Jurnal Kebijakan Reformasi Hukum

Vol. 10 No. 1 Tahun 2026
ISSN: 21102140

PERLINDUNGAN HUKUM TERHADAP KEBOCORAN DATA PRIBADI DI INDONESIA: ANALISIS TANGGUNG JAWAB PENYELENGGARA SISTEM ELEKTRONIK BERDASARKAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI

Asep Rifki Maulana Malik[1], Dewi Puannandini[2], Arya Ash-Shiddiqi Mudrikah[3]
aseprifkimaulanamalik04@gmail.com[1], dewipuannandini@gmail.com[2], aryashiddiqi1@gmail.com[3]
Universitas Islam Nusantara

Abstrak

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan sistem elektronik dalam berbagai sektor kehidupan, baik oleh lembaga pemerintah maupun pihak swasta. Namun, kemajuan tersebut juga diiringi dengan meningkatnya risiko kebocoran data pribadi yang berpotensi merugikan hak privasi masyarakat. Sejumlah kasus kebocoran data pribadi di Indonesia, seperti yang dialami oleh Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan dan platform e-commerce Tokopedia, menunjukkan lemahnya perlindungan data pribadi serta belum optimalnya penerapan tanggung jawab hukum oleh penyelenggara sistem elektronik. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap data pribadi di Indonesia serta menelaah tanggung jawab hukum penyelenggara sistem elektronik atas terjadinya kebocoran data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus, yang didukung oleh bahan hukum primer dan sekunder. Hasil penelitian menunjukkan bahwa Undang-Undang Perlindungan Data Pribadi telah memberikan dasar hukum yang lebih komprehensif terkait kewajiban, larangan, dan sanksi bagi penyelenggara sistem elektronik. Namun, dalam praktiknya, penegakan hukum terhadap pelanggaran perlindungan data pribadi masih menghadapi berbagai kendala, terutama dalam aspek pengawasan dan pertanggungjawaban hukum. Oleh karena itu, diperlukan penguatan implementasi regulasi serta peningkatan kesadaran hukum bagi penyelenggara sistem elektronik guna menjamin perlindungan data pribadi secara efektif.
Kata Kunci: Perlindungan Hukum, Data Pribadi, Kebocoran Data, Penyelenggara Sistem Elektronik, Undang-Undang Perlindungan Data Pribadi.

Abstract

The rapid development of information and communication technology has significantly increased the use of electronic systems in various sectors, both by government institutions and private entities. However, this advancement is accompanied by a growing risk of personal data breaches that may threaten individuals' privacy rights. Several cases of personal data breaches in Indonesia, such as those involving the Social Security Agency for Health (BPJS Kesehatan) and the e-commerce platform Tokopedia, illustrate weaknesses in personal data protection and the inadequate implementation of legal responsibility by electronic system providers. This study aims to analyze the legal protection of personal data in Indonesia and to examine the legal responsibility of electronic system providers for personal data breaches based on Law Number 27 of 2022 concerning Personal Data Protection. This research employs a normative legal research method using statutory and case approaches, supported by primary and secondary legal materials. The findings indicate that the Personal Data Protection Law has established a more comprehensive legal framework regarding obligations, prohibitions, and sanctions for electronic system providers. Nevertheless, in practice, law enforcement related to personal data protection violations still faces various challenges, particularly in supervision and legal accountability. Therefore, strengthening regulatory implementation and enhancing legal awareness among electronic system providers are essential to ensure effective personal data protection.
***Keywords**: Legal Protection, Personal Data, Data Breach, Electronic System Providers, Personal Data Protection Law.*

Vol. 10 No. 1 Tahun 2026
ISSN: 21102140

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi (TIK) telah membawa perubahan signifikan dalam cara data pribadi dikumpulkan, diproses, dan dimanfaatkan oleh berbagai pihak, baik oleh lembaga pemerintah maupun perusahaan swasta di Indonesia. Penggunaan sistem elektronik yang masif dalam kegiatan administrasi, layanan publik, dan bisnis digital telah meningkatkan jumlah serta kompleksitas data pribadi yang tersimpan dalam basis data elektronik. Namun, peningkatan ini juga diiringi dengan tingginya risiko kebocoran data pribadi yang menimbulkan berbagai dampak negatif bagi individu, termasuk potensi penyalahgunaan data, ancaman terhadap privasi, serta kerugian ekonomi dan sosial.

Berbagai kasus kebocoran data pribadi yang terjadi di Indonesia menunjukkan bahwa perlindungan data pribadi belum berjalan optimal di tengah fenomena digitalisasi yang pesat. Salah satu contoh yang menarik perhatian publik adalah kebocoran data pengguna platform e-commerce Tokopedia pada tahun 2020, yang dilaporkan melibatkan sekitar 91 juta akun pengguna dan sejumlah data merchant yang dijual di forum peretas (dark web). Kasus ini menunjukkan kerentanan dalam sistem keamanan data yang dikelola oleh penyelenggara sistem elektronik (PSE) serta kurangnya mekanisme hukum yang kuat untuk menjamin tanggung jawab penyelenggara atas terjadinya kebocoran data tersebut.

Selain itu, kasus kebocoran data yang lebih luas juga terjadi di sektor layanan publik. Misalnya, pada tahun 2021 dilaporkan adanya dugaan kebocoran sekitar 279 juta data penduduk yang identik dengan data BPJS Kesehatan, yang mencakup informasi seperti nama, nomor telepon, dan alamat, yang kemudian diperjualbelikan di forum daring. Kasus tersebut mempertegas bahwa masalah perlindungan data pribadi tidak hanya terbatas pada sektor komersial, tetapi juga menyentuh pelayanan dasar masyarakat dan akses terhadap data publik yang sensitif.

Fenomena kebocoran data juga semakin kompleks seiring dengan pemberitaan dugaan kebocoran data kependudukan dalam jumlah besar yang diklaim berasal dari basis data Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri. Peristiwa ini menimbulkan kekhawatiran publik terkait keamanan data pribadi yang dikelola oleh pemerintah serta efektivitas regulasi yang tersedia dalam menjamin hak privasi warga negara.

Menanggapi berbagai insiden itu, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai bentuk upaya memperkuat dasar hukum perlindungan data pribadi di Indonesia. Regulasi ini dimaksudkan untuk memberikan payung hukum yang lebih komprehensif terkait kewajiban pengendali dan pemroses data pribadi, hak subjek data, serta sanksi bagi pelanggaran perlindungan data. Namun demikian, implementasi dan penegakan hukum dari UU PDP masih menghadapi kendala, antara lain keterlambatan pembentukan lembaga pengawas data pribadi dan belum optimalnya mekanisme pertanggungjawaban penyelenggara sistem elektronik dalam praktiknya.

Berdasarkan kondisi tersebut, isu perlindungan hukum terhadap kebocoran data pribadi menjadi sangat relevan untuk dikaji secara ilmiah, terutama dalam menelaah bagaimana tanggung jawab hukum penyelenggara sistem elektronik dijamin dan diatur dalam perundang-undangan Indonesia, serta sejauh mana regulasi yang ada mampu menjawab tantangan praktik yang terjadi di masyarakat.

Rumusan Masalah dan Tujuan Penelitian

(1) Bagaimana pengaturan tanggung jawab hukum penyelenggara sistem elektronik terhadap kebocoran data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi?

(2) Sejauh mana pengaturan tersebut efektif dalam memberikan perlindungan hukum bagi subjek data pribadi pada kasus kebocoran data yang terjadi di Indonesia?

Tujuannya:

(1) Menganalisis bentuk dan ruang lingkup tanggung jawab hukum penyelenggara sistem elektronik dalam hal terjadinya kebocoran data pribadi berdasarkan Undang-Undang Perlindungan Data Pribadi.
(2) Menilai efektivitas penerapan ketentuan hukum tersebut melalui analisis kasus kebocoran data pribadi yang dilaporkan di media internet, serta merumuskan rekomendasi penguatan perlindungan hukum yang bersifat aplikatif.

Penelitian Terdahulu

Kajian mengenai perlindungan data pribadi dalam perspektif hukum telematika di Indonesia telah dilakukan oleh sejumlah peneliti, khususnya setelah meningkatnya kasus kebocoran data yang melibatkan penyelenggara sistem elektronik. Beberapa penelitian menyoroti bahwa lemahnya sistem keamanan dan belum optimalnya regulasi menjadi faktor utama terjadinya kebocoran data pribadi.

Penelitian oleh Ardika (2023) membahas perlindungan hukum terhadap data pribadi pengguna platform e-commerce dengan studi kasus kebocoran data Tokopedia. Penelitian tersebut menyimpulkan bahwa sebelum berlakunya Undang-Undang Perlindungan Data Pribadi, pengaturan mengenai data pribadi masih bersifat sektoral dan belum memberikan kepastian hukum yang memadai bagi subjek data. Fokus penelitian ini masih terbatas pada aspek normatif, tanpa mengkaji secara mendalam pertanggungjawaban hukum penyelenggara sistem elektronik setelah lahirnya UU PDP.

Penelitian lain yang dilakukan oleh Utami, dkk. (2024) mengkaji fenomena kebocoran data pribadi di Indonesia berdasarkan kasus-kasus yang ramai diberitakan di media internet. Penelitian ini menekankan pentingnya peningkatan kesadaran hukum dan penguatan sistem keamanan data, namun belum secara spesifik menganalisis efektivitas penerapan sanksi dan mekanisme tanggung jawab hukum penyelenggara sistem elektronik berdasarkan Undang-Undang Perlindungan Data Pribadi.

Berdasarkan penelitian terdahulu tersebut, terlihat bahwa masih terdapat ruang kajian yang perlu diperdalam, khususnya terkait analisis tanggung jawab hukum penyelenggara sistem elektronik atas kebocoran data pribadi dengan menggunakan studi kasus nyata pasca berlakunya UU PDP. Penelitian ini diarahkan untuk mengisi kekosongan tersebut dengan pendekatan yang lebih aplikatif dan kontekstual.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan peraturan perundang-undangan (statute approach) dan pendekatan kasus (case approach). Pendekatan peraturan perundang-undangan digunakan untuk menganalisis ketentuan hukum yang mengatur perlindungan data pribadi, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta peraturan terkait lainnya.

Pendekatan kasus dilakukan dengan menganalisis sejumlah peristiwa kebocoran data pribadi yang dilaporkan secara luas melalui media internet, seperti kasus kebocoran data pengguna platform e-commerce dan layanan publik, sebagai bahan untuk menilai implementasi dan tanggung jawab hukum penyelenggara sistem elektronik. Data yang digunakan bersumber dari bahan hukum primer berupa peraturan perundang-undangan, serta bahan hukum sekunder berupa jurnal ilmiah, literatur hukum, dan pemberitaan media daring yang kredibel. Seluruh data dianalisis secara kualitatif dengan metode analisis yuridis untuk memperoleh kesimpulan yang relevan dan aplikatif.

Vol. 10 No. 1 Tahun 2026
ISSN: 21102140

PEMBAHASAN

Fenomena Kebocoran Data Pribadi dan Posisi Penyelenggara Sistem Elektronik di Indonesia

Perkembangan teknologi informasi yang pesat telah mendorong meningkatnya ketergantungan masyarakat terhadap layanan digital, baik dalam sektor privat maupun publik. Namun, di sisi lain, kondisi tersebut turut memunculkan risiko serius berupa kebocoran data pribadi. Dalam beberapa tahun terakhir, Indonesia dihadapkan pada berbagai kasus kebocoran data berskala besar, seperti kebocoran data pengguna Tokopedia, BPJS Kesehatan, hingga dugaan kebocoran data pada platform layanan publik dan keuangan digital. Kasus-kasus tersebut menunjukkan bahwa keamanan sistem elektronik masih menjadi persoalan krusial.

Dalam konteks hukum telematika, penyelenggara sistem elektronik (PSE) memegang peran sentral karena mereka merupakan pihak yang mengelola, menyimpan, dan memproses data pribadi pengguna. Oleh karena itu, setiap kegagalan dalam menjaga keamanan data tidak dapat dipandang semata-mata sebagai kesalahan teknis, melainkan memiliki implikasi hukum yang serius. Kebocoran data pribadi berdampak langsung pada hak privasi subjek data, serta berpotensi menimbulkan kerugian ekonomi, sosial, dan psikologis bagi masyarakat.

Keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi tonggak penting dalam merespons fenomena tersebut. UU PDP secara tegas menempatkan data pribadi sebagai hak asasi yang harus dilindungi, serta memberikan kewajiban hukum yang jelas kepada penyelenggara sistem elektronik untuk menjamin keamanan dan kerahasiaan data. Dengan demikian, setiap kebocoran data tidak lagi dapat disikapi sebagai peristiwa biasa, melainkan sebagai bentuk pelanggaran hukum yang dapat dimintai pertanggungjawaban.

Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Berdasarkan Undang-Undang Perlindungan Data Pribadi

Undang-Undang Perlindungan Data Pribadi mengatur bahwa penyelenggara sistem elektronik wajib melakukan perlindungan data pribadi melalui penerapan prinsip kehati-hatian, keamanan sistem, dan kepatuhan terhadap ketentuan hukum. Kewajiban ini mencakup pengamanan teknis, pengelolaan internal, serta pencegahan terhadap akses ilegal dan penyalahgunaan data pribadi. Apabila terjadi kegagalan dalam memenuhi kewajiban tersebut, PSE dapat dimintai pertanggungjawaban hukum.

Tanggung jawab hukum PSE dalam kasus kebocoran data pribadi dapat dilihat dalam tiga aspek, yaitu administratif, perdata, dan pidana. Secara administratif, UU PDP memberikan kewenangan kepada otoritas untuk menjatuhkan sanksi berupa peringatan, penghentian sementara kegiatan pemrosesan data, hingga denda administratif. Sanksi ini bertujuan untuk mendorong kepatuhan dan meningkatkan standar keamanan sistem elektronik.

Dalam aspek perdata, kebocoran data pribadi membuka ruang bagi subjek data untuk menuntut ganti rugi atas kerugian yang dialami. Hal ini menegaskan bahwa perlindungan data pribadi tidak hanya bersifat preventif, tetapi juga represif dengan memberikan pemulihan hak bagi korban. Sementara itu, dalam kondisi tertentu, terutama apabila kebocoran data disebabkan oleh kelalaian berat atau perbuatan melawan hukum yang disengaja, pertanggungjawaban pidana juga dapat diterapkan.

Dengan demikian, Undang-Undang Perlindungan Data Pribadi memperjelas posisi hukum penyelenggara sistem elektronik sebagai pihak yang bertanggung jawab penuh atas keamanan data yang dikelolanya. Prinsip “accountability” menjadi dasar utama, di mana PSE tidak hanya dituntut untuk mengelola sistem, tetapi juga bertanggung jawab atas setiap konsekuensi hukum yang timbul akibat kegagalan sistem tersebut.

Vol. 10 No. 1 Tahun 2026
ISSN: 21102140

Analisis Studi Kasus Kebocoran Data Pribadi di Indonesia

Salah satu studi kasus yang relevan adalah kebocoran data pengguna Tokopedia yang mencakup jutaan akun pengguna. Dalam kasus ini, data seperti nama, email, dan informasi akun beredar di forum daring. Peristiwa tersebut menimbulkan kekhawatiran publik mengenai lemahnya sistem keamanan platform digital besar sekalipun. Jika dianalisis berdasarkan Undang-Undang Perlindungan Data Pribadi, kebocoran tersebut dapat dikategorikan sebagai kegagalan PSE dalam menjamin keamanan data pribadi, sehingga membuka ruang pertanggungjawaban hukum.

Kasus lain yang juga mencerminkan persoalan serius adalah kebocoran data peserta BPJS Kesehatan. Data yang bocor melibatkan informasi sensitif masyarakat dalam jumlah besar, sehingga dampaknya jauh lebih luas. Dalam konteks ini, PSE sektor publik seharusnya memiliki standar keamanan yang lebih ketat, mengingat data yang dikelola berkaitan langsung dengan hak dasar warga negara. Kebocoran tersebut menunjukkan bahwa baik PSE privat maupun publik memiliki kerentanan yang sama apabila tidak diimbangi dengan sistem pengamanan yang memadai.

Dari kedua kasus tersebut, dapat dilihat bahwa persoalan utama bukan hanya terletak pada serangan siber, tetapi juga pada kesiapan hukum dan teknis penyelenggara sistem elektronik. Undang-Undang Perlindungan Data Pribadi memberikan dasar hukum yang kuat untuk menuntut tanggung jawab PSE, namun efektivitasnya sangat bergantung pada penegakan hukum dan keseriusan negara dalam mengawasi implementasinya.

Implikasi Hukum dan Upaya Penguatan Perlindungan Data Pribadi

Berlakunya Undang-Undang Perlindungan Data Pribadi membawa implikasi penting bagi tata kelola sistem elektronik di Indonesia. PSE dituntut untuk tidak lagi berorientasi semata-mata pada layanan dan keuntungan, tetapi juga pada perlindungan hak privasi pengguna. Hal ini menuntut perubahan paradigma dalam pengelolaan sistem elektronik, dari sekadar kepatuhan formal menuju kepatuhan substantif.

Penguatan perlindungan data pribadi perlu dilakukan melalui peningkatan standar keamanan sistem, transparansi pengelolaan data, serta mekanisme pelaporan yang jelas apabila terjadi kebocoran. Selain itu, penegakan sanksi yang tegas terhadap PSE yang lalai menjadi faktor kunci untuk menciptakan efek jera dan meningkatkan kepercayaan publik terhadap sistem digital.

Dengan demikian, Undang-Undang Perlindungan Data Pribadi tidak hanya berfungsi sebagai instrumen hukum normatif, tetapi juga sebagai alat untuk membangun ekosistem digital yang aman, bertanggung jawab, dan berkeadilan. Pembahasan ini menegaskan bahwa perlindungan data pribadi merupakan tanggung jawab bersama antara negara, penyelenggara sistem elektronik, dan masyarakat.

Analisis Yuridis Berdasarkan Rumusan Masalah dan Temuan Penelitian

Berdasarkan rumusan masalah pertama mengenai bentuk tanggung jawab hukum penyelenggara sistem elektronik atas kebocoran data pribadi, hasil analisis menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan dasar hukum yang jelas dan tegas. Pasal 35 UU PDP mewajibkan pengendali dan prosesor data pribadi untuk melindungi dan menjamin keamanan data pribadi yang diprosesnya. Kewajiban ini bersifat mandatory, sehingga kegagalan dalam mencegah kebocoran data dapat dikualifikasikan sebagai pelanggaran hukum.

Lebih lanjut, Pasal 46 UU PDP mengatur sanksi administratif berupa peringatan tertulis, penghentian sementara pemrosesan data pribadi, hingga denda administratif. Ketentuan ini menegaskan bahwa tanggung jawab penyelenggara sistem elektronik tidak hanya bersifat moral atau etis, tetapi telah dikonstruksikan sebagai tanggung jawab hukum yang dapat

Vol. 10 No. 1 Tahun 2026
ISSN: 21102140

dipaksakan oleh negara. Dengan demikian, kebocoran data pribadi bukan lagi sekadar persoalan teknis keamanan siber, melainkan pelanggaran terhadap hak subjek data yang dijamin oleh undang-undang.

Menjawab rumusan masalah kedua mengenai efektivitas penerapan Undang-Undang Perlindungan Data Pribadi dalam kasus nyata, temuan penelitian menunjukkan bahwa meskipun UU PDP telah memberikan kerangka hukum yang komprehensif, implementasinya masih menghadapi kendala dalam aspek pengawasan dan penegakan hukum. Studi kasus kebocoran data Tokopedia dan BPJS Kesehatan memperlihatkan bahwa pertanggungjawaban hukum penyelenggara sistem elektronik belum sepenuhnya diterapkan secara optimal, khususnya dalam hal transparansi kepada subjek data dan pemberian ganti rugi.

Temuan Penelitian dan Perbedaan dengan Penelitian Terdahulu

Penelitian ini menemukan bahwa kebocoran data pribadi yang terjadi di Indonesia tidak disebabkan oleh kekosongan norma hukum, melainkan oleh lemahnya kepatuhan penyelenggara sistem elektronik terhadap kewajiban hukum yang telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Meskipun UU PDP telah memberikan dasar hukum yang komprehensif, implementasinya dalam praktik belum berjalan secara optimal.

Temuan selanjutnya menunjukkan bahwa penyelenggara sistem elektronik belum sepenuhnya menerapkan prinsip akuntabilitas sebagaimana diamanatkan dalam Pasal 35 dan Pasal 39 UU PDP. Dalam sejumlah kasus kebocoran data yang dianalisis, penyelenggara sistem elektronik cenderung membatasi respons pada klarifikasi publik, tanpa disertai mekanisme pertanggungjawaban hukum yang jelas terhadap subjek data yang dirugikan.

Penelitian ini juga menemukan bahwa penerapan sanksi administratif sebagaimana diatur dalam Pasal 46 UU PDP belum memberikan efek jera yang signifikan. Hal ini disebabkan oleh belum optimalnya pengawasan dan penegakan hukum terhadap penyelenggara sistem elektronik, baik di sektor privat maupun sektor publik. Akibatnya, perlindungan data pribadi masih bersifat normatif dan belum sepenuhnya menjamin pemulihan hak subjek data.

Selain itu, penelitian ini menemukan bahwa pendekatan perlindungan data pribadi di Indonesia masih bersifat reaktif, yaitu berfokus pada penanganan pasca-terjadinya kebocoran data. Padahal, Undang-Undang Perlindungan Data Pribadi menekankan pentingnya langkah preventif melalui sistem keamanan yang memadai dan tata kelola data yang bertanggung jawab. Kondisi ini menunjukkan perlunya penguatan implementasi UU PDP agar mampu memberikan perlindungan hukum yang efektif dan berkelanjutan.

Perbedaan penelitian ini dengan penelitian terdahulu terletak pada fokus analisisnya. Penelitian sebelumnya umumnya menitikberatkan pada aspek normatif perlindungan data pribadi atau mengkaji kebocoran data sebelum berlakunya Undang-Undang Perlindungan Data Pribadi. Sementara itu, penelitian ini secara khusus menganalisis tanggung jawab hukum penyelenggara sistem elektronik pasca berlakunya UU PDP dengan menggunakan studi kasus nyata yang diberitakan di media internet. Dengan demikian, penelitian ini menawarkan perspektif yang lebih aktual dan aplikatif terhadap penegakan hukum perlindungan data pribadi di Indonesia.

KESIMPULAN

Berdasarkan hasil dan pembahasan penelitian ini, dapat disimpulkan bahwa kebocoran data pribadi di Indonesia bukan disebabkan oleh kekosongan norma hukum, melainkan oleh belum optimalnya kepatuhan dan akuntabilitas penyelenggara sistem elektronik dalam melaksanakan kewajiban hukum sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun

2022 tentang Perlindungan Data Pribadi. Undang-undang tersebut telah memberikan dasar hukum yang jelas dan komprehensif terkait perlindungan data pribadi serta tanggung jawab hukum penyelenggara sistem elektronik.

Penelitian ini menunjukkan bahwa kewajiban perlindungan data pribadi sebagaimana diatur dalam Pasal 35 dan kewajiban pemberitahuan kegagalan perlindungan data dalam Pasal 39 UU PDP belum sepenuhnya dilaksanakan secara substantif oleh penyelenggara sistem elektronik. Dalam praktiknya, respons penyelenggara sistem elektronik atas kebocoran data masih terbatas pada klarifikasi publik, tanpa diikuti dengan mekanisme pertanggungjawaban hukum dan pemulihan hak subjek data secara memadai.

Selain itu, penerapan sanksi administratif sebagaimana diatur dalam Pasal 46 UU PDP belum menunjukkan efektivitas yang optimal dalam memberikan efek jera. Hal ini disebabkan oleh lemahnya pengawasan dan penegakan hukum, sehingga perlindungan data pribadi cenderung bersifat reaktif dan belum berorientasi pada pencegahan. Oleh karena itu, dapat disimpulkan bahwa efektivitas Undang-Undang Perlindungan Data Pribadi sangat bergantung pada konsistensi penegakan hukum dan penguatan pengawasan terhadap penyelenggara sistem elektronik, baik di sektor privat maupun sektor publik.

Saran

Berdasarkan kesimpulan penelitian ini, disarankan agar pemerintah dan otoritas terkait memperkuat mekanisme pengawasan dan penegakan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya dalam penerapan sanksi administratif terhadap penyelenggara sistem elektronik yang terbukti lalai dalam melindungi data pribadi. Penegakan hukum yang konsisten diperlukan untuk menciptakan efek jera serta meningkatkan kepatuhan penyelenggara sistem elektronik.

Selanjutnya, penyelenggara sistem elektronik, baik di sektor privat maupun publik, disarankan untuk menginternalisasi prinsip akuntabilitas dan pencegahan dalam pengelolaan data pribadi. Hal ini dapat dilakukan melalui peningkatan standar keamanan sistem, audit perlindungan data secara berkala, serta penerapan prosedur pelaporan yang transparan apabila terjadi kegagalan perlindungan data pribadi sebagaimana diamanatkan dalam Undang-Undang Perlindungan Data Pribadi.

Terakhir, penelitian selanjutnya disarankan untuk mengkaji secara empiris efektivitas penerapan Undang-Undang Perlindungan Data Pribadi, khususnya terkait mekanisme ganti rugi bagi subjek data dan peran lembaga pengawas perlindungan data pribadi. Kajian tersebut diharapkan dapat memperkaya pengembangan hukum telematika serta memperkuat perlindungan hak privasi masyarakat di era digital.

DAFTAR PUSTAKA

Ali, Z. (2021). Metode penelitian hukum. Jakarta: Sinar Grafika.

Ardika, I. K. (2023). Perlindungan data pribadi pengguna e-commerce dalam perspektif hukum Indonesia. Jurnal Hukum IUS QUIA IUSTUM, 30(2), 245–262.

Asshiddiqie, J. (2018). Pengantar ilmu hukum tata negara. Jakarta: Rajawali Pers.

BBC News Indonesia. (2021). Kebocoran data BPJS Kesehatan dan risiko perlindungan data pribadi.

CNN Indonesia. (2021). Data jutaan warga Indonesia bocor di forum daring.

Detik.com. (2021). Kronologi kebocoran data BPJS Kesehatan.

Hakim, L. (2022). Perlindungan privasi di era digital. Jurnal Media Hukum, 29(2), 150–168.

Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. (2016). Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
Katadata.co.id. (2023). Tantangan penerapan Undang-Undang Perlindungan Data Pribadi di Indonesia.
Kominfo.go.id. (2022). Pengesahan Undang-Undang Perlindungan Data Pribadi.
Kompas.com. (2020). Kasus kebocoran data Tokopedia dan dampaknya bagi pengguna.
Lestari, S. (2024). Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia. Jurnal Ilmu Hukum, 13(1), 45–60.
Marzuki, P. M. (2017). Penelitian hukum. Jakarta: Kencana.
Nugroho, B. A. (2021). Aspek yuridis keamanan data dalam sistem elektronik. Jurnal RechtsVinding, 10(2), 289–305.
OECD. (2021). Data protection and privacy in the digital age.
Putra, R. A. (2023). Tanggung jawab penyelenggara sistem elektronik dalam kebocoran data. Jurnal Hukum dan Pembangunan, 53(1), 112–130.
Rahardjo, S. (2014). Ilmu hukum. Bandung: Citra Aditya Bakti.
Sari, D. P. (2022). Urgensi perlindungan data pribadi sebagai hak asasi manusia. Jurnal Konstitusi, 19(3), 601–620.
Susanto, A. F. (2019). Hukum teknologi informasi. Bandung: Refika Aditama.
Tempo.co. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi pasca maraknya kebocoran data.
The Jakarta Post. (2022). Indonesia’s new data protection law and its challenges.
Tirto.id. (2023). Apakah sanksi UU PDP cukup memberi efek jera?
Utami, N. S., & Pratama, R. (2024). Kebocoran data pribadi dan tantangan penegakan hukum di Indonesia. Jurnal Legislasi Indonesia, 21(1), 87–102.
Wahid, A., & Labib, M. (2020). Kejahatan siber (cyber crime). Jakarta: Refika Aditama.