindakan sembrono terhadap kewajiban hukum. Meskipun pengaturannya tersebar di berbagai ketentuan, peran *Federal Trade Commission* sangat krusial karena lembaga ini aktif melakukan investigasi, menginisiasi gugatan, dan memberi rekomendasi penindakan, sehingga kewenangan pidana dan administratifnya saling menguatkan.[46] Keberadaan *Federal Trade Commission* menjadi elemen penting yang menentukan efektivitas penegakan hukum perlindungan data pribadi di Amerika Serikat.

Jika membandingkan pengaturan di Indonesia, Uni Eropa, dan Amerika Serikat, terlihat bahwa perbedaan mendasar bukan hanya terletak pada keberadaan lembaga pengawas, melainkan pada konstruksi normatif yang menentukan luasnya jangkauan pertanggungjawaban pidana korporasi. Uni Eropa melalui *General Data Protection Regulation* memadukan norma substantif yang rinci dengan kewenangan luas bagi otoritas pengawas, sehingga penegakan hukum dapat menjangkau pelaku di luar wilayah yurisdiksinya. Amerika Serikat, meskipun tidak

[40] *Ibid.*

[41] Federal Trade Commission, *Privacy and Security Enforcement*, Oktober 31, 2018, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[42] AP News, "Ex-Uber Security Chief Sentenced for Data-Breach Cover-Up."

[43] BakerHostetler, A. Kaltsounis, dan E. McAndrew, *Former Uber Chief Security Officer Convicted of Federal Obstruction and Concealment Crimes in Connection with Extortionate Data Breach | BakerHostetler - JDSupra*, Oktober 12, 2022, https://www.jdsupra.com/legalnews/former-uber-chief-security-officer-6836316.

[44] C. Nghiem, D. Lopez, dan A. Sievers, "FEDERAL TRADE COMMISSION V. FACEBOOK: A Case Study of the Effects of Antitrust Laws on Consumers' Data Privacy Protection", *The Maastricht Journal of Liberal Arts* 13 (Maret 15, 2022), https://doi.org/10.26481/mjla.2021.v13.855.

[45] *Ibid.*

[46] Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Federal Trade Commission, Juli 24, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

memiliki undang-undang federal tunggal, mengandalkan pendekatan sektoral dengan kombinasi ketentuan pidana dan kewenangan regulator seperti *Federal Trade Commission*, yang bahkan memungkinkan pemidanaan atas kelalaian berat (*gross negligence*) dan *reckless disregard*. Indonesia, melalui KUHP 2023 dan UU PDP, memang telah mengakui pertanggungjawaban pidana korporasi, namun belum sepenuhnya mengatur secara detail tentang standar kesalahan yang mencakup kelalaian berat ataupun mekanisme koordinasi penegakan lintas yurisdiksi.[47]

Prinsip *strict liability* atau tanggung jawab mutlak menjadi benang merah yang menghubungkan sistem hukum Uni Eropa, Amerika Serikat, dan Indonesia dalam pertanggungjawaban pidana korporasi atas kebocoran data pribadi. Ketiganya mengakui bahwa perusahaan digital dapat dimintai pertanggungjawaban tanpa pembuktian unsur kesengajaan.[48] Dalam perspektif teori positivisme hukum *John Austin*, hukum hanya dapat berfungsi efektif apabila memenuhi tiga unsur utama, yaitu (1) adanya perintah yang sah dari penguasa atau otoritas yang berwenang, (2) aturan tertulis yang jelas, dan (3) sanksi yang dapat ditegakkan secara nyata.[49] Uni Eropa memenuhi ketiga unsur tersebut melalui *General Data Protection Regulation* yang berlaku langsung, ditegakkan oleh *Data Protection Authorities* dan *European Data Protection Board*, serta memiliki sanksi tegas.[50] Amerika Serikat menerapkannya secara sektoral melalui *Federal Trade Commission Act* yang memberi *Federal Trade Commission* kewenangan sanksi administratif tanpa pembuktian niat jahat, didukung ketentuan pidana 18 U.S.C. § 1505 dan § 4, sehingga unsur teori Austin terpenuhi.[51] Di Indonesia, meskipun Pasal 57 dan Pasal 67–73 UU PDP telah mengatur tanggung jawab mutlak dan sanksi, ketiadaan lembaga pengawas independen sebagaimana diamanatkan Pasal 58 membuat penegakan lemah dan berpotensi menjadi *lex imperfecta*.[52] Hal ini menunjukkan bahwa keberhasilan penerapan *strict liability* tidak hanya bergantung pada aturan tertulis, tetapi terutama pada keberadaan otoritas penegak hukum yang sah dan efektif.

2. Penerapan Pertanggungjawaban Pidana Korporasi Atas Kasus Kebocoran Data Pribadi di Indonesia Dibandingkan dengan Praktik Penegakan Hukum di Amerika Serikat dan Uni Eropa

Kebocoran data pribadi telah menjadi ancaman serius di era digital. Kejadian-kejadian ini bukan sekadar pelanggaran administratif, melainkan bentuk kelalaian atau pembiaran sistemik oleh korporasi dalam menjaga hak-hak fundamental individu atas privasi, keamanan informasi, dan kendali atas data pribadinya. Untuk itu, pengaturan mengenai pertanggungjawaban pidana korporasi atas pelanggaran ini menjadi elemen penting dalam sistem hukum modern. Kasus kebocoran data Tokopedia pada Mei 2020 menjadi salah satu insiden terbesar di Indonesia, di mana lebih dari 91 juta akun pengguna mengalami kebocoran, dengan data seperti nama, *email*,

[47] G. Halbert, S. Rusdiana, dan R. H. Hutauruk, "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia", *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, no. 3 (Desember 21, 2023): 304–321, https://doi.org/10.55809/tora.v9i3.275.

[48] G. Bimantara, T. A. Handayani, dan M. A. Y. A. Irsyad, "The Corporate Legal Responsibility for The Leak of Personal Data of Application Consumers in Indonesia", *JURNAL AKTA* 11, no. 4 (Desember 6, 2024): 1213–1221, https://doi.org/10.30659/akta.v11i4.41409.

[49] A. A. T. Ananda, "Teori Positivisme Hukum", *Jurnal Penelitian Ilmiah Multidisiplin* 8, no. 11 (2024): 60–69, https://sejurnal.com/pub/index.php/jpim/article/download/5130/5983/10353.

[50] W. Li, dan D. Yang, "Decentralized but Coordinated", dalam *Global Digital Data Governance*, 1st ed., by C. Aguerre, M. Campbell-Verduyn, dan J. A. Scholte (London: Routledge, Januari 3, 2024), 105–124, ISBN: 978-1-003-38841-8, https://doi.org/10.4324/9781003388418-9.

[51] *Ibid.*

[52] A. Yesidora, *Lembaga Pengawas Data Belum Dibentuk, Komdigi Buat Ditjen Khusus*, katadata.co.id, 2024, https://katadata.co.id/digital/teknologi/6731e7ba7b77b/lembaga-pengawas-data-belum-dibentuk-komdigi-buat-ditjen-khusus.

nomor telepon, tanggal lahir, dan *user ID* diperjualbelikan di forum *dark web* oleh peretas bernama samaran *ShinyHunters*. Meskipun pihak Tokopedia menyatakan data pembayaran tidak terdampak, kebocoran tersebut tetap menimbulkan risiko pencurian identitas dan penipuan digital.[53] Namun yang mengkhawatirkan, hingga kini tidak tercatat adanya sanksi pidana maupun administratif yang dijatuhkan kepada Tokopedia atas insiden tersebut, sehingga menimbulkan kesan lemahnya penegakan hukum dalam perlindungan data pribadi di Indonesia.[54] Padahal, Pasal 67 ayat (2) UU PDP secara tegas mengatur ancaman pidana penjara hingga lima tahun dan/atau denda maksimal Rp5,000,000,000.00 bagi pelaku yang dengan sengaja dan tanpa hak mengungkapkan data pribadi, dan ketentuan tersebut juga berlaku untuk korporasi karena UU PDP tidak membedakan antara perorangan dan badan hukum.[55] Namun, ketiadaan lembaga pengawas independen yang diamanatkan Pasal 58 UU PDP menjadikan ketentuan tersebut tidak operatif secara nyata, sehingga UU PDP cenderung hanya berfungsi sebagai perangkat hukum formal tanpa kekuatan implementatif yang efektif.[56]

Ketimpangan ini semakin nyata jika dibandingkan dengan dua kasus besar di negara maju yang telah memiliki sistem penegakan hukum lebih kuat, yakni kasus Uber Technologies di Amerika Serikat dan kasus Vastaamo di Uni Eropa. Salah satu kasus kebocoran data terbesar di Amerika Serikat menimpa Uber Technologies Inc., ketika pada 2016 peretas mencuri data pribadi sekitar 57 juta pengguna dan mitra pengemudi, termasuk nama, *email*, nomor telepon, dan lisensi kendaraan.[57] Alih-alih melaporkan insiden sesuai kewajiban hukum, *Chief Security Officer* Uber, *Joseph Sullivan*, justru menyembunyikannya dengan membayar USD 100,000 kepada peretas melalui program *bug bounty* dan meminta mereka menandatangani perjanjian kerahasiaan tanpa bukti teknis bahwa data telah dihapus.[58] Kasus ini terungkap pada 2017 setelah CEO baru *Dara Khosrowshahi* melaporkannya kepada publik dan otoritas, memicu penyelidikan *Department of Justice* dan *Federal Trade Commission*. Pelanggaran ini diperburuk oleh riwayat teguran *Federal Trade Commission* pada 2014 terkait kelemahan sistem keamanan Uber, yang telah mewajibkan perusahaan menerapkan program privasi menyeluruh dan audit independen selama 20 tahun.[59] Kegagalan memenuhi komitmen tersebut membuat kasus ini semakin berat, sehingga pada 2023 *Joseph Sullivan* divonis bersalah atas *obstruction of justice* dan *misprision of felony* dengan hukuman tiga tahun masa percobaan, 200 jam kerja sosial, dan denda USD 50,000.[60] Uber sebagai korporasi juga didenda USD 148,000,000.00 oleh 50 jaksa agung negara bagian dan Washington DC serta diwajibkan melakukan reformasi keamanan dan audit selama 20 tahun. Kasus ini menunjukkan bahwa baik kelalaian sistemik maupun upaya

[53] D. Komalawati, M. Dewi M R, dan R. D. Kartika, "Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data", *Jurnal Health Sains* 2, no. 1 (Januari 23, 2021): 49–56, https://doi.org/10.46799/jsa.v2i1.167.

[54] A. Sylfia dkk. "Tanggungjawab Yuridis PT. Tokopedia Atas Kebocoran Data Pribadi Dan Privasi Konsumen Dalam Transaksi Online", *Bhirawa Law Journal* 2, no. 1 (Mei 31, 2021): 21–27, https://doi.org/10.26905/blj.v2i1.5850.

[55] *Ibid.*

[56] J. N. Saly dkk. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022", *Jurnal Serina Sosial Humaniora* 1, no. 3 (Oktober 18, 2023): 145–153, https://journal.untar.ac.id/index.php/JSSH/article/view/28615.

[57] U.S. Department of Justice, *Former Chief Security Officer of Uber Sentenced to Three Years' Probation for Covering Up Data Breach Involving Millions of Uber User Records*, Mei 5, 2023, https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data.

[58] K. Mandarano, *When in Doubt, Report It Out: What Uber's Ex-CSO's Conviction Means for Companies' Mandatory Reporting Duties Following a Data Breach*, University of Maryland Francis King Carey School of Law, 2023, https://www.law.umaryland.edu/content/articles/name-659560-en.html.

[59] Federal Trade Commission, *Privacy and Security Enforcement*, Oktober 31, 2018, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[60] *Ibid.*

E-ISSN: 2721-7671, DOI: https://doi.org/10.30812/fundamental.v7i1.6237

menutupi pelanggaran dapat menimbulkan sanksi pidana bagi individu dan sanksi administratif bagi korporasi. Hal ini juga membuktikan bahwa meskipun Amerika Serikat belum memiliki regulasi federal komprehensif untuk perlindungan data pribadi seperti *General Data Protection Regulation*, keberadaan *Federal Trade Commission* terbukti efektif menegakkan aturan perlindungan privasi.[61]

Salah satu kasus pelanggaran data pribadi paling serius di Uni Eropa menimpa Vastaamo, perusahaan layanan kesehatan mental di Finlandia, ketika pada Maret 2019 peretas mencuri data sensitif lebih dari 33,000 pasien, termasuk nama, nomor identitas, catatan terapi, dan diagnosis psikologis, namun perusahaan tidak segera melaporkannya sebagaimana diwajibkan *General Data Protection Regulation*.[62] Serangan kedua pada Maret 2020 menyebabkan kebocoran lebih luas, dan pada Oktober 2020 pelaku memeras pasien dengan ancaman menyebarkan catatan terapi jika tebusan kripto tidak dibayar, menimbulkan kepanikan publik.[63] Investigasi *Office of the Data Protection Ombudsman* mengungkap kelalaian serius, termasuk ketiadaan enkripsi dan pembaruan sistem, sehingga perusahaan dijatuhi sanksi administratif sebesar 608,000 euro sesuai Pasal 83 *General Data Protection Regulation*.[64] Mantan CEO *Ville Tapio* dijatuhi hukuman percobaan tiga bulan penjara karena gagal bertindak, sementara pelaku utama *Aleksanteri Julius Kivimäki* dipenjara enam tahun tiga bulan atas peretasan dan pemerasan.[65] Kasus ini menunjukkan bahwa *General Data Protection Regulation* tidak hanya merupakan norma tertulis, tetapi ditegakkan secara efektif dengan sanksi administratif bagi korporasi dan pidana bagi individu yang bertanggung jawab, sehingga memastikan perlindungan data pribadi melalui mekanisme penegakan yang nyata.[66]

Penerapan tanggung jawab pidana terhadap perusahaan dalam kasus kebocoran data pribadi sejatinya mencerminkan pergeseran paradigma hukum pidana kontemporer, di mana subjek hukum tidak lagi terbatas pada individu, melainkan juga entitas hukum yang secara nyata memiliki kontrol dan tanggung jawab atas sistem informasi serta keamanan data. Dalam konteks ini, teori *strict liability* dan teori positivisme berperan penting dalam menjelaskan cara negara-negara seperti Indonesia, Amerika Serikat, dan Uni Eropa memberikan sanksi terhadap pelanggaran yang melibatkan perusahaan digital.

Prinsip *strict liability* menempatkan tanggung jawab hukum langsung pada korporasi tanpa perlu pembuktian unsur kesengajaan atau kelalaian (*mens rea*). Dalam konteks kebocoran data, prinsip ini penting karena kerusakan sering disebabkan oleh kelalaian sistem keamanan atau ketidakpatuhan terhadap standar perlindungan, meskipun tanpa niat jahat manajemen. Penerapan prinsip ini terlihat jelas dalam kasus Uber Technologies Inc. di Amerika Serikat pada 2016 yang mengalami kebocoran data yang mengekspos informasi pribadi 57 juta pengguna dan mitra pengemudi. Berdasarkan Section 5 *Federal Trade Commission Act*, Uber tetap dikenai sanksi meski tidak ditemukan bukti niat jahat, karena gagal melindungi konsumen. *Joseph Sullivan* dijatuhi hukuman tiga tahun masa percobaan dan denda USD 50,000, sedangkan Uber membayar denda administratif sebesar USD 148,000,000.00 kepada 50 jaksa agung negara bagian dan diwajibkan memperkuat program keamanan data dengan audit selama 20

[61] *Ibid.*

[62] European Data Protection Board, *Guidelines on the Application of GDPR*, https://www.edpb.europa.eu/edpb_en.

[63] P. Paganini, *Finnish Hacker Sentenced to More Than Six Years in Prison*, April 30, 2024, https://securityaffairs.com/162571/cyber-crime/finnish-hacker-sentenced-6-years-prison.html.

[64] D. Bennett, *A Psychotherapy Hack in Finland: Crime Leaves Patients Exposed*, Bloomberg, Mei 9, 2024, https://www.bloomberg.com/news/newsletters/2024-05-09/a-psychotherapy-hack-in-finland-crime-leaves-patients-exposed.

[65] *Ibid.*

[66] S. Shreya, *Guide to GDPR Fines and Penalties | 20 Biggest Fines So Far [2025]*, CookiesYes, 2025, https://www.cookieyes.com/blog/gdpr-fines/.

tahun.[67] Penerapan prinsip *strict liability* pada kasus Uber menunjukkan bahwa meskipun tidak ada bukti niat jahat, tanggung jawab hukum tetap dibebankan karena kelalaian pelaporan dan perlindungan data. Hal ini dimungkinkan berkat kewenangan *Federal Trade Commission* yang dapat menindak pelanggaran privasi tanpa aduan korban, membuktikan bahwa *strict liability* efektif diterapkan jika didukung otoritas penegak yang kuat.[68]

Di Uni Eropa, prinsip *strict liability* ditegakkan melalui *General Data Protection Regulation*. Kasus Vastaamo di Finlandia menjadi bukti nyata penerapan prinsip *strict liability* secara menyeluruh. Investigasi mengungkap bahwa Vastaamo gagal mengenkripsi data dan memperbarui sistem, sehingga dijatuhi denda administratif sebesar €608,000 berdasarkan Pasal 83 *General Data Protection Regulation* tanpa perlu pembuktian niat atau kelalaian.[69] Hal ini menegaskan bahwa pelanggaran terhadap kewajiban perlindungan data pribadi secara faktual sudah cukup untuk menimbulkan pertanggungjawaban hukum berdasarkan prinsip *strict liability*.[70] Meskipun pelanggaran terjadi secara sistemik melalui kelalaian perusahaan, mantan CEO Vastaamo, yaitu *Ville Tapio*, tetap dijatuhi hukuman percobaan tiga bulan karena tidak segera melakukan mitigasi, sementara peretas *Aleksanteri Julius Kivimäki* dipenjara enam tahun tiga bulan. Kasus ini menunjukkan bahwa Uni Eropa menerapkan *strict liability* baik secara administratif maupun pidana, dengan sanksi dijatuhkan semata-mata karena lalai menjalankan tanggung jawab manajerialnya.[71] Prinsip *strict liability* diakomodasi secara eksplisit dalam *General Data Protection Regulation*. Otoritas perlindungan data memiliki kewenangan untuk menjatuhkan sanksi administratif berdasarkan Pasal 83 *General Data Protection Regulation* tanpa harus membuktikan adanya unsur niat atau kelalaian. Dalam praktiknya, sanksi dijatuhkan semata-mata karena pelanggaran terhadap kewajiban perlindungan data, seperti tidak melaporkan insiden atau tidak menyediakan sistem keamanan yang memadai. Penerapan ini membuktikan bahwa *strict liability* di Uni Eropa tidak hanya menjadi prinsip normatif, tetapi telah dioperasionalkan secara konkret oleh lembaga pengawas di masing-masing negara anggota.[72]

Sementara itu, jika dibandingkan dengan kasus Tokopedia di Indonesia, tampak perbedaan yang jelas dalam hal implementasi tanggung jawab pidana korporasi. Dalam insiden kebocoran data Tokopedia 2020, lebih dari 91 juta akun pengguna dilaporkan terkena kebocoran dan datanya dijual oleh peretas di forum gelap.[73] Secara faktual, peristiwa ini mencerminkan kegagalan perusahaan dalam melindungi sistem keamanan data pengguna, yang berdasarkan prinsip *strict liability* seharusnya memadai untuk dikenakan sanksi pidana atau administratif. Namun, dalam praktiknya, tidak ada langkah hukum pidana yang diambil terhadap Tokopedia sebagai sebuah perusahaan, dan tanggung jawab dibiarkan tanpa penerapan yang nyata. Dalam perspektif *strict liability*, tanggung jawab Tokopedia seharusnya timbul bukan karena terbukti melanggar secara sadar, melainkan karena sebagai pengelola data, perusahaan tidak memenuhi standar minimum perlindungan data yang ditetapkan oleh sistem hukum.[74] Fakta bahwa tidak ada penegakan hukum menunjukkan bahwa prinsip *strict liability* belum berfungsi

[67] *Ibid.*
[68] A. Sinduningrum, dan H. Marlyna, "Penerapan Strict Liability Dalam Hukum Pelindungan Konsumen Di Indonesia: Perbandingan Negara Lain", *UNES Law Review* 6, no. 2 (Desember 11, 2023): 5021–5030, https://doi.org/10.31933/unesrev.v6i2.1321.
[69] *Ibid.*
[70] *Ibid.*
[71] *Ibid.*
[72] *Ibid.*
[73] *Ibid.*
[74] Perkasa dan Saly, "Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection."

optimal sebagai dasar utama dalam praktik penegakan hukum terhadap perusahaan digital di Indonesia.[75]

Dalam konteks teori positivisme hukum yang diusulkan oleh *John Austin*, hukum yang dianggap sah dan efektif harus memenuhi tiga elemen utama, yaitu otoritas yang sah dalam merumuskan hukum, norma hukum yang terdokumentasi dan jelas, serta kemampuan untuk menegakkan hukum melalui sanksi yang nyata.[76] Uni Eropa dan Amerika Serikat, dalam dua contoh tersebut, telah membuktikan bahwa undang-undang perlindungan data mereka berfungsi dalam konteks ini. *General Data Protection Regulation* dari Uni Eropa dan *Federal Trade Commission Act* dari Amerika Serikat memiliki efek yang signifikan karena didukung oleh badan yang memiliki kekuatan untuk menegakkan serta mekanisme yang dapat memberikan sanksi tanpa perlu membuktikan elemen kesalahan subjektif.[77]

Dengan demikian, pembandingan kasus-kasus tersebut memperlihatkan bahwa prinsip *strict liability* dan teori positivisme hukum bukan hanya konsep akademik, tetapi merupakan alat penting dalam menjamin efektivitas hukum pidana korporasi di ranah perlindungan data. Keberhasilan penerapan pertanggungjawaban pidana korporasi di Uni Eropa dan Amerika Serikat menegaskan bahwa prinsip tersebut harus diadopsi sebagai dasar reformasi penegakan hukum di Indonesia agar hak privasi masyarakat terlindungi secara efektif di tengah perkembangan teknologi digital.[78]

3. Implikasi Perbandingan Pengaturan dan Penerapan Pertanggungjawaban Pidana Korporasi Tersebut bagi Penguatan Regulasi Serta Lembaga Pengawas Perlindungan Data Pribadi di Indonesia

Hasil perbandingan pengaturan dan penerapan pertanggungjawaban pidana korporasi atas kebocoran data pribadi di Amerika Serikat, Uni Eropa, dan Indonesia menunjukkan faktor kunci yang memengaruhi efektivitas perlindungan data pribadi. Amerika Serikat dan Uni Eropa membuktikan bahwa regulasi yang jelas saja tidak cukup. Faktor kelembagaan, kapasitas pengawasan, serta kemampuan menjatuhkan sanksi yang tegas dan konsisten menjadi unsur yang tidak terpisahkan dari keberhasilan penegakan hukum di kedua wilayah tersebut.[79]

Di Amerika Serikat, meskipun tidak ada undang-undang federal tunggal yang mengatur perlindungan data pribadi secara menyeluruh, sistem hukum tetap berjalan efektif melalui pendekatan sektoral yang terdesentralisasi. *Federal Trade Commission* menjadi contoh lembaga pengawas independen yang memegang peran sentral dalam memastikan kepatuhan perusahaan terhadap standar perlindungan data. *Federal Trade Commission* memiliki kewenangan untuk menyelidiki, menggugat, menjatuhkan sanksi administratif, dan mengawasi pelaksanaan kewajiban perbaikan jangka panjang. Dalam kasus Uber Technologies, *Federal Trade Commission* bersama *Department of Justice* Amerika Serikat menjatuhkan denda administratif besar dan menetapkan kewajiban audit keamanan selama 20 tahun. Langkah ini menunjukkan bahwa keberhasilan penegakan hukum bergantung pada

[75] P. Purwoto dkk. "Corporate Responsibility For Personal Data Breach Cases", *International Journal of Multidisciplinary Research and Analysis* 06, no. 06 (Juni 22, 2023), https://doi.org/10.47191/ijmra/v6-i6-75.

[76] *Ibid.*

[77] A. Malik, S. Sanusi, dan F. Sudewo, "Corporate Strict Liability in Environmental Crimes in Indonesia and the Netherlands", Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, MALAPY 2022, 28 May 2022, Tegal, Indonesia (Agustus 15, 2022), ISBN: 978-1-63190-362-5, https://eudl.eu/doi/10.4108/eai.28-5-2022.2320558.

[78] G. Buckley, T. Caulfield, dan I. Becker, "GDPR and the Indefinable Effectiveness of Privacy Regulators: Can Performance Assessment Be Improved?", *Journal of Cybersecurity* 10, no. 1 (Januari 2, 2024): tyae017, https://doi.org/10.1093/cybsec/tyae017.

[79] K. Houser, dan W. G. Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, SSRN Scholarly Paper, 3212210, Rochester, NY, Juli 11, 2018, https://doi.org/10.2139/ssrn.3212210, Social Science Research Network: 3212210.

kemampuan lembaga pengawas menggabungkan fungsi penindakan dan pengawasan jangka panjang. Keberhasilan di Amerika Serikat juga terletak pada sifat proaktif lembaga pengawas dalam mendeteksi pelanggaran. *Federal Trade Commission* tidak menunggu laporan korban atau pengaduan resmi, tetapi memulai investigasi berdasarkan indikasi pelanggaran yang ditemukan.

Uni Eropa memberikan contoh berbeda namun sama efektifnya. *General Data Protection Regulation* berlaku langsung di seluruh negara anggota dan memastikan aturan perlindungan data pribadi yang seragam, jelas, dan memiliki mekanisme sanksi yang kuat. Setiap negara anggota memiliki *Data Protection Authorities* (DPAs) yang berwenang penuh untuk menyelidiki, menjatuhkan denda besar, dan merekomendasikan penuntutan pidana terhadap individu atau korporasi. Struktur ini dikoordinasikan oleh *European Data Protection Board* agar penegakan *General Data Protection Regulation* konsisten di seluruh wilayah Uni Eropa. Kasus Vastaamo di Finlandia membuktikan efektivitas sistem tersebut. Perusahaan dijatuhi denda besar, mantan CEO dikenai hukuman pidana, dan pelaku peretasan dipenjara. Penindakan dilakukan terhadap korporasi dan individu sekaligus. Pendekatan ini mendorong akuntabilitas personal di samping tanggung jawab korporasi. Indonesia dapat meniru model ini agar penegakan tidak hanya berhenti pada entitas perusahaan, tetapi juga menyentuh pengambil keputusan yang lalai.

Perbedaan utama Indonesia terletak pada kelembagaan dan penegakan hukum. UU PDP sudah memuat ketentuan pidana dan administratif, tetapi belum ada lembaga pengawas independen sebagaimana diamanatkan Pasal 58. Kondisi ini melemahkan daya paksa UU PDP. Kasus kebocoran data Tokopedia membuktikan bahwa tanpa otoritas pengawas yang memiliki kewenangan penuh, pelanggaran besar tidak diikuti tindakan hukum yang berarti. Pembentukan lembaga pengawas independen menjadi langkah prioritas. Lembaga ini harus memiliki kewenangan untuk menyelidiki, menjatuhkan sanksi administratif, merekomendasikan penuntutan pidana, dan memantau kepatuhan jangka panjang. Kapasitas teknis juga harus memadai untuk mengidentifikasi kerentanan sistem keamanan dan memberikan instruksi perbaikan yang mengikat secara hukum.

Dari perbandingan antara Amerika Serikat, Uni Eropa, dan Indonesia, terlihat jelas bahwa keberhasilan perlindungan data pribadi tidak hanya bergantung pada kekuatan regulasi, tetapi juga pada keberadaan lembaga pengawas yang independen, tegas, dan memiliki kewenangan penuh. Indonesia sudah memiliki kerangka hukum melalui UU PDP, namun tanpa lembaga pengawas yang berfungsi efektif, aturan tersebut berisiko menjadi sekadar teks hukum tanpa daya paksa. Pembentukan lembaga pengawas independen yang mampu menyelidiki, menindak, memberikan sanksi, serta bekerja sama dengan otoritas internasional menjadi syarat mutlak agar perlindungan data pribadi benar-benar terlaksana.[80] Tanpa langkah ini, kebocoran data akan terus terjadi tanpa akuntabilitas yang jelas, kepercayaan publik akan menurun, dan hak privasi masyarakat akan tetap rentan di tengah pesatnya perkembangan dunia digital.

KESIMPULAN

Penelitian ini menegaskan bahwa maraknya kebocoran data pribadi di era digital, sebagaimana tercermin dalam kasus Tokopedia, bukan semata persoalan teknis keamanan siber, melainkan menunjukkan adanya kelemahan struktural dalam sistem penegakan hukum perlindungan data di Indonesia. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah mengatur sanksi administratif dan pidana,

[80] R. Budiman, "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022", *Jurnal Smart Hukum (JSH)* 2, no. 1 (September 30, 2023): 24–36, https://doi.org/10.55299/jsh.v2i1.1352.

efektivitasnya belum optimal karena ketiadaan lembaga pengawas independen sebagaimana diamanatkan Pasal 58. Perbandingan dengan praktik di Amerika Serikat dan Uni Eropa memperlihatkan bahwa keberhasilan perlindungan data pribadi sangat ditentukan oleh keberadaan otoritas pengawas yang mandiri, aktif, dan memiliki kewenangan tegas. Di Amerika Serikat, peran *Federal Trade Commission* melalui pendekatan sektoral terbukti mampu menciptakan efek jera, misalnya dalam penanganan kasus Uber, sementara di Uni Eropa, efektivitas *General Data Protection Regulation* tercermin dari kemampuan otoritasnya menjatuhkan sanksi signifikan, termasuk dalam kasus Vastaamo.

Secara konseptual, temuan ini memperkuat relevansi teori pertanggungjawaban pidana korporasi yang menempatkan korporasi sebagai subjek hukum yang dapat dimintai pertanggungjawaban atas perbuatan yang dilakukan untuk kepentingannya, serta selaras dengan pandangan positivisme hukum *John Austin* yang menekankan bahwa efektivitas hukum ditentukan oleh keberadaan otoritas yang sah, norma yang jelas, dan sanksi yang dapat ditegakkan. Dalam konteks Indonesia, dua unsur pertama telah terpenuhi, namun aspek penegakan masih lemah akibat belum terbentuknya institusi pengawas yang berfungsi secara efektif. Selain itu, penerapan prinsip *strict liability* sebagai dasar pertanggungjawaban mutlak dalam pelanggaran data pribadi belum dijalankan secara konsisten, berbeda dengan praktik di Uni Eropa dan Amerika Serikat yang telah menggunakannya secara progresif untuk memastikan akuntabilitas korporasi tanpa bergantung pada pembuktian unsur kesalahan subjektif.

Dengan demikian, penguatan sistem perlindungan data pribadi di Indonesia menuntut reformasi kelembagaan yang konkret melalui pembentukan lembaga pengawas independen yang memiliki kewenangan penyelidikan, penjatuhan sanksi administratif, serta koordinasi penegakan pidana. Tanpa keberadaan institusi tersebut, norma dalam UU PDP berpotensi menjadi *lex imperfecta*, yaitu aturan yang tidak memiliki daya paksa dalam praktik. Di samping itu, diperlukan penguatan pola penegakan hukum yang bersifat proaktif melalui kombinasi sanksi administratif dan pidana secara simultan, serta peningkatan literasi digital bagi masyarakat dan pelaku usaha agar tercipta kesadaran hukum yang lebih luas. Dengan langkah tersebut, sistem perlindungan data pribadi di Indonesia tidak hanya berhenti pada tataran normatif, tetapi benar-benar mampu memberikan jaminan perlindungan yang efektif dan berkelanjutan.

DAFTAR PUSTAKA

Ananda, A. A. T. "Teori Positivisme Hukum". *Jurnal Penelitian Ilmiah Multidisiplin* 8, no. 11 (2024): 60–69. https://sejurnal.com/pub/index.php/jpim/article/download/5130/5983/10353.

AP News. *Ex-Uber Security Chief Sentenced for Data-Breach Cover-Up*, Mei 5, 2023. https://apnews.com/article/uber-data-breach-coverup-sentenced-san-francisco-05b2ded36daf55012f03651cf2c7c931.

Arsjad, J., S. D. Rosadi, dan R. R. Permata. "Pengaturan Dan Tanggung Jawab Penyedia Jasa Layanan Komputasi Awan (Cloud Computing) Atas Penyimpanan Data Pribadi Pengguna Dari Kebocoran Data Elektronik". *JIHK* 2, no. 1 (Juli 30, 2020): 97–106. https://doi.org/10.46924/jihk.v2i1.136.

Azhar, D. P., dan A. Mahyani. "Pertanggungjawaban Pidana Korporasi sebagai Pelaku Tindak Pidana Penyebaran Data Pribadi". *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 3, no. 1 (2023): 540–558. https://doi.org/10.53363/bureau.v3i1.200.

BakerHostetler, A. Kaltsounis, dan E. McAndrew. *Former Uber Chief Security Officer Convicted of Federal Obstruction and Concealment Crimes in Connection with Extortionate Data Breach | BakerHostetler - JDSupra*, Oktober 12, 2022. https://www.jdsupra.com/legalnews/former-uber-chief-security-officer-6836316.

Bennett, D. *A Psychotherapy Hack in Finland: Crime Leaves Patients Exposed*. Bloomberg, Mei 9, 2024. https://www.bloomberg.com/news/newsletters/2024-05-09/a-psychotherapy-hack-in-finland-crime-leaves-patients-exposed.

Bimantara, G., T. A. Handayani, dan M. A. Y. A. Irsyad. "The Corporate Legal Responsibility for The Leak of Personal Data of Application Consumers in Indonesia". *JURNAL AKTA* 11, no. 4 (Desember 6, 2024): 1213–1221. https://doi.org/10.30659/akta.v11i4.41409.

Buckley, G., T. Caulfield, dan I. Becker. "GDPR and the Indefinable Effectiveness of Privacy Regulators: Can Performance Assessment Be Improved?" *Journal of Cybersecurity* 10, no. 1 (Januari 2, 2024): tyae017. https://doi.org/10.1093/cybsec/tyae017.

Budi, E., D. Wira, dan A. Infantono. "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0". *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* 3 (Desember 21, 2021): 223–234. https://doi.org/10.54706/senastindo.v3.2021.141.

Budiman, R. "The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022". *Jurnal Smart Hukum (JSH)* 2, no. 1 (September 30, 2023): 24–36. https://doi.org/10.55299/jsh.v2i1.1352.

CNN Indonesia. *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*, 2020. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

Davison, C. B., dkk. "Data Privacy in the Age of Big Data Analytics". *Issues In Information Systems* 22, no. 2 (2021): 177–186. https://doi.org/10.48009/2_iis_2021_185-195.

Disemadi, H. S. "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property". *Jurisdictie: Jurnal Hukum dan Syariah* 13, no. 2 (2022): 188–209. https://doi.org/10.18860/j.v13i2.17384.

European Data Protection Board. *Guidelines on the Application of GDPR*. https://www.edpb.europa.eu/edpb_en.

Federal Trade Commission. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Federal Trade Commission, Juli 24, 2019. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

Federal Trade Commission. *Privacy and Security Enforcement*, Oktober 31, 2018. https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

Ghanbari, H., dan K. Koskinen. "When Data Breach Hits a Psychotherapy Clinic: The Vastaamo Case". *Journal of Information Technology Teaching Cases*, Juni 7, 2024, 20438869241258235. https://doi.org/10.1177/20438869241258235.

Greenleaf, G., dan B. Cottier. "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis". *Computer Law & Security Review* 44 (April 1, 2022): 105638. https://doi.org/10.1016/j.clsr.2021.105638.

Halawi, L., dan A. Makwana. "The GDPR and U GDPR and Its Impact on US Academic Institutions". *Issues In Information Systems* 24, no. 2 (2023): 232–241. https://doi.org/10.48009/2_iis_2023_120.

Halbert, G., S. Rusdiana, dan R. H. Hutauruk. "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia". *Jurnal Hukum to-ra : Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, no. 3 (Desember 21, 2023): 304–321. https://doi.org/10.55809/tora.v9i3.275.

Houser, K., dan W. G. Voss. *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?* SSRN Scholarly Paper, 3212210, Rochester, NY, Juli 11, 2018. https://doi.org/10.2139/ssrn.3212210. Social Science Research Network: 3212210.

International Telecommunication Union. *Measuring Digital Development: Facts and Figures 2024*, 2024. https://www.itu.int:443/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx.

Isaak, J., dan M. J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". *Computer* 51, no. 8 (Agustus 2018): 56–59. https://doi.org/10.1109/MC.2018.3191268.

Joel, O. T., dan V. U. Oguanobi. "Data-Driven Strategies for Business Expansion: Utilizing Predictive Analytics for Enhanced Profitability and Opportunity Identification". *International Journal of Frontiers in Engineering and Technology Research* 6, no. 2 (Mei 30, 2024): 071–081. https://doi.org/10.53294/ijfetr.2024.6.2.0035.

Komalawati, D., M. Dewi M R, dan R. D. Kartika. "Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data". *Jurnal Health Sains* 2, no. 1 (Januari 23, 2021): 49–56. https://doi.org/10.46799/jsa.v2i1.167.

Kusnadi, S. A. "Perlindungan Hukum Data Pribadi sebagai Hak Privasi". *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (April 21, 2021): 9–16. https://doi.org/10.47776/alwasath.v2i1.127.

Li, W., dan D. Yang. "Decentralized but Coordinated". Dalam *Global Digital Data Governance*, 1st ed., by C. Aguerre, M. Campbell-Verduyn, dan J. A. Scholte, 105–124. London: Routledge, Januari 3, 2024. ISBN: 978-1-003-38841-8. https://doi.org/10.4324/9781003388418-9.

Malik, A., S. Sanusi, dan F. Sudewo. "Corporate Strict Liability in Environmental Crimes in Indonesia and the Netherlands". Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, MALAPY 2022, 28 May 2022, Tegal, Indonesia. Agustus 15, 2022. ISBN: 978-1-63190-362-5. https://eudl.eu/doi/10.4108/eai.28-5-2022.2320558.

Mandarano, K. *When in Doubt, Report It Out: What Uber's Ex-CSO's Conviction Means for Companies' Mandatory Reporting Duties Following a Data Breach*. University of Maryland Francis King Carey School of Law, 2023. https://www.law.umaryland.edu/content/articles/name-659560-en.html.

Mascellino, A. *Data Breaches Rise By 70% Globally in Q3 2022*. Infosecurity Magazine, Oktober 25, 2022. https://www.infosecurity-magazine.com/news/data-breaches-rise-by-70-q3-2022/.

Muzakkie, S. A., dan E. Juarsa. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Pada Aplikasi Pinjaman Online Ilegal Menurut Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi". *Bandung Conference Series: Law Studies* 3, no. 2 (Agustus 1, 2023): 984–987. https://doi.org/10.29313/bcsls.v3i2.7284.

Nghiem, C., D. Lopez, dan A. Sievers. "FEDERAL TRADE COMMISSION V. FACEBOOK: A Case Study of the Effects of Antitrust Laws on Consumers' Data Privacy Protection". *The Maastricht Journal of Liberal Arts* 13 (Maret 15, 2022). https://doi.org/10.26481/mjla.2021.v13.855.

Otoritas Jasa Keuangan (OJK). *Roadmap Penguatan Bank Pembangunan Daerah 2024-2027*. Jakarta, 2024. https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Roadmap%20Penguatan%20Bank%20Pembangunan%20Daerah%202024-2027.pdf.

Paganini, P. *Finnish Hacker Sentenced to More Than Six Years in Prison*, April 30, 2024. https://securityaffairs.com/162571/cyber-crime/finnish-hacker-sentenced-6-years-prison.html.

Panjaitan, R. M. "Pertanggungjawaban Pidana Korporasi Sebagai Penyelenggara Sistem Elektronik Dalam Terjadinya Kebocoran Data Pengguna Sistem Elektronik". *Jurnal Hukum Adigama* 4, no. 2 (2021): 2624–2643. https://doi.org/10.24912/adigama.v4i2.17761.

Perkasa, J., dan J. N. Saly. "Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020):" 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021). Jakarta, Indonesia, 2022. https://doi.org/10.2991/assehr.k.220404.096.

Primanta, A. I. "Pertanggungjawaban Pidana Pada Penyalahgunaan Data Pribadi". *Jurist-Diction* 3, no. 4 (Juni 28, 2020): 1431. https://doi.org/10.20473/jd.v3i4.20214.

Purwoto, P., dkk. "Corporate Responsibility For Personal Data Breach Cases". *International Journal of Multidisciplinary Research and Analysis* 06, no. 06 (Juni 22, 2023). https://doi.org/10.47191/ijmra/v6-i6-75.

Rahmawati, D., M. D. A. Aksana, dan S. Mukaromah. "Privasi Dan Keamanan Data Di Media Sosial: Dampak Negatif Dan Strategi Pencegahan". *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* 3, no. 1 (November 11, 2023): 571–580. https://doi.org/10.33005/sitasi.v3i1.354.

Rochman, H. N., B. K. Heriawanto, dan I. K. Ayu. "Tanggung Gugat Penyedia Platform Marketplace Terhadap Kebocoran Data Pribadi Konsumen Pengguna Platform Marketplace Di Indonesia". *Dinamika* 27, no. 2 (Januari 19, 2021): 237–250. https://jim.unisma.ac.id/index.php/jdh/article/view/9392.

Saly, J. N., dkk. "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022". *Jurnal Serina Sosial Humaniora* 1, no. 3 (Oktober 18, 2023): 145–153. https://journal.untar.ac.id/index.php/JSSH/article/view/28615.

Shreya, S. *Guide to GDPR Fines and Penalties | 20 Biggest Fines So Far [2025]*. CookiesYes, 2025. https://www.cookieyes.com/blog/gdpr-fines/.

Sinduningrum, A., dan H. Marlyna. "Penerapan Strict Liability Dalam Hukum Pelindungan Konsumen Di Indonesia: Perbandingan Negara Lain". *UNES Law Review* 6, no. 2 (Desember 11, 2023): 5021–5030. https://doi.org/10.31933/unesrev.v6i2.1321.

Sylfia, A., dkk. "Tanggungjawab Yuridis PT. Tokopedia Atas Kebocoran Data Pribadi Dan Privasi Konsumen Dalam Transaksi Online". *Bhirawa Law Journal* 2, no. 1 (Mei 31, 2021): 21–27. https://doi.org/10.26905/blj.v2i1.5850.

Tan, D. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum". *NUSANTARA : Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (Desember 28, 2021): 2463–2478. https://doi.org/10.31604/jips.v8i8.2021.2463-2478.

U.S. Department of Justice. *Former Chief Security Officer of Uber Sentenced to Three Years' Probation for Covering Up Data Breach Involving Millions of Uber User Records*, Mei 5, 2023. https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data.

Undang-Undang (UU) Nomor 27 Tahun 2022: Pelindungan Data Pribadi. Database Peraturan BPK, 2022. http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

UU No. 1 Tahun 2023. Database Peraturan BPK, 2023. http://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023.

UUD 1945 Dan Amandemen. Database Peraturan BPK, 1945. http://peraturan.bpk.go.id/Details/101646/uud-no--.

Yanova, M. H., P. Komarudin, dan H. Hadi. "Metode Penelitian Hukum: Analisis Problematika Hukum dengan Metode Penelitian Normatif dan Empiris". *Badamai Law Journal* 8, no. 2 (September 11, 2023): 394–408. https://doi.org/10.32801/damai.v8i2.17423.

Yesidora, A. *Lembaga Pengawas Data Belum Dibentuk, Komdigi Buat Ditjen Khusus*. katadata.co.id, 2024. https://katadata.co.id/digital/teknologi/6731e7ba7b77b/lembaga-pengawas-data-belum-dibentuk-komdigi-buat-ditjen-khusus.

[Halaman ini sengaja dikosongkan.]