

Meningkatnya Kasus Kebobolan Data: Dampaknya Bagi Masyarakat

Yunda Rahayu Nisrina¹, Hanifa Mayada², Muhammad Raihan³,
Muhammad Fahmi Afriza⁴, Gusti Dico Laudry⁵

^{1,2,3}Hukum Tata Negara, Fakultas Syari'ah, Universitas Islam Negeri Palangka Raya, Indonesia

E-mail: gustidicolaudry21@gmail.com

Article Info

Article history:

Received December 11, 2025

Revised December 23, 2025

Accepted December 27, 2025

Keywords:

Data Breach, Personal Data Protection, Digital Security, Privacy, Society.

ABSTRACT

The increasing number of data breaches poses a serious threat to society in the digital age. These incidents result in privacy violations, economic losses, identity theft, and a decline in public trust in data management institutions. Weak security systems, low digital literacy, and suboptimal law enforcement exacerbate these risks. Therefore, strengthening data protection, increasing public awareness, and implementing strict regulations are necessary to minimize the impact of data breaches.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Article Info

Article history:

Received December 11, 2025

Revised December 23, 2025

Accepted December 27, 2025

Keywords:

Kebobolan Data, Perlindungan Data Pribadi, Keamanan Digital, Privasi, Masyarakat.

ABSTRACT

Meningkatnya kasus kebobolan data menjadi ancaman serius bagi masyarakat di era digital. Insiden ini berdampak pada pelanggaran privasi, kerugian ekonomi, penyalahgunaan identitas, serta menurunnya kepercayaan publik terhadap institusi pengelola data. Lemahnya sistem keamanan, rendahnya literasi digital, dan kurang optimalnya penegakan hukum memperparah risiko tersebut. Oleh karena itu, penguatan perlindungan data, peningkatan kesadaran masyarakat, serta regulasi yang tegas diperlukan untuk meminimalkan dampak kebobolan data.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Gusti Dico Laudry

Hukum Tata Negara, Fakultas Syari'ah, Universitas Islam Negeri Palangka Raya, Indonesia

E-mail: gustidicolaudry21@gmail.com

PENDAHULUAN

Berkembangnya sebuah teknologi, informasi dan komunikasi penetrasi internet sudah banyak menjangkau masyarakat di seluruh penjuru dunia tanpa ada batasan ruang dan waktu.¹ Pada saat ini, penggunaan internet sangat memerlukan perlindungan terhadap data pribadi individu. Internet yang pada awalnya hanya dimanfaatkan sebagai media untuk menyebarkan informasi, kini telah berkembang menjadi sistem yang bersifat interaktif serta berfungsi sebagai sarana untuk melakukan berbagai aktivitas dan transaksi.

Data pribadi saat ini memiliki peran yang sangat penting karena berkaitan langsung dengan privasi setiap individu. Perlindungan data pribadi merupakan bagian dari hak privasi sekaligus hak personal seseorang. Ketentuan mengenai hal ini telah diatur dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menegaskan bahwa setiap orang berhak atas perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada dalam kekuasaannya. Selain itu, setiap individu juga berhak memperoleh rasa aman dan perlindungan dari segala bentuk ancaman yang menimbulkan rasa takut untuk bertindak maupun tidak bertindak, yang keseluruhannya merupakan bagian dari hak asasi manusia dan berkaitan erat dengan hak privasi.²

Pengumpulan dan penyebaran data pribadi dapat dikategorikan sebagai pelanggaran terhadap privasi seseorang, karena hak privasi mencakup kewenangan individu untuk menentukan apakah data pribadinya akan diberikan atau tidak. Data pribadi juga memiliki nilai sebagai aset atau komoditas dengan nilai ekonomi yang tinggi. Isu mengenai urgensi perlindungan data pribadi semakin mengemuka seiring dengan meningkatnya penggunaan telepon seluler dan internet. Berbagai kasus yang terjadi, khususnya yang berkaitan dengan kebocoran data pribadi yang berujung pada tindakan penipuan maupun kejahatan pornografi, semakin menegaskan pentingnya pembentukan regulasi hukum yang secara khusus mengatur dan melindungi data pribadi.³

Meningkatnya kasus kebocoran data menunjukkan adanya kerentanan serius dalam sistem keamanan informasi yang digunakan oleh berbagai pihak, baik instansi pemerintah maupun swasta. Kebocoran data pribadi yang terjadi secara berulang tidak hanya memperlihatkan lemahnya pengelolaan dan pengawasan data, tetapi juga memperbesar risiko penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Dampak langsung yang dirasakan masyarakat antara lain maraknya penipuan berbasis digital, pencurian identitas, hingga penyalahgunaan data untuk kepentingan ekonomi dan kriminal, yang pada akhirnya merugikan individu secara finansial maupun psikologis.

Lebih jauh, meningkatnya kasus kebocoran data juga berdampak pada menurunnya kepercayaan masyarakat terhadap layanan digital dan sistem elektronik. Rasa tidak aman dalam menggunakan internet dapat menghambat partisipasi masyarakat dalam aktivitas digital, termasuk transaksi ekonomi, layanan publik, dan pertukaran informasi. Kondisi ini berpotensi menghambat perkembangan ekonomi digital serta menciptakan ketimpangan akses dan pemanfaatan teknologi. Oleh karena itu, peningkatan keamanan data dan perlindungan hukum terhadap data pribadi menjadi kebutuhan mendesak guna meminimalkan dampak negatif kebocoran data serta menjamin rasa aman bagi masyarakat dalam ruang digital.

¹ Huda, M. N., & Kifli, Z., "Perlindungan Hukum Data Pribadi Dalam Keilmuan Multi Disipliner", *Desiderata Law Review 1*, No. 2, (2024): 44-58.

² Navis, A. A., "Kebocoran Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Perspektif Siyasah Dusturiyah", *Al-Balad: Journal of Constitutional Law 5*, No.1, (2023).

³ Niffari, H., "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)", *Jurnal Yuridis 7*, No. 1, (2020): 105-119.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Penelitian ini mengkaji ketentuan hukum yang mengatur perlindungan data pribadi serta kebocoran data, khususnya yang berkaitan dengan hak privasi dan dampaknya bagi masyarakat, melalui analisis terhadap peraturan perundang-undangan, doktrin hukum, dan asas-asas hukum yang relevan.

Sumber data yang digunakan berupa bahan hukum primer, seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan peraturan perundang-undangan terkait perlindungan data pribadi, serta bahan hukum sekunder berupa buku, jurnal ilmiah, hasil penelitian, dan artikel yang membahas kebocoran data dan dampaknya. Teknik pengumpulan data dilakukan melalui studi kepustakaan, sedangkan teknik analisis data menggunakan analisis kualitatif, yaitu dengan menafsirkan dan mengkaji bahan hukum secara sistematis untuk menarik kesimpulan yang relevan dengan permasalahan penelitian.

Selain itu, penelitian ini juga menggunakan pendekatan analitis dengan menelaah keterkaitan antara norma hukum yang mengatur perlindungan data pribadi dengan realitas sosial berupa meningkatnya kasus kebocoran data di Indonesia. Pendekatan ini dilakukan untuk melihat sejauh mana efektivitas norma hukum dalam memberikan perlindungan terhadap hak privasi masyarakat, serta untuk mengidentifikasi celah hukum yang masih memungkinkan terjadinya kebocoran data pribadi secara berulang. Dengan demikian, penelitian ini tidak hanya berhenti pada pengkajian norma secara tekstual, tetapi juga menilai relevansi dan daya berlakunya dalam konteks perkembangan teknologi informasi.

Analisis bahan hukum dilakukan secara preskriptif, yaitu dengan memberikan argumentasi hukum mengenai bagaimana seharusnya perlindungan data pribadi diterapkan oleh negara dan penyelenggara sistem elektronik. Analisis preskriptif ini bertujuan untuk merumuskan rekomendasi normatif terkait penguatan perlindungan data pribadi, baik melalui optimalisasi penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi maupun melalui peran aktif negara dalam pengawasan dan penegakan hukum. Dengan pendekatan tersebut, penelitian ini diharapkan mampu memberikan kontribusi pemikiran bagi pengembangan hukum perlindungan data pribadi di Indonesia.

Seluruh bahan hukum yang dianalisis disusun dan dikaji secara sistematis dengan memperhatikan konsistensi logika hukum dan kesesuaian dengan asas-asas hukum yang berlaku. Hasil analisis kemudian disajikan dalam bentuk uraian deskriptif-analitis, sehingga dapat menggambarkan secara jelas hubungan antara pengaturan hukum perlindungan data pribadi dan dampak kebocoran data bagi masyarakat. Metode ini dipilih agar kesimpulan yang dihasilkan bersifat argumentatif, objektif, dan dapat dipertanggungjawabkan secara akademik.

HASIL DAN PEMBAHASAN

Salah satu perkembangan yang terus berkembang pesat adalah di bidang teknologi informasi, yang tercermin dalam lahirnya internet, yang secara ilmiah dikenal sebagai cyberspace (Iskandar Wibawa, 2016).⁴ Pada era digital yang terus mengalami perkembangan pesat, pertukaran informasi melalui berbagai platform daring telah menjadi bagian penting dari aktivitas sehari-hari, sehingga mengubah pola interaksi, cara bekerja, dan komunikasi masyarakat (Angeline Xiao, 2018). Teknologi modern memungkinkan proses pengumpulan,

⁴ Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H., "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi", *Innovative: Journal Of Social Science Research* 3, No. 6, (2023): 2898-2905.

penyimpanan, pengolahan, serta distribusi data dalam skala yang sangat besar. Namun demikian, tingginya kecepatan dan besarnya volume arus data tersebut juga menimbulkan konsekuensi yang serius terhadap perlindungan privasi individu (Sautunnida, 2018). Pelanggaran terhadap data pribadi di Indonesia terjadi dalam jumlah yang sangat besar, mulai dari data pribadi yang bersifat umum hingga data yang bersifat sangat vital, seperti data kependudukan yang dapat digunakan untuk keperluan validasi transaksi keuangan. Pelanggaran terhadap perlindungan data pribadi di Indonesia sejatinya tidak hanya muncul seiring dengan perkembangan teknologi informasi, melainkan telah terjadi jauh sebelum era digital berkembang pesat.

Sebagai contoh, telah menjadi rahasia umum bahwa agen asuransi kerap memperjualbelikan data pribadi nasabah kepada agen lain. Hal serupa juga terjadi pada agen penjual kartu kredit maupun agen pemasaran lainnya. Akibatnya, seseorang yang pernah mendaftarkan diri untuk memperoleh kartu kredit dapat menerima berbagai penawaran kartu kredit lain beberapa bulan kemudian, meskipun tidak pernah mengajukan permohonan kembali ke bank lain. Praktik serupa juga dialami oleh pembeli kendaraan bermotor roda empat, di mana beberapa tahun setelah pembelian, mereka kembali dihubungi oleh pihak tertentu yang telah memiliki data lengkap untuk menawarkan penggantian merek atau pembelian kendaraan baru. Praktik-praktik tersebut telah berlangsung selama puluhan tahun di Indonesia, namun sering kali tidak dilaporkan karena dianggap tidak menimbulkan kerugian secara langsung. Padahal, kebocoran data pribadi seperti contoh tersebut merupakan pelanggaran yang sangat serius, bahkan dapat dikatakan lebih berbahaya dibandingkan kebocoran privasi pada akun media sosial, seperti kasus Facebook yang sempat marak terjadi beberapa tahun terakhir.⁵

Kebocoran data pribadi yang terjadi secara sistematis dan berulang tersebut menunjukkan bahwa persoalan perlindungan data pribadi di Indonesia bukanlah fenomena baru, melainkan masalah struktural yang telah mengakar lama. Perbedaannya, pada masa lalu kebocoran data sering dipandang sebagai praktik bisnis yang “wajar” dan tidak dianggap sebagai pelanggaran hukum yang serius, karena belum adanya kesadaran publik mengenai hak atas data pribadi. Selain itu, minimnya regulasi yang secara khusus mengatur perlindungan data pribadi turut memperkuat anggapan bahwa praktik pengumpulan dan penyebaran data tanpa persetujuan subjek data merupakan hal yang dapat ditoleransi. Akibatnya, pelanggaran data pribadi berlangsung dalam ruang abu-abu hukum yang sulit disentuh oleh mekanisme pertanggung jawaban.

Seiring dengan meningkatnya ketergantungan masyarakat terhadap layanan digital, risiko kebocoran data pribadi mengalami eskalasi yang jauh lebih kompleks dan masif. Jika sebelumnya kebocoran data terbatas pada informasi dasar seperti nama, alamat, atau nomor telepon, maka pada era digital kebocoran data dapat mencakup data identitas kependudukan, data biometrik, riwayat transaksi keuangan, hingga data kesehatan. Karakteristik data digital yang mudah digandakan, disebarluaskan, dan disimpan dalam jangka waktu lama menjadikan dampak kebocoran data bersifat berkelanjutan dan sulit dipulihkan. Sekali data pribadi tersebar, pemilik data hampir tidak memiliki kendali untuk menarik kembali atau membatasi penggunaannya.⁶

Tidak hanya berdampak pada aspek ekonomi dan privasi individu, kebocoran data juga berimplikasi pada kepercayaan masyarakat terhadap layanan digital dan institusi yang

⁵ Sutrisna, C., “Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia”, *Wacana Paramarta: Jurnal Ilmu Hukum* 20, No. 5, (2021): 1-10.

⁶ L. Sautunnida, “Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia,” *Kanun Jurnal Ilmu Hukum*, no. 20 (2018): 369-384.

mengelola data tersebut. Ketika data pribadi suatu kelompok besar individu bocor, masyarakat menjadi skeptis terhadap keamanan layanan digital, sehingga menurunkan partisipasi publik dalam sistem yang sebenarnya dirancang untuk kemudahan layanan masyarakat. Hal ini berpotensi memperlambat adopsi teknologi digital secara luas karena rasa takut atau tidak percayanya masyarakat terhadap proteksi data yang ada.

Secara hukum, fenomena kebocoran data pribadi di Indonesia menjadi sorotan utama seiring dengan munculnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang merupakan payung hukum komprehensif pertama di Indonesia untuk melindungi data personal warga negara.⁷ Meskipun UU PDP telah disahkan, berbagai studi menunjukkan bahwa penerapannya di lapangan masih menghadapi kendala signifikan, termasuk rendahnya kesadaran hukum masyarakat dan kepatuhan penyelenggara sistem elektronik dalam menjalankan kewajiban perlindungan data pribadi.

Lebih jauh, tanggung jawab hukum atas kebocoran data pribadi pada penyelenggara sistem elektronik tidak hanya terbatas pada sektor privat, tetapi juga negara sendiri sebagai pengendali data publik. Misalnya, kasus kebocoran data peserta layanan publik seperti Badan Penyelenggara Jaminan Sosial (BPJS) menunjukkan bahwa lemahnya sistem pengelolaan data dapat melukai hak atas privasi warga negara dan menimbulkan pertanyaan mengenai akuntabilitas lembaga publik dalam menjamin kerahasiaan data yang mereka simpan.

Peran negara dan lembaga pengawas menjadi sangat penting untuk menjawab tantangan kebocoran data ini. Keberadaan UU PDP memang menyediakan kerangka hukum, tetapi implementasi dan pengawasan tetap menjadi elemen krusial yang menentukan efektivitas perlindungan data pribadi. Sejumlah penelitian menyatakan bahwa meskipun kerangka hukum telah kuat secara normatif, praktik penegakan hukum terhadap pelanggaran data pribadi di Indonesia masih belum optimal karena keterbatasan mekanisme pengawasan dan sumber daya penegak hukum yang memahami ranah siber.⁸

Selain itu, literasi digital masyarakat juga menjadi bagian penting dari sistem perlindungan data pribadi. Rendahnya literasi digital membuat banyak individu tidak menyadari hak-hak mereka terkait data pribadi, atau bahkan tidak tahu bagaimana melindungi data mereka sendiri saat menggunakan layanan digital. Upaya pendidikan dan kesadaran hukum ini menjadi bagian integral dari penguatan sistem perlindungan data, sehingga masyarakat tidak hanya menjadi objek data tetapi juga subjek yang aktif dalam memperjuangkan hak privasi mereka.

Pengaturan perlindungan data pribadi pada dasarnya merupakan perwujudan dari pengakuan negara terhadap hak asasi manusia, khususnya hak atas perlindungan diri pribadi. Data pribadi tidak hanya memiliki dimensi privat, tetapi juga berdimensi hukum dan sosial karena berkaitan langsung dengan martabat manusia. Niffari menegaskan bahwa perlindungan data pribadi merupakan bagian tidak terpisahkan dari hak asasi manusia atas perlindungan diri pribadi, yang menuntut adanya jaminan hukum dari negara agar data tersebut tidak disalahgunakan oleh pihak mana pun tanpa persetujuan pemiliknya.⁹ Dalam konteks ini,

⁷ Esi Anindya Azzahra and Ema Nurkhaerani, "Analisis Yuridis Kebocoran Data LinkedIn 2021 Dalam Kerangka UU Perlindungan Data Pribadi Indonesia Fakultas Hukum , Universitas Pembangunan Nasional ' Veteran ' Jakarta , Perubahan Besar Terhadap Cara Orang Berinteraksi , Bekerja , Dan Mengatur Identitas," *ALADALAH : Jurnal Politik, Sosial, Hukum Dan Humaniora* 4, no. 1 (2021): 99-108.

⁸ Muhammad Dhifan Fadlih et al., "Pengembangan Umkm Produk Kebaya Melalui Pemanfaatan Platform Tiktok," *Jurnal Pengabdian Masyarakat (JPM) SENSAS* 4, no. 2 (2024): 91-97.

⁹ H. Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *Jurnal Yuridis* 7, No. 1 (2020): 105-119.

negara memiliki kewajiban konstitusional untuk melindungi data pribadi warga negara sebagai bagian dari perlindungan hak asasi manusia.

Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam sistem hukum Indonesia, karena untuk pertama kalinya perlindungan data pribadi diatur secara komprehensif dan sistematis. UU PDP memberikan definisi yang jelas mengenai data pribadi, subjek data, pengendali data, serta prosesor data, sekaligus menetapkan prinsip-prinsip pengolahan data pribadi yang harus dipatuhi. Menurut Sautunnida, keberadaan undang-undang khusus mengenai perlindungan data pribadi sangat penting untuk memberikan kepastian hukum dan mencegah praktik penyalahgunaan data yang selama ini terjadi akibat kekosongan hukum.¹⁰ Dengan demikian, UU PDP diharapkan mampu menjadi instrumen preventif dan represif dalam menanggulangi kebocoran data pribadi.

efektivitas UU PDP dalam praktik masih menghadapi berbagai tantangan. Salah satu persoalan utama adalah rendahnya tingkat kepatuhan penyelenggara sistem elektronik terhadap kewajiban perlindungan data pribadi. Banyak institusi, baik swasta maupun publik, belum memiliki standar keamanan data yang memadai, sehingga rentan terhadap serangan siber dan kebocoran data. Sutrisna menyebutkan bahwa kondisi darurat kebocoran data pribadi di Indonesia tidak hanya disebabkan oleh serangan eksternal, tetapi juga oleh lemahnya tata kelola data dan kurangnya kesadaran hukum dari pengelola data itu sendiri.¹¹ Hal ini menunjukkan bahwa penguatan regulasi harus diiringi dengan peningkatan kapasitas teknis dan budaya kepatuhan hukum.

Kasus kebocoran data besar, seperti kebocoran data pengguna LinkedIn pada tahun 2021, menjadi contoh nyata bagaimana lemahnya sistem perlindungan data dapat berdampak luas terhadap masyarakat. Azzahra dan Nurkhaerani menjelaskan bahwa kebocoran data LinkedIn tidak hanya merugikan individu secara personal, tetapi juga menunjukkan belum optimalnya mekanisme pertanggungjawaban hukum lintas negara dalam kasus kebocoran data berbasis platform global.¹² Fenomena ini memperlihatkan bahwa perlindungan data pribadi tidak lagi dapat dipandang sebagai isu domestik semata, melainkan sebagai persoalan global yang membutuhkan kerja sama lintas yurisdiksi.

Selain aspek regulasi dan penegakan hukum, literasi digital masyarakat memegang peranan penting dalam upaya perlindungan data pribadi. Rendahnya pemahaman masyarakat mengenai pentingnya menjaga data pribadi sering kali membuat individu secara sukarela membagikan data mereka tanpa mempertimbangkan risiko yang mungkin timbul. Daeng et al. menekankan bahwa perlindungan data pribadi dalam era digital tidak hanya bergantung pada regulasi, tetapi juga pada kesadaran kolektif masyarakat untuk bersikap bijak dalam menggunakan teknologi dan layanan digital.¹³ Oleh karena itu, edukasi dan peningkatan literasi digital harus menjadi bagian integral dari kebijakan perlindungan data pribadi.

¹⁰ L. Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, No. 20 (2018): 369–384.

¹¹ C. Sutrisna, "Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia", *Wacana Paramarta: Jurnal Ilmu Hukum* 20, No. 5 (2021): 1–10.

¹² Esi Anindya Azzahra dan Ema Nurkhaerani, "Analisis Yuridis Kebocoran Data LinkedIn 2021 dalam Kerangka UU Perlindungan Data Pribadi Indonesia", *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora* 4, No. 1 (2021): 99–108.

¹³ Y. Daeng et al., "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi", *Innovative: Journal of Social Science Research* 3, No. 6 (2023): 2898–2905.

Selain dari faktor eksternal dan lemahnya sistem keamanan, fenomena kebobolan data juga erat kaitannya dengan aspek tata kelola data (data governance) yang belum optimal di banyak lembaga, baik publik maupun swasta. Tata kelola data yang baik mencakup kebijakan, prosedur, dan standar teknis yang jelas dalam pengelolaan data pribadi, mulai dari pengumpulan, penyimpanan, pemrosesan, hingga penghapusan. Namun, dalam praktiknya, banyak organisasi yang belum menerapkan prinsip *privacy by design* dan *security by default*, sehingga celah keamanan sering kali muncul dari dalam sistem itu sendiri. Penelitian oleh Adiwijaya dan Putra (2022) menunjukkan bahwa lebih dari 60% kebocoran data di Indonesia disebabkan oleh kesalahan manusia (*human error*) dan kurangnya protokol internal yang ketat, seperti penggunaan kata sandi yang lemah, kegagalan dalam pembaruan sistem, serta akses data yang tidak terkendali. Hal ini mengindikasikan bahwa perlindungan data tidak hanya bergantung pada regulasi, tetapi juga pada budaya organisasi yang menempatkan keamanan informasi sebagai prioritas utama.¹⁴

Di sisi lain, perkembangan teknologi seperti artificial intelligence (AI) dan big data analytics turut memunculkan tantangan baru dalam perlindungan data pribadi. Teknologi ini memungkinkan pengolahan data dalam skala masif dengan kecepatan tinggi, yang sering kali dilakukan tanpa sepengetahuan atau persetujuan subjek data. Data yang terkumpul dapat dianalisis untuk memprediksi perilaku, preferensi, bahkan kondisi kesehatan seseorang, yang berpotensi digunakan untuk tujuan komersial, politik, atau pengawasan yang melanggar privasi. Dalam konteks ini, UU PDP memang telah mengatur prinsip *purpose limitation* dan *data minimization*, yaitu bahwa pengumpulan data harus dibatasi sesuai tujuan yang jelas dan data yang diambil harus relevan serta tidak berlebihan. Namun, implementasi prinsip ini dalam praktik masih sulit diawasi, terutama ketika pemrosesan data dilakukan oleh platform digital global yang memiliki pusat data di luar yurisdiksi Indonesia. Oleh karena itu, diperlukan kerangka kerja sama internasional dan harmonisasi regulasi untuk memastikan bahwa perlindungan data pribadi dapat diberlakukan secara efektif lintas batas negara.

Peran masyarakat sipil dan organisasi non-pemerintah juga menjadi faktor penting dalam mendorong akuntabilitas pelaku pengelola data. Di beberapa negara, adanya lembaga independen seperti otoritas perlindungan data yang dilengkapi dengan kewenangan investigasi dan sanksi telah terbukti mampu meningkatkan kepatuhan terhadap regulasi perlindungan data. Di Indonesia, meskipun UU PDP telah mengamanatkan pembentukan otoritas serupa, proses implementasinya masih berjalan lambat. Sementara itu, inisiatif dari kelompok masyarakat, seperti pengaduan kolektif (*class action*) atau kampanye kesadaran publik, dapat menjadi penggerak awal untuk menekan pihak yang lalai dalam melindungi data pribadi. Contoh nyata adalah gugatan hukum terhadap beberapa perusahaan teknologi terkait kebocoran data, yang berhasil mengangkat isu ini ke permukaan dan mendorong perbaikan sistem keamanan. Partisipasi aktif masyarakat dalam mengawal penerapan UU PDP merupakan elemen krusial untuk menciptakan ekosistem digital yang lebih aman dan responsif terhadap hak-hak pengguna.

Selanjutnya, pendekatan holistik yang menggabungkan aspek hukum, teknologi, dan edukasi perlu dikembangkan untuk menanggulangi masalah kebobolan data secara berkelanjutan. Dari sisi hukum, penegakan sanksi yang tegas dan tidak diskriminatif terhadap pelanggar UU PDP harus konsisten dilakukan, baik terhadap entitas swasta maupun instansi pemerintah. Dari sisi teknologi, investasi dalam pengembangan sistem keamanan siber, enkripsi data, dan mekanisme two-factor authentication (2FA) perlu ditingkatkan, terutama

¹⁴ Adiwijaya, A., & Putra, R. D., 2022, "Analisis Faktor Penyebab Kebocoran Data Pribadi di Indonesia: Studi Kasus pada Sektor Keuangan dan Kesehatan", Jurnal Teknologi Informasi dan Ilmu Komputer, Vol. 9, No. 2.

pada layanan yang mengelola data sensitif. Sementara itu, dari sisi edukasi, kurikulum literasi digital dan kesadaran hukum mengenai perlindungan data pribadi harus diintegrasikan ke dalam sistem pendidikan formal maupun non-formal, sehingga masyarakat tidak hanya menjadi korban pasif, tetapi juga aktor yang mampu melindungi diri mereka sendiri. Sinergi antara ketiga aspek tersebut akan membentuk lapisan pertahanan yang lebih kuat dalam menghadapi ancaman kebocoran data di era digital yang terus berkembang.¹⁵

Akhirnya, penting untuk disadari bahwa perlindungan data pribadi bukanlah tujuan akhir, melainkan bagian dari upaya yang lebih besar untuk menciptakan tatanan masyarakat digital yang beretika, inklusif, dan berdaulat. Data pribadi adalah cerminan dari identitas dan martabat manusia, sehingga pengelolaannya harus dilakukan dengan penuh tanggung jawab dan penghormatan terhadap hak asasi individu. Dengan demikian, upaya penanganan kebocoran data tidak boleh dilihat sekadar sebagai masalah teknis atau hukum semata, tetapi juga sebagai komitmen kolektif untuk membangun kepercayaan dan keberlanjutan dalam interaksi digital di masa depan.¹⁶

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa meningkatnya kasus kebocoran data di Indonesia merupakan masalah struktural yang bersifat multidimensional, melibatkan aspek hukum, teknologi, tata kelola, dan sosial-budaya. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan landasan hukum yang komprehensif, efektivitas implementasinya masih terhambat oleh rendahnya kepatuhan pelaku pengelola data, lemahnya mekanisme pengawasan, serta keterbatasan kesadaran hukum dan literasi digital masyarakat. Selain itu, perkembangan teknologi seperti *big data* dan kecerdasan buatan turut memperumit tantangan perlindungan data, sementara kerjasama internasional dan pendekatan holistik—yang mengintegrasikan penegakan hukum, peningkatan keamanan siber, serta edukasi public menjadi kebutuhan mendesak untuk membangun ekosistem digital yang aman, berkeadilan, dan menghormati hak privasi sebagai bagian dari hak asasi manusia. Oleh karena itu, upaya perlindungan data pribadi harus dipandang sebagai komitmen bersama yang berkelanjutan, tidak hanya untuk mencegah kerugian individu, tetapi juga untuk memperkuat kepercayaan masyarakat dan keberlanjutan transformasi digital di Indonesia.

DAFTAR PUSTAKA

Artikel Jurnal

- Adiwijaya, A., & Putra, R. D., “Analisis Faktor Penyebab Kebocoran Data Pribadi di Indonesia: Studi Kasus pada Sektor Keuangan dan Kesehatan”, *Jurnal Teknologi Informasi dan Ilmu Komputer*, Vol. 9, No. 2, 2022.
- Azzahra, Esi Anindya dan Ema Nurkhaerani, “Analisis Yuridis Kebocoran Data LinkedIn 2021 dalam Kerangka UU Perlindungan Data Pribadi Indonesia”, *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 4, No. 1, 2021.

¹⁵ Fitriani, L., 2023, "Peran Gugatan Kolektif dalam Mendorong Akuntabilitas Pelaku Usaha atas Kebocoran Data Pribadi", *Jurnal Hukum Bisnis*, Vol. 28, No. 1.

¹⁶ Santoso, B., 2022, "Tantangan Regulasi Perlindungan Data Pribadi di Era Big Data dan Kecerdasan Buatan", *Jurnal Hukum dan Pembangunan*, Vol. 52, No. 3.

- Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H., "Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi", *Innovative: Journal Of Social Science Research*, Vol. 3, No. 6, 2023.
- Fadlih, Muhammad Dhifan et al., "Pengembangan Umkm Produk Kebaya Melalui Pemanfaatan Platform Tiktok", *Jurnal Pengabdian Masyarakat (JPM) SENSAS*, Vol. 4, No. 2, 2024.
- Fitriani, L., "Peran Gugatan Kolektif dalam Mendorong Akuntabilitas Pelaku Usaha atas Kebocoran Data Pribadi", *Jurnal Hukum Bisnis*, Vol. 28, No. 1, 2023.
- Huda, M. N., & Kifli, Z., "Perlindungan Hukum Data Pribadi Dalam Keilmuan Multi Disipliner", *Desiderata Law Review*, Vol. 1, No. 2, 2024.
- Navis, A. A., "Kebocoran Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Perspektif Siyasah Dusturiyah", *Al-Balad: Journal of Constitutional Law*, Vol. 5, No. 1, 2023.
- Niffari, H., "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)", *Jurnal Yuridis*, Vol. 7, No. 1, 2020.
- Santoso, B., "Tantangan Regulasi Perlindungan Data Pribadi di Era Big Data dan Kecerdasan Buatan", *Jurnal Hukum dan Pembangunan*, Vol. 52, No. 3, 2022.
- Sautunnida, L., "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia", *Kanun Jurnal Ilmu Hukum*, No. 20, 2018.
- Sutrisna, C., "Aspek Hukum Perlindungan Data Pribadi dan Kondisi Darurat Kebocoran atas Data Pribadi di Indonesia", *Wacana Paramarta: Jurnal Ilmu Hukum*, Vol. 20, No. 5, 2021.