

Urgensi Regulasi Perlindungan Data Pribadi dalam Menghadapi Ancaman Kebocoran Data di Indonesia

Sri Ratih Indah

Politeknik Bombana Kendari, Indonesia

e-mail: fsriratihindah385@gmail.com

Abstract

The rapid development of information technology and digital transformation in Indonesia has significantly increased the use of personal data across various sectors, including public services, electronic commerce, banking, and social media. However, the growing number of personal data breach incidents indicates that the protection of personal data remains challenged by legal and institutional issues. This study aims to analyze the legal framework governing personal data protection in Indonesia and to examine the urgency of strengthening regulations in addressing the threat of data breaches. This research employs a normative legal research method using statutory and conceptual approaches. The data were collected through library research by examining laws and regulations, legal literature, and relevant scholarly works. The findings reveal that Indonesia has established a legal basis for personal data protection through Law Number 27 of 2022 concerning Personal Data Protection, supported by provisions contained in the Electronic Information and Transactions Law. Nevertheless, the implementation of these regulations has not yet been fully effective due to weak supervisory mechanisms, limited institutional capacity, low levels of public digital literacy, and ineffective law enforcement against personal data violations. It is necessary to strengthen the regulatory framework through more practical and enforceable provisions, establish effective oversight mechanisms, enhance institutional capacity, and promote continuous public education to ensure comprehensive personal data protection and legal certainty in the digital era.

Keywords: *Personal Data Protection; Data Breach; Cybersecurity; Digital Regulation; Legal Certainty.*

Abstrak

Perkembangan teknologi informasi dan transformasi digital di Indonesia telah meningkatkan penggunaan data pribadi dalam berbagai sektor, termasuk layanan publik, perdagangan elektronik, perbankan, dan media sosial. Di sisi lain, meningkatnya kasus kebocoran data pribadi menunjukkan bahwa perlindungan terhadap data pribadi masih menghadapi berbagai tantangan hukum dan kelembagaan. Penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai perlindungan data pribadi di Indonesia serta mengkaji urgensi penguatan regulasi dalam menghadapi ancaman kebocoran data. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Data diperoleh melalui studi kepustakaan



terhadap peraturan perundang-undangan, literatur hukum, dan hasil penelitian yang relevan. Hasil penelitian menunjukkan bahwa Indonesia telah memiliki landasan hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang didukung oleh ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik. Namun, implementasi regulasi tersebut belum berjalan secara optimal akibat lemahnya mekanisme pengawasan, keterbatasan kapasitas kelembagaan, rendahnya literasi digital masyarakat, serta belum efektifnya penegakan hukum terhadap pelanggaran data pribadi. Oleh karena itu, diperlukan penguatan regulasi yang lebih implementatif, pembentukan sistem pengawasan yang efektif, peningkatan kapasitas lembaga terkait, serta edukasi masyarakat secara berkelanjutan guna menjamin perlindungan data pribadi yang komprehensif dan mewujudkan kepastian hukum di era digital.

Kata Kunci : Perlindungan Data Pribadi; Kebocoran Data; Keamanan Siber; Regulasi Digital; Kepastian Hukum

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong terjadinya transformasi digital yang signifikan di berbagai sektor kehidupan masyarakat Indonesia. Digitalisasi tidak hanya mengubah pola interaksi sosial, tetapi juga memengaruhi aktivitas ekonomi, pemerintahan, pendidikan, kesehatan, hingga layanan keuangan. Pemanfaatan teknologi digital yang semakin luas menyebabkan meningkatnya kebutuhan terhadap pengumpulan, penyimpanan, dan pemrosesan data pribadi oleh berbagai penyelenggara sistem elektronik. Dalam era ekonomi digital, data pribadi bahkan telah menjadi aset strategis yang memiliki nilai ekonomi tinggi sehingga sering disebut sebagai “the new oil” dalam perkembangan teknologi modern.¹

Indonesia merupakan salah satu negara dengan tingkat pertumbuhan ekonomi digital terbesar di kawasan Asia Tenggara. Berdasarkan laporan *e-Conomy SEA* yang diterbitkan oleh Google, Temasek, dan Bain & Company, nilai ekonomi digital Indonesia terus mengalami peningkatan dan diproyeksikan mencapai lebih dari USD 130 miliar dalam beberapa tahun mendatang.² Pertumbuhan tersebut ditopang oleh meningkatnya penggunaan internet, transaksi perdagangan elektronik (*e-commerce*), layanan keuangan digital (*financial technology*), komputasi awan (*cloud computing*), serta berbagai platform media sosial yang memerlukan pemrosesan data pribadi pengguna secara masif. Kondisi ini menunjukkan bahwa data pribadi telah menjadi bagian integral dari aktivitas

¹ Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (London: John Murray, 213AD).

² & Bain & Company Google, Temasek, *E-Conomy SEA 2024 Report* (Singapore: Google Southeast Asia, 2024).



masyarakat modern sehingga perlindungannya merupakan kebutuhan yang tidak dapat diabaikan.

Peningkatan pemanfaatan teknologi digital juga diikuti oleh meningkatnya risiko penyalahgunaan dan kebocoran data pribadi. Dalam beberapa tahun terakhir, Indonesia dihadapkan pada berbagai kasus kebocoran data yang melibatkan institusi pemerintah maupun sektor swasta. Kebocoran data yang menimpa berbagai platform digital menunjukkan bahwa sistem keamanan informasi yang diterapkan oleh banyak penyelenggara sistem elektronik masih memiliki berbagai kelemahan. Kebocoran data tersebut mencakup informasi identitas penduduk, alamat surat elektronik, nomor telepon, hingga data sensitif lainnya yang berpotensi dimanfaatkan untuk tindak pidana siber seperti pencurian identitas, penipuan daring, pemerasan, maupun penyalahgunaan data untuk kepentingan komersial tanpa persetujuan pemilik data.³

Fenomena kebocoran data pribadi tidak hanya menimbulkan kerugian ekonomi, tetapi juga berimplikasi terhadap perlindungan hak asasi manusia. Hak atas privasi merupakan salah satu hak fundamental yang diakui dalam berbagai instrumen hukum internasional maupun hukum nasional. Pasal 12 Universal Declaration of Human Rights (UDHR) menegaskan bahwa tidak seorang pun boleh mengalami campur tangan sewenang-wenang terhadap kehidupan pribadinya. Di Indonesia, perlindungan terhadap hak privasi dapat ditelusuri dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin perlindungan diri pribadi, keluarga, kehormatan, martabat, dan rasa aman bagi setiap warga negara. Oleh karena itu, perlindungan data pribadi pada hakikatnya merupakan manifestasi dari perlindungan hak privasi sebagai bagian dari hak asasi manusia yang wajib dijamin oleh negara.⁴

Urgensi perlindungan data pribadi semakin meningkat seiring dengan berkembangnya teknologi berbasis kecerdasan buatan (*artificial intelligence*), *big data*, dan *Internet of Things* (IoT). Teknologi tersebut memungkinkan pengumpulan dan analisis data dalam jumlah besar sehingga memperbesar risiko terjadinya penyalahgunaan data apabila tidak diimbangi dengan regulasi yang memadai. Dalam praktiknya, banyak pengguna layanan digital yang belum sepenuhnya memahami bagaimana data pribadi mereka dikumpulkan, disimpan, dan digunakan oleh penyedia layanan. Rendahnya tingkat

³ Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Keamanan Siber Indonesia 2024*, ed. BSSN (Jakarta, 2024).

⁴ “Undang-Undang Dasar Negara Republik Indonesia Tahun 1945” (n.d.).



literasi digital masyarakat menjadi salah satu faktor yang memperbesar kerentanan terhadap pelanggaran data pribadi.⁵

Secara normatif, Indonesia telah memiliki berbagai regulasi yang mengatur perlindungan data pribadi. Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengaturan mengenai data pribadi tersebar dalam berbagai peraturan perundang-undangan, antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta beberapa peraturan sektoral lainnya. Namun, pengaturan yang bersifat sektoral tersebut dinilai belum mampu memberikan kepastian hukum yang komprehensif karena belum mengatur secara rinci mengenai hak subjek data, kewajiban pengendali data, mekanisme pengawasan, serta sanksi yang efektif terhadap pelanggaran perlindungan data pribadi.⁶

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan langkah progresif dalam memperkuat sistem hukum nasional di bidang perlindungan data. Undang-undang tersebut mengadopsi berbagai prinsip perlindungan data yang berkembang secara internasional, seperti prinsip *lawful processing*, *purpose limitation*, *transparency*, *accountability*, dan *data security*. Efektivitas implementasi undang-undang tersebut masih menghadapi berbagai tantangan, antara lain belum optimalnya kelembagaan pengawas, keterbatasan sumber daya manusia, rendahnya tingkat kepatuhan penyelenggara sistem elektronik, serta minimnya kesadaran hukum masyarakat mengenai hak-hak atas data pribadi yang dimilikinya.⁷

Berbagai penelitian sebelumnya telah membahas perlindungan data pribadi dari perspektif hukum dan hak asasi manusia. Sebagian besar penelitian lebih berfokus pada analisis normatif terhadap substansi pengaturan perlindungan data pribadi atau perbandingan regulasi dengan negara lain. Penelitian yang secara khusus mengkaji urgensi penguatan regulasi pasca berlakunya Undang-Undang Perlindungan Data Pribadi dengan mempertimbangkan meningkatnya ancaman kebocoran data serta tantangan implementasinya di Indonesia masih relatif terbatas. Terdapat kesenjangan penelitian

⁵ UNESCO, *Digital Literacy Global Framework* (Paris: UNESCO Institute for Statistics, 2023).

⁶ “Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah Terakhir Dengan Undang-Undang Nomor 1 Tahun 2024” (n.d.).

⁷ “Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi” (n.d.).



(*research gap*) berupa belum optimalnya kajian yang menghubungkan aspek normatif perlindungan data pribadi dengan efektivitas implementasi regulasi dalam menghadapi ancaman kebocoran data pada era transformasi digital.

Berdasarkan uraian tersebut, penelitian ini memiliki kebaruan berupa analisis mengenai urgensi penguatan regulasi perlindungan data pribadi yang tidak hanya meninjau aspek normatif peraturan perundang-undangan, tetapi juga mengkaji tantangan implementasi hukum dalam menghadapi meningkatnya ancaman kebocoran data di Indonesia pasca berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini bertujuan untuk menganalisis pengaturan hukum perlindungan data pribadi di Indonesia serta mengkaji urgensi penguatan regulasi dan implementasinya dalam menghadapi ancaman kebocoran data guna mewujudkan perlindungan hak privasi dan kepastian hukum di era digital.

B. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) yang berfokus pada kajian terhadap norma-norma hukum yang mengatur perlindungan data pribadi di Indonesia. Penelitian hukum normatif dipilih karena penelitian ini bertujuan untuk menganalisis pengaturan hukum yang berlaku serta mengkaji urgensi penguatan regulasi dalam menghadapi ancaman kebocoran data pribadi di era digital. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta berbagai regulasi terkait lainnya. Sementara itu, pendekatan konseptual digunakan untuk memahami konsep-konsep hukum, prinsip perlindungan data pribadi, hak atas privasi, dan teori negara hukum yang berkembang dalam doktrin hukum modern.⁸

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan dan dokumen hukum resmi yang berkaitan dengan

⁸ Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi* (Jakarta: Kencana, 2021).

perlindungan data pribadi. Bahan hukum sekunder berupa buku, artikel jurnal ilmiah, hasil penelitian, serta pendapat para ahli hukum yang relevan dengan objek penelitian. Adapun bahan hukum tersier mencakup kamus hukum, ensiklopedia hukum, dan sumber referensi lain yang mendukung pemahaman terhadap isu yang dikaji. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*), sedangkan analisis bahan hukum dilakukan secara kualitatif dengan menggunakan metode interpretasi hukum secara sistematis, gramatikal, dan teleologis untuk memperoleh pemahaman yang komprehensif mengenai efektivitas regulasi perlindungan data pribadi dalam menghadapi ancaman kebocoran data di Indonesia.⁹

C. Pembahasan

Pengaturan Hukum Perlindungan Data Pribadi di Indonesia sebagai Fondasi Perlindungan Hak Warga Negara

Perkembangan teknologi informasi dan komunikasi telah mengubah cara masyarakat berinteraksi, bertransaksi, serta menyimpan dan mendistribusikan informasi. Dalam konteks tersebut, data pribadi menjadi aset yang memiliki nilai ekonomi sekaligus berkaitan erat dengan hak privasi individu. Perlindungan data pribadi merupakan bagian penting dari perlindungan hak asasi manusia yang harus dijamin oleh negara.

Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pengaturan mengenai data pribadi di Indonesia masih bersifat sektoral dan tersebar dalam berbagai peraturan perundang-undangan. Beberapa regulasi yang mengatur perlindungan data pribadi antara lain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Kondisi tersebut menimbulkan permasalahan berupa tumpang tindih pengaturan, ketidakpastian hukum, serta lemahnya mekanisme perlindungan bagi pemilik data pribadi.¹⁰

⁹ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Pers, 2019).

¹⁰ Mamudji.



Kehadiran UU PDP menjadi tonggak penting dalam pembangunan sistem hukum perlindungan data pribadi di Indonesia. Undang-undang ini mengadopsi berbagai prinsip yang telah berkembang dalam rezim perlindungan data internasional, seperti *lawfulness*, *fairness*, *transparency*, *purpose limitation*, *data minimization*, dan *accountability*. Melalui prinsip-prinsip tersebut, pemrosesan data pribadi harus dilakukan secara sah, transparan, dan bertanggung jawab.

Temuan penelitian menunjukkan bahwa UU PDP telah memberikan pengakuan yang lebih komprehensif terhadap hak-hak subjek data. Hak tersebut meliputi hak memperoleh informasi mengenai pemrosesan data pribadi, hak mengakses data, hak memperbaiki data yang tidak akurat, hak menarik persetujuan, hak menghapus data pribadi, hingga hak mengajukan keberatan terhadap pemrosesan data tertentu.¹¹ Pengaturan ini menunjukkan bahwa negara berupaya menempatkan individu sebagai subjek utama yang memiliki kendali atas data pribadinya.

Dibandingkan dengan penelitian sebelumnya yang lebih banyak menyoroti kekosongan hukum perlindungan data pribadi di Indonesia, hasil penelitian ini menunjukkan adanya perkembangan signifikan setelah pengesahan UU PDP. Namun demikian, efektivitas regulasi tersebut masih menghadapi berbagai kendala implementasi. Salah satu kendala utama adalah belum optimalnya pembentukan kelembagaan pengawas yang independen serta masih terbatasnya kesiapan sektor publik dan swasta dalam menyesuaikan tata kelola data sesuai ketentuan UU PDP.¹²

Penelitian Liuhua (2025) menegaskan bahwa keberhasilan perlindungan data pribadi tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh sinergi antara pemerintah, sektor swasta, dan masyarakat sipil dalam membangun budaya perlindungan data.¹³ Temuan tersebut relevan dengan kondisi Indonesia yang masih menghadapi tantangan dalam membangun kesadaran kolektif mengenai pentingnya perlindungan data pribadi. Kesimpulannya bahwa pengesahan UU PDP merupakan langkah progresif dalam memperkuat perlindungan hak warga negara di era digital. Namun, keberadaan regulasi

¹¹ Sinta Dewi Rosadi, *Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia* (Bandung: Refika Aditama, 2018).

¹² Edmon Makarim, "Tantangan Implementasi Perlindungan Data Pribadi Di Indonesia Pasca Disahkannya UU PDP," *Jurnal Hukum Dan Pembangunan* 53, no. 2 (2023): 215.

¹³ Liuhua, "Personal Data Protection Governance in the Digital Era," *International Journal of Law and Information Technology* 33, no. 1 (2025): 45.

semata belum cukup tanpa didukung oleh mekanisme pengawasan yang efektif dan budaya kepatuhan yang kuat.

Dari perspektif perlindungan hak asasi manusia, data pribadi tidak hanya dipandang sebagai informasi yang melekat pada individu, tetapi juga sebagai bagian dari identitas yang harus dilindungi oleh negara. Dalam perkembangan hukum modern, perlindungan data pribadi telah menjadi salah satu indikator penting dalam menilai tingkat penghormatan suatu negara terhadap hak privasi warga negaranya. Oleh karena itu, keberadaan UU PDP menunjukkan komitmen Indonesia untuk menyesuaikan sistem hukumnya dengan perkembangan global yang semakin menempatkan perlindungan data sebagai hak fundamental dalam masyarakat digital.

Selain memberikan perlindungan bagi individu, pengaturan data pribadi yang komprehensif juga berfungsi untuk meningkatkan akuntabilitas penyelenggara sistem elektronik. Setiap pengendali data dituntut untuk menerapkan prinsip kehati-hatian dalam pengumpulan, penyimpanan, penggunaan, dan penghapusan data pribadi. Kewajiban tersebut bertujuan untuk meminimalkan risiko penyalahgunaan data sekaligus mendorong terciptanya tata kelola data yang transparan dan bertanggung jawab. Perlindungan data pribadi tidak hanya berorientasi pada pemenuhan hak individu, tetapi juga mendorong terciptanya budaya kepatuhan hukum di kalangan penyelenggara layanan digital.

Keberhasilan implementasi UU PDP akan sangat menentukan arah transformasi digital Indonesia di masa mendatang. Semakin tinggi tingkat perlindungan data yang diberikan, semakin besar pula kepercayaan masyarakat terhadap layanan digital yang disediakan oleh pemerintah maupun sektor swasta. Kepercayaan tersebut merupakan modal penting dalam mendukung pengembangan ekonomi digital, inovasi teknologi, serta investasi berbasis data. Penguatan perlindungan data pribadi harus dipandang sebagai investasi jangka panjang dalam mewujudkan ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Urgensi Perlindungan Data Pribadi dalam Menghadapi Ancaman Kebocoran Data di Indonesia

Temuan penelitian menunjukkan bahwa urgensi perlindungan data pribadi semakin meningkat seiring dengan tingginya intensitas penggunaan teknologi digital dalam berbagai sektor kehidupan. Digitalisasi layanan publik, transaksi keuangan elektronik,



layanan kesehatan digital, perdagangan elektronik (*e-commerce*), hingga penggunaan media sosial menyebabkan volume data pribadi yang diproses oleh berbagai institusi terus meningkat setiap tahun.

Dalam perspektif hak asasi manusia, data pribadi merupakan bagian dari hak privasi yang memperoleh perlindungan konstitusional. Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan rasa aman. Oleh karena itu, kebocoran data pribadi bukan sekadar persoalan teknis, melainkan juga pelanggaran terhadap hak konstitusional warga negara.¹⁴

Nafiah dan Prastyanti (2025) menjelaskan bahwa perlindungan data pribadi merupakan instrumen penting dalam menjaga martabat manusia di tengah perkembangan teknologi digital yang semakin kompleks.¹⁵ Temuan penelitian ini memperkuat pandangan tersebut dengan menunjukkan bahwa kebocoran data tidak hanya menyebabkan kerugian ekonomi, tetapi juga dapat menimbulkan dampak psikologis, sosial, dan hukum bagi korban.

Urgensi perlindungan data pribadi juga berkaitan erat dengan upaya pencegahan kejahatan siber. Data yang bocor dapat dimanfaatkan oleh pelaku kejahatan untuk melakukan pencurian identitas (*identity theft*), penipuan daring (*online fraud*), *phishing*, hingga pemerasan digital. Dalam banyak kasus, informasi yang diperoleh dari kebocoran data digunakan untuk mengakses akun keuangan korban sehingga menimbulkan kerugian yang signifikan.

Temuan lain menunjukkan bahwa perlindungan data pribadi memiliki korelasi langsung dengan tingkat kepercayaan publik terhadap layanan digital. Kepercayaan merupakan faktor utama yang menentukan keberhasilan transformasi digital. Apabila masyarakat merasa bahwa data pribadinya tidak aman, maka tingkat partisipasi dalam ekosistem digital akan menurun. Kondisi tersebut pada akhirnya dapat menghambat pertumbuhan ekonomi digital nasional.

Dalam konteks ekonomi digital, perlindungan data pribadi berfungsi sebagai instrumen yang menciptakan kepastian hukum bagi pelaku usaha maupun konsumen. Negara-negara yang memiliki sistem perlindungan data yang kuat cenderung memperoleh

¹⁴ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

¹⁵ Nafiah dan Prastyanti, "Perlindungan Data Pribadi Sebagai Hak Privasi Dalam Perspektif Hak Asasi Manusia," *Jurnal RechtsVinding* 14 (2025): 88.



tingkat kepercayaan investasi yang lebih tinggi dibandingkan negara yang memiliki regulasi lemah. Perlindungan data pribadi tidak hanya berkaitan dengan hak individu, tetapi juga menjadi faktor penting dalam meningkatkan daya saing ekonomi nasional.

Berdasarkan hasil analisis, penelitian ini menemukan bahwa urgensi perlindungan data pribadi di Indonesia tidak lagi dapat dipandang sebagai isu pelengkap dalam kebijakan digital. Perlindungan data pribadi telah menjadi kebutuhan mendasar yang harus diintegrasikan ke dalam seluruh kebijakan transformasi digital nasional guna menjamin keamanan, kepercayaan, dan keberlanjutan pembangunan ekonomi digital.

Urgensi perlindungan data pribadi semakin terlihat dari meningkatnya jumlah kasus kebocoran data yang melibatkan institusi publik maupun swasta dalam beberapa tahun terakhir. Kebocoran data yang terjadi pada berbagai sektor menunjukkan bahwa data pribadi telah menjadi target utama dalam kejahatan siber modern. Kondisi tersebut mengindikasikan bahwa ancaman terhadap keamanan data tidak lagi bersifat hipotetis, melainkan telah menjadi risiko nyata yang dapat memengaruhi jutaan masyarakat. Oleh karena itu, perlindungan data pribadi harus dipandang sebagai bagian dari strategi keamanan nasional yang memerlukan perhatian serius dari seluruh pemangku kepentingan.¹⁶

Selain aspek keamanan, perlindungan data pribadi juga memiliki dimensi sosial yang sangat penting. Kebocoran data dapat menimbulkan hilangnya rasa aman dan kepercayaan masyarakat terhadap institusi yang mengelola data mereka. Dalam era digital, kepercayaan merupakan modal utama bagi keberlangsungan layanan berbasis teknologi. Apabila masyarakat kehilangan kepercayaan akibat lemahnya perlindungan data, maka pemanfaatan layanan digital akan menurun dan berdampak pada terhambatnya agenda transformasi digital yang sedang dijalankan oleh pemerintah.¹⁷

Dari perspektif tata kelola pemerintahan yang baik (*good governance*), perlindungan data pribadi merupakan bagian dari prinsip akuntabilitas dan transparansi dalam penyelenggaraan layanan publik. Setiap institusi yang mengumpulkan dan mengelola data masyarakat memiliki tanggung jawab hukum dan moral untuk memastikan keamanan data tersebut. Kegagalan dalam melindungi data pribadi tidak hanya mencerminkan kelemahan sistem keamanan informasi, tetapi juga menunjukkan kurang

¹⁶ Sinta Dewi Rosadi, *Perlindungan Data Dan Privasi Di Era Digital* (Bandung: Refika Aditama, 2021).

¹⁷ Daniel J. Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).



optimalnya tata kelola organisasi dalam mengelola risiko digital yang berkembang secara dinamis.¹⁸

Perkembangan teknologi seperti kecerdasan buatan (*artificial intelligence*), komputasi awan (*cloud computing*), dan analisis data besar (*big data analytics*) semakin meningkatkan kompleksitas pengelolaan data pribadi. Teknologi tersebut memungkinkan pengumpulan, pemrosesan, dan pemanfaatan data dalam jumlah yang sangat besar sehingga berpotensi menimbulkan pelanggaran privasi apabila tidak diimbangi dengan regulasi dan mekanisme pengawasan yang memadai. Perlindungan data pribadi harus terus diperkuat melalui pembaruan regulasi yang adaptif terhadap perkembangan teknologi agar mampu memberikan perlindungan hukum yang efektif bagi masyarakat di era digital.¹⁹

Tantangan Implementasi dan Strategi Penguatan Regulasi Perlindungan Data Pribadi di Indonesia

1. Fenomena Kebocoran Data sebagai Indikator Lemahnya Tata Kelola Data

Maraknya kasus kebocoran data di Indonesia menunjukkan bahwa tantangan utama tidak terletak pada ketersediaan regulasi semata, melainkan pada implementasi dan tata kelola perlindungan data yang belum optimal. Berbagai kasus kebocoran data yang terjadi pada sektor kesehatan, layanan digital, lembaga publik, dan sektor perdagangan elektronik mengindikasikan masih lemahnya sistem keamanan informasi yang digunakan oleh pengelola data.

Temuan penelitian menunjukkan bahwa faktor penyebab kebocoran data dapat diklasifikasikan ke dalam empat kategori utama, yaitu kelemahan teknologi keamanan, rendahnya kepatuhan terhadap prinsip perlindungan data, kelalaian manusia (*human error*), serta lemahnya pengawasan regulator. Faktor-faktor tersebut saling berkaitan dan menciptakan risiko yang semakin besar terhadap keamanan data pribadi masyarakat.

Berbeda dengan penelitian terdahulu yang lebih berfokus pada aspek normatif perlindungan data, penelitian ini menegaskan bahwa ancaman kebocoran data

¹⁸ Irma Devita Purnamasari, "Urgensi Tata Kelola Perlindungan Data Pribadi Dalam Sistem Elektronik Di Indonesia," *Jurnal RechtsVinding* 12, no. 3 (2023): 421.

¹⁹ Paul M. Schwartz dan Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," *New York University Law Review* 86, no. 6 (2011): 1834–36.

merupakan persoalan multidimensional yang memerlukan pendekatan hukum, teknologi, dan sosial secara bersamaan.

2. Analisis Efektivitas Hukum Perlindungan Data Pribadi

Untuk menganalisis efektivitas perlindungan data pribadi di Indonesia, penelitian ini menggunakan teori efektivitas hukum yang dikemukakan oleh Soerjono Soekanto. Menurut Soekanto, keberhasilan suatu hukum dipengaruhi oleh lima faktor, yaitu hukum itu sendiri, aparat penegak hukum, sarana dan fasilitas, masyarakat, serta budaya hukum.²⁰

Pertama, dari aspek substansi hukum, Indonesia telah memiliki UU PDP yang relatif komprehensif. Akan tetapi, masih diperlukan berbagai peraturan pelaksana agar norma yang terdapat dalam undang-undang dapat diterapkan secara efektif.

Kedua, dari aspek struktur hukum, keberadaan lembaga pengawas yang independen menjadi kebutuhan mendesak. Tanpa pengawasan yang kuat, kepatuhan pengendali data terhadap ketentuan perlindungan data akan sulit diwujudkan.

Ketiga, dari aspek budaya hukum, tingkat kesadaran masyarakat mengenai pentingnya perlindungan data pribadi masih tergolong rendah. Banyak pengguna layanan digital yang belum memahami hak-haknya sebagai subjek data maupun risiko yang muncul akibat penyebaran data pribadi secara tidak terkendali.

Keempat, dari aspek sarana dan prasarana, masih terdapat kesenjangan kemampuan teknologi keamanan informasi antara institusi besar dan organisasi yang memiliki sumber daya terbatas. Kondisi ini menyebabkan standar perlindungan data belum diterapkan secara merata.

Temuan tersebut menunjukkan bahwa efektivitas perlindungan data pribadi tidak dapat dicapai hanya melalui pendekatan legislasi, tetapi juga membutuhkan penguatan institusi, peningkatan kapasitas teknologi, dan pembangunan budaya hukum digital.

3. Strategi Penguatan Regulasi Perlindungan Data Pribadi

Berdasarkan temuan penelitian, terdapat beberapa strategi yang dapat dilakukan untuk memperkuat efektivitas perlindungan data pribadi di Indonesia.

²⁰ Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: RajaGrafindo Persada, 2019).



Pertama, mempercepat pembentukan dan penguatan lembaga pengawas perlindungan data pribadi yang independen. Lembaga ini harus memiliki kewenangan investigasi, pengawasan, serta penjatuhan sanksi administratif terhadap pelanggaran perlindungan data.

Kedua, menyusun peraturan pelaksana yang lebih rinci dan implementatif guna memberikan kepastian hukum bagi pengendali dan pemroses data.

Ketiga, meningkatkan kapasitas aparat penegak hukum melalui pelatihan khusus terkait kejahatan siber dan perlindungan data pribadi. Kompetensi yang memadai akan meningkatkan efektivitas penegakan hukum terhadap pelanggaran data pribadi.

Keempat, memperluas program literasi digital kepada masyarakat. Edukasi mengenai keamanan digital dan hak-hak subjek data harus menjadi bagian dari strategi nasional perlindungan data pribadi.

Kelima, mendorong penerapan standar keamanan teknologi yang lebih tinggi melalui mekanisme audit keamanan, sertifikasi sistem elektronik, serta penerapan prinsip *privacy by design* dan *privacy by default*.

Dengan menerapkan strategi tersebut secara konsisten, perlindungan data pribadi di Indonesia dapat berkembang menuju sistem yang lebih efektif, adaptif, dan mampu menghadapi berbagai ancaman kebocoran data di era digital.

D. Penutup

Kesimpulan penelitian ini menunjukkan bahwa perlindungan data pribadi di Indonesia telah memiliki dasar hukum yang lebih kuat setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Keberadaan UU PDP menjadi langkah penting dalam memberikan kepastian hukum, memperjelas hak subjek data, serta menetapkan kewajiban bagi pengendali dan pemroses data pribadi. Temuan utama penelitian ini menegaskan bahwa urgensi penguatan regulasi perlindungan data pribadi tidak hanya berkaitan dengan aspek hukum, tetapi juga berkaitan dengan perlindungan hak privasi, pencegahan kejahatan siber, peningkatan kepercayaan publik, dan dukungan terhadap pertumbuhan ekonomi digital. Dengan demikian, perlindungan data pribadi harus dipandang sebagai bagian dari perlindungan hak asasi manusia sekaligus



sebagai fondasi penting dalam pembangunan ekosistem digital nasional yang aman dan berkelanjutan.

Meskipun demikian, penelitian ini menemukan bahwa implementasi perlindungan data pribadi di Indonesia masih menghadapi sejumlah kelemahan, antara lain belum optimalnya pengawasan, rendahnya literasi digital masyarakat, keterbatasan infrastruktur keamanan teknologi, serta penegakan hukum yang belum sepenuhnya efektif. Kelebihan dari temuan penelitian ini terletak pada penegasan bahwa penguatan perlindungan data pribadi membutuhkan pendekatan yang komprehensif, yaitu melalui pembentukan lembaga pengawas yang independen, penyusunan peraturan turunan yang aplikatif, peningkatan kapasitas aparat penegak hukum, serta edukasi publik secara berkelanjutan. Adapun keterbatasan penelitian ini adalah pembahasannya masih bersifat yuridis normatif sehingga belum menggambarkan secara empiris tingkat kepatuhan lembaga publik maupun swasta dalam menerapkan UU PDP. Oleh karena itu, penelitian selanjutnya dapat dikembangkan melalui pendekatan empiris dengan mengkaji efektivitas penerapan UU PDP pada sektor tertentu, seperti layanan kesehatan, perbankan, e-commerce, atau administrasi kependudukan.

REFERENSI

- Badan Siber dan Sandi Negara (BSSN). *Laporan Tahunan Keamanan Siber Indonesia 2024*. Edited by BSSN. Jakarta, 2024.
- Cukier, Viktor Mayer-Schönberger & Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray, 2013AD.
- Hasibuan, N. S., & Anisa, D. (2026). Perkembangan Pembaruan Hukum Islam di Indonesia. *Islamic Studies and Law*, 1(2), 55-60.
- Google, Temasek, & Bain & Company. *E-Conomy SEA 2024 Report*. Singapore: Google Southeast Asia, 2024.
- Liuhua. "Ersonal Data Protection Governance in the Digital Era," *International Journal of Law and Information Technology* 33, no. 1 (2025): 45.
- Makarim, Edmon. "Tantangan Implementasi Perlindungan Data Pribadi Di Indonesia Pasca Disahkannya UU PDP." *Jurnal Hukum Dan Pembangunan* 53, no. 2 (2023): 215.
- Mamudji, Soerjono Soekanto dan Sri. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers, 2019.



- Marzuki, Peter Mahmud. *Penelitian Hukum, Edisi Revisi*. Jakarta: Kencana, 2021.
- Prastyanti, Nafiah dan. “Perlindungan Data Pribadi Sebagai Hak Privasi Dalam Perspektif Hak Asasi Manusia.” *Jurnal RechtsVinding* 14 (2025): 88.
- Purnamasari, Irma Devita. “Urgensi Tata Kelola Perlindungan Data Pribadi Dalam Sistem Elektronik Di Indonesia.” *Jurnal RechtsVinding* 12, no. 3 (2023): 421.
- Rosadi, Sinta Dewi. *Perlindungan Data Dan Privasi Di Era Digital*. Bandung: Refika Aditama, 2021.
- . *Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia*. Bandung: Refika Aditama, 2018.
- Soekanto, Soerjono. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: RajaGrafindo Persada, 2019.
- Solove, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.
- Solove, Paul M. Schwartz dan Daniel J. “The PII Problem: Privacy and a New Concept of Personally Identifiable Information.” *New York University Law Review* 86, no. 6 (2011): 1834–36.
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (n.d.).
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 (n.d.).
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (n.d.).
- UNESCO. *Digital Literacy Global Framework*. Paris: UNESCO Institute for Statistics, 2023.