Journal of Law and Nation (JOLN)
Vol. 3 No. 1 2024 hal. 721-730
e-ISSN: 2962-9675

IMPLEMENTASI ASAS KEHATI-HATIAN DALAM PERLINDUNGAN DATA PRIBADI BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL 5.0

Andri Pranata[1*], Agustinus Arif Juono[2], Binarida[3], Aullia Vivi Yulianigrum[4]
Universitas Muhammadiyah Kalimantan Timur
andriypranata@gmail.com, agustinusadvokat.12@gmail.com, binaridha90@gmail.com, avy598@umkt.ac.id

ABSTRACT

In the digital era, personal data protection has become a crucial aspect to maintain social stability and public trust. This article examines the implementation of the principle of caution in personal data protection in Indonesia based on Law Number 27 of 2022 concerning Personal Data Protection. This research uses a normative method with a conceptual and legislative approach, supported by descriptive-qualitative analysis. The results show that despite the regulations being implemented, there are still several obstacles such as lack of understanding, technological limitations, high costs, shortage of experts, and suboptimal coordination between institutions. To overcome these obstacles, efforts are needed to increase education and socialization, invest in security technology, train experts, and enhance coordination between related institutions. Thus, personal data protection in Indonesia can be more effective in facing the challenges of the digital era.

Keywords: *Principle of caution, Personal Data Protection, Implementation.*

ABSTRAK

Dalam era digital, perlindungan data pribadi menjadi aspek yang sangat penting untuk menjaga stabilitas sosial dan kepercayaan publik. Artikel ini meneliti implementasi asas kehati-hatian dalam perlindungan data pribadi di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini menggunakan metode normatif dengan pendekatan konseptual dan perundang-undangan, yang didukung oleh analisis deskriptif-kualitatif. Hasil penelitian menunjukkan bahwa meskipun regulasi telah diterapkan, masih terdapat beberapa kendala seperti kurangnya pemahaman, keterbatasan teknologi, biaya tinggi, kekurangan tenaga ahli, serta koordinasi antar lembaga yang belum optimal. Untuk mengatasi kendala ini, diperlukan upaya peningkatan edukasi dan sosialisasi, investasi dalam teknologi keamanan, pelatihan tenaga ahli, serta peningkatan koordinasi antar lembaga terkait. Dengan demikian, perlindungan data pribadi di Indonesia dapat lebih efektif dalam menghadapi tantangan era digital.

Kata Kunci: Asas kehati-hatian, Perlindungan Data Pribadi, Implementasi.

PENDAHULUAN

Keamanan data pribadi merupakan aspek penting dalam menjaga stabilitas sosial dan kepercayaan publik. Ketika data pribadi dilindungi dengan baik, masyarakat merasa lebih aman dan terlindungi dari potensi ancaman seperti pencurian identitas, penipuan, dan penyalahgunaan data. Kepercayaan ini sangat penting dalam membangun hubungan yang sehat antara warga negara dan berbagai institusi, termasuk pemerintah dan sektor swasta.

Dalam era digital, banyak transaksi dan interaksi terjadi secara online. Keamanan data pribadi memastikan bahwa informasi sensitif yang dibagikan secara digital tidak jatuh ke tangan yang salah. Hal ini mendukung ekosistem digital yang aman dan terpercaya, memungkinkan masyarakat untuk memanfaatkan teknologi dengan lebih percaya diri. Dengan demikian, inovasi dan pertumbuhan ekonomi digital dapat berkembang tanpa mengorbankan privasi individu.

Penyalahgunaan data pribadi dapat mengakibatkan kerugian yang signifikan bagi individu maupun masyarakat secara keseluruhan. Dengan adanya perlindungan data yang ketat, risiko penyalahgunaan data dapat diminimalkan. Hal ini tidak hanya melindungi individu dari kerugian pribadi, tetapi juga membantu mencegah kejahatan siber yang dapat merusak stabilitas sosial dan ekonomi negara.

Ketika data pribadi dilindungi dengan baik, instansi pemerintah dan penyedia layanan publik dapat meningkatkan kualitas layanan mereka. Data yang akurat dan aman memungkinkan pengambilan keputusan yang lebih baik dan pelayanan yang lebih efisien. Masyarakat pun akan lebih percaya untuk memberikan data mereka ketika merasa yakin bahwa data tersebut akan dikelola dengan aman dan bertanggungjawab.

Keamanan data pribadi juga berperan penting dalam memupuk persatuan dan kesatuan bangsa. Ketika seluruh warga negara merasa bahwa privasi dan data pribadi mereka dihargai dan dilindungi, hal ini akan memperkuat rasa kebersamaan dan kepercayaan di antara mereka. Kepercayaan yang terbangun ini penting dalam menjaga harmoni sosial dan memperkuat solidaritas nasional.Perlindungan data pribadi memberikan perlindungan yang setara bagi semua warga negara tanpa diskriminasi. Ini mendukung prinsip keadilan sosial dengan memastikan bahwa setiap individu mendapatkan hak yang sama dalam perlindungan data mereka.

Dalam Pasal 28G ayat (1) Undang-Undang Dasar Republik Indonesia (UUD RI) 1945 disebutkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. oleh karena itu, perlindungan data pribadi merupakan bagian dari hak atas perlindungan diri pribadi, keluarga, dan harta benda.

Saat ini, urgensi untuk melindungi data pribadi semakin meningkat sejalan dengan meningkatnya penggunaan internet dan teknologi digital dalam berbagai aspek kehidupan sehari-hari. Maraknya kasus penyalahgunaan data pribadi, seperti pencurian identitas, penipuan, dan penyebaran informasi pribadi tanpa izin, telah menimbulkan kekhawatiran di kalangan masyarakat.

Pemerintah menyadari pentingnya perlindungan data pribadi untuk menjaga privasi dan keamanan warganya. Oleh karena itu, berbagai upaya telah dilakukan untuk mengatur dan melindungi data pribadi. Salah satu langkah signifikan yang diambil adalah pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU

PDP bertujuan untuk memberikan kerangka hukum yang jelas mengenai pengumpulan, penyimpanan, pemrosesan, dan pengungkapan data pribadi di Indonesia.

UU PDP mengatur hak-hak individu terkait data pribadi mereka, termasuk hak untuk mengakses data mereka, hak untuk memperbaiki data yang salah, dan hak untuk menghapus data yang tidak lagi diperlukan. Selain itu, undang-undang ini juga menetapkan kewajiban bagi pengendali data untuk menjaga keamanan data pribadi dan melaporkan pelanggaran data kepada otoritas yang berwenang.

Dengan adanya regulasi ini diharapkan Indonesia dapat menghadapi tantangan perlindungan data pribadi dengan lebih baik, serta memberikan perlindungan yang memadai bagi privasi dan keamanan setiap individu di era digital ini. Akan tetapi justru pada bulan juni hingga juli tahun 2024 ini, Indonesia dihebohkan dengan 2 (dua) kasus besar terkait data pribadi, yang pertama kasus Pusat Data Nasional (PDN) mengalami peretasan oleh hacker dengan meminta imbalan sebesar 131 Miliar Rupiah. Hacker yang terafiliasi dengan geng peretas kawakan LockBit berhasil menyerang Pusat Data Nasional Sementara (PDNS) di Surabaya. Hal ini berdampak pada 282 data kementerian/lembaga pemerintah yang tidak dapat diakses dan hal ini diperparah bahwa data-data tersebut 98% tidak memiliki backup data, lalu yang kedua kasus data pelamar kerja yang dipakai untuk pinjaman online (PINJOL) yang dilakukan oleh salah satu karyawan toko ponsel di Pusat Grosir Cililitan (PGC) Jakarta Timur, dengan nilai kerugian sebesar 1 Miliar Rupiah jika diakumulasikan dari 26 orang yang menjadi korban. Sehingga hal inilah yang kemudian menjadi pertanyaan terkait bagaimana penerapan prinsip kehati-hatian oleh pengendali data dalam melindungi data pribadi milik orang yang dikuasainya.

Khusus untuk kasus kebocoran data nasional, menurut Menteri Keuangan Sri Mulyani mengatakan bahwa Kementerian Komunikasi dan Informasi menjadi salah satu lembaga yang memiliki anggaran belanja paling besar di antara kementerian lainnya. Sampai Mei 2024, dia mengatakan Kementerian Kominfo telah membelanjakan hingga Rp 4,9 triliun APBN.[1] Dan khusus ntuk pemeliharaan dan operasional BTS 4G sebanyak Rp 1,6 triliun dan pemeliharaan data center nasional yag mencapai Rp 700 miliar. Artinya anggaran yang diberikan oleh negara untuk pengelolaan data-data nasional tersebut sangat besar, akan tetapi yang menjadi pertanyaan mengapa kebocoran data tersebut dapat terjadi. Oleh karena itu ini pertanyaan besarnya adalah bagaimana implementasi asas kehati-hatian dalam perlindungan data pribadi berdasarkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi dan apa yang menjadi kendala-kendala bagi pemerintah sehingga permasalahan tersebut dapat terjadi.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif, Penelitian hukum normatif adalah penelitian yang dilakukan melalui studi kepustakaan dalam mencari data sumber yang bersifat teori yang berguna untuk memecahkan masalah. Pendekatan ini dikenal dengan nama pendekatan kepustakaan atau yang biasa disebut dengan studi kepustakaan, yakni dengan mempelajari buku-buku, peraturan perundangan-undangan dan dokumentasi lainnya yang berhubungan dengan penelitian ini.[2]

Dalam penelitian ini juga menggunakan pendekatan konsep *(Conceptual approach)*, yang memberikan sudut pandang analisa penyelesaian permasalahan dalam penelitian hukum dilihat dari aspek konsep-konsep hukum yang melatarbelakanginya, atau bahkan dapat dilihat dari nilai-nilai yang terkandung dalam pernormaan sebuah peraturan kaitannya dengan konsep-konsep yang berkaitan dengan pernormaan dalam suatu perundang-perundangan.

Pandangan/doktrin akan memperjelas ide-ide dengan memberikan pengertian-pengertian hukum, konsep hukum, maupun asas hukum yang relevan dengan permasalahan. Penelitian hukum normatif berdasarkan data sekunder.

Pendekatan masalah yang digunakan dalam penelitian ini menggunakan metode pendekatan perundang-undangan (*Statute approach*). Dalam menggunakan pendekatan Perundang-undangan (*Statue approach*). Dalam penelitian ini, peneliti menggunakan metode penyajian dengan analisis deskriptif kualitatif.

HASIL PENELITIAN

Implementasi Asas Kehati-Hatian Dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Asas kehati-hatian dalam konteks perlindungan data pribadi mengacu pada tindakan proaktif dan pencegahan yang diambil oleh pemerintah untuk memastikan bahwa data pribadi dikelola dan dilindungi dengan cara yang aman dan sesuai dengan peraturan perundang-undangan yang ada. Hal ini mencakup berbagai tindakan preventif untuk mencegah pelanggaran data dan meminimalkan risiko penyalahgunaan data pribadi.

Dalam implementasi asas kehati-hatian sebagai Perlindungan Data Pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yaitu pengendali data, baik itu pemerintah, pihak swasta atau siapapun yang melakukan pengelolaan data pribadi seseorang wajib mendapatkan persetujuan yang jelas dan eksplisit dari pemilik data sebelum mengumpulkan data pribadi agar memastikan bahwa pemilik data memahami dan menyetujui penggunaan data mereka.

Mendapatkan persetujuan eksplisit dari pemilik data sebelum mengumpulkan data pribadi adalah langkah krusial dalam melindungi hak dan privasi individu. Persetujuan ini harus didasarkan pada informasi yang jelas dan lengkap, dan diberikan secara sadar oleh pemilik data. Dengan menerapkan praktik terbaik dalam proses persetujuan dan memastikan bahwa prosedur ini dilakukan dengan transparan dan bertanggung jawab, pengendali data

dapat membangun kepercayaan dan memastikan bahwa data pribadi dikelola dengan cara yang aman dan sesuai dengan regulasi dan pengendali data harus menjelaskan dengan jelas tujuan pengumpulan data, cara penggunaan, dan siapa saja yang akan memiliki akses ke data tersebut, hal ini dilakukan sebagai bentuk transparasi yang dilakukan pengendali data terhadap data yang dikumpulkannya.

Pada prinsipnya, data pribadi hanya boleh digunakan untuk tujuan yang telah disetujui oleh pemilik data. Penggunaan data di luar tujuan yang disetujui memerlukan persetujuan tambahan dari pemilik data. Pengendali data harus transparan dalam komunikasi, mendokumentasikan persetujuan, dan memastikan kepatuhan terhadap tujuan yang disetujui. Dengan menerapkan sistem manajemen persetujuan yang baik dan mengedukasi seluruh *stakeholder* dapat menjaga kepercayaan dan mematuhi regulasi perlindungan data pribadi yang berlaku.

Dan hal yang paling penting, Pengendali data harus menerapkan langkah-langkah keamanan yang sesuai, baik secara teknis maupun organisasi, untuk melindungi data pribadi dari akses yang tidak sah, hacking, kehilangan, atau kerusakan. Ini termasuk penggunaan enkripsi, firewall, dan protokol keamanan lainnya. Oleh karena itu, pengendali data wajib melakukan audit secara berkala untuk memastikan bahwa kebijakan dan prosedur keamanan data tetap efektif dan sesuai dengan perkembangan teknologi serta ancaman keamanan terbaru.

Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menetapkan adanya otoritas perlindungan data yang bertugas mengawasi kepatuhan terhadap undang-undang tersebut. Otoritas ini memiliki wewenang untuk melakukan inspeksi, menyelidiki pelanggaran, dan memberikan sanksi jika diperlukan dan apabila ditemukan pelanggaran terhadap ketentuan Undang-Undang, maka pengendali data dapat dikenai sanksi administratif berupa denda, serta sanksi pidana bagi pelanggaran yang lebih serius, seperti penyalahgunaan data pribadi.

Pemerintah dan lembaga terkait harus aktif melakukan edukasi kepada masyarakat tentang pentingnya perlindungan data pribadi dan bagaimana cara melindungi data mereka sendiri. Oleh karena itu, seluruh *stakeholder*, perlu mendapatkan pelatihan yang memadai tentang asas kehati-hatian dan praktik terbaik dalam pengelolaan data pribadi. Sehingga Indonesia perlu mengadopsi standar internasional dalam perlindungan data pribadi untuk memastikan bahwa perlindungan data di Indonesia sejajar dengan praktik terbaik global. Karena dengan adanya kerjasama dengan negara lain dalam berbagi informasi dan teknologi terkait keamanan data dapat membantu meningkatkan perlindungan data pribadi di Indonesia sehingga kejadian peretasan yang yang baru-baru ini tidak terjadi.

Sebenarnya Pemerintah Indonesia telah mengambil berbagai langkah sebagai bentuk kehati-hatian dalam melindungi data pribadi warga negara, terutama setelah beberapa insiden peretasan besar yang terjadi baru-baru ini. Upaya ini dilakukan dengan cara :

1. Melakukan penguatan regulasi dan kebijakan, hal ini dilakukan dengan mengimplementasikan aturan-aturan yang diamanatkan dalam undang-undang tersebut. Ini

termasuk pembuatan peraturan turunan yang lebih rinci untuk memastikan semua aspek perlindungan data tertangani dengan baik.

2. Melakukan peningkatan standar keamanan dengan cara menetapkan standar teknis keamanan yang harus dipatuhi oleh semua pengendali data. Ini mencakup penggunaan enkripsi, firewall, dan protokol keamanan lainnya yang sesuai dengan perkembangan teknologi terbaru.
3. Melakukan penguatan infrastruktur keamanan siber, hal ini dilakukan oleh tim BSSN yang bertugas mengawasi dan mengkoordinasikan upaya perlindungan siber di Indonesia. BSSN juga berperan dalam melakukan audit dan evaluasi terhadap sistem keamanan data yang dimiliki oleh instansi pemerintah maupun sektor swasta.
4. Melakukan peningkatan kapasitas keamanan siber, hal ini dilakukan dengan melakukan investasi dalam pelatihan dan pengembangan sumber daya manusia yang ahli dalam keamanan siber. Ini termasuk pelatihan teknis dan pengetahuan tentang ancaman siber terkini serta cara menanggulanginya.
5. Melakukan penegakan hukum yang ketat, hal ini dilakukan dengan cara membangun kerjasama dengan penegak hukum karena pemerintah dapat bekerjasama dengan kepolisian dan instansi penegak hukum lainnya untuk menyelidiki dan menindak pelanggaran terkait peretasan dan penyalahgunaan data pribadi. Oleh karena itu, penerapan sanksi administratif dan pidana yang tegas terhadap pelaku peretasan dan pelanggaran perlindungan data pribadi untuk memberikan efek jera.
6. Melakukan edukasi dan kesadaran publik dengan kampanye nasional, pemerintah berusaha meningkatkan kesadaran masyarakat tentang pentingnya menjaga keamanan data pribadi. Ini mencakup informasi tentang cara melindungi data dari ancaman digital dan langkah-langkah yang harus diambil jika terjadi pelanggaran data. Selain Pemerintah mengadakan pelatihan reguler bagi pengendali data di sektor publik dan swasta untuk memastikan mereka memahami dan menerapkan praktik terbaik dalam melindungi data pribadi.
7. Melakukan kolaborasi dan kerjasama internasional, hal ini dilakukan dengan menjalin kerjasama dengan negara-negara lain untuk bertukar informasi dan teknologi terkait keamanan siber. Ini termasuk berpartisipasi dalam forum internasional dan mengambil bagian dalam inisiatif global untuk meningkatkan perlindungan data. Sehingga Pemerintah dapat mengadopsi standar internasional dalam perlindungan data pribadi untuk memastikan bahwa regulasi di Indonesia sejalan dengan praktik terbaik global, sehingga memperkuat kerjasama lintas negara dalam menghadapi ancaman siber.

Kendala kendala dalam implementasi asas kehati-hatian dalam perlindungan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Dalam melindungi data pribadi tidak hanya menjadi tugas pemerintah, pihak swasta atau siapapun yang melakukan pengelolaan data pribadi seseorang, tapi merupakan tugas dari pemilik data itu sendiri sehingga seluruh *stakeholder* memiliki peran dalam melakukan atau menerapkan prinsip kehati-hatian dalam melindungi data pribadi yang dimiliki.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur bahwa perlindungan data pribadi seseorang dilaksanakan melalui beberapa asas, salah satunya yaitu asas kehati-hatian, asas kehati-hatian ini menjelaskan bahwa para pihak yang terkait dengan pemrosesan dan pengawasan data pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian. Asas ini menuntut adanya perhatian khusus terhadap berbagai aspek yang bisa menimbulkan risiko atau kerugian, baik secara langsung maupun tidak langsung. Oleh karena itu para pihak harus mengidentifikasi berbagai jenis risiko yang mungkin muncul dalam pemrosesan data pribadi. Ini termasuk risiko kebocoran data, akses yang tidak sah, pencurian data, dan berbagai ancaman lainnya terhadap integritas dan kerahasiaan data pribadi. Setelah mengidentifikasi risiko, langkah selanjutnya adalah mengambil tindakan pencegahan yang tepat untuk meminimalkan atau menghilangkan risiko tersebut. hal ini dapat dilakukan dengan menerapkan teknologi keamanan seperti enkripsi dan firewall serta penggunaan sistem autentikasi yang kuat.

Seluruh stakeholder harus memastikan bahwa semua tindakan mereka sesuai dengan Undang-Undang dan peraturan yang berlaku, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Ini mencakup kepatuhan terhadap prosedur pengumpulan, penyimpanan, pengolahan, dan penghapusan data pribadi. Oleh karena itu seluruh stakeholder dapat melakukan pengawasan dan audit secara berkala terhadap proses pemrosesan data untuk memastikan bahwa semua langkah yang diambil berjalan sesuai rencana dan tidak ada pelanggaran yang terjadi. Ini juga membantu dalam mengidentifikasi area yang memerlukan perbaikan. Dengan menerapkan asas kehati-hatian ini, diharapkan bahwa semua pihak yang terlibat dalam pemrosesan dan pengawasan data pribadi dapat mencegah potensi kerugian yang mungkin ditimbulkan terhadap individu, sehingga melindungi hak-hak privasi mereka secara efektif.

Meskipun dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur terkait asas kehati-hatian dalam perlindungan data pribadi, akan tetapi dalam implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi masih terdapat beberapa kendala-kendala, seperti :

1. Kurangnya Pemahaman organisasi dan individu terkait pentingnya perlindungan data pribadi dan implikasi hukum dari pelanggaran dan penyalahgunaan data pribadi, hal ini dapat terjadi karena kurangnya sosialisasi dan edukasi dari pemerintah dan lembaga terkait mengenai detail Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan implementasinya.
2. Keterbatasan teknologi menjadi salah satu kendala dalam upaya memberikan perlindungan yang optimal, masih terdapat beberapa instansi, institusi, organisasi, yang tidak memiliki infrastruktur teknologi yang memadai untuk melindungi data pribadi sesuai dengan

standar. Hal ini disebabkan salah satunya karena teknologi keamanan data canggih sering kali memerlukan investasi besar yang mungkin tidak terjangkau.

3. Biaya tinggi selalu menjadi alasan utama dalam implementasi kebijakan program jika tidak terlaksana, termasuk dalam upaya perlindungan data pribadi ini, karena upaya ini pasti membutuhkan biaya besar untuk teknologi, pelatihan, dan penyesuaian proses. Hal ini karena keterbatasan anggaran yang dimiliki oleh instansi, institusi, organisasi atau lembaga.
4. Kekurangan tenaga ahli yang memahami secara mendalam tentang keamanan data dan perlindungannya. Masih banyak instansi, institusi, atau organisasi, yang belum memiliki staf khusus untuk mengelola perlindungan data pribadi.
5. Penegakan hukum yang belum sepenuhnya matang atau konsisten dan ditambah dengan sulitnya mengidentifikasi pelanggaran menjadi tantangan tersendiri dalam mengidentifikasi dan menindak pelanggaran perlindungan data pribadi.
6. Perlindungan data pribadi sering melibatkan berbagai lembaga, dan kurangnya koordinasi antar lembaga dapat menghambat pelaksanaan kebijakan yang efektif. Hal ini karena masih tingginya ego sektoral dari setiap instansi, institusi, organisasi atau lembaga terkait. Selain itu, Ketidakjelasan mengenai tanggung jawab dan peran masing-masing instansi, institusi, organisasi atau lembaga. Sehingga ketika terjadi masalah seperti kasus peretasan yang baru baru terjadi maka instansi, institusi, organisasi, atau lembaga tersebut akan saling melempar tanggungjawab.

Simpulan

Implementasi asas kehati-hatian dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia bertujuan untuk memastikan bahwa data pribadi warga negara dilindungi dengan baik. Dengan menerapkan langkah-langkah preventif yang komprehensif, mulai dari pengumpulan hingga penghapusan data, serta pengawasan dan penegakan hukum yang ketat, Indonesia dapat menciptakan lingkungan digital yang aman dan terpercaya bagi seluruh masyarakat. Edukasi publik dan kerjasama internasional juga merupakan kunci penting dalam menghadapi tantangan perlindungan data pribadi di era digital ini.

Meskipun Pemerintah Indonesia telah mengambil berbagai langkah preventif dan reaktif untuk sebagai upaya untuk melindungi data pribadi warga negara tetap saja terdapat beberapa kendala-kendala dalam implementasi asas kehati-hatian, hal ini terjadi seperti kurangnya pemahaman karena minimnya sosialisasi, edukasi dan pelatihan, selain itu, keterbatasan teknologi, sumber daya masnusia yang mengoperasikan teknologi tersebut dan biaya investasi dalam operasi teknologi tersebut juga menjadi kendala tersendiri, ditambah dengan masih tingginya ego sektoral antar instansi, institusi, organisasi atau lembaga yang menjadi pemicu akan terjadinya lempar-lemparan tanggungjawab ketika terjadi permasalahan.

Saran

Untuk meningkatkan implementasi perlindungan data pribadi di Indonesia, berikut beberapa saran yang dapat dipertimbangkan:

1. Peningkatan Edukasi dan Sosialisasi;
   Pemerintah perlu meningkatkan sosialisasi dan edukasi terkait UU PDP kepada masyarakat dan semua pihak yang terlibat dalam pengelolaan data pribadi. Ini termasuk pelatihan reguler bagi pengendali data di sektor publik dan swasta.
2. Penguatan Infrastruktur Teknologi;
   Diperlukan investasi dalam teknologi keamanan data yang canggih dan infrastruktur yang memadai untuk memastikan perlindungan data pribadi yang optimal.
3. Penegakan Hukum yang Kuat;
   Penegakan hukum yang tegas dan konsisten terhadap pelanggaran perlindungan data pribadi harus dilakukan untuk memberikan efek jera bagi para pelanggar.
4. Kolaborasi Internasional;
   Membangun kerjasama dengan negara lain dalam berbagi informasi dan teknologi terkait keamanan data dapat membantu meningkatkan perlindungan data pribadi di Indonesia.
5. Pelatihan dan Pengembangan SDM;
   Meningkatkan kapasitas sumber daya manusia dalam bidang keamanan siber melalui pelatihan teknis dan pengetahuan tentang ancaman siber terkini.

Dengan mengikuti rekomendasi ini, diharapkan Indonesia dapat lebih baik dalam melindungi data pribadi warganya dan mencegah insiden peretasan serta penyalahgunaan data yang dapat merugikan banyak pihak.

DAFTAR PUSTAKA

Buku-buku :

Fajar, M & Ahmad Y. (2010). Dualisme Penelitian Hukum Normatif dan Empiris. Yogyakarta. Pustaka Pelajar.

Karo-Karo R.P.P. (2020). Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermartabat. Bandung : Nusamedia

Mansur, D. M.A. & Gultom, E. (2009). Cyber Law Aspek Hukum Teknologi Informasi. Bandung Refika Aditama.

Muhammad Fathurrohman dan Sulistyorini, Implementasi Manajemen Peningkatan Mutu Pendidikan Islam Peningkatan Lembaga Pendidikan Islam Secara Holistik, Yogyakarta: Teras, 2012.

Jurnal Ilmiah

Aswandi, R dkk. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). Jurnal Legislatif. Volume 3 Nomor 2. Juni 2020.

Rai Mantili, Putu Eka Trisna Dewi, (2020), Prinsip Kehati-hatian dalam penyelenggaraan system elektronik dalam upaya perlindungan data pribadi di Indonesia. Aktual Justice, Volume 5 Nomor 2. Desember 2020

Rosadi, S.D., (2018), Perlindungan Privasi Data Pribadi dalam Era Ekonomi Digital di Indonesia, VeJ, Volume 4, Nomor 1.

Sautunnida, L, (2018), Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia, Kanun Jurnal Ilmu Hukum, Vol.20 No.2 Agustus 2018

Yuniarti, S, (2019) Perlindungan Hukum Data Pribadi di Indonesia, Jurnal BECOS, Vol.1 No.1 September 2019.

Artikel Internet

Abdulkadir, Muhammad, *Hukum dan Penelitian Hukum,* Bandung: Citra Aditya Bakti, 2004.

M Rosseno Aji Nugroho, CNBC Indonesia, https://www.cnbcindonesia.com/news/20240627192435-4-550013/sri-mulyani-pemeliharaan-pusat-data-nasional-makan-anggaran-rp-700-m

Putri Zaskia Salsabila, (2019), 4Cara Menjaga Keamanan Data Pribadi dari Kejahatan Siber, availablefrom:https://tekno.kompas.com/read/2019/12/11/09430057/4-cara-menjaga-keamanan-data-pribadi-dari-kejahatan-siber?page=all, diakses tanggal 10-11-2020.

Peraturan Perundang-Undangan

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.