CONSTITUTION JOURNAL
Volume 5 Number 1 June 2026
Published by the UIN KHAS Jember, Indonesia
ISSN (Print) 2987-8918 ISSN (Online) 2962-1720
Phone : +6285217243207 Email :jurnalconstitution@uinkhas.ac.id
Journal Home Page: https://constitution.uinkhas.ac.id/index.php/cj/index

Analisis Yuridis Tanggung Jawab KOMDIGI terhadap Kebocoran Data Pribadi Berdasarkan Undang-Undang Perlindungan Data Pribadi

A Juridical Analysis of KOMDIGI's Liability for Personal Data Breaches Under the Personal Data Protection Law

Ady Kriesna,[1] Siti Marwiyah,[2] Noenik Soekorini,[3] Sri Astutik,[4]

Article Information

Article History
Submitted : 19/03/2026
Revised : 26/03/2026
Accepted : 27/06/2026

Keywords: *Data Breach, Official Liability, Personal Data Protection*

Kata Kunci : *Kebocoran Data, Tanggungjawab Pejabat, Perlindungan Data Pribadi.*

10.35719/constitution.v5i1.330

Corresponding Author
Email:
kriesnaadynata@gmail.com

Pages : 97-118

Abstract

The Ministry of Communication and Digital (Komdigi), as the manager of the country's personal data, is responsible for the security of digital infrastructure through the implementation of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The purpose of this study is to identify data breaches within the Ministry. The purpose is to analyze the policies of government officials within the Ministry as a form of accountability for government agencies regarding data breaches under the PDP Law. This study uses a normative research method. The legal material collection procedure in this study is a literature review. The results indicate that factors causing data breaches include human error, IT system weaknesses, and a lack of cyber audits, such as the 2023 case that affected 1.3 million users. Officials' responsibilities are regulated in Article 55 of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which concerns data security due diligence, with administrative sanctions ranging from fines to criminal penalties or dismissal. Implementation still faces challenges such as a lack of cyber human resource training and cross-agency coordination.

Abstrak

Kementerian Komunikasi dan Digital (Komdigi) selaku pengelola data pribadi negara bertanggung jawab atas keamanan infrastruktur digital melalui penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Tujuan penelitian ini adalah untuk mengidentifikasi celah kebocoran data di Kementerian Komdigi. Untuk menganalisis kebijakan pejabat pemerintahan di Kementerian Komdigi sebagai bentuk tanggung jawab lembaga pemerintahan terkait kebocoran data berdasarkan UU PDP. Penelitian ini menggunakan metode penelitian normatif. Prosedur pengumpulan bahan hukum dalam penelitian ini yaitu kajian literatur atau studi kepustakaan. Hasil penelitian menunjukkan bahwa faktor penyebab kebocoran data meliputi kelalaian manusia, kelemahan sistem TI, minimnya audit siber, seperti kasus 2023 yang menyasar 1,3 juta pengguna.

[1]kriesnaadynata@gmail.com, Fakultas Hukum, Universitas Dr. Soetomo, Indonesia.
[2]siti.marwiyahsh@unitomo.ac.id, Fakultas Hukum, Universitas Dr. Soetomo, Indonesia.
[3]noenik.soekorini@unitomo.ac.id, Fakultas Hukum, Universitas Dr. Soetomo, Indonesia.
[3]sri.astutik@unitomo.ac.id, Fakultas Hukum, Universitas Dr. Soetomo, Indonesia.

Tanggung jawab pejabat diatur dalam Pasal 55 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) tentang due diligence pengamanan data, dengan sanksi administratif hingga pidana berupa denda atau pemecatan. Implementasi masih menghadapi tantangan seperti kurangnya pelatihan SDM siber dan koordinasi lintas instansi.

Pendahuluan

Dalam era digital, pemerintah Indonesia menghadapi tantangan besar dalam menjaga keamanan dan integritas data, termasuk di Kementerian Komunikasi dan Digital yang selanjutnya disebut sebagai (KOMDIGI), karena kebocoran data tidak hanya menjadi persoalan teknis tetapi juga menyangkut aspek hukum, etika, dan kepercayaan publik. Meningkatnya aktivitas internet dan transaksi daring membuat data pribadi masyarakat semakin rentan menjadi sasaran kejahatan siber, sehingga pejabat KOMDIGI memiliki tanggung jawab penting dalam mengelola, mengawasi, dan melindungi infrastruktur komunikasi serta memastikan keamanan data dari akses tidak sah. Selain itu, kementerian juga berkewajiban melakukan edukasi terkait perlindungan data pribadi, karena kegagalan dalam menjalankan fungsi tersebut dapat menurunkan reputasi lembaga dan kepercayaan masyarakat terhadap pemerintah. Kebocoran data sendiri dapat disebabkan oleh berbagai faktor seperti kesalahan manusia, kurangnya pelatihan keamanan, serta kelemahan sistem teknologi informasi, termasuk kelalaian dalam pengelolaan sistem keamanan yang sering menjadi penyebab insiden kebocoran data pengguna layanan digital pemerintah.[1] Pejabat di Kementerian KOMDIGI harus mampu mengidentifikasi potensi risiko dan mengambil langkah-langkah proaktif untuk mencegah terjadinya kebocoran data. Hal ini mencakup peningkatan sistem keamanan siber, penerapan kebijakan privasi yang ketat, serta peningkatan kapasitas sumber daya manusia dalam bidang teknologi informasi.

Tanggung jawab pejabat di KOMDIGI dalam kasus kebocoran data mencakup aspek akuntabilitas dan transparansi, di mana publik berhak mengetahui penyebab insiden serta langkah penanganan, perbaikan, dan pencegahan yang dilakukan untuk memulihkan kepercayaan masyarakat. Dalam konteks hukum, kebocoran data memiliki implikasi serius karena pejabat dapat

[1] Hartoyo Budi Santoso, Vieta Imelda Cornelis, Ernu Widodo, "Penggunaan Teknologi Informasi Dalam Administrasi Kependudukan Pada Era Digital," *Lex Journal: Kajian Hukum & Keadilan* 9 No. 2 (2025): 345–61.

dikenai sanksi apabila terbukti lalai, sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menegaskan kewajiban pengendali data, termasuk instansi pemerintah, untuk melindungi data pribadi serta menjunjung prinsip akuntabilitas dan transparansi. Regulasi ini menjadi dasar penting bagi pejabat KOMDIGI untuk memastikan perlindungan data sekaligus menghindari konsekuensi hukum akibat pelanggaran. Salah satu contoh nyata adalah insiden kebocoran data di KOMDIGI pada tahun 2023 yang melibatkan sekitar 1,3 juta data pengguna, yang menunjukkan pentingnya penguatan sistem keamanan, kepatuhan regulasi, serta peningkatan tanggung jawab dalam pengelolaan data publik.[2] Kasus ini menyoroti kelalaian dalam pengelolaan data dan sistem keamanan yang lemah. Data yang bocor mencakup informasi sensitif seperti nama, alamat, nomor telepon, dan data lainnya. Insiden ini bukan hanya merugikan individu yang datanya bocor, tetapi juga berdampak pada reputasi pemerintah dan KOMDIGI sebagai lembaga yang seharusnya melindungi data masyarakat.

Sebelum menganalisis tanggung jawab pejabat di KOMDIGI, penting untuk menguraikan fakta empiris mengenai kebocoran data di Indonesia. Berbagai insiden, seperti dugaan kebocoran 1,3 miliar data registrasi kartu SIM pada tahun 2022 dan 34,9 juta data paspor pada tahun 2023, menunjukkan bahwa keamanan data pribadi masih menghadapi tantangan serius. Peristiwa tersebut tidak hanya mengancam hak privasi masyarakat, tetapi juga berdampak pada menurunnya kepercayaan publik terhadap penyelenggara sistem elektronik pemerintah. Berdasarkan fakta tersebut, analisis penelitian ini difokuskan pada bentuk tanggung jawab pejabat sebagai pengendali data pribadi serta sanksi yang dapat dikenakan apabila terbukti lalai dalam memenuhi kewajiban perlindungan data sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mewajibkan setiap pengendali data menerapkan prinsip akuntabilitas, keamanan pemrosesan data, dan pemberitahuan atas insiden kebocoran.[3]

Kebocoran data di KOMDIGI menunjukkan bahwa tanggung jawab pejabat diatur secara tegas dalam Undang-Undang Nomor 27 Tahun 2022 tentang

[2] Nafiatul Munawaroh, "Tanggung Jawab Pemerintah Atas Kebocoran Data Pribadi," Hukum Online2, 2023, https://www.hukumonline.com/klinik/a/tanggung-jawab-pemerintah-atas kebocoran-data-pribadi-lt66881c826cc33/ .

[3] CNN Indonesia. *Diduga 1,3 Miliar Data Registrasi SIM Card Bocor*. https://www.cnnindonesia.com/teknologi/20220901102120-192-841845/diduga-13-miliar-data-registrasi-sim-card-bocor

Perlindungan Data Pribadi (UU PDP), di mana kelalaian dalam melindungi data dapat dikenai sanksi administratif hingga pidana seperti denda, pemecatan, atau penjara sesuai tingkat pelanggaran, sehingga menegaskan pentingnya akuntabilitas dan kepatuhan hukum. Kondisi ini juga menuntut adanya evaluasi dan reformasi kebijakan pengelolaan data melalui penguatan infrastruktur keamanan siber, pembaruan sistem dan prosedur, serta pelatihan dan peningkatan kesadaran pegawai, disertai audit berkala untuk mencegah terulangnya insiden serupa. Selain itu, diperlukan penguatan mekanisme pengawasan internal berbasis manajemen risiko melalui unit khusus yang melakukan audit, uji kepatuhan, dan evaluasi kerentanan sistem sesuai Pasal 55 UU PDP, serta kolaborasi lintas instansi dengan Badan Siber dan Sandi Negara (BSSN) dalam pertukaran intelijen ancaman dan koordinasi respons insiden sebagaimana sejalan dengan regulasi keamanan informasi nasional. Dari perspektif etika administrasi publik, kebocoran data juga mencerminkan pentingnya integritas moral pejabat selain kepatuhan hukum, karena akuntabilitas pemerintahan tidak hanya diukur dari aspek legal formal tetapi juga dari tanggung jawab etis dalam menjaga kepercayaan publik dan penggunaan kewenangan secara bertanggung jawab.[4] Kegagalan dalam menjaga data pribadi masyarakat mencerminkan pelanggaran etika publik yang serius, karena menyangkut penyalahgunaan kepercayaan (*breach of public trust*). Kondisi ini berpotensi memperdalam krisis legitimasi institusional, sebagaimana tercermin dalam Indeks Persepsi Korupsi (IPK) *Transparency International* yang menunjukkan adanya kecenderungan menurunnya kepercayaan publik terhadap institusi pemerintah di Indonesia.[5]

Dari perspektif tata kelola pemerintahan yang baik (good governance), kebocoran data menunjukkan kegagalan negara dalam menerapkan prinsip transparansi, akuntabilitas, dan responsivitas secara efektif. World Bank melalui Worldwide Governance Indicators juga menegaskan bahwa lemahnya sistem pengelolaan dan keamanan informasi tidak hanya meningkatkan risiko pelanggaran privasi, tetapi juga dapat menimbulkan dampak luas berupa kerugian ekonomi, sosial, dan politik yang signifikan bagi negara.[6] Oleh karena itu, pejabat KOMDIGI dituntut untuk mengadopsi pendekatan reformasi berbasis *good*

[4] Dennis F. Thompson, "Moral Responsibility of Public Officials: The Problem of Many Hands," *American Political Science Review* 74 (2014): 905.
[5] Transparency International, "Corruption Perceptions Index 2024," Transparency International, 2024, https://www.transparency.org/en/cpi/2024.
[6] World Bank, "Worldwide Governance Indicators 2023," Washington, DC: World Bank, 2023, https://info.worldbank.org/governance/wgi/ .

governance, antara lain melalui penerapan *Data Protection Impact Assessment (DPIA)* secara wajib dan sistematis sebagai instrumen pencegahan dini, sekaligus sebagai wujud pertanggungjawaban negara dalam melindungi hak konstitusional warga negara atas keamanan data pribadi.

Kasus kebocoran data di KOMDIGI pada tahun 2023 memicu tuntutan hukum dari masyarakat sipil, yang menunjukkan meningkatnya kesadaran publik terhadap hak perlindungan data pribadi, termasuk dorongan dari organisasi seperti *Indonesia Corruption Watch (ICW)* untuk menegakkan UU PDP melalui gugatan perdata. Peristiwa ini menegaskan bahwa pejabat pemerintah tidak memiliki kekebalan hukum, melainkan tetap dapat dimintai pertanggungjawaban yudisial, sebagaimana diatur dalam Pasal 66 UU PDP yang memberikan hak kepada subjek data untuk menuntut ganti rugi atas pelanggaran pengelolaan data. Dengan demikian, kasus ini memperkuat prinsip persamaan di hadapan hukum *(equality before the law)* dalam tata kelola pemerintahan digital.[7]

Pencegahan kebocoran data di masa depan menuntut peningkatan kapasitas sumber daya manusia sebagai langkah strategis, melalui pelatihan berkelanjutan mengenai keamanan siber, tata kelola data, dan pemahaman UU PDP tentang Perlindungan Data Pribadi bagi seluruh pegawai KOMDIGI di semua level. Kebijakan ini sejalan dengan rekomendasi *Organisation for Economic Co-operation and Development* (*OECD)* yang menekankan pentingnya kompetensi aparatur sebagai garda terdepan dalam perlindungan data dan keamanan informasi.[8] Urgensi pelatihan ini diperkuat oleh laporan *Verizon Data Breach Investigations Report 2024* yang mencatat bahwa sekitar 74% insiden kebocoran data global disebabkan oleh faktor human error, menunjukkan bahwa kelemahan sumber daya manusia sering kali menjadi titik rawan dalam sistem keamanan digital.[9]

Selain peningkatan kapasitas aparatur, pencegahan kebocoran data juga membutuhkan adopsi teknologi mutakhir seperti enkripsi *end-to-end,* autentikasi berlapis, dan pemanfaatan blockchain untuk meningkatkan keamanan serta integritas sistem pengelolaan data. Pengalaman Singapura melalui Personal Data *Protection Act* menunjukkan bahwa integrasi kecerdasan buatan (AI) untuk deteksi

[7] Indonesia Corruption Watch (ICW), "Laporan Advokasi Kebocoran Data Kominfo 2023," Jakarta: ICW, 2023, https://antikorupsi.org/id.
[8] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publishing, 2013).
[9] Verizon, "Data Breach Investigations Report 2024," New York: Verizon Business, 2024, https://www.verizon.com/business/resources/reports/dbir.html.

ancaman secara real-time dapat secara signifikan memperkuat ketahanan sistem digital dan mengurangi risiko kebocoran data.[10] Model ini dapat dijadikan rujukan oleh KOMDIGI dalam memperkuat infrastruktur digital nasional yang adaptif terhadap perkembangan ancaman siber.

Evaluasi pasca berlakunya UU PDP menunjukkan perlunya penyempurnaan regulasi pelaksana agar lebih operasional dan selaras secara hierarkis, termasuk revisi Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yang sudah tidak relevan dengan rezim hukum baru. Dalam implementasinya, pejabat struktural memiliki peran penting melalui sosialisasi internal, penyusunan SOP, serta pengawasan kebijakan di tiap unit kerja, yang kemudian diperkuat dengan reformasi organisasi berbasis *Key Performance Indicators (KPI)* keamanan data seperti respons insiden, kepatuhan audit, dan mitigasi risiko sesuai prinsip *performance-based accountability*. Selain itu, diperlukan penguatan sistem pemantauan pasca insiden melalui mekanisme perlindungan whistleblower sebagai early warning system yang didukung Pasal 10 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban berbunyi: Pasal 10 ayat (1) Saksi, Korban, Saksi Pelaku, dan/atau Pelapor tidak dapat dituntut secara hukum, baik pidana maupun perdata atas kesaksian dan/atau laporan yang akan, sedang, atau telah diberikannya, kecuali kesaksian atau laporan tersebut diberikan tidak dengan iktikad baik. Ayat (2) Dalam hal terdapat tuntutan hukum terhadap Saksi, Korban, Saksi Pelaku, dan/atau Pelapor atas kesaksian dan/atau laporan yang akan, sedang, atau telah diberikan, tuntutan hukum tersebut wajib ditunda hingga kasus yang ia laporkan atau ia berikan kesaksian telah diputus oleh pengadilan dan memperoleh kekuatan hukum tetap. untuk mendorong transparansi dan mencegah budaya birokrasi yang represif. Secara keseluruhan, tanggung jawab pejabat KOMDIGI tidak hanya bersifat formal yuridis, tetapi juga menuntut transformasi sistemik dalam tata kelola digital melalui kepemimpinan yang akuntabel, kolaboratif, dan inovatif guna menjadikan perlindungan data sebagai pilar utama kepercayaan publik di era digital. Selain itu, penelitian ini menegaskan kebaruan dengan fokus pada pengaturan normatif kewajiban pencegahan kebocoran data serta penentuan pihak yang bertanggung jawab berdasarkan UU PDP, yang membedakannya dari studi sebelumnya.

[10] Nikolas Ioannidis, *Border Control and New Technologies*, *Uitgeverij ASP (Academic and Scientific Publishers Nv)* (Cophenhagen, 2021), 78.

Metode

Penelitian ini merupakan penelitian normatif yang berfokus pada kajian hukum dan peraturan terkait tanggung jawab pejabat Kementerian KOMDIGI dalam kasus kebocoran data, dengan menggunakan pendekatan konseptual dan pendekatan perundang-undangan. Pendekatan konseptual digunakan untuk memahami secara mendalam konsep tanggung jawab hukum, keamanan data, dan akuntabilitas publik dalam perlindungan data pribadi, sedangkan pendekatan perundang-undangan digunakan untuk menganalisis regulasi yang berlaku, terutama UU PDP beserta aturan terkait lainnya. Selain itu, penelitian ini menggunakan analisis deskriptif untuk menggambarkan fenomena kebocoran data di KOMDIGI, termasuk faktor penyebab dan dampaknya terhadap perlindungan data masyarakat, serta didukung oleh studi literatur dari berbagai sumber seperti buku, artikel, dan jurnal hukum yang relevan.[11]

Sumber penelitian ini terdiri dari bahan hukum primer dan sekunder yang relevan, di mana bahan hukum primer mencakup UU PDP, peraturan pemerintah, dokumen resmi terkait pengelolaan data pribadi, serta putusan pengadilan mengenai kebocoran data dan tanggung jawab pejabat, sedangkan bahan hukum sekunder meliputi buku, artikel jurnal, penelitian sebelumnya, dan literatur tentang perlindungan data, tanggung jawab hukum, dan kebijakan publik. Pengumpulan bahan hukum dilakukan melalui identifikasi sumber hukum seperti peraturan perundang-undangan, doktrin, dan literatur ilmiah yang relevan, kemudian diikuti dengan proses pengolahan secara sistematis melalui analisis terhadap teks hukum. Analisis tersebut berfokus pada ketentuan dalam UU PDP dan regulasi terkait untuk menilai pengaturan tanggung jawab pejabat pemerintahan dalam perlindungan data pribadi serta implikasi hukumnya apabila terjadi kebocoran data.

Hasil dan Pembahasan

Pengaturan Normatif Kewajiban Pemerintah dalam Mencegah Kebocoran Data Pribadi menurut UU No. 27 Tahun 2022

Kebocoran data merupakan isu global yang semakin mendesak seiring berkembangnya teknologi digital, di mana informasi pribadi atau sensitif dapat

[11] Peter Mahmud, *Penelitian Hukum* (Jakarta: Kencana Pranada Media Group, 2019). 56.

tersebar kepada pihak tidak berwenang baik secara sengaja maupun tidak sengaja. Data seperti identitas, kesehatan, keuangan, dan transaksi menjadi target utama kejahatan siber karena nilainya yang tinggi. Kondisi ini menunjukkan meningkatnya kerentanan sistem penyimpanan data di sektor publik maupun swasta. Berdasarkan laporan *Privacy Rights Clearinghouse (2020),* sejak 2005 lebih dari 8,4 miliar catatan data pribadi telah bocor secara global, dengan tren peningkatan signifikan dalam beberapa tahun terakhir.[12]

Kebocoran data menimbulkan dampak serius bagi individu maupun organisasi. Bagi individu, dampaknya meliputi pencurian identitas, penipuan finansial, hingga kerusakan reputasi jangka panjang. Sementara itu, organisasi dapat mengalami kerugian finansial, turunnya kepercayaan publik, serta risiko tuntutan hukum. Laporan *IBM Cost of a Data Breach Report* 2020 mencatat rata-rata biaya kebocoran data global mencapai 3,86 juta dolar AS, dengan sektor kesehatan sebagai yang paling terdampak. Selain itu, pelanggaran terhadap regulasi seperti *General Data Protection Regulation (GDPR)* di Eropa dapat memperberat konsekuensi hukum bagi organisasi yang lalai dalam melindungi data.[13]

Kasus kebocoran data di Kementerian Komunikasi dan Digital menunjukkan bahwa keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) tidak serta-merta menjamin terlindunginya data pribadi apabila norma yang diatur tidak diimplementasikan secara efektif. Dalam perspektif UU PDP, KOMDIGI sebagai penyelenggara sistem elektronik sekaligus pengendali data memiliki kewajiban menerapkan prinsip akuntabilitas, menjamin keamanan pemrosesan data, serta melakukan pengendalian risiko terhadap setiap aktivitas pengelolaan data pribadi. Oleh karena itu, apabila kebocoran data terjadi akibat lemahnya sistem keamanan, kelalaian pengawasan, atau tidak diterapkannya standar perlindungan yang memadai, maka kondisi tersebut menunjukkan tidak terpenuhinya kewajiban hukum pengendali data sebagaimana diatur dalam UU PDP. Dengan demikian, substansi permasalahan hukum tidak hanya terletak pada terjadinya kebocoran data, tetapi juga pada ada atau tidaknya kelalaian pejabat dalam memenuhi standar perlindungan data yang diwajibkan oleh peraturan perundang-undangan.[14]

---

[12] "Chronology of Data Breaches," Privacy Right Clearinghouse, 2020.
[13] IBM Security, "Cost of a Data Breach Report 2020," IBM, 2020.
[14] Simanjuntak, P. H. (2024). Perlindungan Hukum terhadap Data Pribadi pada Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Esensi Hukum*. Artikel ini mengevaluasi efektivitas penerapan UU PDP dan membandingkannya dengan GDPR. https://journal.upnvj.ac.id/index.php/esensihukum/article/view/412?utm_source=

Lebih lanjut, penerapan norma UU PDP terhadap kasus kebocoran data KOMDIGI harus dianalisis melalui konsep pertanggungjawaban pejabat administrasi negara. UU PDP mewajibkan pengendali data untuk bertanggung jawab atas seluruh proses pemrosesan data pribadi, termasuk menyampaikan pemberitahuan kepada subjek data dan lembaga yang berwenang apabila terjadi kegagalan pelindungan data, serta melakukan langkah penanganan dan pemulihan. Oleh karena itu, apabila pejabat yang bertanggung jawab tidak melaksanakan kewajiban tersebut secara tepat waktu atau tidak mampu membuktikan bahwa sistem perlindungan data telah dikelola sesuai prinsip akuntabilitas, maka selain berpotensi dikenai sanksi administratif berdasarkan UU PDP, tindakan tersebut juga mencerminkan tidak terpenuhinya prinsip *good governance*, khususnya akuntabilitas, transparansi, dan kehati-hatian dalam penyelenggaraan pemerintahan digital. Pendekatan ini menegaskan bahwa analisis hukum terhadap kasus kebocoran data KOMDIGI harus berorientasi pada efektivitas penerapan norma, bukan hanya pada uraian normatif mengenai isi peraturan.[15]

Seiring dengan meningkatnya ancaman kebocoran data, banyak negara di seluruh dunia mulai mengembangkan regulasi perlindungan data pribadi yang lebih ketat. Salah satu contoh regulasi yang paling terkenal adalah *General Data Protection Regulation (GDPR)* yang diberlakukan di Uni Eropa pada tahun 2018.[16] Regulasi perlindungan data seperti *GDPR* di Eropa menetapkan standar tinggi dengan mewajibkan transparansi pengelolaan data, perlindungan dari kebocoran, serta pemberian kontrol kepada individu atas data pribadinya. Selain *GDPR*, sejumlah negara juga mengembangkan regulasi serupa, seperti Brasil melalui *LGPD* dan California melalui *CCPA*, yang menunjukkan meningkatnya kesadaran global terhadap pentingnya perlindungan data pribadi. Di Indonesia, kebocoran data menjadi isu serius dengan banyaknya insiden di sektor publik dan swasta, termasuk pada platform digital dan e-commerce yang melibatkan jutaan data pengguna. Berdasarkan laporan KOMDIGI, pada tahun 2020 tercatat lebih dari 1.500 insiden kebocoran data yang mencakup data pribadi, keuangan, dan

[15] Christine, B. (2022). Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Syntax Literate*. Membahas kendala implementasi UU PDP dalam praktik. https://jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/13936/9046?utm_source=

[16] European Union, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union*, no. Data Protection (2018).

informasi sensitif lainnya.[17] Insiden ini menunjukkan betapa pentingnya pengelolaan dan perlindungan data yang lebih baik oleh perusahaan dan instansi pemerintah di Indonesia.

Indonesia pada tahun 2022 telah memiliki UU PDP yang memberikan dasar hukum kuat bagi perlindungan data, termasuk pengaturan hak individu, kewajiban pengelola data untuk mencegah dan melaporkan kebocoran, serta sanksi bagi pihak yang lalai. Namun, implementasi regulasi ini masih menghadapi tantangan besar, terutama dalam pengawasan, kesadaran institusi, serta keterbatasan infrastruktur dan sumber daya manusia di bidang keamanan siber. Di sektor pemerintahan, khususnya KOMDIGI, berbagai insiden kebocoran data menunjukkan lemahnya sistem pengamanan, seperti kasus kebocoran data Sistem Informasi Administrasi Kependudukan (SIAK) pada 2019 yang berdampak pada jutaan data penduduk. Selain itu, pada 2022 kasus peretasan oleh Bjorka semakin menegaskan kerentanan perlindungan data di Indonesia, dengan bocornya data sensitif termasuk data *SIM card* lebih dari 10 juta pengguna serta data dari berbagai instansi pemerintah dan platform digital. Kondisi ini menunjukkan bahwa meskipun UU PDP telah hadir, efektivitas perlindungan data masih sangat bergantung pada penguatan implementasi, pengawasan, dan kapasitas keamanan siber nasional.[18]

Kasus kebocoran data oleh Bjorka menimbulkan kekhawatiran besar terhadap keamanan data pribadi di Indonesia karena data sensitif seperti NIK, nomor telepon, email, hingga informasi akun transaksi digital berhasil dibobol, yang berdampak pada risiko pencurian identitas, penipuan online, phishing, serta menurunnya kepercayaan publik terhadap pemerintah dan penyedia layanan. Pemerintah melalui KOMDIGI merespons dengan investigasi dan imbauan kehati-hatian, namun kasus ini menunjukkan lemahnya implementasi UU PDP, baik dari sisi pengawasan, penegakan hukum, maupun kesiapan sistem keamanan siber, terlebih pelaku hingga kini belum tertangkap. Insiden ini menegaskan perlunya peningkatan tanggung jawab pejabat, penguatan pelatihan SDM, serta kesiapan lembaga dalam menghadapi ancaman siber yang semakin canggih, sekaligus mendorong kesadaran digital masyarakat dalam melindungi data pribadi mereka. Di sisi teknis, kasus ini juga mengungkap kelemahan sistem seperti minimnya

[17] Kementerian Komunikasi dan Informatika Republik Indonesia, "Laporan Insiden Kebocoran Data Di Indonesia," 2020.
[18] CNN Indonesia, "Deret Respons Pemerintah Yang Dianggap Angin Lalu Oleh Bjorka," CNN, 2022.

enkripsi, kurangnya segmentasi jaringan, tidak adanya SOP pemantauan berkelanjutan, serta lemahnya cadangan data nasional, yang menyebabkan kebocoran berdampak luas dan sulit dipulihkan.

Faktor penyebab kebocoran data di KOMDIGI bersifat kompleks dan melibatkan aspek teknis serta sumber daya manusia. Dari sisi teknis, kerentanan sistem informasi seperti kurangnya pembaruan sistem, lemahnya penerapan enkripsi data, serta tidak optimalnya autentikasi berlapis menjadi celah yang dapat dimanfaatkan peretas untuk mengakses data pribadi. Sementara itu, faktor manusia juga berperan besar, seperti kesalahan pengelolaan akses, penggunaan kata sandi yang lemah, serta minimnya pelatihan keamanan siber bagi pegawai. Hal ini menunjukkan bahwa meskipun teknologi yang digunakan sudah canggih, tanpa pengelolaan dan kesadaran keamanan yang baik, risiko kebocoran data tetap tinggi.[19]

Faktor kebocoran data di KOMDIGI juga dipengaruhi oleh lemahnya kebijakan internal, seperti tidak tegasnya aturan perlindungan data, tidak jelasnya prosedur akses data, serta kurangnya audit dan pengawasan sistem secara berkala yang menyebabkan kebocoran sulit terdeteksi sejak awal. Dalam konteks ini, pejabat pemerintahan memiliki tanggung jawab penting berdasarkan UU PDP untuk memastikan pengelolaan data dilakukan secara sah, transparan, dan akuntabel, termasuk melakukan pemantauan rutin serta melaporkan insiden kebocoran dalam waktu 72 jam kepada pihak berwenang. Tanggung jawab tersebut tidak hanya mencakup pencegahan, tetapi juga respons cepat dan penanganan insiden secara efektif dengan melibatkan pihak kompeten, sehingga perlindungan data dapat berjalan optimal sesuai prinsip hukum perlindungan data pribadi.[20]

Kebocoran data di KOMDIGI merupakan akibat dari kelemahan sistemik yang mencakup aspek teknologi, kebijakan internal, dan sumber daya manusia, sehingga mencerminkan kegagalan tata kelola pemerintahan digital secara menyeluruh, bukan sekadar kesalahan teknis. Dalam perspektif negara hukum, kondisi ini menunjukkan pelanggaran terhadap kewajiban konstitusional negara dalam melindungi hak asasi atas keamanan dan data pribadi warga, yang dalam UU PDP ditegaskan sebagai tanggung jawab wajib dan mengikat bagi pengendali data, termasuk lembaga pemerintah. Karena itu, tanggung jawab hukum dalam kasus ini tidak hanya bersifat individual, tetapi institusional, yang menuntut

[19] Budi Santosa, *Keamanan Sistem Informasi* (Yogyakarta: Andi Publisher, 2019).56.
[20] Siti Rahayu, *Hukum Perlindungan Data Pribadi* (Jakarta: Sinar Grafika, 2021). 17.

perbaikan sistem tata kelola agar tidak terjadi pengulangan. Kasus ini juga menjadi ujian prinsip good governance, terutama akuntabilitas, kehati-hatian, dan profesionalitas, sekaligus penting untuk memulihkan kepercayaan publik melalui penegakan hukum yang tegas. Selain bersifat represif, pertanggungjawaban juga harus mencakup langkah preventif dan korektif seperti penguatan sistem keamanan, peningkatan SDM, dan pengawasan yang efektif, sehingga perlindungan data pribadi dapat terjamin secara berkelanjutan sebagai wujud nyata negara hukum di era digital.

Pertanggungjawaban Hukum atas Kebocoran Data Pribadi menurut UU No. 27 Tahun 2022

Dalam era digital, data pribadi menjadi aset penting yang rentan terhadap kebocoran, sehingga menimbulkan risiko besar bagi individu, organisasi, dan negara, tidak hanya dari sisi teknis tetapi juga hukum dan etika. KOMDIGI (KOMDIGI) sebagai pengelola informasi elektronik memiliki tanggung jawab besar dalam melindungi data pribadi sesuai UU PDP, yang menegaskan kewajiban pejabat pemerintah untuk menjaga keamanan, kerahasiaan, transparansi, serta akuntabilitas data, termasuk pencegahan dan penanganan kebocoran secara cepat. UU PDP juga mengatur bahwa data pribadi mencakup setiap informasi yang dapat mengidentifikasi individu baik secara langsung maupun tidak langsung, mencakup data umum seperti nama dan NIK hingga data yang terbentuk dari kombinasi informasi lain, serta berlaku baik pada sistem elektronik maupun non-elektronik. Selain itu, data pribadi diklasifikasikan menjadi data umum dan data spesifik yang memiliki tingkat perlindungan berbeda, di mana keduanya sama-sama harus dilindungi dari penyalahgunaan. Dalam konteks KOMDIGI, pejabat tidak hanya dituntut untuk mencegah kebocoran data, tetapi juga wajib memberikan penjelasan transparan kepada publik jika terjadi insiden serta melakukan langkah mitigasi dan perbaikan. Hal ini menunjukkan bahwa perlindungan data pribadi merupakan bagian penting dari tata kelola pemerintahan yang baik untuk menjaga kepercayaan publik dan memastikan negara hadir dalam melindungi hak warga di era digital.

Data Pribadi Spesifik merupakan informasi sensitif yang memerlukan perlindungan lebih ketat karena dampaknya yang besar jika terjadi kebocoran, seperti data kesehatan, biometrik (sidik jari dan pengenalan wajah), data genetika, catatan kriminal, serta data anak dan informasi pribadi lain yang dilindungi undang-undang. Sensitivitas ini berkaitan langsung dengan perlindungan hak asasi manusia, termasuk hak privasi dan perlindungan anak sebagaimana dijamin

dalam UUD NRI 1945 Pasal 28G. Dalam pengaturannya, Data Pribadi Spesifik memiliki standar perlindungan yang lebih tinggi dibanding Data Pribadi Umum, karena pengolahannya wajib disertai persetujuan eksplisit dari subjek data dan sering membutuhkan dasar hukum tambahan, sementara data umum dapat diproses dengan persetujuan implisit atau kepentingan yang sah. Ketentuan ini menunjukkan adanya perbedaan tingkat perlindungan yang lebih ketat, meskipun masih terdapat kritik terhadap aspek pembuktian dalam UU PDP yang dinilai membebani pemilik data dalam kasus pelanggaran.[21]

Konsep data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mencakup individu yang teridentifikasi atau dapat diidentifikasi, termasuk penerapan prinsip pseudonimisasi dan anonimisasi sebagaimana praktik GDPR, di mana data anonim tidak lagi termasuk data pribadi, sedangkan data pseudonim tetap dilindungi karena masih dapat ditelusuri. UU PDP membagi data menjadi data umum dan data spesifik, dengan data spesifik seperti biometrik, kesehatan, genetika, data anak, dan catatan kriminal yang memerlukan perlindungan lebih ketat serta persetujuan eksplisit karena dampaknya yang lebih serius terhadap hak asasi manusia. Dalam implementasinya, KOMDIGI memiliki peran strategis sebagai pengawas sekaligus pengelola kebijakan perlindungan data, termasuk kewajiban memastikan standar keamanan, melakukan audit berkala, serta meningkatkan kapasitas aparatur melalui pelatihan dan sosialisasi. Berdasarkan Pasal 15 dan Pasal 29 UU PDP, pejabat wajib mencegah kebocoran data, melaporkannya maksimal dalam 72 jam jika terjadi, serta melakukan mitigasi dampak secara transparan dan akuntabel kepada publik. Jika terjadi kelalaian, Pasal 45A UU PDP memberikan dasar sanksi administratif hingga pencabutan izin, menunjukkan adanya pertanggungjawaban hukum negara dan pejabatnya. Secara keseluruhan, prinsip akuntabilitas dan transparansi menjadi fondasi utama yang menuntut pejabat KOMDIGI untuk memastikan pengelolaan data dapat diawasi publik, dipertanggungjawabkan, serta mampu menjaga kepercayaan masyarakat dalam tata kelola data pribadi di era digital.[22]

Implementasi UU PDP dalam penanganan kebocoran data di KOMDIGI masih menghadapi tantangan serius, terutama pada aspek pengawasan, penegakan hukum, dan kapasitas kelembagaan yang belum optimal, terlebih pada

[21] Bagas Fadhli and Dzil Ikrom, "Terhadap Kebocoran Data Pribadi Di Indonesia Universitas Islam Negeri Fakultas Syariah Juni 2024 Indonesia," 2024. 67.
[22] Tim Hukum Online, "Dasar Hukum Perlindungan Data Pribadi," Hukum Online, 2023.

insiden yang terjadi sebelum UU PDP berlaku penuh sehingga masih merujuk pada UU ITE dan regulasi sebelumnya yang sanksinya belum seketat rezim baru. Meski demikian, setelah UU PDP berlaku efektif pada Oktober 2023, termasuk dalam kasus dugaan kebocoran data seperti NIK dan nomor telepon, tanggung jawab pejabat tetap mengikat karena data tersebut tergolong data pribadi umum yang tetap memiliki risiko tinggi terhadap penyalahgunaan identitas. Dalam kerangka Pasal 55 UU PDP, pengendali data wajib menerapkan prinsip due diligence secara aktif untuk menjamin keamanan data tanpa membedakan tingkat sensitivitasnya, sehingga kelalaian dalam pengamanan sistem, lemahnya pengawasan internal, dan kurangnya standar keamanan dapat dikualifikasikan sebagai pelanggaran hukum administrasi bahkan penyalahgunaan wewenang. Selain itu, kewajiban ini juga selaras dengan prinsip kehati-hatian dalam AUPB yang menuntut pengelolaan risiko tinggi secara maksimal, bukan minimal. Oleh karena itu, pejabat KOMDIGI tetap dapat dimintai pertanggungjawaban hukum meskipun data yang bocor dikategorikan sebagai data umum, karena UU PDP menekankan perlindungan berdasarkan risiko, bukan sekadar klasifikasi data. Dalam konteks negara hukum, pertanggungjawaban ini tidak hanya bersifat represif tetapi juga preventif dan korektif untuk memperkuat sistem keamanan, meningkatkan kapasitas SDM, serta memperbaiki tata kelola pengawasan internal. Dengan demikian, penerapan UU PDP terhadap KOMDIGI menjadi penting sebagai bentuk penegakan supremasi hukum, perlindungan hak konstitusional warga negara, dan penguatan prinsip good governance dalam tata kelola data digital nasional.[23]

Kasus KOMDIGI 2023 menunjukkan bahwa data pribadi umum seperti NIK dan nomor HP, ketika dikombinasikan, dapat memiliki tingkat risiko yang setara bahkan lebih berbahaya dibanding data spesifik, sehingga tetap berada dalam perlindungan ketat UU PDP sesuai Pasal 1 angka 1 yang menekankan identifiabilitas data melalui kombinasi informasi. Dalam kerangka Pasal 55 UU PDP, pejabat KOMDIGI wajib melakukan due diligence secara aktif sejak tahap perancangan sistem, termasuk pengamanan, pembatasan akses, audit, dan pengawasan pihak ketiga, sehingga kelalaian dalam aspek ini dapat dikualifikasikan sebagai kelalaian jabatan (ambtelijke nalatigheid) dan pelanggaran asas kecermatan, akuntabilitas, serta kepastian hukum dalam Hukum Administrasi Negara. Diskresi pejabat tidak dapat dijadikan alasan pembenar

[23] Nafiatul Munawaroh, "Tanggung Jawab Pemerintah Atas Kebocoran Data Pribadi."

apabila justru menyebabkan lemahnya sistem keamanan, karena UU PDP membatasi diskresi agar tetap sesuai kepentingan umum, kehati-hatian, dan tidak bertentangan dengan kewajiban perlindungan data; penggunaan diskresi yang mengabaikan audit atau rekomendasi teknis dapat dikategorikan sebagai penyalahgunaan wewenang *(detournement de pouvoir)* atau diskresi cacat hukum. Dengan demikian, kegagalan memperkuat sistem keamanan data NIK dan nomor HP menunjukkan pelanggaran terhadap kewajiban hukum aktif pengendali data, di mana tanggung jawab tidak hanya bersifat administratif tetapi juga dapat bersifat institusional dan individual jika terdapat kesalahan serius. UU PDP menegaskan bahwa perlindungan data didasarkan pada tingkat risiko, bukan sekadar klasifikasi data, sehingga data umum dengan daya identifikasi tinggi tetap menuntut standar keamanan maksimal. Secara keseluruhan, kelalaian dan pembatasan diskresi dalam kasus ini memperkuat posisi Pasal 55 UU PDP sebagai norma imperatif yang mengikat pejabat publik, serta menegaskan bahwa perlindungan data merupakan bagian dari good governance dan perlindungan hak asasi manusia, di mana setiap kegagalan pengamanan tetap menimbulkan tanggung jawab hukum dalam bentuk administratif, perdata, maupun konseptual sesuai teori tanggung jawab hukum.[24]

Dalam konteks pejabat publik, termasuk di Kementerian KOMDIGI, tanggung jawab hukum menjadi sangat krusial. Pejabat publik memiliki tanggung jawab untuk melindungi kepentingan masyarakat, terutama dalam hal pengelolaan data pribadi. Menurut Asmara, tanggung jawab pejabat publik mencakup aspek etika dan legalitas, di mana mereka harus bertindak sesuai dengan norma yang berlaku dan mempertimbangkan dampak dari keputusan yang diambil.[25] Apabila terjadi kebocoran data, pejabat tersebut dapat dimintai pertanggung jawaban, baik secara pidana maupun perdata, tergantung pada penyebab dan dampak dari kebocoran tersebut.

Lebih lanjut, dalam penerapan tanggung jawab hukum, terdapat beberapa unsur yang harus diperhatikan, yaitu kesalahan, kerugian, dan hubungan kausal. Menurut Mulyadi, untuk dapat menjatuhkan tanggung jawab hukum, harus ada bukti yang menunjukkan bahwa tindakan yang diambil oleh pejabat publik mengandung unsur kesalahan, baik berupa kelalaian maupun niat jahat.[26] Dalam

[24] R. Subekti, *Pokok-Pokok Hukum Perdata* (Jakarta: Intermasa, 2013).
[25] H. Asmara, *Tanggung Jawab Hukum Pejabat Publik: : Teori Dan Praktik* (Jakarta: Sinar Grafika, 2019).
[26] S. Mulyadi, *Hukum Perdata Dan Tanggung Jawab Hukum: Sebuah Pendekatan Praktis* (Bandung: Mandar Maju, 2020).

konteks kebocoran data, jika terbukti bahwa pejabat pemerintah tidak mengambil langkah-langkah yang memadai untuk melindungi data pribadi, maka mereka dapat dimintai pertanggungjawaban atas kerugian yang ditimbulkan.

Dalam beberapa kasus, tanggung jawab hukum pejabat publik tidak hanya bersifat individu, tetapi juga kolektif. Artinya, jika kebijakan yang diambil oleh suatu instansi pemerintah menyebabkan kebocoran data, maka seluruh lembaga tersebut dapat dimintai pertanggung jawaban. Ini menciptakan dinamika yang kompleks dalam penegakan hukum, di mana keputusan dan tindakan kolektif menjadi sorotan. Sebagaimana diungkapkan oleh Sutedi, tanggung jawab kolektif ini penting untuk memastikan bahwa institusi pemerintah bertindak sesuai dengan prinsip akuntabilitas dan transparansi.[27]

Setelah UU PDP mulai berlaku, pejabat pemerintah di KOMDIGI memiliki tanggung jawab lebih besar untuk memastikan perlindungan data pribadi yang lebih ketat. Jika terjadi kebocoran data setelah UU PDP berlaku, lembaga pemerintah, termasuk KOMDIGI, harus menghadapi kemungkinan penerapan sanksi administratif atau denda jika ditemukan adanya kelalaian dalam pengelolaan data pribadi. Denda sebesar Rp 10 miliar dikenakan bagi badan atau penyelenggara yang terbukti melakukan pelanggaran serius terhadap ketentuan perlindungan data pribadi, termasuk jika terjadi kebocoran data dan tidak dilaksanakan dengan benar kewajiban perlindungan yang diatur dalam UU PDP. Penerapan sanksi ini mencakup semua entitas yang mengelola data pribadi, baik lembaga pemerintah maupun sektor swasta, yang tidak memenuhi kewajiban perlindungan data pribadi yang sesuai dengan ketentuan yang berlaku dalam UU PDP.

Penerapan sanksi administratif dalam UU PDP menandakan transformasi paradigma hukum perlindungan data pribadi di Indonesia, yang bergeser dari strategi preventif semata menuju rezim represif-korektif yang lebih tegas dan berorientasi hasil. Negara kini tidak puas dengan sekadar norma kepatuhan formal, melainkan menuntut akibat konkret berupa denda, penghentian pemrosesan data, hingga pembatasan operasional bagi pelaku pelanggaran. Sanksi administratif ini menjadi alat paksa utama untuk memaksa pengendali data termasuk kementerian dan lembaga negara menjalankan kewajiban secara sungguh-sungguh, mencegah sikap cuek terhadap risiko kebocoran yang masif.

[27] Sutedi, *Hukum Perlindungan Data Pribadi* (Jakarta: Sinar Grafika, 2014).

Bagi institusi publik seperti KOMDIGI, pengenaan sanksi administratif sama sekali bukan upaya kriminalisasi kebijakan negara, melainkan mekanisme esensial penegakan hukum administrasi modern yang mengakui state liability. Hukum administrasi kontemporer, sebagaimana diatur dalam Pasal 18 Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan, menyatakan bahwa kelalaian organ negara yang menimbulkan kerugian publik wajib direspons dengan pertanggungjawaban proporsional. Oleh karena itu, status KOMDIGI sebagai data controller utama membuatnya tidak kebal hukum, dan sanksi justru menjadi konsekuensi alami dari mandatnya mengelola sistem elektronik nasional.

UU PDP juga memperkokoh posisi warga negara sebagai subjek hukum aktif dengan hak gugat konkret atas data pribadinya, melampaui sifat deklaratif semata melalui jaminan remediasi via lembaga pengawas independen seperti OJK atau Kemenkumham. Negara di sini berperan ganda sebagai regulator sekaligus penegak kepentingan publik. Sehingga diwajibkan proaktif melindungi hak konstitusional dari pada bersikap pasif, sebagaimana Pasal 28G UUD NRI 1945. Kegagalan lembaga seperti KOMDIGI dalam hal ini bukan hanya pelanggaran regulasi, tapi pengkhianatan mandat pelayanan publik yang harus dikoreksi melalui sanksi bertingkat.

Pertanggungjawaban KOMDIGI atas kebocoran data harus dilihat melalui lensa tanggung jawab institusional yang holistik, di mana kegagalan sistemik seperti lemahnya enkripsi, kurangnya audit rutin, atau protokol respons insiden yang buruk lebih dominan daripada kesalahan personal. Evaluasi hukumnya menuntut analisis menyeluruh terhadap tata kelola data internal, termasuk rantai komando, alokasi anggaran keamanan siber. Pendekatan ini membedakan antara strict liability (tanggung jawab ketat) untuk pengendali data dengan pembuktian kelalaian individu, memastikan reformasi struktural jangka panjang.

Dari perspektif good government, insiden kebocoran data mencerminkan kegagalan fatal dalam prinsip kehati-hatian (duty of care), profesionalisme birokrasi, dan akuntabilitas vertikal-horizontal, yang semestinya menjadi inti legitimasi kekuasaan negara. Doktrin ini, sebagaimana diuraikan Jimly Asshiddiqie, menuntut setiap wewenang dijalankan dengan orientasi maksimalisasi kepentingan publik, sehingga pengelolaan data yang ceroboh bukan hanya maladministrasi tapi juga penggerus kepercayaan sosial. Sanksi administratif menjadi instrumen korektif untuk memulihkan kredibilitas institusi di mata publik.

Lebih dari sekadar hukuman, sanksi administratif dalam UU PDP berfungsi preventif jangka panjang dengan mendorong investasi masif pada infrastruktur keamanan siber, pelatihan SDM anti-phishing, dan audit berbasis AI untuk deteksi ancaman real-time. Metode ini memaksa birokrasi berpikir ulang prioritas anggaran, mengubah paradigma dari "cost center" keamanan menjadi "value driver" pelayanan digital. Hasilnya, sanksi menciptakan efek domino perbaikan berkelanjutan di seluruh ekosistem e-government.

Pengenaan sanksi terhadap lembaga negara tidaklah bertabrakan dengan esensi pelayanan publik. Justru sebaliknya, ia menjadi pengawal agar transformasi digital seperti Sistem Pemerintahan Berbasis Elektronik (SPBE) tidak mengorbankan privasi warga demi efisiensi semata. Dalam era big data, pemerintahan berbasis teknologi harus diimbangi dengan *privacy by design* sebagai standar wajib, di mana sanksi berperan sebagai deteren bagi sikap komplasen. Transformasi ini selaras dengan Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), yang menjadikan keamanan data sebagai pilar utama.

Di bawah supremasi hukum, UU PDP menegaskan egaliter hukum: tidak ada imunitas absolut bagi kementerian, karena Pasal 53 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi UU PDP secara eksplisit mencakup sanksi administratif bagi pelanggaran oleh organ negara. Prinsip ini menempatkan hukum sebagai norma dasar yang mengikat semua pihak, memastikan KOMDIGI tunduk pada proses due diligence (uji tuntas) transparan jika terbukti lalai. Keniscayaan pertanggungjawaban ini memperkuat negara hukum Pancasila yang berkeadilan.

Pertanggungjawaban KOMDIGI juga mencerminkan prinsip keadilan administratif, di mana korban kebocoran berhak atas pemulihan penuh baik kompensasi finansial maupun notifikasi wajib tanpa dalih eksternal seperti serangan siber pihak ketiga. Bukti forensik yang menunjukkan vulnerabilitas pencegah (misalnya SQL injection) akan memperberat posisi institusi, sebagaimana kasus serupa di BPJS atau Ditjen Pajak. Negara wajib proaktif, bukan reaktif, dalam memitigasi risiko yang dapat diramalkan.

Implikasi lebih luas dari kebocoran data adalah erosi kepercayaan publik sebagai modal utama demokrasi digital, di mana survei CSIS menunjukkan penurunan 30% kepercayaan terhadap e-government pasca insiden KOMDIGI (CNN Indonesia, 2022). Ketidak mampuan melindungi data NIK atau nomor telepon mengancam efektivitas program seperti Kartu Prakerja atau vaksinasi

digital, sehingga sanksi menjadi alat restoratif untuk membangun kembali legitimasi.

Pasal 56 UU PDP menerapkan prinsip proporsionalitas sanksi, di mana skala kebocoran jutaan data memicu denda maksimal plus publikasi pelanggaran, membenarkan respons berat demi public interest. Pendekatan bertingkat ini (peringatan → denda → pidana) memastikan keadilan tanpa *over-penalization*, selaras dengan asas *lex certa*.

Secara edukatif, penegakan terhadap KOMDIGI menciptakan preseden bagi Kementerian Keuangan, Kesehatan, atau Polri yang mengelola big data, membentuk budaya compliance culture melalui efek jera institusional. Hukum bertransformasi dari deklaratif menjadi perilaku pembentuk, mendorong benchmark global seperti *NIST cybersecurity framework.* Sanksi administratif dapat eskalasi ke ranah perdata via Pasal 1365 KUHPerdata jika terbukti onrechtmatige daad (perbuatan melawan hukum), memungkinkan gugatan class action korban untuk ganti rugi immaterial seperti trauma identitas curian. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang multidimensi ini menjamin perlindungan komprehensif. Pengawasan *hybrid* (internal via Inspektorat, eksternal via Ombudsman dan masyarakat) menjadi kunci, dengan transparansi laporan insiden sebagai metrik keseriusan negara. KOMDIGI wajib publikasikan *root cause analysis* untuk akuntabilitas publik.

Dengan diberlakukannya UU PDP, negara dituntut untuk bertransformasi dari sekadar pengumpul data menjadi pelindung data. Perubahan peran ini menuntut adanya perubahan paradigma birokrasi, dari orientasi kekuasaan menuju orientasi perlindungan hak. Kegagalan dalam beradaptasi dengan paradigma ini berpotensi menimbulkan konflik hukum dan sosial. Pertanggungjawaban institusional KOMDIGI mencerminkan evolusi hukum administrasi yang citizen-centric, memposisikan negara sebagai pelayan akuntabel bukan penguasa superior sinergi dengan sila kedua Pancasila tentang kemanusiaan adil beradab.

Penerapan sanksi UU PDP terhadap KOMDIGI adalah fondasi pemerintahan transparan berbasis HAM, dengan perlindungan data sebagai barometer demokrasi digital dan good government. Penegakan ini menegaskan kebocoran data bukan insiden teknis, melainkan krisis konstitusional yang menguji supremasi hukum, hak warga, dan legitimasi negara strategi krusial untuk negara hukum Indonesia modern.

Simpulan

Penerapan UU PDP dalam kasus kebocoran data di KOMDIGI menunjukkan bahwa pertanggungjawaban pejabat tidak hanya bersifat normatif sebagai pengendali data pribadi, tetapi juga memiliki konsekuensi hukum yang konkret apabila terbukti lalai memenuhi kewajiban perlindungan data. Bentuk pertanggungjawaban tersebut meliputi pertanggungjawaban administratif melalui pemberian sanksi administratif sesuai UU PDP, pertanggungjawaban perdata berupa kewajiban pemulihan dan ganti kerugian kepada subjek data yang dirugikan, serta pertanggungjawaban pidana apabila kelalaian atau perbuatan pejabat memenuhi unsur tindak pidana sebagaimana diatur dalam UU PDP. Hasil analisis juga menunjukkan bahwa kebocoran data di KOMDIGI lebih mencerminkan kegagalan tata kelola pemerintahan digital daripada sekadar kegagalan teknis, karena lemahnya penerapan prinsip akuntabilitas, kehati-hatian, manajemen risiko, dan pengawasan internal. Oleh karena itu, efektivitas implementasi UU PDP tidak hanya bergantung pada keberadaan norma hukum, tetapi juga pada kemampuan pejabat dan institusi untuk menerapkan *due diligence* melalui penguatan sistem keamanan siber, audit berkala, peningkatan kapasitas sumber daya manusia, serta mekanisme pengawasan yang transparan dan akuntabel sebagai prasyarat terwujudnya perlindungan data pribadi dan pemulihan kepercayaan publik terhadap penyelenggaraan pemerintahan digital.

Referensi

Buku

A. Sutedi. (2011). Hukum Perlindungan Data Pribadi. Sinar Grafika.

Budi Santosa. (2019). Keamanan Sistem Informasi. Andi Publisher.

Chronology of Data Breaches. (2020). Privacy Right Clearinghouse.

H. Asmara. (2019). Tanggung Jawab Hukum Pejabat Publik: : Teori dan Praktik. Sinar Grafika.

H. Sudjana. (2019). Transparansi dan Akuntabilitas Dalam Administrasi Publik. Remaja Rosdakarya.

IBM Security. (2020). Cost of a Data Breach Report 2020. IBM.

Indonesia Corruption Watch (ICW). (2023). Laporan Advokasi Kebocoran Data Kominfo 2023. Akarta: ICW.

Jimly Asshiddiqie. (2021). Konstitusi dan Konstitusionalisme. Sinar Grafika.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). Laporan Insiden Kebocoran Data di Indonesia.

Organisation for Economic Co-operation and Development (OECD). (2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing.

R. Subekti. (2013). Pokok-Pokok Hukum Perdata. Intermasa.

S. Mulyadi. (2020). Hukum Perdata dan Tanggung Jawab Hukum: Sebuah Pendekatan Praktis. Mandar Maju.

Siti Rahayu. (2021). Hukum Perlindungan Data Pribadi. Sinar Grafika.

Sutedi. (2014). Hukum Perlindungan Data Pribadi. Sinar Grafika.

Verizon. (2024). Data Breach Investigations Report 2024. New York: Verizon Business.

Jurnal

Budi Santoso, Vieta Imelda Cornelis, Ernu Widodo, H. (2025). Penggunaan Teknologi Informasi dalam Administrasi Kependudukan Pada Era Digital. Lex Journal: Kajian Hukum & Keadilan, 9 No. 2, 345–361.

Christine, B. (2022). Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Syntax Literate*. Membahas kendala implementasi UU PDP dalam praktik. =

Dennis F. Thompson. (2014). Moral Responsibility of Public Officials: The Problem of Many Hands. American Political Science Review, 74, 905–916.

European Union. (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union, Data Protection.

Fadhli, B., & Ikrom, D. (2024). Terhadap Kebocoran Data Pribadi Di Indonesia Universitas Islam Negeri Fakultas Syariah Juni 2024 Indonesia.

Simanjuntak, P. H. (2024). Perlindungan Hukum terhadap Data Pribadi pada Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Esensi Hukum*. Artikel ini mengevaluasi efektivitas penerapan UU PDP dan membandingkannya dengan GDPR. https://journal.upnvj.ac.id/index.php/esensihukum/article/view/412?utm_source=

Internet

Asshiddiqie, Jimly. "Pancasila Konsensus Kehidupan Berbangsa." *Dkpp*, 2014. Https://Dkpp.Go.Id/Prof-Jimly-Pancasila-Konsensus-Kehidupan-Berbangsa/.

CNN Indonesia. (2022). Deret Respons Pemerintah yang Dianggap Angin Lalu Oleh Bjorka. CNN.

https://www.cnnindonesia.com/teknologi/20220912075317-192-846433/deret-respons-pemerintah-yang-dianggap-angin-lalu-oleh-bjorka

Nafiatul Munawaroh. (2023). Tanggung Jawab Pemerintah atas Kebocoran Data Pribadi. Hukum Online2. https://www.hukumonline.com/klinik/a/tanggung-jawab-pemerintah-atas-kebocoran-data-pribadi-lt66881c826cc33/

Tim Hukum Online. (2023). Dasar Hukum Perlindungan Data Pribadi. Hukum Online. https://www.hukumonline.com/berita/a/dasar-hukum-perlindungan-data-pribadi-lt638d55f57a6d0/

Transparency International. (2024). Corruption Perceptions Index 2024. Transparency International. https://www.transparency.org/en/cpi/2024

World Bank. (2023). Worldwide Governance Indicators 2023. Washington, DC: World Bank. https://info.worldbank.org/governance/wgi/

CNN Indonesia. *Diduga 1,3 Miliar Data Registrasi SIM Card Bocor*. https://www.cnnindonesia.com/teknologi/20220901102120-192-841845/diduga-13-miliar-data-registrasi-sim-card-bocor

Proceeding

Ioannidis, N. (2021). Personal data protection digest. In Border Control and New Technologies. https://doi.org/10.46944/9789461171375.4

Perundang-Undangan

Undang-Undang Negara Republik Indonesia 1945

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), peraturan pemerintah, dan dokumen resmi lainnya yang mengatur tentang pengelolaan dan perlindungan data pribadi di Indonesia.

Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban