Jurnal Hukum dan HAM West Science
Vol. 01, No. 01,November, pp. 21-26

Urgensi perlindungan data pribadi dalam menjamin keamanan data

Denda Ginanjar[1]
[1] STKIP PGRI Sukabumi dan dendaginanjar85@gmail.com

Article Info

Article history:

Received 01 Novemeber 2022
Revised 03 November 2022
Accepted 09 November 2022

Kata Kunci:

Data pribadi,Hak Privasi, Keamanan Data.

Keywords:

Personal data, Privacy Rights, Data Security.

ABSTRAK

Mengingat pelanggaran dan aktivitas ilegal kini telah berkembang di ruang yang dikenal dengan cyber space, dengan menyasar informasi tentang data, kita dihantui oleh kejahatan yang tidak bisa kita lihat secara langsung, perlindungan negara saat ini tidak hanya dilakukan secara fisik melalui aktivitas yang terjadi di lapangan. , tetapi harus lebih ditingkatkan. Pelanggaran keamanan data pribadi sekarang berada dalam tahap pengembangan yang sangat awal. Memberikan perlindungan hukum atas data pribadi menjadi isu utama. Informasi dikumpulkan dengan mempelajari atau meninjau karya sastra, dan dilakukan analisis kualitatif.

Menurut temuan penelitian, perlindungan data pribadi yang ada di Indonesia dipandang kurang efektif, dan negara saat ini tidak cukup kuat untuk mengamankan data pribadi. Padahal, hingga saat ini, belum ada undang-undang khusus yang mengatur tentang perlindungan data pribadi. Berdasarkan hal ini, penulis ingin menekankan pentingnya peraturan perlindungan data yang unik.

ABSTRACT

Given that violations and illegal activities have now grown in a space known as cyberspace, by targeting information about data, we are haunted by crimes that we cannot see directly, the protection of the state is currently not only done physically through activities that occur in the field. , but should be further improved. Personal data security breaches are now in a very early stage of development. Providing legal protection for personal data is a major issue. Information is collected by studying or reviewing literary works, and qualitative analysis is carried out. According to research findings, the existing protection of personal data in Indonesia is seen as less effective, and the current state is not strong enough to secure personal data. In fact, until now, there is no specific law that regulates the protection of personal data. Based on this, the authors would like to emphasize the importance of unique data protection regulations.

Corresponding Author:

Name: Denda Ginanjar
Institution: STKIP PGRI Sukabumi
Email: dendaginanjar85@gmail.com

1. PENDAHULUAN

Telah terjadi kemajuan yang signifikan di era globalisasi, khususnya di bidang komunikasi dan teknologi. Beberapa sektor masyarakat mulai terkena dampak teknologi, termasuk bidang pemerintahan (Astawa & Dewi, 2018). Pesatnya kemajuan teknologi dan informasi telah membawa dampak besar pada setiap aspek kehidupan. Melalui berbagai instrumen teknis yang muncul saat ini, teknologi mendorong semua aktivitas manusia yang dulunya analog ke digital. Tidak dapat dipungkiri bahwa pertumbuhan teknologi dan informasi telah berperan sebagai penopang utama kemajuan globalisasi. Mayoritas aktivitas masyarakat di era globalisasi saat ini dilakukan melalui platform digital. Namun perlu ditegaskan, bahwa untuk mencapai tujuan negara Indonesia sebagaimana digariskan dalam konstitusi, kemajuan teknologi dan informasi di bidang ekonomi harus dilakukan untuk kepentingan rakyat banyak. Selain itu, dimulainya perkembangan periode revolusi industri 4.0 dapat dilihat dengan datangnya era revolusi industri keempat yang menuntut dibangunnya sistem siber-fisik untuk mengoptimalkan digitalisasi (Fahmi, 2019).

Sistem elektronik yang mengontrol integrasi data pribadi dengan teknologi informasi, media, dan telekomunikasi bertujuan untuk data itu sendiri (Makarim, 2010) Undang - Undang Perlindungan Data Pribadi (UU PDP) yang telah berjalan sejak tahun 2019, adalah akhirnya diratifikasi pada 2019, sama seperti ada lebih banyak contoh data pribadi orang yang disusupi. Seperti yang dia katakan dalam pemikirannya, undang-undang ini bertujuan untuk membela hak privasi warga negara, meningkatkan pemahaman publik tentang perlunya menjaga informasi pribadi, dan memastikan hak-hak itu diakui dan ditegakkan. Undang-undang ini diharapkan dapat berfungsi sebagai kerangka hukum yang kuat untuk administrasi dan perlindungan data pribadi orang dan pegawai negeri. Salah satu hak asasi manusia yang terkait dengan perlindungan pribadi adalah perlindungan informasi pribadi. Pasal 28G UUD 1945 mengatur hak atas perlindungan pribadi ini. Dalam arti banyak negara mengakuinya, keamanan atau privasi pribadi ini bersifat universal. Mengenai informasi pribadi, sejak Tuhan menciptakan manusia, mereka memiliki informasi tentang diri mereka sendiri, khususnya informasi Biometrik (Kindt, 2013).

Pengertian data pribadi menurut Pasal 1 Ayat 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi adalah: Data pribadi tertentu yang disimpan, dipelihara, dan dijaga kebenaran dan kerahasiaannya. Pasal 3 Undang - Undang Nomor 43 Tahun 2009 Tentang Kearsipan menyebutkan bahwa untuk menjaga perlindungan dan keamanan data, maka arsip harus tertata rapi. Definisi lain dari data pribadi disediakan dalam Undang - Undang Perlindungan Data Inggris tahun 1998, yang menyatakan bahwa itu adalah informasi apa pun yang berhubungan dengan individu hidup yang dapat dikenali dari informasi atau dari informasi lain yang dimiliki atau akan dimiliki oleh pengontrol data. Informasi pribadi juga dapat dikaitkan dengan karakteristik responden, seperti jenis kelamin, usia, nama, dan lain-lain.

Badan Siber dan Sandi Nasional (BSSN) melaporkan bahwa lebih dari 700 juta serangan siber terjadi di Indonesia pada tahun 2022, sehingga menimbulkan sejumlah masalah terkait perlindungan data pribadi. Ransomware, atau perangkat lunak dengan mode permintaan tebusan, adalah jenis serangan siber yang paling umum. Menurut data BSSN, ada 714.170.967 anomali lalu lintas atau serangan siber sepanjang tahun 2022, dengan bulan Januari mengalami serangan terbanyak dengan 272.962.734 lebih dari sepertiga dari semua serangan selama paruh pertama tahun ini. Serangan Ransomware, juga dikenal sebagai serangan malware yang menuntut tebusan dari pemilik data, adalah jenis serangan siber paling umum yang sering ditemukan BSSN. Web defacement pernah digunakan dalam serangan siber di BSSN itu sendiri pada satu titik, tepatnya pada Oktober 2021. Seorang hacker menggunakan moniker "theMx0nday" sebagai aliasnya menyerang situs BSSN saat itu.

Indonesia menduduki puncak daftar negara ASEAN untuk serangan malware, menurut data ASEAN Cyberthreat 2021 Interpol. Peringkat pertama dengan 1,3 juta kasus adalah Indonesia. Jumlah ini mewakili kira-kira setengah dari keseluruhan ancaman ransomware yang dihadapi oleh negara-negara ASEAN. Di posisi kedua dengan 886.874 kasus adalah Vietnam. Dengan 257 kasus, Brunei menjadi negara dengan jumlah terendah. Menurut analisis terbaru oleh National Cyber Security Index (NCSI), keamanan siber Indonesia berada di peringkat ke-83 secara global dan keenam di antara negara-negara anggota ASEAN.

Oleh karena itu, di era modern ini, perlindungan data pribadi ditandai dengan standar pengoperasian penyelenggara sistem elektronik, di mana sistem elektronik harus dapat diandalkan, aman, dan akuntabel untuk pengoperasian sistem elektronik dengan baik, mengacu pada Pasal 15 Undang - Undang Nomor 11 Tahun 2008 diubah menjadi Undang – Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Hal ini menunjukkan bahwa administrator sistem elektronik dilindungi dari pencurian data dan serangan kriminal. Selain itu, perlindungan informasi pribadi ini sangat penting karena menurut Pasal 2 Undang - Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yang menyebutkan wilayah sebagai wilayah Indonesia dan darah manusia sebagai darah yang bersangkutan, negara wajib melindungi seluruh wilayah dan pertumpahan darahnya. Oleh karena itu, pemerintah harus menjaga informasi pribadi warganya (Indonesia, 2006) Karena masalah ini, penulis termotivasi dan merasa terdorong untuk membahas nilai perlindungan data secara lebih rinci serta berfungsi sebagai pengingat bahwa kejahatan baru telah terjadi. terjadi dan harus segera ditangani.

2. METODE PENELITIAN

Penulis penelitian ini menggunakan metodologi penelitian normatif, meninjau prinsip dan aplikasi setiap artikel sambil memasukkan literatur dari buku, jurnal, makalah, media cetak, dan sumber berita internet yang berkaitan dengan perlindungan data. Data target yang dikumpulkan terkait dengan kasus kejahatan dunia maya, perlindungan data, makna, dan undang-undang terkait. Pendekatan hukum, pendekatan kasus, dan metode komparatif semuanya digunakan.

3. HASIL DAN PEMBAHASAN

1. Perlindungan Data Pribadi

Hak atas privasi, menurut (Westin, 1967), adalah hak orang, kelompok, atau institusi untuk memutuskan sendiri bagaimana dan kapan informasi tentang mereka dibagikan kepada orang lain. Biasanya ada beberapa pengaturan privasi di suatu negara, baik jenis maupun tingkatannya, karena definisi privasi yang luas. Ide ini sebanding dengan yang dikemukakan oleh (Miller, 1971), yang berfokus pada ide privasi dan kekuatan orang untuk menentukan bagaimana informasi pribadi mereka dibagikan. Selain itu, (Innes, 1998) mendefinisikan privasi sebagai keadaan memiliki kendali atas keputusan sendiri, termasuk pilihan mengenai akses seseorang, penggunaan, dan perilaku dalam kaitannya dengan informasi pribadi dan tindakan. Sementara digambarkan sebagai hasil dari cinta, kesukaan, dan kepedulian terhadap orang lain, privasi itu sendiri. Hal ini sesuai dengan argumen (Solove, 2008) bahwa konteks privasi terdiri dari keluarga, tubuh, tipe orang, komunikasi, dan komunikasi rumah. Sebaliknya, (Gavison, 1980) melihat privasi sebagai "kompleks faktor dependen," khususnya: "kerahasiaan, anonimitas, dan kesendirian." Masing-masing komponen ini berbeda dari yang lain karena salah satu dari mereka dapat menghasilkan kerugian atau pelanggaran.

Menurut berbagai definisi "privasi" yang telah dikemukakan, ada sejumlah polarisasi, yang secara mendasar mendefinisikan privasi sebagai klaim, hak, atau hak individu untuk memilih semua informasi tentang dirinya (dirinya sendiri) yang dapat dikomunikasikan. Kerahasiaan informasi pribadi seseorang, seperti informasi tentang diri mereka sendiri, (ii) kerahasiaan identifikasi mereka, atau (iii) pihak yang memiliki akses sensorik ke orang tersebut, juga telah

disorot sebagai faktor kontrol (Schoeman, 1984) . Data pribadi berisi informasi tentang individu yang bersifat pribadi, sensitif, atau rahasia yang ingin dirahasiakan oleh subjek atau ingin mencegah orang lain memperoleh, memanfaatkan, atau mengungkapkannya kepada pihak lain (Sautunnida, 2018).

Orang pertama yang mengartikulasikan ide privasi adalah Warren dan Brandheis, yang menerbitkan sebuah artikel berjudul "Hak atas Privasi" di majalah akademik Harvard University Law School. Menurut Warren dan Brandheis, dengan munculnya dan pertumbuhan perkembangan teknologi, kesadaran bahwa orang memiliki hak untuk menikmati hidup atau bahasa lain, serta hak untuk tidak privasi mereka dilanggar oleh pemerintah atau orang lain, terjadi. Mengingat hal ini, hak atas privasi harus diakui dan dilindungi oleh undang-undang. Karena setiap orang memiliki batasan yang berbeda, mungkin sulit untuk mendefinisikan konsep privasi (Dewi, 2009). Kebebasan mendasar dan hak demokratis adalah hak atas privasi (Solove, 2008). Kebutuhan untuk mengakui bahwa orang, kelompok, atau institusi memiliki hak untuk membuat keputusan independen mengenai pelepasan informasi mereka adalah bagaimana Westin mencirikan hak atas privasi (Westin, 1967). Ketika orang lain memperoleh informasi pribadi seseorang, memperhatikan mereka, atau memperoleh akses ke mereka, hak privasi mereka telah dilanggar. Ingatlah bahwa hak atas privasi harus dihormati setiap saat dan tidak diberikan. Menurut (Wiranata, 2021) Sesuai dengan hukum dan masyarakat demokratis, otoritas publik dapat memberlakukan pembatasan hak atas privasi. Menurut (Halstead, 2014), ada enam keadaan di mana pelaksanaan hak-hak ini harus dibatasi, terutama yang menyangkut perlindungan hak atau kebebasan lainnya, keamanan nasional, keamanan publik, kesejahteraan ekonomi suatu bangsa, dan pencegahan kejahatan. Hak privasi seseorang dibatasi jika salah satu dari enam keadaan ini ada.

Selain itu, penting untuk mempertimbangkan Kitab Undang - Undang Hukum Perdata (Burgerlijk Wetboek) dan Undang - Undang Informasi dan Transaksi Elektronik (UU ITE) ketika menentukan apakah suatu pelanggaran hukum terjadi secara Online atau tidak. Karena sampai saat ini peraturan perundang-undangan di Indonesia belum sepenuhnya mengatur aturan yang mewajibkan ganti rugi akibat perbuatan yang melanggar hukum dalam transaksi elektronik. Terlepas dari apakah suatu argumen ada atau aturan telah dikembangkan sepenuhnya, hakim tidak diizinkan untuk menolak masalah perdata apa pun yang diajukan ke hadapan mereka. Oleh karena itu, Burgelijk Wetboek dapat digunakan sebagai kerangka hukum dalam Pasal 1365 untuk memutuskan tuntutan ganti rugi dalam suatu sengketa hukum dalam setiap transaksi tersebut. Alat bukti yang digunakan untuk menunjukkan pelanggaran tersebut harus berasal dari data atau sumber elektronik yang dapat dicatat secara sah sebagai alat bukti. Menurut Pasal 5 ayat 1 UU ITE Indonesia, hal ini dilarang, dan mengacu pada informasi dan/atau data elektronik selain cetakan elektronik (Slamet, 2013).

Jenis Perundangan	Nomor	Tahun	Tentang
Undang-Undang	11	2008	Informasi dan Transaksi Elektronik
Undang-Undang	19	2016	Perubahan atas Undang-Undang Tahun 2008 Informasi dan Transaksi Elektronik
Peraturan Menteri Komunikasi dan Informatika	20	2016	Perlindungan Data Pribadi Dalam Sistem Elektronik.
Peraturan Pemerintah	71	2019	Penyelenggaraan Sistem dan Transaksi Elektronik
Peraturan Pemerintah	80	2019	Perdagangan Melalui Sistem Elektronik

Gambar 1 Jenis Perundangan Mengatur Informasi Elektronik

2. Pentingnya Undang-Undang Khusus Terhadap Perlindungan Data

Mengapa penerapan Undang - Undang Perlindungan Data Pribadi begitu penting? Pertama, sekarang ini disyaratkan oleh UUD 1945, yang menyatakan bahwa "Setiap orang berhak atas perlindungan diri, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari bahaya ketakutan untuk melakukan atau tidak melakukan sesuatu." Setiap orang berhak untuk mencari perlindungan politik di luar negeri dan kebebasan dari penyiksaan atau perlakuan kejam lainnya yang melanggar martabat manusia.

menggabungkan pertahanan ini ke dalam hak asasi manusia yang mendasar. Hal ini dilakukan untuk mencapai kehidupan yang berkualitas (the right of a quality life), yang didefinisikan dalam Pasal 28A dan 28I sebagai hak yang tidak dapat dikecualikan atau dibatasi dengan alasan apapun (non derogable). Kehidupan yang berkualitas jauh melampaui hak untuk hidup sendiri. Komponen data privasi, atau hak satu orang atau lebih untuk melindungi sesuatu yang bersifat pribadi atau rahasia, adalah data pribadi. Perlindungan privasi mengacu pada hak untuk dibiarkan sendiri, untuk memiliki akses ke informasi pribadi hanya dengan otorisasi, dan memiliki beberapa tingkat kontrol atas informasi tersebut (Yuwinanto, 2015). Perlindungan data pribadi, di sisi lain, menunjukkan adanya pembatasan yang harus diikuti, hak atau kewajiban untuk mengelola informasi yang diberikan atau diterima, dan hak atau kepentingan yang tidak dapat diintervensi di luar konteks penyebarannya. Secara khusus, bagaimana undang-undang dapat melindungi dan mengontrol aliran pengumpulan data pribadi - pribadi, termasuk cara mengumpulkan, mencatat, menyimpan, dan menyebarkan data.

Oleh karena itu, kebutuhan akan peraturan khusus tentang perlindungan data sangat penting karena diperkirakan akan berisi alat yang nantinya akan menghukum mereka yang mencuri data, serta menjatuhkan hukuman kepada mereka yang mengoperasikan sistem elektronik dan menetapkan kriteria minimum untuk dipatuhi semua orang. Menurut Kominfo, organisasi dan badan pemerintah yang menggunakan sistem manajemen keamanan ISO untuk sistem elektronik harus mematuhi persyaratan ISO 27001. Worldwide Organization for Standardization, atau ISO, adalah organisasi non-pemerintah yang mempromosikan standardisasi internasional. Selain itu, Kominfo berharap agar operator sistem elektronik menggunakan sistem untuk dokumentasi dan administrasi yang memenuhi persyaratan ini (Prasetya et al., 2015).

4. KESIMPULAN

Dua implikasi kunci dapat diambil dari diskusi di atas. Pertama, ada persepsi bahwa pendekatan yang ada di Indonesia untuk melindungi data pribadi kurang berhasil, yang tidak diragukan lagi ditegaskan dengan tidak adanya peraturan di bidang ini. Kini, hanya Pasal 26 Undang - Undang Nomor 11 Tahun 2008, sebagaimana telah diubah dengan Undang - Undang Nomor 19 Tahun 2016, tentang Informasi dan Transaksi Elektronik, yang mengatur penggunaan data pribadi di Indonesia. Dampak hukum dari pelanggaran data pribadi setidaknya dijelaskan dalam artikel ini. Selain itu dijelaskan pula tata cara hukum yang dapat digunakan, termasuk mengajukan gugatan ganti rugi, namun tidak jelas apakah batas tersebut benar-benar merupakan kerugian sebagaimana dimaksud dalam Pasal 26 ini. Bahkan harus memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna.

Kedua, meskipun potensi data pribadi sangat besar, Indonesia masih belum cukup kuat untuk mengamankannya. Padahal, hingga saat ini belum ada undang-undang khusus yang mengatur tentang perlindungan data pribadi. Penulis tentu berharap hal ini dapat segera terwujud dan dapat diimplementasikan dengan benar karena dari kasus-kasus yang telah diuraikan, kita dapat melihat dampak signifikan yang akan terjadi jika data kita dicuri atau bocor ke publik. RUU

Perlindungan Data Pribadi saat ini masuk dalam Program Legislasi Nasional dan kabarnya akan segera disahkan.

DAFTAR PUSTAKA

Astawa, I. P. M., & Dewi, K. C. (2018). e-Government facilities analysis for public services in higher education. *Journal of Physics: Conference Series*, *953*(1), 012061.

Dewi, S. (2009). Cyberlaw Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional. *Bandung: Widya Padjajaran*.

Fahmi, M. M. (2019). Inspirasi QurAni Dalam Pengembangan Fintech Syariah: Membaca Peluang, Tantangan, Dan Strategi Di Era Revolusi Industri 4.0. *UIN Maulana Malik Ibrahim Malang*.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421–471.

Halstead, P. (2014). *Unlocking human rights*. Routledge.

Innes, J. M. (1998). A qualitative insight into the experiences of postgraduate radiography students: causes of stress and methods of coping. *Radiography*, *4*(2), 89–100.

Kindt, E. J. (2013). An introduction into the use of biometric technology. In *Privacy and Data Protection Issues of Biometric Applications* (pp. 15–85). Springer.

Makarim, E. (2010). *Tanggung jawab hukum penyelenggara sistem elektronik*. Rajajawali Pers.

Miller, A. R. (1971). *Assault on privacy*.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384.

Schoeman, F. D. (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Slamet, S. R. (2013). Tuntutan Ganti Rugi Dalam Perbuatan Melawan Hukum: Suatu Perbandingan Dengan Wanprestasi. *Lex Jurnalica*, *10*(2), 18068.

Solove, D. J. (2008). *Understanding privacy*.

Westin, A. (1967). Privacy and freedom new york atheneum, 1967. *Privacy and Personnel Records, The Civil Liberties Review (Jan./Feb., 1976) S*, 28–34.

Wiranata, A. (2021). Analogi Sistem Perlindungan Hak Atas Data Pribadi Antara Indonesia Dengan Singapura. *Jurnal Ilmiah Mahasiswa Hukum [JIMHUM]*, *1*(3).

Yuwinanto, H. P. (2015). Privasi online dan keamanan data. *Palimpsest*, *31*(11).