

PERLINDUNGAN HUKUM KEBOCORAN DATA PRIBADI YANG DILAKUKAN PEMERINTAH BERDASARKAN PERATURAN PERUNDANG-UNDANGAN DI INDONESIA

Priska Anggreini Korompis¹, Reynold Simandjuntak², Marven A. Kasenda³

Program Studi Ilmu Hukum, Universitas Negeri Manado, Indonesia ^{1,2,3}

Corresponding Author: anggreinipriska@gmail.com^{1*}, reynoldssimanjuntak@unima.ac.id², marvenkasenda@unima.ac.id³

Info Artikel

Received: 08 Mei 2026

Revised : 21 Mei 2026

Accepted: 19 Juni 2026

Published: 30 Juni 2026

Keywords: legal protection, personal data breaches, government, Personal Data Protection Act.

Kata Kunci: perlindungan hukum, kebocoran data pribadi, pemerintah, UU PDP.

Abstract

This study aims to analyze legal protections against personal data breaches committed by the government and to identify the forms of government liability for such breaches based on Indonesian laws and regulations. The background of this study is rooted in the increasing risk of data breaches in the digital age, where personal data has become a valuable asset. One of the cases examined is the alleged leak of 6 million Taxpayer Identification Numbers (NPWP) involving data ranging from government officials to the general public. The research method employed is normative legal research using a statutory approach and a conceptual approach. Primary legal sources include the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection (PDP Law), and Government Regulation No. 71 of 2019. The research findings indicate that the protection of personal data constitutes a constitutional right of citizens guaranteed under Article 28G(1) of the 1945 Constitution of the Republic of Indonesia. Under the Personal Data Protection Act (PDP Act), the government, in carrying out its public service functions, acts as both a "Public Body" and a "Personal Data Controller" with an absolute obligation to safeguard the public's data. In theory, the government should act as a guardian that provides a sense of security. However, weak cybersecurity systems and negligence in meeting security standards have led to failures in fulfilling this protective role. The government has a legal responsibility to process data in accordance with robust security principles to protect data subjects from harm resulting from information leaks.

Abstrak

Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap kebocoran data pribadi yang dilakukan oleh pemerintah serta mengetahui bentuk pertanggungjawaban pemerintah atas kebocoran tersebut berdasarkan peraturan perundang-undangan di Indonesia. Latar belakang penelitian ini didasarkan pada meningkatnya risiko kebocoran data di era digital, di mana data pribadi telah menjadi aset berharga. Salah satu kasus yang diangkat adalah dugaan kebocoran 6 juta data Nomor Pokok Wajib Pajak (NPWP) yang melibatkan data pejabat negara hingga masyarakat umum. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konsep (*conceptual approach*). Bahan hukum primer mencakup Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang

Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan Peraturan Pemerintah Nomor 71 Tahun 2019. Hasil penelitian menunjukkan bahwa perlindungan data pribadi merupakan hak konstitusional warga negara yang dijamin dalam Pasal 28G ayat (1) UUD NRI 1945. Berdasarkan UU PDP, pemerintah dalam menjalankan fungsi pelayanan publik berkedudukan sebagai "Badan Publik" sekaligus "Pengendali Data Pribadi" yang memiliki kewajiban mutlak untuk menjaga keamanan data masyarakat. Secara teoretis, pemerintah harus bertindak sebagai pengayom yang memberikan rasa aman. Namun, lemahnya sistem keamanan siber dan kelalaian dalam memenuhi standar keamanan mengakibatkan kegagalan dalam menjalankan fungsi pengayoman tersebut. Pemerintah memiliki tanggung jawab hukum untuk melakukan pemrosesan data dengan prinsip keamanan yang kuat guna melindungi subjek data dari kerugian akibat kebocoran informasi.



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

Publisher: Lembaga Penerbit Penelitian Multidisipliner

PENDAHULUAN

Indonesia, negara kepulauan terbesar di dunia, masih menyandang status sebagai negara berkembang. Hal ini tercermin dari beberapa indikator kunci seperti pendapatan per kapita yang relatif rendah, tingkat kemiskinan yang masih perlu ditekan, serta ketimpangan ekonomi yang cukup tinggi. Meskipun angka pengangguran menunjukkan tren penurunan, namun kualitas lapangan kerja dan tingkat upah layak menjadi tantangan tersendiri.

Di sisi lain, Indonesia memiliki modal kuat untuk bertransformasi menjadi negara maju. Sumber daya alam yang melimpah, jumlah penduduk yang besar, dan posisi geografis yang strategis merupakan aset berharga yang perlu dioptimalkan. Bonus demografi, di mana penduduk usia produktif mendominasi, menjadi peluang emas untuk akselerasi pertumbuhan ekonomi. Pemerintah Indonesia menyadari tantangan dan peluang tersebut, dan terus berupaya meningkatkan pembangunan di berbagai sector. Pengembangan ekonomi digital dan pemanfaatan teknologi juga didorong untuk menciptakan lapangan kerja baru dan meningkatkan daya saing.

Meskipun jalan menuju negara maju masih panjang, Indonesia memiliki potensi besar untuk mencapai tujuan tersebut. Dengan komitmen kuat dari pemerintah, dukungan dari seluruh elemen masyarakat, dan pemanfaatan teknologi secara optimal, Indonesia optimis dapat meraih kemajuan dan kesejahteraan bagi seluruh rakyatnya. Di era digital saat ini semua serba terhubung, data pribadi telah menjelma menjadi aset berharga, bahkan sering disebut sebagai "emas baru". Sayangnya, semakin meningkatnya nilai data pribadi juga diiringi dengan meningkatnya risiko kebocoran data. Fenomena kebocoran data pribadi kini menjadi ancaman serius yang menghantui individu, organisasi,

bahkan negara.

Warga negara memiliki hak konstitusional yakni hak yang dijamin oleh Undang-Undang. Negara memiliki kewajiban konstitusional, untuk melindungi seluruh warga negara. Kewajiban konstitusional negara ini telah tertuang dalam Pembukaan Alinea keempat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD RI 1945) yang menyatakan bahwa negara wajib melindungi segenal bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial.

Setiap orang pasti memiliki data pribadi, data pribadi merupakan sesuatu yang melekat pada setiap orang. Data pribadi merupakan sesuatu yang bersifat sensitif dan harus dilindungi karena sejatinya merupakan hak privasi setiap orang. Hak privasi adalah hak konstitusional warga negara yang telah diatur dalam Undang – Undang Dasar Negara republik Indonesia Tahun 1945.¹ Dasar hukum dalam perlindungan data pribadi yaitu Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.² Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat Data Pribadi.³

Hak pribadi merupakan hal yang sensitif yang berkaitan dengan data pribadi atau identitas seseorang. Identitas tersebut mulai dari Kartu Tanda Penduduk (KTP), Surat Ijin Mengemudi (SIM), paspor, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), nomor rekening, sidik jari, ciri khas seseorang dan sebagainya. Jual beli data pribadi telah menjadi bayang-bayang gelap di era digital. Informasi pribadi yang seharusnya dilindungi, kini diperdagangkan layaknya komoditas di pasar gelap dunia maya. Data seperti nama, alamat, nomor telepon, hingga informasi keuangan menjadi incaran para pelaku kejahatan siber yang tak bertanggung jawab.

Kasus kebocoran data pribadi ini bukan pertama kali terjadi. Selama kepemimpinan Presiden Joko Widodo, kasus kebocoran data terus berulang. Sebanyak 6 juta data nomor pokok wajib pajak atau NPWP diduga diperjualbelikan dengan harga sekitar Rp 150 juta. Hal ini didasarkan pada unggahan akun Bjorka pada Rabu, 18 September 2024. Data yang bocor antara lain nomor induk kependudukan (NIK), NPWP, alamat, nomor kontak telepon seluler, dan surat elektronik atau e-mail.

¹ Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, *Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*, Jurnal Ilmu Hukum, Vol. 2, No. 1, 1 April 2021, hlm. 2

² Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

³ Pasal 1 angka 6 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Dugaan bocornya data NPWP mencuat ketika pendiri Ethical Hacker Indonesia, Teguh Aprianto, mengunggah tangkapan layar situs web Breach Forums yang berisi tentang telah diretasnya 6 juta data NPWP. Di antara 6 juta data yang diretas itu termasuk milik Presiden Joko Widodo; anak sulungnya, Gibran Rakabuming Raka; Menteri Keuangan Sri Mulyani; dan Menteri Koordinator Perekonomian Airlangga Hartarto.⁴

Motif di balik praktik ilegal ini beragam, mulai dari keuntungan finansial hingga kepentingan politik. Data pribadi yang bocor dapat dimanfaatkan untuk berbagai tindakan kriminal, seperti pencurian identitas, penipuan online, hingga manipulasi data untuk memengaruhi opini publik. Ironisnya, kemajuan teknologi yang seharusnya memudahkan kehidupan justru menjadi celah bagi perdagangan data pribadi. Kebocoran data dari berbagai platform digital, kurangnya kesadaran masyarakat akan pentingnya melindungi informasi pribadi, serta lemahnya penegakan hukum menjadi faktor pendorong maraknya praktik ini.

Dampak dari jual beli data pribadi sangat merugikan, baik bagi individu maupun masyarakat luas. Kehilangan privasi, kerugian finansial, hingga terganggunya stabilitas keamanan nasional menjadi ancaman nyata. Oleh karena itu, upaya pencegahan dan penindakan perlu dilakukan secara serius dan terkoordinasi. Penguatan regulasi dan penegakan hukum yang tegas, peningkatan sistem keamanan siber, serta edukasi kepada masyarakat menjadi kunci dalam memberantas jual beli data pribadi. Perlindungan data pribadi bukan hanya tanggung jawab pemerintah atau lembaga tertentu, melainkan tanggung jawab kita bersama dalam mewujudkan ruang digital yang aman dan terpercaya.

METODE PENELITIAN

Jenis Penelitian

Penelitian secara ilmiah dilakukan oleh manusia untuk menyalurkan hasrat ingin tahu yang telah mencapai taraf ilmiah, disertai dengan suatu kenyataan bahwa setiap gejala akan dapat ditelaah dan dicari hubungan sebab akibatnya. Jenis penelitian skripsi ini adalah penelitian normatif. Banyak sarjana yang telah menjelaskan pemahaman terhadap penelitian Hukum Normatif, lebih lanjut dikemukakan oleh Pieter Mahmud Marzuki penelitian hukum adalah suatu proses untuk menemukan aturan hukum, prinsip prinsip hukum maupun doktrin doktrin hukum guna menjawab isu hukum yang dihadapi. Penelitian hukum ini dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai perspektif dalam menyelesaikan masalah masalah yang dihadapi, sehingga jawaban yang

⁴ Tempo, 21 September 2024, Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah, <https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403>

diharapkan dalam penelitian adalah benar. Dengan demikian dapat dikatakan bahwa hasil yang diperoleh didalam penelitian hukum sudah mengandung nilai.⁵

Untuk kajian dogmatik hukum, kajiannya dilakukan terhadap Perlindungan Hukum Kebocoran Data Pribadi Yang Dilakukan Pemerintah Berdasarkan Peraturan Perundang-undangan di Indonesia. Untuk teori hukum yang digunakan dilakukan telaah sebagai pisau analisis dalam masalah penerapan hukum.

Pendekatan Penelitian

Metode pendekatan yang dipakai dalam penelitian ini disesuaikan dengan penelitian yang dilakukan, dimana penelitian ini merupakan penelitian hukum normatif. Di dasarkan pada isu hukum yang ada dalam penelitian ini, maka penelitian ini menggunakan pendekatan yaitu:

1. Pendekatan perundang undangan (statuta approach) dipakai untuk menelaah semua peraturan perundang undangan dan regulasi yang berkaitan dengan Data Pribadi.
2. Pendekatan konsep (conceptual approach) dipakai untuk mempelajari konsep-konsep atau doktrin-doktrin yang berkembang terkait dengan Perlindungan Hukum Data Pribadi. Dengan mempelajari konsep konsep tersebut maka peneliti mampu membangun argumentasi hukum dalam memecahkan isu hukum dalam penelitian.

Jenis dan Sumber Bahan Hukum

Bahan hukum yang dibutuhkan dalam jenis penelitian ini berupa bahan hukum baik hukum primer, bahan hukum sekunder maupun bahan hukum tersier. Bahan hukum primer adalah bahan hukum yang terdiri atas peraturan perundang-undangan, catatan resmi atau risalah dalam peraturan perundang-undangan. Bahan hukum primer meliputi UUD NRI Tahun 1945 dan peraturan perundang undangan antara lain:

1. Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi
2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Sedangkan Bahan Hukum Sekunder dalam penelitian ini adalah: Jurnal Hukum, buku buku referensi, skripsi. Bahan Hukum Tersier terdiri Kamus Hukum, Kamus Bahasa Indonesia dan Ensiklopedia.

Teknik Penelusuran Bahan Hukum

⁵ Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta; Prana Media, 2005), hlm 29.

Teknik penelusuran hukum primer dan bahan hukum sekunder dilakukan dengan cara studi literatur (kajian pustaka) dan searching internet serta inventarisasi peraturan perundang-undanganyang terkait dengan permasalahan yang akan dibahas, kemudian peraturan perundang-undangan tersebut dikelompokkan berdasarkan hirarkinya. Bahan hukum yang telah diperoleh kemudian dipelajari, diedit dan dikelompokkan serta dianalisis sesuai dengan rumusan masalah yang dikemukakan dalam skripsi ini.

Teknik Analisa Bahan Hukum

Setelah semua bahan hukum terkumpul, kegiatan selanjutnya yang dilakukan adalah melakukan analisis terhadap bahan hukum primer dan sekunder yang telah diperoleh. Adapun teknik analisis dalam penelitian ini dilakukan secara perspektif analitis, yang bertujuan untuk menghasilkan apa yang seharusnya sebagai esensial dalam penelitian hukum yang berpegang pada karakter ilmu hukum sebagai ilmu serapan. Hasil analitis menggunakan logika hukum, argumentasi hukum dan asas hukum yang akan menghasilkan kesimpulan atau conclusion sebagai jawaban atas rumusan masalah dalam penelitian.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Kebocoran Data Pribadi Yang Dilakukan Pemerintah Berdasarkan Peraturan Perundang-undangan di Indonesia

Negara Indonesia sebagai negara hukum (Rechtsstaat)⁶ memiliki konsekuensi logis bahwa segala tindakan penyelenggaraan negara harus didasarkan pada hukum yang bertujuan untuk melindungi warga negaranya. Secara filosofis, keberadaan negara dibentuk atas dasar kesepakatan masyarakat (kontrak sosial) untuk menjamin keamanan dan kesejahteraan bersama. Dalam konteks era digital saat ini, rasa aman tidak hanya dimaknai secara fisik, melainkan juga mencakup keamanan dalam ranah siber, khususnya perlindungan terhadap data pribadi yang telah menjadi aset berharga bagi setiap individu.

Landasan konstitusional yang paling fundamental bagi tanggung jawab pemerintah dalam melindungi data pribadi terdapat dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945). Pada Alinea keempat, secara tegas dinyatakan bahwa tujuan dibentuknya Pemerintah Negara Indonesia adalah untuk "melindungi segenap bangsa Indonesia dan

⁶ M. Tasbir Rais, Negara Hukum Indonesia: Gagasan Dan Penerapannya, Jurnal Hukum Unsulbar , Vol 5 No 2 (2022), 11-31

seluruh tumpah darah Indonesia" serta "memajukan kesejahteraan umum".⁷ Frasa "melindungi segenap bangsa" mengandung mandat imperatif bahwa negara wajib hadir memberikan perlindungan terhadap segala ancaman yang dapat merugikan warganya, termasuk ancaman kebocoran data pribadi yang dikelola oleh pemerintah itu sendiri.

Kewajiban konstitusional tersebut semakin dipertegas dalam batang tubuh UUD NRI 1945, khususnya Pasal 28G ayat (1). Pasal ini menjamin bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".⁸ Ketentuan ini menjadi landasan yuridis bahwa data pribadi merupakan bagian dari "diri pribadi" yang melekat pada hak asasi manusia. Oleh karena itu, perlindungan data pribadi adalah hak konstitusional warga negara yang tidak dapat ditawar.

Dalam perspektif hak asasi manusia, data pribadi bukan sekadar kumpulan informasi administratif, melainkan representasi dari identitas dan privasi seseorang yang harus dihormati. Hak privasi adalah hak konstitusional warga negara yang telah diatur dalam konstitusi.⁹ Ketika data pribadi seperti NIK atau NPWP bocor, hal itu sama dengan terlanggarnya martabat dan privasi warga negara tersebut. Negara, dalam hal ini pemerintah, memiliki peran ganda: sebagai pengumpul data untuk keperluan administrasi negara, sekaligus sebagai penjamin hak asasi agar data tersebut tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Untuk menganalisis efektivitas perlindungan tersebut, penelitian ini menggunakan Teori Perlindungan Hukum yang dikemukakan oleh Fitzgerald. Sebagaimana dikutip oleh Satjipto Raharjo, teori ini bersumber dari aliran hukum alam yang memandang hukum dan moral tidak dapat dipisahkan. Fitzgerald menjelaskan teori perlindungan hukum Salmond bahwa hukum bertujuan mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat. Perlindungan terhadap kepentingan tertentu (seperti data pribadi warga) hanya dapat dilakukan dengan cara membatasi kepentingan di lain pihak (kewenangan pemerintah atau akses pihak ketiga).

Lebih lanjut, Satjipto Raharjo mendefinisikan perlindungan hukum sebagai upaya

⁷ Tomy Michael, Korelasi Alinea Keempat Undang-Undang Dasar NRI Tahun 1945 Dengan Pemikiran Immanuel Kant, *Jurnal Hukum Samudra Keadilan*, Volume 11, Nomor 2, Juli-Desember 2016, 185-195

⁸ Ita Iya Pulina Perangin-angin, Rahayu, Nuswantoro Dwiwarno, Kewajiban Dan Tanggungjawab Negara Memberikan Perlindungan Hukum Terhadap Perempuan Korban Revenge Porn di Indonesia, *Diponegoro Law Journal*, Volume 8, Nomor 1, Tahun 2019, 457-482

⁹ Sekaring Ayumeida Kusnadi, Andy Usmina Wijaya, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *JA: Jurnal Al-Wasath* 2 No.1: 19-32

memberikan pengayoman kepada hak asasi manusia yang dirugikan oleh orang lain.¹⁰ Definisi "pengayoman" ini sangat relevan jika dikaitkan dengan kasus kebocoran data yang dilakukan oleh pemerintah. Pemerintah harusnya bertindak sebagai pengayom yang memberikan rasa aman, bukan justru menjadi sumber kerawanan karena kelalaian dalam menjaga sistem keamanan data. Perlindungan hukum harus dimaknai sebagai upaya aktif aparat penegak hukum dan pemerintah untuk memberikan rasa aman baik secara pikiran maupun fisik dari gangguan dan ancaman.

Dalam konteks kebocoran data NPWP, teori perlindungan hukum ini menyoroti ketimpangan posisi antara pemerintah sebagai penguasa data dan masyarakat sebagai pemilik data. Masyarakat diwajibkan menyerahkan data pribadi (seperti NIK dan NPWP) kepada negara sebagai syarat administrasi. Sesuai teori perlindungan hukum, ketika masyarakat telah menyerahkan hak privasinya demi kepatuhan hukum, maka hukum wajib memberikan timbal balik berupa jaminan keamanan. Jika pemerintah gagal melindungi data tersebut, maka pemerintah telah gagal menjalankan fungsi pengayoman yang menjadi inti dari perlindungan hukum itu sendiri.

Analisis berdasarkan teori ini juga sejalan dengan pandangan Setiono, yang menyatakan bahwa perlindungan hukum adalah tindakan untuk melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum. Kebocoran data yang disebabkan oleh lemahnya sistem keamanan siber pemerintah dapat dikategorikan sebagai bentuk "kesewenang-wenangan" pasif bukan karena niat jahat, tetapi karena kelalaian dalam memenuhi standar keamanan yang diwajibkan undang-undang. Masyarakat menjadi korban karena ketidakmampuan penguasa dalam mengelola amanah data tersebut.

Konsekuensi yuridis dari status sebagai Pengendali Data Pribadi adalah melekatnya kewajiban untuk menjaga kerahasiaan dan keamanan data. Pasal-pasal dalam UU PDP menegaskan bahwa Pengendali Data Pribadi wajib melakukan pemrosesan data dengan prinsip keamanan yang kuat guna melindungi data dari akses yang tidak sah, pengungkapan yang tidak sah, atau penyalahgunaan lainnya. Kewajiban ini bersifat mutlak dan tidak gugur hanya karena statusnya sebagai lembaga negara. Pemerintah harus menjamin bahwa data yang dikumpulkan yang sering kali bersifat wajib bagi warga negara untuk diserahkan, seperti data kependudukan atau perpajakan dikelola dengan standar keamanan sistem elektronik yang andal dan terpercaya.

Relevansi kedudukan ini terlihat jelas dalam kasus dugaan kebocoran 6 juta data Nomor Pokok Wajib Pajak (NPWP) yang mencuat ke publik. Dalam kasus ini, Direktorat Jenderal Pajak

¹⁰ JH. Sinaulan, *Perlindungan Hukum Terhadap Warga Masyarakat*, IDEAS : Volume 04 Nomor 01 Februari 2018, 79-84

(DJP) di bawah Kementerian Keuangan bertindak sebagai Badan Publik sekaligus Pengendali Data Pribadi. Masyarakat menyerahkan data sensitif berupa NIK, NPWP, alamat, hingga data keuangan kepada DJP sebagai bentuk kepatuhan terhadap undang-undang perpajakan. Karena pengumpulan data ini bersifat mandatori (wajib), maka beban tanggung jawab pemerintah menjadi lebih besar dibandingkan sektor swasta. Kegagalan dalam melindungi data tersebut menempatkan instansi pemerintah terkait sebagai pihak yang telah lalai dalam menjalankan kewajibannya sebagai Pengendali Data Pribadi sebagaimana diamanatkan oleh undang-undang.

Kedudukan pemerintah sebagai Pengendali Data Pribadi juga mengharuskan adanya akuntabilitas. Jika terjadi kebocoran data, pemerintah tidak dapat berlindung di balik dalih "kesalahan sistem" atau serangan siber eksternal semata. Sebagai subjek hukum yang mengendalikan data, pemerintah wajib membuktikan bahwa mereka telah menerapkan langkah-langkah teknis dan organisasional yang memadai untuk melindungi data tersebut. Dalam teori kepastian hukum, masyarakat membutuhkan jaminan bahwa data yang mereka serahkan kepada negara dikelola oleh entitas yang bertanggung jawab. Kebocoran data NPWP, yang bahkan menimpa Presiden dan para menteri, menunjukkan bahwa "benteng" perlindungan data di instansi pemerintah masih rapuh, padahal kedudukan hukum mereka mewajibkan standar keamanan tertinggi.

Perlindungan hukum dalam konteks kebocoran data pribadi tidak hanya berbicara mengenai bagaimana menyelesaikan masalah setelah data tersebar, melainkan lebih diutamakan pada aspek pencegahan atau perlindungan hukum preventif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya sengketa atau pelanggaran hukum sebelum hal itu terjadi.¹¹ Dalam ranah tata kelola data pemerintahan, perlindungan ini mewujudkan dalam bentuk kewajiban hukum bagi pemerintah untuk membangun dan memelihara infrastruktur keamanan siber yang kuat. Kewajiban ini bukan sekadar imbauan moral, melainkan perintah undang-undang yang mengikat pemerintah sebagai pengendali data untuk menutup segala celah kemungkinan terjadinya kebocoran.

Dasar hukum utama bagi perlindungan preventif ini tertuang dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Pemerintah, sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Publik, dibebani kewajiban mutlak untuk menyelenggarakan sistem elektronik secara andal dan aman. Frasa "andal dan aman" memiliki implikasi hukum bahwa sistem yang digunakan oleh instansi pemerintah seperti server Direktorat Jenderal Pajak (DJP) harus memiliki ketahanan terhadap serangan siber, kegagalan sistem,

¹¹ Socha Tcefortin Indera Sakti, *Perlindungan Hukum Bagi Para Pihak Dalam Perjanjian Jual Beli Tanah Letter C Di Bawah Tangan*, Jurnal Privat Law Vol. VIII No. 1 Januari-Juni 2020, 144-150

serta kesalahan manusia (human error).

Tanpa adanya kepastian hukum dalam aspek preventif, masyarakat kehilangan pegangan. Van Apeldoorn, yang pandangannya sejalan dengan konsep kepastian hukum, menyebutkan bahwa kepastian hukum memiliki dua segi: dapat ditentukannya hukum dalam hal konkret dan keamanan hukum. Aspek "keamanan hukum" inilah yang tercederai. Masyarakat (yustisiabel) menyerahkan data pribadi dengan harapan memperoleh keamanan hukum. Ketika perlindungan preventif gagal, masyarakat merasa tidak ada lagi batas yang jelas antara ruang privat dan ruang publik, yang berujung pada ketidakpercayaan terhadap sistem hukum negara.

Analisis ini juga relevan dengan pandangan bahwa hukum harus mampu melindungi masyarakat dari tindakan yang merugikan dan menjadi pedoman hidup. Jika perlindungan preventif dijalankan dengan benar sesuai prinsip kepastian hukum, maka pemerintah seharusnya memiliki Prosedur Operasional Standar (SOP) yang ketat dan sanksi internal yang tegas untuk mencegah kebocoran. Ketiadaan atau lemahnya implementasi SOP keamanan siber di instansi pemerintah merupakan bentuk pengabaian terhadap asas kepastian hukum itu sendiri.

Dengan demikian, perlindungan hukum preventif sejatinya adalah wujud nyata dari asas kepastian hukum di era digital. Aturan-aturan dalam PP PSTE dan UU PDP adalah instrumen untuk menciptakan kepastian tersebut. Namun, instrumen ini menjadi tumpul ketika pelaksanaannya (pemerintah) tidak menjalankannya dengan disiplin tinggi. Kepastian hukum menuntut agar pemerintah, sebagai pembuat sekaligus pelaksana aturan, konsisten dalam menerapkan standar keamanan siber yang tinggi.

Kesimpulannya, kegagalan perlindungan preventif yang berujung pada kebocoran data pribadi oleh pemerintah bukan hanya masalah teknis informatika, melainkan masalah hukum yang serius. Hal ini mencederai asas kepastian hukum yang mensyaratkan adanya jaminan keamanan bagi subjek hukum. Tanpa perbaikan fundamental pada aspek preventif yakni penguatan sistem keamanan siber yang sesuai dengan amanat undang-undang maka kepastian hukum dalam perlindungan data pribadi di Indonesia hanya akan menjadi aturan di atas kertas tanpa memberikan perlindungan nyata bagi masyarakat.

Berdasarkan keseluruhan analisis yang telah diuraikan, dapat disimpulkan bahwa secara normatif, perlindungan hukum terhadap data pribadi yang dikelola oleh pemerintah Indonesia sesungguhnya telah memiliki landasan yang kuat dan berlapis. Dimulai dari landasan filosofis tertinggi dalam Pembukaan UUD NRI 1945 dan Pasal 28G ayat (1) yang menempatkan hak privasi sebagai hak konstitusional, hingga aturan teknis dalam Undang-Undang Nomor 27 Tahun 2022

tentang Pelindungan Data Pribadi (UU PDP) serta PP Nomor 71 Tahun 2019. Regulasi ini secara tegas mendudukan pemerintah bukan hanya sebagai regulator, melainkan sebagai subjek hukum berupa "Badan Publik" dan "Pengendali Data Pribadi" yang memikul tanggung jawab mutlak untuk menjamin kerahasiaan dan keamanan data masyarakat melalui standar sistem elektronik yang andal. Dengan demikian, dalam tataran teoritis (Das Sollen), hukum Indonesia telah memenuhi unsur Teori Perlindungan Hukum sebagaimana dikemukakan Satjipto Raharjo, di mana negara hadir memberikan pengayoman terhadap hak asasi warganya.

Aanalisis fakta hukum melalui kasus kebocoran 6 juta data NPWP menunjukkan adanya kegagalan serius dalam implementasi perlindungan hukum tersebut, khususnya pada aspek preventif atau pencegahan. Fakta bahwa data strategis milik publik, bahkan milik pejabat tinggi negara, dapat diperjualbelikan dengan mudah membuktikan bahwa sistem keamanan siber pemerintah tidak memenuhi standar "aman dan andal" yang diperintahkan undang-undang. Kegagalan ini mencederai Teori Kepastian Hukum dari Gustav Radbruch, karena hukum yang tertulis di atas kertas tidak sejalan dengan fakta empiris di lapangan, sehingga masyarakat kehilangan jaminan keamanan dan prediktabilitas atas nasib data pribadi yang mereka serahkan kepada negara. Pemerintah terbukti lalai menerapkan prinsip kehati-hatian dalam memproses data yang bersifat sensitif.

Sebagai konsekuensinya, mekanisme perlindungan hukum represif menjadi instrumen terakhir yang harus ditegakkan untuk memulihkan hak korban. Meskipun UU PDP menyediakan jalur hak gugat ganti rugi dan kewajiban notifikasi kegagalan perlindungan bagi pemerintah, efektivitasnya masih terhambat oleh lemahnya penegakan hukum dan budaya penyangkalan dalam birokrasi. Terjadi kesenjangan (gap) yang lebar antara regulasi yang ideal (Das Sollen) dengan realitas kebocoran yang terus berulang (Das Sein). Oleh karena itu, perlindungan hukum yang ada saat ini dinilai belum efektif karena hanya kuat secara tekstual namun rapuh secara operasional, yang menuntut adanya evaluasi menyeluruh terhadap infrastruktur keamanan siber pemerintah serta penerapan sanksi yang lebih tegas tanpa pandang bulu demi mengembalikan kepercayaan publik.

Pertanggung Jawaban Pemerintah atas Kebocoran Data Pribadi Berdasarkan Peraturan Perundang-undangan di Indonesia

Pemerintah adalah organisasi jabatan (ambt) yang tersusun atas berbagai organ untuk menjalankan fungsi publik. Dalam menguraikan pertanggungjawaban pemerintah atas kebocoran data pribadi, langkah fundamental yang harus dilakukan adalah membedah konstruksi hukum mengenai siapa sesungguhnya yang memikul beban tanggung jawab tersebut. Apakah beban itu jatuh

pada institusi negara secara kelembagaan, ataukah kepada individu pejabat yang sedang menduduki kursi kekuasaan? Pertanyaan ini krusial karena dalam Hukum Administrasi Negara (HAN), pemerintah dipandang sebagai sebuah entitas yang kompleks, bukan sekadar kumpulan individu.

Secara teoritis, pemahaman mengenai tanggung jawab negara tidak dapat dilepaskan dari konsep "jabatan" (ambt). Jabatan adalah lingkungan pekerjaan tetap yang diadakan dan dilakukan guna kepentingan negara atau kepentingan umum. Jabatan merupakan subjek hukum yang mandiri, yang kepadanya dilekatkan hak dan kewajiban serta kewenangan untuk melakukan tindakan hukum publik.¹² Oleh karena itu, dalam kacamata hukum publik, yang bertindak melayani masyarakat atau mengelola data warga negara sejatinya adalah "jabatan", bukan manusia pribadi.

Jabatan sebagai subjek hukum adalah entitas yang abstrak dan mati. Ia tidak dapat berpikir, berkehendak, atau bertindak sendiri. Agar jabatan tersebut dapat beroperasi, diperlukan manusia-manusia yang menjalankannya. Manusia inilah yang disebut sebagai "pejabat" (ambtsdrager). Pejabat adalah personifikasi dari jabatan; ia bertindak untuk dan atas nama jabatan. Pemisahan yang tegas antara "jabatan" sebagai institusi dan "pejabat" sebagai personel merupakan prinsip dasar dalam hukum modern untuk menjamin kelangsungan pelayanan publik.

Keseimbangan antara Tanggung Jawab Jabatan dan Tanggung Jawab Pribadi inilah yang menjadi inti dari akuntabilitas publik. Tanpa pemisahan ini, pemerintah akan selalu berlindung di balik imunitas jabatan, atau sebaliknya, pejabat akan selalu takut mengambil keputusan karena ancaman gugatan pribadi. Dalam era digital di mana data adalah aset strategis, pejabat pemerintah harus menyadari bahwa kelalaian mereka dalam menjaga data tidak hanya berisiko administratif bagi instansi, tetapi juga dapat menyeret mereka ke dalam pertanggungjawaban pribadi yang serius di hadapan hukum.

Sebagai simpulan analisis pada bagian ini, kasus kebocoran data NPWP idealnya dilihat dari dua sisi mata uang. Di satu sisi, instansi pemerintah telah gagal secara kelembagaan (institutional failure) dalam menyediakan benteng pertahanan siber yang memadai, sehingga Tanggung Jawab Jabatan berlaku mutlak. Di sisi lain, potensi keterlibatan oknum mengharuskan hukum untuk siap mengejar Tanggung Jawab Pribadi, memastikan bahwa tidak ada satu pun pejabat yang dapat bersembunyi di balik jubah kekuasaan negara ketika mereka dengan sengaja menggadaikan privasi warga negaranya.

Dalam kerangka hukum positif Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang

¹² Tedi Sudrajat, *Hukum Birokrasi Pemerintah Kewenangan dan Jabatan*, Sinar Grafika, Jakarta, 2017, h 8

Pelindungan Data Pribadi (UU PDP) hadir sebagai *lex specialis* yang mengatur secara spesifik mengenai tata kelola data pribadi. Undang-undang ini menjadi landasan utama dalam menentukan bentuk pertanggungjawaban yang harus dipikul oleh pihak-pihak yang memproses data pribadi, termasuk pemerintah. Secara yuridis, pertanggungjawaban administratif merupakan mekanisme penegakan hukum yang paling kedepan (*primum remedium*) dalam rezim hukum administrasi negara untuk memastikan kepatuhan terhadap standar perlindungan data. Oleh karena itu, analisis mengenai pertanggungjawaban pemerintah harus dimulai dari bagaimana UU PDP menempatkan posisi pemerintah dalam struktur kewajiban administratif tersebut.

Berdasarkan ketentuan UU PDP, pemerintah dikategorikan sebagai "Badan Publik". Definisi ini menempatkan instansi pemerintah seperti kementerian, lembaga negara, dan pemerintah daerah dalam posisi sebagai Pengendali Data Pribadi ketika mereka melakukan pemrosesan data masyarakat untuk tujuan pelayanan publik. Sebagai Pengendali Data Pribadi, instansi pemerintah terikat penuh pada kewajiban untuk melindungi data yang dikelolanya. Jika terjadi kebocoran data akibat kelalaian atau kegagalan sistem, maka instansi tersebut secara hukum telah melakukan pelanggaran administratif dan wajib dimintai pertanggungjawaban sesuai mekanisme yang diatur dalam undang-undang tersebut.

Bentuk sanksi administratif yang dapat dijatuhkan kepada Pengendali Data Pribadi diatur secara rinci dalam Pasal 57 UU PDP. Sanksi-sanksi ini dijatuhkan oleh lembaga pengawas yang berwenang. Adapun jenis sanksi administratif yang dikenakan meliputi peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, hingga denda administratif. Secara teoritis, sanksi administratif ini bertujuan untuk memulihkan keadaan dan memaksa pelanggar untuk menghentikan pelanggaranannya (*reparatoir*), bukan semata-mata untuk menghukum (*punitif*).

Namun, ketika masuk pada ranah implementasi sanksi terhadap pemerintah atau Badan Publik, terdapat perbedaan perlakuan yang signifikan dibandingkan dengan sektor swasta. UU PDP mengatur bahwa sanksi administratif berupa denda administratif tidak berlaku bagi Badan Publik. Artinya, instansi pemerintah yang terbukti lalai menjaga data warganya seperti dalam kasus dugaan kebocoran data NPWP hanya dapat dikenai sanksi berupa peringatan tertulis, penghentian sementara, atau perintah pemusnahan data, tanpa adanya konsekuensi finansial berupa pembayaran denda kepada negara.

Pengecualian sanksi denda bagi pemerintah ini menjadi titik krusial yang perlu dikritik menggunakan perspektif hukum. Secara normatif, hal ini menciptakan disparitas atau ketimpangan

dalam penegakan hukum. Korporasi swasta yang membocorkan data dapat didenda hingga 2% dari pendapatan tahunan mereka, sebuah angka yang sangat masif dan memaksa mereka untuk berinvestasi besar-besaran pada keamanan siber. Sebaliknya, pemerintah yang mengelola data dalam skala yang jauh lebih besar dan sensitif (seperti data kependudukan dan perpajakan) justru dibebaskan dari ancaman kerugian finansial tersebut.

Analisis menggunakan Teori Keadilan sebagaimana dikemukakan oleh Gustav Radbruch menunjukkan adanya ketidakadilan substantif dalam pengaturan ini. Keadilan menuntut perlakuan yang sama bagi subjek hukum yang melakukan pelanggaran yang sama (*equality before the law*).¹³ Ketika data warga bocor, kerugian yang diderita oleh subjek data adalah sama, tidak peduli apakah kebocoran itu disebabkan oleh bank swasta atau oleh Direktorat Jenderal Pajak. Namun, UU PDP memberikan privilese kepada pemerintah yang justru seharusnya menjadi teladan dalam kepatuhan hukum. Ketiadaan sanksi denda bagi pemerintah mencederai rasa keadilan masyarakat yang menjadi korban kelalaian negara.

Selanjutnya, ditinjau dari Teori Kepastian Hukum (*Rechtssicherheit*), sanksi hukum bertujuan untuk memberikan jaminan kepastian bahwa aturan akan ditegakkan dan pelanggaran akan dicegah.¹⁴ Efektivitas penegakan hukum sangat bergantung pada efek jera (*deterrent effect*) yang ditimbulkan oleh sanksi tersebut. Sanksi administratif berupa "peringatan tertulis" sering kali dianggap remeh dalam budaya birokrasi dan tidak memiliki daya paksa yang kuat. Tanpa adanya ancaman sanksi denda yang dapat membebani anggaran instansi, dorongan bagi pemerintah untuk memperbaiki sistem keamanan sibernya menjadi lemah.

Mekanisme penjatuhan sanksi oleh lembaga pengawas juga menjadi sorotan dalam pertanggungjawaban administratif ini. UU PDP mengamanatkan pembentukan lembaga pengawas yang ditetapkan oleh Presiden. Independensi lembaga ini akan diuji ketika harus menjatuhkan sanksi kepada sesama organ eksekutif (Badan Publik). Jika sanksi yang tersedia hanyalah sanksi ringan non-finansial, maka peran lembaga pengawas berpotensi hanya menjadi "macan ompong" di hadapan instansi pemerintah yang kuat, sehingga pertanggungjawaban administratif hanya menjadi formalitas di atas kertas tanpa dampak perbaikan yang nyata.

Sebagai simpulan analisis pada bagian ini, pertanggungjawaban administratif pemerintah

¹³ Maria Odilia Kolo, Aksi Sinurat, Karolus Kopong Medan, Tinjauan Yuridis Perlindungan Hukum terhadap Korban dan Pelaku Kejahatan Berdasarkan Asas *Equality Before the Law*, Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara Vol.2, No.2 Mei 2024, 130-142

¹⁴ Ronal Hasudungan Sianturi, Ahmad Feri Tanjung, Rony Andre Christian Naldo, Kepastian Hukum Implementasi Denda Damai Untuk Perkara Tindak Pidana Korupsi (*Legal Certainty in the Implementation of Peaceful Fines for Corruption Crime Cases*), JURNAL ILMIAH PENEGAKAN HUKUM : Vol. 12 No. 1 JUNI (2025), 41-47

berdasarkan UU PDP memang telah diatur, namun memiliki kelemahan mendasar pada aspek sanksi. Pengecualian denda administratif bagi Badan Publik menciptakan celah hukum yang melemahkan akuntabilitas pemerintah. Hal ini tidak hanya mencederai prinsip keadilan karena adanya diskriminasi perlakuan antara publik dan swasta, tetapi juga menggerus kepastian hukum karena minimnya efek jera yang dapat memaksa pemerintah untuk meningkatkan standar perlindungan data pribadinya secara serius.

Dasar hukum utama bagi gugatan ini bersandar pada Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata), yang menyatakan bahwa "tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk mengganti kerugian tersebut".¹⁵ Dalam konteks kebocoran data, unsur "melawan hukum" terpenuhi ketika pemerintah melanggar kewajiban hukumnya yang telah diatur dalam peraturan perundang-undangan, khususnya Undang-Undang Perlindungan Data Pribadi (UU PDP). Ketika instansi pemerintah gagal menjaga keamanan data sebagaimana dimandatkan oleh UU PDP, maka kegagalan tersebut dikualifikasikan sebagai perbuatan melawan hukum, baik karena kelalaian (*negligence*) maupun karena kurangnya kehati-hatian dalam menjalankan kewajiban undang-undang.

Melalui gugatan perdata ini, Subjek Data Pribadi memiliki hak untuk menuntut dua jenis ganti rugi, yaitu ganti rugi materiil dan imateriil. Ganti rugi materiil mencakup kerugian nyata yang dapat dihitung dengan uang, seperti terkurasnya saldo rekening akibat data perbankan yang bocor atau biaya yang dikeluarkan untuk memulihkan akses akun. Sementara itu, ganti rugi imateriil mencakup kerugian yang bersifat moril, seperti rasa malu, kecemasan, ketakutan, dan terganggunya privasi akibat data pribadinya tersebar luas di internet. Pengakuan terhadap kerugian imateriil ini sangat penting dalam kasus perlindungan data, mengingat dampak kebocoran sering kali lebih menyerang aspek psikologis dan reputasi korban daripada aspek finansial semata.

Analisis terhadap urgensi pertanggungjawaban perdata ini tidak dapat dilepaskan dari landasan filosofis tanggung jawab negara. Pemerintah wajib memberikan ganti rugi bukan hanya karena aturan teknis KUHPerdata, melainkan karena telah gagal menjalankan kewajiban konstitusionalnya untuk "melindungi segenap bangsa Indonesia". Kegagalan melindungi data warga negara adalah bentuk cidera janji konstitusi. Hal ini sejalan dengan Teori Perlindungan Hukum dari Satjipto Raharjo yang menekankan bahwa hukum harus memberikan pengayoman kepada hak asasi

¹⁵ Mendy Cevitra, Gunawan Djajaputra, Perbuatan Melawan Hukum (Onrechtmatige Daad) Menurut Pasal 1365 Kitab Undang-Undang Hukum Perdata dan Perkembangannya, *UNES Law Review* : Vol. 6, No. 1, September 2023, 2722-2731

manusia yang dirugikan. Ketika pengayoman preventif gagal (data bocor), maka hukum harus hadir memberikan pengayoman represif berupa pemulihan hak (*restitutio in integrum*) melalui mekanisme gugatan perdata, sehingga keadilan bagi korban dapat terwujud.

Ketentuan pidana terkait data pribadi diatur secara tegas dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Undang-undang ini memuat larangan keras bagi "setiap orang" yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain. Frasa "setiap orang" ini menjangkau siapa saja, termasuk pegawai negeri atau pejabat pemerintah. Ancaman sanksi bagi pelanggaran ini tidak main-main, yakni berupa pidana penjara dan denda yang berat. Aturan ini menjadi dasar hukum untuk menjerat pelaku kebocoran data yang memiliki niat jahat (*mens rea*), memisahkannya dari sekadar kelalaian administratif.

Dengan demikian, penerapan sanksi pidana berfungsi sebagai *ultimum remedium* atau upaya terakhir dalam penegakan hukum data pribadi. Instrumen pidana digunakan ketika mekanisme administratif dan perdata dianggap tidak lagi memadai untuk memulihkan keadilan, terutama menghadapi pejabat yang menyalahgunakan wewenang secara koruptif. Penjeratan pidana terhadap oknum pelaku baik dari unsur internal pemerintah maupun peretas eksternal diperlukan untuk memberikan efek jera (*deterrent effect*) yang nyata, sekaligus membersihkan instansi pemerintah dari elemen-elemen yang mengkhianati amanat konstitusi untuk melindungi data segenap bangsa Indonesia.

Berdasarkan analisis mengenai pertanggungjawaban pemerintah atas kebocoran data pribadi, dapat disimpulkan bahwa rezim pertanggungjawaban di Indonesia terbagi secara dikotomis antara tanggung jawab jabatan (*ambtshalve*) dan tanggung jawab pribadi (*persoonlijke aansprakelijkheid*). Secara kelembagaan, pemerintah sebagai Badan Publik dan Pengendali Data Pribadi memikul tanggung jawab administratif dan perdata. Tanggung jawab administratif ditegakkan melalui Undang-Undang Nomor 27 Tahun 2022 (UU PDP) berupa sanksi teguran, penghentian pemrosesan, atau pemusnahan data. Sementara itu, tanggung jawab perdata muncul melalui gugatan Perbuatan Melawan Hukum oleh Penguasa (*Onrechtmatige Overheidsdaad*) berdasarkan Pasal 1365 KUHPerdata, di mana pemerintah wajib membayar ganti rugi materiil maupun imateriil kepada masyarakat akibat kelalaiannya dalam menjalankan amanat konstitusi untuk melindungi data warga negara.

Di sisi lain, batas pertanggungjawaban institusi pemerintah berhenti ketika ditemukan unsur kesengajaan (*dolus*) atau motif ekonomi jahat dari aparatur negara, seperti dalam kasus dugaan

penjualan data NPWP. Dalam kondisi ini, selubung jabatan terbuka dan tanggung jawab beralih sepenuhnya menjadi tanggung jawab pribadi pejabat atau oknum terkait. Pertanggungjawaban pidana sebagai *ultimum remedium* hanya dapat diterapkan kepada individu (*natuurlijke persoon*) yang terbukti menyalahgunakan wewenang untuk keuntungan pribadi, karena institusi negara tidak dapat dipidana. Oleh karena itu, efektivitas penegakan hukum dalam kasus kebocoran data pemerintah sangat bergantung pada kemampuan aparat penegak hukum untuk memilah antara kelalaian sistemik (tanggung jawab negara) dan kejahatan personal (tanggung jawab pidana oknum).

SIMPULAN

1. Perlindungan Hukum Kebocoran Data Pribadi oleh Pemerintah Secara normatif, perlindungan hukum terhadap data pribadi yang dikelola oleh pemerintah Indonesia telah memiliki landasan yuridis yang kuat, mulai dari amanat konstitusi dalam UUD NRI 1945 yang menjamin hak privasi sebagai hak asasi manusia, hingga pengaturan teknis dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan PP Nomor 71 Tahun 2019. Pemerintah dikategorikan sebagai "Badan Publik" dan "Pengendali Data Pribadi" yang wajib menjamin keamanan data melalui sistem elektronik yang andal dan aman. Namun, dalam tataran implementasi (Das Sein), perlindungan hukum preventif ini terbukti belum efektif, ditandai dengan berulangnya kasus kebocoran data strategis seperti 6 juta data NPWP, yang menunjukkan lemahnya sistem keamanan siber pemerintah dan pengabaian prinsip kehati-hatian. Kegagalan ini mencederai asas kepastian hukum karena masyarakat kehilangan jaminan keamanan atas data yang wajib mereka serahkan kepada negara, sementara mekanisme perlindungan represif seperti hak gugat dan kewajiban notifikasi masih terhambat oleh kendala pembuktian dan respons birokrasi yang lambat.
2. Pertanggungjawaban Pemerintah atas Kebocoran Data Pribadi Rezim pertanggungjawaban pemerintah atas kebocoran data pribadi di Indonesia terbagi menjadi tanggung jawab jabatan (*ambtshalve*) dan tanggung jawab pribadi (*persoonlijke aansprakelijkheid*). Secara kelembagaan, pemerintah bertanggung jawab secara administratif dan perdata; di mana sanksi administratif diatur dalam UU PDP berupa teguran atau penghentian pemrosesan data, namun memiliki kelemahan fundamental karena adanya pengecualian sanksi denda bagi Badan Publik yang mencederai rasa keadilan dan mengurangi efek jera. Pertanggungjawaban perdata dapat ditempuh melalui gugatan Perbuatan Melawan Hukum oleh Penguasa (*Onrechtmatige Overheidsdaad*) untuk menuntut ganti rugi materiil dan imateriil atas kelalaian negara melindungi warganya.

Adapun pertanggungjawaban pidana hanya berlaku secara terbatas kepada oknum pejabat atau individu yang terbukti secara sengaja menyalahgunakan wewenang atau mengambil keuntungan pribadi dari data tersebut (seperti motif ekonomi dalam jual beli data), karena institusi negara tidak dapat dipidana.

DAFTAR PUSTAKA

Buku

Bagir Manan dan Kuntanan Magnar. Beberapa Masalah Hukum Tata Negara, (Bandung: PT.Alumni, 2017).

C.S.T. Kansil. Pengantar Ilmu Hukum dan Tata Hukum Indonesia, (Balai Pustaka, Jakarta : 1980).

Julista Mustamu, Diskresi Dalam Pemerintahan: Hak, Batas Dan Konsekuensi Hukumnya, Widina Media Utama, Bandung, 2025

Oktaviani Sugiarto, 2019, Tinjauan Hukum Internasional terkait Perlindungan Data Pribadi, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar.

Peter Mahmud Marzuki, Penelitian Hukum, (Jakarta; Pranada Media, 2005),

Philipus M Hadjon. DKK. Pengantar Hukum Administrasi Negara Indonesia. Gaja Muda University Press Catakan Ke Tiga 1994, Surabaya.

Ridwan HR. Hukum Administrasi Negara, PT, RajaGrafindo Perseda, Jakarta 2006.

Satjipto Rahardjo, 2012, Ilmu Hukum, Bandung, Citra Aditya Bakti, hlm 19.

Satjipto Raharjo, Ilmu Hukum, (PT. Citra Aditya Bakti, Cet-IV, Bandung: 2000).

Sudikno Mertokusumo, Bab-Bab Tentang Penemuan Hukum, Citra Aditya Bakti: Bandung, 1993.

Sinta Dewi, 2009, Cyber Law: Perlindungan Privasi atas Informasi Pribadi dalam Ecommerce menurut Hukum Internasional, Widya Pajajaran, Bandung.

Tedi Sudrajat, Hukum Birokrasi Pemerintah Kewenangan dan Jabatan, Sinar Grafika, Jakarta, 2017

W.J.S. Poerwadarminta, Kamus Umum Bahasa Indonesia Edisi Ketiga, Balai Pustaka, 2006.

Jurnal

Achmad Ali, Menguk Teori Hukum (Legal Theory) & Teori Peradilan (Judicialprudence) Termasuk Undang-Undang (Legisprudence) Volume I Pemahaman Awal, Kencana Prenada Media Group, Jakarta, 2010 , hlm 288.

Dewa Gede Atmaja, “Asas-Asas Hukum Dalam Sistem Hukum”, Jurnal Kertha Wicaksana, Volume 12, Nomor 2, 2018, hlm. 146

M. Tasbir Rais, Negara Hukum Indonesia: Gagasan Dan Penerapannya, Jurnal Hukum Unsulbar , Vol 5 No 2 (2022), 11-31

Mario Julyano dan Aditya Yuli Sulistyawan, Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum, JURNAL CREPIDO : Jurnal Mengenai Dasar-Dasar Pemikiran Hukum: Filsafat dan Ilmu Hukum , Volume 01, Nomor 01, Juli 2019, 13-22

Maria Odilia Kolo, Aksi Sinurat, Karolus Kopong Medan, Tinjauan Yuridis Perlindungan Hukum terhadap Korban dan Pelaku Kejahatan Berdasarkan Asas Equality Before the Law, Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara Vol.2, No.2 Mei 2024, 130-142

Mendy Cevitra, Gunawan Djajaputra, Perbuatan Melawan Hukum (Onrechtmatige Daad) Menurut Pasal 1365 Kitab Undang-Undang Hukum Perdata dan Perkembangannya, UNES Law Review : Vol. 6, No. 1, September 2023, 2722-2731

Nelson Bastian Nope, Mutasi Pejabat Fungsional Ke Dalam Jabatan Struktural Di Era Otonomi Daerah, Yustisia. Vol. 4 No. 2 Mei – Agustus 2015. 349-368

Nehru Asyikni, Adam Setiawan, Tanggung Jawab Jabatan dan Tanggung Jawab Pribadi Dalam Penggunaan Diskresi, Kosmik Hukum : Vol. 20 No.1 (2020), 1-13

Ronal Hasudungan Sianturi , Ahmad Feri Tanjung , Rony Andre Christian Naldo, Kepastian Hukum Implementasi Denda Damai Untuk Perkara Tindak Pidana Korupsi (Legal Certainty in the Implementation of Peaceful Fines for Corruption Crime Cases), JURNAL ILMIAH PENEGAKAN HUKUM : Vol. 12 No. 1 JUNI (2025), 41-47

Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, Jurnal Ilmu Hukum, Vol. 2, No. 1, 1 April 2021, hlm. 2 Socha Tcefortin Indera Sakti, Perlindungan Hukum Bagi Para Pihak Dalam Perjanjian Jual Beli Tanah Letter C Di Bawah Tangan, Jurnal Privat Law Vol. VIII No. 1 Januari-Juni 2020, 144-150

Usman, Andi Najemi, Mediasi Penal di Indonesia: Keadilan, Kemanfaatan, dan Kepastian Hukumnya, Undang: Jurnal Hukum, Vol. 1 No. 1 (2018): 65-83

Wiwin Yulianingsih, Perlindungan Represif dalam Awig-Awig di Bali pada Penyelesaian Sengketa Adat, UNES Law Review : Vol. 6, No. 4, Juni2024. 9889-9897

Peraturan-Peraturan

European Union General Data Protection Regulation (GDPR).

Undang-Undang nomor 27 tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Internet

Tempo, 21 September 2024, Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah, <https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403>