I.dn.J.of Law 7(1) : 46-51, Desember 2024
DOI: 10.35965/ijlf.v7i1.5267

Indonesian Journal of Legality of Law
e-ISSN : 2477-197X
https://postgraduate.universitasbosowa.ac.id/

PERLINDUNGAN HUKUM DATA PRIBADI DALAM PERSPEKTIF HAK ASASI MANUSIA

Legal Protection of Personal Data in The Perspective of Human Rights in Indonesia

Novita Angraini K*, Zulkifli Makkawaru, Almusawir
Program Studi Ilmu Hukum Program Pascasarjana Universitas Bosowa
*Email: angrabussinessthing@gmail.com

Diterima: 10 Agustus 2024/Disetujui: 30 Desember 2024

ABSTRAK

Penelitian ini bertujuan untuk mengkaji dan menganalisis integrasi hukum perlindungan data pribadi dengan konsep hak asasi manusia dan hambatan-hambatan dalam perlindungannya. Penelitian ini menggunakan penelitian normatif empiris. Hasil penelitian menunjukkan bahwa: 1) Integrasi hukum perlindungan data pribadi dengan konsep hak asasi manusia telah berjalan secara substansial, meskipun implementasi perlindungan data pribadi belum sepenuhnya sesuai harapan. 2) Hambatan dalam pelaksanaan perlindungan data pribadi dipengaruhi oleh faktor internal dan faktor eksternal. Faktor internal meliputi kurangnya kesadaran di kalangan Subjek dan Pengendali Data Pribadi, kompleksitas dalam pemrosesan data, lemahnya sistem keamanan data di Indonesia, belum disahkannya Rancangan Peraturan Pelaksanaan Undang-Undang Pelindungan Data Pribadi, serta ketiadaan Lembaga Independen Khusus yang bertanggung jawab atas perlindungan data pribadi. Di sisi lain, faktor eksternal meliputi intersepsi atau penyadapan yang mengakibatkan kegagalan perlindungan data, terutama di instansi pemerintah dan sektor jasa keuangan.

Kata Kunci: Pelindungan Data Pribadi, Hak Asasi Manusia, Integrasi Hukum, Hambatan Pelaksanaan

ABSTRACT

This research aims to review and analyze the legal integration of personal data protection with the concept of human rights and obstacles in its protection. This research uses empirical normative research. The results of the research show that: 1) The integration of personal data protection law with the concept of human rights has been running substantially, although the implementation of personal data protection has not been fully as expected. 2) Obstacles in the implementation of personal data protection are influenced by internal factors and external factors. Internal factors include a lack of awareness among Subjects and Controllers of Personal Data, complexity in data processing, weak data security systems in Indonesia, the absence of a Draft Implementing Regulation of the Personal Data Protection Law, and the absence of a Special Independent Institution responsible for the protection of personal data. On the other hand, external factors include interception or eavesdropping that results in data protection failures, especially in government agencies and the financial services sector.

Keywords: *Personal Data Protection, Human Rights, Legal Integration, Implementation Obstacles*

1. PENDAHULUAN

Perlindungan data pribadi merupakan salah satu hak asasi manusia (HAM) yang sangat penting dan menjadi bagian integral dari hak perlindungan diri pribadi. Hak ini bertujuan untuk menjamin privasi setiap individu, dengan mengedepankan perlindungan terhadap data pribadi yang dimiliki oleh setiap warga negara. Selain itu, perlindungan data pribadi juga berfungsi untuk meningkatkan kesadaran masyarakat tentang pentingnya melindungi informasi pribadi dan memastikan bahwa hak-hak tersebut diakui serta dihormati dalam berbagai aspek kehidupan, terutama dalam penggunaan teknologi informasi dan komunikasi.

Perlindungan data pribadi menjadi semakin penting dalam era kemajuan teknologi dan informasi yang terus berkembang pesat. Inovasi yang terus muncul dalam bidang teknologi menyebabkan potensi pengumpulan dan pemanfaatan data pribadi semakin besar dan tidak terbatas. Sebagian besar individu kini terhubung ke internet tanpa batas waktu dan tempat, dan media sosial menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari. Media sosial digunakan oleh hampir setiap orang untuk berbagi serta memperoleh informasi, sehingga memudahkan siapa saja untuk mengakses berbagai data pribadi.

Kemudahan dalam menggunakan berbagai layanan online, terutama media sosial, juga semakin berkembang dengan adanya fitur integrasi antar platform. Fitur ini memungkinkan pengguna untuk membuat akun secara otomatis menggunakan informasi yang telah mereka isi di platform media sosial lain. Dengan hanya sekali klik, sebuah akun baru dapat terbentuk dengan mudah, tanpa perlu menginput data pribadi secara manual. Hal ini tentunya

mempermudah pengguna, namun juga membuka potensi penyalahgunaan data pribadi.

Namun, kemudahan tersebut datang dengan berbagai konsekuensi. Sebelum membuat akun di berbagai platform digital, setiap calon pengguna biasanya diminta untuk mengisi berbagai data pribadi mereka, seperti nama, alamat email, nomor telepon, hingga informasi sensitif lainnya. Dengan demikian, pengendali data, yaitu perusahaan atau pihak yang mengelola platform, secara otomatis memperoleh akses terhadap data pribadi pengguna. Potensi kebocoran data pribadi pun meningkat, terutama jika pengendali data tidak menerapkan sistem keamanan yang memadai untuk melindungi data tersebut.

Kasus kebocoran data pribadi sering terjadi dan menunjukkan betapa rentannya informasi yang kita bagikan secara online. Misalnya, pada Mei 2021, hacker dengan nama Kotz berhasil membobol data BPJS dan menjualnya di situs RaidForums. Data yang dibocorkan meliputi nama tertanggung, NPWP, tanggal lahir, dan nomor telepon. Pada September 2022, hacker Bjorka juga membocorkan data pribadi penduduk Indonesia, yang terdiri dari NIK, nomor KK, alamat, nomor telepon, dan informasi lain seperti nomor vaksin. Kasus kebocoran ini menunjukkan betapa pentingnya perlindungan data pribadi dalam konteks kemajuan teknologi.

Selain itu, pada Mei 2023, hacker Lockbit berhasil membobol data nasabah dan karyawan BSI, yang terdiri dari informasi pribadi nasabah, data karyawan, serta data internal BSI. Pada Juli 2023, hacker dengan nama RRR membocorkan data Dukcapil yang berisi informasi pribadi warga negara Indonesia, seperti NIK, nama lengkap, tanggal lahir, golongan darah, status pernikahan, serta nomor akta nikah dan cerai. Kebocoran data ini menimbulkan potensi penyalahgunaan yang merugikan individu yang datanya bocor, serta memperburuk kepercayaan masyarakat terhadap sistem keamanan data pribadi yang ada.

Kasus-kasus kebocoran dan peretasan data yang disebutkan di atas mengindikasikan bahwa sebagai pengendali data pribadi, masih banyak pihak yang lalai dalam melindungi kepentingan pribadi individu. Meskipun banyak platform telah berusaha meningkatkan sistem keamanan data, kenyataannya kebocoran informasi masih dapat terjadi, dan ini mengarah pada potensi penyalahgunaan data yang merugikan individu maupun masyarakat secara luas. Oleh karena itu, diperlukan langkah-langkah yang lebih konkret dalam memastikan perlindungan data pribadi.

Untuk itu, pemerintah Indonesia telah mengambil langkah penting dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini hadir untuk memberikan landasan hukum dalam melindungi data pribadi warga negara Indonesia. Sebagaimana tercantum dalam konsideran undang-undang, perlindungan data pribadi bertujuan untuk menjamin hak warga negara atas perlindungan diri pribadi, sekaligus menumbuhkan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi.

Undang-Undang Nomor 27 Tahun 2022 menegaskan bahwa pengendali data pribadi, yaitu pihak yang mengelola dan memproses data pribadi, memiliki kewajiban untuk menjaga kerahasiaan dan melindungi data pribadi dari akses yang tidak sah. Mereka juga diwajibkan untuk memastikan bahwa data pribadi yang diproses dan disimpan terlindungi dengan sistem keamanan yang memadai, guna menghindari terjadinya kebocoran atau penyalahgunaan data. Hal ini sangat penting untuk mencegah kerugian yang dapat timbul akibat kebocoran data pribadi yang bersifat sensitif.

Secara keseluruhan, undang-undang ini memberikan kerangka hukum yang jelas mengenai kewajiban dan tanggung jawab pengendali data dalam melindungi data pribadi. Pemerintah juga diharapkan dapat mengawasi implementasi peraturan tersebut dengan lebih ketat, serta memberikan sanksi yang tegas bagi pelanggar yang tidak mematuhi ketentuan perlindungan data pribadi. Dengan demikian, diharapkan perlindungan data pribadi dapat lebih efektif, dan masyarakat dapat merasa lebih aman dalam menggunakan layanan digital yang semakin berkembang pesat.

Penelitian ini bertujuan untuk mengkaji dan menganalisis integrasi hukum perlindungan data pribadi dengan konsep hak asasi manusia dan hambatan-hambatan dalam perlindungannya.

2. METODE

Penelitian ini menggunakan penelitian normatif empiris. Pengumpulan data dilakukan dengan wawancara Subjek Data Pribadi dan studi literatur yang berkaitan dengan tema penelitian, berupa peraturan perundang-undangan, buku, dokumen, jurnal, webinar dan situs internet. Data tersebut kemudian dianalisis dengan metode kualitatif.

3. HASIL DAN PEMBAHASAN

3.1. Integrasi Hukum Perlindungan Data Pribadi dengan Konsep Hak Asasi Manusia

Setiap hak asasi manusia mengandung kewajiban untuk menghormati hak asasi orang lain, sehingga dalam hak asasi manusia terdapat kewajiban dasar yang harus dihormati, dilindungi, dan ditegakkan. Oleh karena itu, pemerintah memiliki kewajiban dan tanggung jawab untuk menjamin penghormatan, perlindungan, dan penegakan hak asasi manusia.

Pada Desember 1948 PBB menyelenggarakan Deklarasi Umum Hak Asasi Manusia (DUHAM) yang di dalamnya memuat pokok-pokok tentang hak-hak sipil, politik, ekonomi, sosial, dan budaya yang kemudian dijabarkan dalam dua kovenan, yaitu International Covenant on Civil and Political Rights (ICCPR) dan International Covenant on Economic, Social, and Cultural Rights (ICESCR). Dalam ICCPR, khususnya hak sipil dijelaskan hak-hak menyangkut kebutuhan hidup yang salah satunya meliputi perlindungan atas privasi, kehormatan dan reputasi.

Kebijakan perlindungan data pribadi sebenarnya telah diatur dalam berbagai peraturan perundang-undangan, namun masih tersebar dan belum secara spesifik terintegrasi.

a. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Tabel 1.
Integrasi Hukum Perlindungan Data Pribadi dalam Undang-Undang HAM dengan konsepsi HAM.

Undang-Undang HAM	Konsepsi HAM	Undang-Undang PDP
Pasal 3 Ayat (2) "Setiap orang berhak atas pengakuan, jaminan, perlindungan dan perlakuan hukum yang adil serta mendapat kepastian hukum dan perlakuan yang sama di depan hukum"	Hak untuk diakui dan dijamin perlindungannya, hak untuk mendapatkan kepastian hukum dan diperlakukan secara adil di depan hukum	Pasal 16 Ayat (2) huruf e "pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi…"
Pasal 29 Ayat (1) "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya"	Hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya	Pasal 20 Ayat (2) huruf d "Dasar pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi: pemenuhan pelindungan kepentingan vital Subjek Data Pribadi"
Pasal 30 "Setiap orang berhak atas rasa aman dan tentram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu"	Hak atas rasa aman, hak atas rasa tentram dan perlindungan terhadap ancaman ketakutan	Pasal 35 "Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya…"

Sumber data sekunder 2024

b. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Tabel 2.
Integrasi Hukum Perlindungan Data Pribadi dalam Undang-Undang ITE dengan konsepsi HAM.

Permen Kominfo tentang PSE Lingkup Privat	Konsepsi HAM	Undang-Undang PDP
Pasal 9 Ayat (1) "PSE Lingkup Privat bertanggung jawab atas penyelenggaraan Sistem Elektronik dan pengelolaan Informasi Elektronik dan/atau Dokumen Elektronik di dalam Sistem Elektronik secara andal, aman, dan bertanggung jawab"	Hak atas rasa aman terhadap penyalahgunaan dan kegagalan perlindungan data pribadi, hak atas privasi	Pasal 39 Ayat (2) "Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan sistem keamanan terhadap Data Pribadi yang diproses dan/ atau memproses Data Pribadi sistem elektronik secara andal, aman, dan bertanggung jawab"
Pasal 30 (1) Akses terhadap Sistem Elektronik yang disampaikan oleh PSE Lingkup Privat bersifat terbatas dan rahasia (3) Pemberian akses terhadap Sistem Elektronik harus menjaga dan melindungi: a. integritas, ketersediaan, dan kerahasiaan dari Data Elektronik; b. keandalan dan keamanan Sistem Elektronik; dan c. Data Pribadi yang disimpan, ditransmisikan, atau diproses di dalam Sistem Elektronik	Hak atas privasi, hak atas perlindungan data pribadi secara rahasia dan terbatas, hak atas rasa aman	Pasal 36 "Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi" Pasal 16 Ayat (2) huruf e "Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan prinsip Pelindungan Data Pribadi meliputi: pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan Data Pribadi"

Sumber data sekunder 2024

Dalam hal pemrosesan data, Pengendali Data Pribadi wajib memiliki dasar pemrosesan. Dasar pemrosesan yang dimaksud adalah sah secara hukum dan memenuhi kriteria sebagai berikut, yakni:

1) Pemrosesan data pribadi berdasarkan persetujuan yang sah secara eksplisit. Bahwa Pengendali Data Pribadi wajib menyampaikan informasi dan wajib menyediakan mekanisme perolehan persetujuan terkait setiap pemrosesan data pribadi;
2) Pemenuhan kewajiban perjanjian dapat dilakukan jika Subjek Data Pribadi dan Pengendali Data Pribadi menyepakati akan menandatangani suatu perjanjian dan harus berhenti saat tujuan perjanjian terpenuhi;
3) Pemenuhan kewajiban hukum dilakukan dalam hal diwajibkan oleh ketentuan perundang-undangan, perintah dan/atau putusan pengadilan, dan perintah berdasarkan keputusan Pejabat Tata Usaha Negara;
4) Pemenuhan perlindungan kepentingan vital dilakukan dalam hal: (1) terdapat ancaman terhadap hidup, fisik dan/atau properti/aset Subjek Data Pribadi atau pihak ketiga lainnya; (2) sulit mendapatkan persetujuan Subjek Data Pribadi; dan (3) potensi penolakan pemrosesan yang rendah oleh Subjek Data Pribadi;
5) Pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik atau pelaksanaan kewenangan dilakukan dalam hal: (1) melaksanakan ketentuan peraturan perundang-undangan untuk melakukan tindakan dalam rangka kepentingan umum dan/atau pelayanan publik; dan (2) terdapat kepentingan publik yang secara langsung terancam jika pemrosesan data pribadi tidak dilakukan;
6) Pemenuhan kepentingan yang sah lainnya dapat digunakan dalam hal: (1) telah melakukan analisis terhadap keperluan, tujuan dan keseimbangan hak Subjek Data Pribadi dan kepentingan Pengendali Data Pribadi; dan (2) telah melakukan penilaian bahwa pemrosesan tidak berdampak secara hukum atau merugikan Subjek Data Pribadi.

3.2. Hambatan Penerapan Perlindungan Data Pribadi

a. Faktor Internal

1. Kurangnya Kesadaran Hukum Subjek Data Pribadi dan Pengendali Data Pribadi

Dalam tujuan hukum pidana di Indonesia, tujuan hukum Danny Kobrata dalam webinarnya mengungkapkan hambatan dan tantangan yang dihadapi terkait perlindungan data pribadi

"Karena Undang-Undang Pelindungan Data Pribadi masih baru, banyak orang yang belum memahami

> pentingnya melindungi data pribadi. Sosialisasi belum merata, sehingga banyak perusahaan yang belum tahu cara melindungi data pribadi, sehingga data pribadi rentan bocor. Meskipun perusahaan sudah menyadari pentingnya perlindungan data pribadi, kesadaran tersebut biasanya hanya ada di level manajemen dan belum mencapai level pekerja operasional yang berurusan langsung dengan data pribadi setiap hari".

Berdasarkan pernyataan tersebut, terdapat kesenjangan tingkat kesadaran pentingnya perlindungan data pribadi antara Pengendali Data Pribadi dan Subjek Data Pribadi. Untuk itu, pentingnya membangun kesadaran perlindungan data pribadi oleh perusahaan sebagai Pengendali Data Pribadi adalah dengan merutinkan pelatihan maupun sosialisasi terkait pentingnya perlindungan data pribadi kepada pekerja-pekerja operasional sebagai Subjek Data Pribadi.

Namun, menurut penulis, Pengendali Data Pribadi masih belum sepenuhnya menyadari pentingnya perlindungan data pribadi. Sebagai contoh, Universitas Bosowa sebagai Pengendali Data Pribadi tidak memberikan himbauan untuk memperbarui password di situs SIAKAD. Username dan password yang diberikan hanya berupa Nomor Induk Mahasiswa (NIM), yang dapat diakses oleh siapa saja hanya dengan mengetahui NIM. Demikian pula, mahasiswa sebagai Subjek Data Pribadi juga kurang memiliki kesadaran untuk mengganti password SIAKAD mereka. Situasi ini menunjukkan rendahnya kesadaran baik dari Pengendali Data Pribadi maupun Subjek Data Pribadi dalam menjaga keamanan data mereka.

2. Kompleksitas Pemrosesan Data Pribadi

Menurut Kurnia Rosyada , dalam pemrosesan data pribadi, tantangan justru dihadapi pada tahap-tahap dalam alur pemrosesan. Dalam memperoleh data, persetujuan Subjek Data Pribadi menjadi penting. Persetujuan memerlukan Standar Operating System (SOP) yang jelas terkait petunjuk dan prosedur persetujuan. Di dalamnya harus ada persetujuan yang bersifat mandatori maupun opsional, seperti persetujuan nasabah (dalam hal ini Subjek Data Pribadi) untuk dihubungi terkait kebutuhan pemasaran melalui saluran tertentu.

Lebih lanjut, Pengendali Data Pribadi wajib memastikan akurasi, konsisten dan kelengkapan data, termasuk memenuhi hak Subjek Data Pribadi untuk melakukan maintenance maupun pengkinian data pribadi.

Asriadi, Subjek Data Pribadi, pernah mengeluhkan terkait data pribadinya di Kelurahan Kapasa Raya yang membuatnya gagal mendaftar beasiswa LPDP Jalur Afirmasi karena tidak terpenuhinya hak sebagai Subjek Data Pribadi dalam hal melengkapi, memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sebagaimana Pasal 6 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

> "Salah satu jalur beasiswa LPDP 2024 adalah Afirmasi. Pada platform pendaftaran, terdapat kolom yang harus terintegrasi dengan Data Terpadu Kesejahteraan Sosial (DTKS), yang dikelola oleh Kelurahan dan diperbarui melalui musyawarah kelurahan bulanan. Namun, karena musyawarah kelurahan terakhir diadakan pada Desember 2023, tidak ada pembaruan data pribadi yang dilakukan."

Hal di atas mengindikasikan, Kelurahan Kapasa Raya belum sepenuhnya melakukan kewajibannya sebagai Pengendali Data Pribadi untuk memperbarui data sebagaimana dimaksud pada Pasal 30 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Lebih lanjut Kurnia Sofia Rosyada menuturkan dalam sektor jasa keuangan sendiri, seperti Bank Mandiri, tantangan yang dihadapi dalam kaitannya dengan perlindungan data pribadi adalah banyaknya kuantitas data pribadi yang diproses. Ada 30 juta lebih jumlah nasabah, 150 ribu lebih jumlah pengguna Kopra, 20 juta lebih jumlah pengguna Livin, 74 ribu lebih jumlah karyawan, 150 lebih aplikasi atau saluran layanan, berbagai produk aset dan liabilities, multi industri perusahaan anak, 100 lebih mitra atau pihak lain yang bekerjasama, 170 lebih ketentuan internal yang terdampak, 18 aplikasi membutuhkan pengembangan.

3. Lemahnya Sistem Keamanan Data Indonesia (Indonesian Data Security System)

Lemahnya sistem keamanan data Indonesia merupakan salah satu penyebab terjadinya banyak kasus penyalahgunaan data pribadi. Kelemahan sistem pengamanan siber Pusat Data Nasional Sementara (PDNS) yaitu belum adanya keseriusan Kemenkominfo dalam mempersiapkan pengamanan siber PDNS. Keinginan untuk mengimplementasikan Satu Data Nasional belum diimbangi dengan pondasi infrastruktur pengamanan yang memadai. Permasalahan tersebut berimbas pada ketidaksiapan Sumber Daya Manusia (SDM) yang berkompeten dalam menghadapi serangan siber.

Kegagalan dalam perlindungan data pribadi yang sering terjadi menunjukkan bahwa sistem keamanan data masih belum dibangun dengan optimal. Ini mencakup kelemahan pada server atau domain yang digunakan untuk penyimpanan data, serta keterbatasan sumber daya manusia yang merancang dan mengoperasikan sistem tersebut.

Belum lagi penyediaan infrastruktur teknologi anti serangan siber pada PDNS dan penyiapan SDM yang profesional untuk mengoperasikan teknologi tersebut membutuhkan dukungan anggaran yang besar. Padahal pada Pasal 39 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 menyebutkan sistem keamanan yang digunakan untuk mencegah data pribadi diakses secara tidak sah, diproses dan atau memprosesnya menggunakan sistem elektronik secara andal, aman dan bertanggung jawab.

4. Belum Disahkannya Rancangan Peraturan Pelaksanaan Undang-Undang Pelindungan Data Pribadi

Belum disahkannya peraturan pelaksana Undang-Undang Pelindungan Data Pribadi, dikhawatirkan dapat menimbulkan interpretasi dan penafsiran liar terhadap undang-undang tersebut. Bahwa apabila terjadi penyalahgunaan data pribadi, maka sewajarnya Subjek Data Pribadi meminta ganti rugi dan atau menggugat Pengendali Data Pribadi yang telah melalaikan kewajibannya dan mengingkari hak Subjek Data Pribadi. Namun, mekanisme maupun pengadilan yang berwenang terkait upaya gugatan terhadap pelanggaran perlindungan data pribadi tidak dirincikan dalam Undang-Undang Pelindungan Data Pribadi, melainkan diatur lebih lanjut dalam peraturan pemerintah. Hal ini menimbulkan kekosongan hukum dan ketidakjelasan terkait mekanisme ganti rugi maupun pengajuan gugatan.

Pembentukan peraturan pemerintah yang tidak kunjung dibentuk memang tidak berpengaruh terhadap keberlakuan suatu undang-undang. Namun, hal tersebut akan mempengaruhi efektivitas pelaksanaan dari suatu undang-undang.

5. Belum Dibentuknya Lembaga Independen Khusus Pelindungan Data Pribadi di Indonesia

Implikasi lain dari belum disahkannya peraturan pelaksana Undang-Undang Pelindungan Data Pribadi

menyebabkan terganggunya efektivitas undang-undang ini. Pasal 58 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengamanatkan pembentukan sebuah lembaga pelindungan data pribadi yang ditetapkan dan bertanggung jawab kepada presiden dalam mewujudkan penyelenggaraan pelindungan data pribadi.

Pelindungan Data Pribadi merumuskan tugas Lembaga Pelidungan Data Pribadi untuk merumuskan dan menetapkan kebijakan dan strategi pelindungan data pribadi yang akan menjadi panduan bagi Subjek Data Pribadi, Pengendali Data Pribadi dan Prosesor Data Pribadi. Tidak hanya itu, lembaga ini berfungsi melakukan pengawasan terhadap penyelenggaraan pelindungan data pribadi, penegakan hukum administratif terhadap pelanggaran Undang-Undang Pelindungan Data Pribadi dan memfasilitasi penyelesaian sengketa di luar pengadilan.

Oleh karenanya, salah satu faktor yang menjadi hambatan dalam perlindungan data pribadi di Indonesia dipengaruhi karena belum adanya Lembaga Independen Khusus Pelindungan Data Pribadi.

b. Faktor Eksternal

1. Intersepsi atau Penyadapan oleh Hacker

Danny Kobrata berpendapat bahwa hambatan yang dihadapi masyarakat beragam sesuai dengan jenis penyalahgunaan data pribadi. Jutaan kejahatan siber ancam industri keuangan selama 2023. BSSN menilai sektor keuangan menjadi industri yang rentan terhadap kejahatan siber. Sebanyak 151,4 juta kasus terkait dengan anomali trafik internet di Indonesia.

Tren anomali trafik internet Indonesia pada tahun 2023 sebanyak 151,4 juta. Anomali tersebut diartikan sebagai ada usaha untuk menyerang sistem. Dalam laporan yang disampaikan oleh BSSN disebutkan ada 3 sektor yang paling banyak mengalami anomali internet, yaitu administrasi pemerintahan, energi dan keuangan.

Dalam menghadapi berbagai ancaman terkini terhadap perlindungan hak atas privasi di internet, Dewan HAM PBB menekankan bahwa praktik pemindaian dan intersepsi komunikasi yang melanggar hukum, serta pengumpulan data pribadi secara sewenang-wenang, merupakan tindakan yang sangat meresahkan. Tindakan tersebut tidak hanya melanggar hak atas privasi dan kebebasan berekspresi, tetapi juga bertentangan dengan prinsip-prinsip fundamental masyarakat demokratis. Yang dimaksud intersepsi atau penyadapan atau peretasan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti elektromagnetis atau radio frekuensi.

Pada Oktober 2020, situs DPR RI (www.dpr.go.id) sempat diretas. Halaman depan situs tersebut diretas dan diubah dari "Dewan Perwakilan Rakyat" menjadi "Dewan Penghianat Rakyat". Peretasan tersebut diduga didasari oleh penolakan pengesahan Undang-Undang Cipta Kerja.

Dalam administrasi pemerintahan, data pribadi pejabat merupakan informasi yang sangat krusial, selain karena terkait dengan privasi individu, data ini juga berpotensi mempengaruhi stabilitas publik dan kepercayaan masyarakat.

Dalam penyelenggaraan negara, sektor keuangan adalah yang paling berisiko dan berdampak terhadap penyalahgunaan data pribadi karena kerugian secara materil dirasakan secara langsung, baik oleh Pengendali Data Pribadi maupun Subjek Data Pribadi. Pemanfaatan teknologi yang sangat besar, risiko yang timbul dari pemanfaatan teknologi pun semakin besar. Berikut adalah beberapa contoh penyalahgunaan data yang berawal dari akses tidak sah atau intersepsi/penyadapan, yang pada akhirnya dapat memicu tindak kriminal lainnya.

Data theft atau pencurian data merupakan jenis penyalahgunaan data yang secara melawan hukum memperoleh data pribadi milik orang lain tanpa persetujuan dari Subjek Data Pribadi.

Unauthorized disclosure of data yakni pengungkapan data melawan hukum atau pengungkapan data tanpa akses atau persetujuan yang sah dari otoritas yang berwenang

Data breach atau kebocoran merupakan situasi dalam ruang siber di mana informasi atau data rahasia yang dimiliki oleh Subjek Data Pribadi diakses dan diungkap kepada publik oleh pihak yang mengancam tanpa sepengetahuan pemilik sistem. Pusat Operasi Keamanan Siber Nasional BSSN mencatat kasus percobaan data breach sepanjang periode Januari hingga Agustus 2020, terdapat 190 juta serangan siber dan 36.771 akun data yang tercuri, termasuk sektor jasa keuangan. Pada survei nasional "Persepsi Masyarakat atas Perlindungan Data Pribadi" oleh Kominfo terhadap 11.305 responden pada Juli 2021, masyarakat menyampaikan kebocoran data yang pernah dialami pada sektor finansial. Berdasarkan survei tersebut, sebanyak 44,1% berkurangnya uang tabungan di rekening bank. Sebanyak 28,1% melakukan transfer atau pembelian karena dihubungi oleh orang atau perusahaan tertentu. Sebanyak 32,2% berkurangnya uang saldo di dompet digital. Dan sebanyak 16,5% kartu kredit atau ATM dibelanjakan oleh orang tak dikenal.

Pada 2023, BSSN kembali melakukan penelusuran dugaan insiden siber dengan jumlah total 347 dugaan insiden siber dengan jumlah jenis dugaan insiden tertinggi adalah data breach. Hasil penelusuran pada darknet, ditemukan adanya 1.674.185 temuan kebocoran data yang berdampak pada 429 stakeholder di Indonesia.

Phising yakni penipuan melalui pesan palsu (email, SMS, telepon) yang seolah-olah dari perusahaan resmi untuk mencuri data pribadi korban. Misalnya, sebuah pesan untuk mengisi data atau mengklik link tertentu dengan tujuan untuk mengumpulkan data pribadi dengan tujuan mentransfer saldo korban ke milik mereka. Phising ini sering ditemui di WhatsApp.

Fajrin B, Subjek Data Pribadi, mengaku pernah mengklik pesan spam berupa link yang mengarahkannya untuk mengisi data pribadi. Seperti yang disebutkan di atas, tujuannya untuk mengumpulkan data pribadi agar dapat mengakses mobile banking maupun e-Wallet korban untuk menguras saldo di dalamnya.

Ransomware merupakan insiden siber yang dipicu oleh malware yang menyerang perangkat, melakukan enkripsi pada data yang ada di dalamnya, dan juga mencuri data dengan tujuan untuk mengintimidasi korban agar membayar sejumlah tebusan guna mendapatkan kembali akses ke data tersebut. Saat ini, taktik ransomware telah berkembang menjadi ekstorsi ganda, yaitu selain melakukan penyanderaan data melalui enkripsi, pelaku juga mengancam untuk mengungkapkan data sensitif jika tebusan tidak diserahkan oleh pemilik sistem

4. KESIMPULAN DAN SARAN

Hasil penelitian dan pembahasan dapat disimpulkan bahwa integrasi hukum perlindungan data pribadi dengan hak asasi manusia telah dilakukan secara substansial melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menyatukan regulasi-regulasi sebelumnya dan mengadopsi standar perlindungan data yang komprehensif, baik untuk data elektronik maupun non-elektronik. Meskipun

demikian, implementasi perlindungan data pribadi masih menghadapi berbagai hambatan, baik dari faktor internal seperti kurangnya kesadaran hukum, kompleksitas pemrosesan data, lemahnya sistem keamanan, serta belum disahkannya peraturan pelaksanaan, maupun faktor eksternal yang berkaitan dengan maraknya penyalahgunaan data, terutama di sektor pemerintahan. Hal ini menunjukkan bahwa meskipun regulasi telah ada, perlindungan data pribadi belum sepenuhnya efektif.

Penting untuk meningkatkan kesadaran masyarakat sebagai Subjek Data Pribadi melalui berbagai program sosialisasi dan pelatihan secara berkala, sehingga mereka lebih memahami pentingnya perlindungan data pribadi. Perusahaan, baik swasta maupun BUMN, perlu membentuk tim respons insiden untuk menangani penyalahgunaan data dan mengembangkan kebijakan internal yang mengatur penanganan insiden perlindungan data pribadi. Pemerintah harus mempercepat pembentukan Lembaga Independen yang memiliki kewenangan untuk memberikan sanksi kepada Pengendali Data Pribadi yang melanggar, serta mempercepat pengesahan Peraturan Pelaksana untuk mengatur aspek teknis perlindungan data pribadi. Selain itu, pemerintah perlu memperkuat sistem keamanan data, khususnya di sektor pemerintahan dan jasa keuangan, guna mencegah kebocoran dan pelanggaran data yang sering terjadi

5. DAFTAR PUSTAKA

Ardipandanto, Aryojati. “Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber.” Pusat Analisis Keparlemenan Badan Keahlian DPR RI, Vol. XVI, No. 13, 2024.

Bachtiar, Naylawati. “Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah”. Lab. Riset Kebijakan Manajemen Publik Universitas Hasanuddin. Departemen Ilmu Administrasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin.

Christine, Bella, and Fakultas Hukum Tarumanegara. “Hambatan Penerapan Perlindungan Data Pribadi di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.” Jurnal Ilmiah Indonesia, Vol. 7, No. 9, 2022.

Direktorat Operasi Keamanan Siber, Lanskap Keamanan Siber Indonesia, 2023.

Djafar, Wahyudi dan Asep Komarudin. Perlindungan Hak Atas Privasi di Internet: Beberapa Penjelasan Kunci. ELSAM. Jakarta. 2024.

Nugroho, Inaz Indra. “Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia.” IPMHI Law Journal, Vol. 1, No. 2, 2021.

Renggong, Ruslan & Dyah Aulia Rachma Ruslan. Hak Asasi Manusia dalam Perspektif Hukum Nasional. Kencana. Jakarta. 2021.

Subiakto, Henri. Guru Besar FISIP Universitas Airlangga. Perlindungan Data Pribadi dan Tantangannya. hal. 5