Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital

Dwi Nirwana[1], Ely Nurjannah[2], Charoline Renta Anggriani Marpaung[3], Hansein Arif Wijaya[4]
[1,2,3,4]Universitas Jambi, Indonesia
E-mail: dwinirwana567@gmail.com, elinurjanah2019@gmail.com, charolineanggriani1903@gmail.com, hanseinwijaya@unja.ac.id

Article Info
Article History
Received: 2024-05-07
Revised: 2024-06-27
Published: 2024-07-07

Keywords:
Implementation;
Privacy;
Data;
Protection.

Abstract
Personal Data is the concept of regulating privacy and personal data in one legal instrument. In Indonesia, this arrangement has not yet converged. The principle of the right to privacy for personal data is important in the digital era to protect and control data ethically. Implementation of personal data protection on social media through Republic of Indonesia Law no. 27 of 2022 and the Indonesia Data Protection System (IDPS) system still requires cooperation and clear regulations. Convergence in personal data protection is important to increase trust and face cyber security challenges in the digital economy era. Protection of personal data on social media is regulated by Republic of Indonesia Law no. 27 of 2022 concerning Personal Data Protection. The Indonesia Data Protection System (IDPS) system helps minimize cyber crime and ensures appropriate management of personal data. IDPS involves the Ministry of Communication and Information (Kominfo) with a focus on central data and data officers. However, implementation still requires cooperation between institutions and clearer regulations.

Artikel Info
Sejarah Artikel
Diterima: 2024-05-07
Direvisi: 2024-06-27
Dipublikasi: 2024-07-07

Kata kunci:
Implementasi;
Privasi;
Data;
Perlindungan.

Abstrak
Data Pribadi adalah konsep pengaturan privasi dan data pribadi dalam satu instrumen hukum. Di Indonesia, pengaturan ini belum konvergen. Prinsip hak privasi terhadap data pribadi penting dalam era digital untuk melindungi dan mengontrol data secara etis. Implementasi perlindungan data pribadi di media sosial melalui Undang-Undang RI No. 27 Tahun 2022 dan sistem Indonesia Data Protection System (IDPS) masih memerlukan kerjasama dan peraturan yang jelas. Konvergensi dalam perlindungan data pribadi penting untuk meningkatkan kepercayaan dan menghadapi tantangan keamanan siber di era ekonomi digital. Perlindungan data pribadi di media sosial diatur oleh Undang-Undang RI No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sistem Indonesia Data Protection System (IDPS) membantu meminimalisasi kejahatan siber dan memastikan pengelolaan data pribadi sesuai. IDPS melibatkan Kementerian Komunikasi dan Informatika (Kominfo) dengan fokus pada central data dan data officer. Namun, implementasi masih memerlukan kerjasama antarlembaga dan peraturan yang lebih jelas.

I. PENDAHULUAN

Dalam era digital, perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam kehidupan manusia. Dalam prosesnya, data pribadi menjadi semakin penting dan sensitif karena banyak aktivitas yang dilakukan secara online. Data pribadi mencakup informasi seperti nama, alamat, nomor identitas, informasi finansial, riwayat kesehatan, dan informasi sensitif lainnya yang berkaitan dengan individu.

Di tengah era digital yang pesat, data pribadi individu semakin rentan terhadap potensi penyalahgunaan dan pelanggaran privasi. Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati. Indonesia, sebagai negara berkembang dengan adopsi teknologi yang pesat, memiliki tanggung jawab untuk melindungi data pribadi sebagai hak privasi. Dalam konteks ini, hak privasi menjadi isu yang mendesak untuk diatasi. Hak privasi adalah hak asasi setiap individu untuk menjaga kerahasiaan dan keamanan data pribadi mereka. Dengan meningkatnya kasus pelanggaran privasi dan penyalahgunaan data pribadi, penting bagi setiap negara untuk memiliki peraturan perundang-undangan yang efektif untuk melindungi hak privasi warganya.

Keamanan siber merupakan sebuah rangkaian aktivitas yang diarahkan untuk melindungi dari ancaman, gangguan, serangan jaringan komputer (perangkat keras dan perangkat lunak), terkait informasi di dalamnya, dan elemen-elemen ruang siber lainnya. Keamanan siber dapat digunakan

sebagai sarana melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen. Dengan demikian, keamanan siber adalah semua mekanisme perlindungan yang digunakan untuk meminimalisir gangguan pada ketersediaan (availability), integritas (integrity), dan kerahasiaan (confidentiality) dari sebuah informasi. Kerahasiaan data merujuk pada akses yang disetujui terhadap sebuah data, yang berarti hanya pihak yang memiliki akses saja yang dapat membukanya. Usaha untuk mendapatkan akses dengan cara mencuri informasi diartikan sebagai tindakan membahayakan kerahasiaan data.

Selanjutnya, dalam upaya perlindungan terhadap data pribadi Menurut Privacy International dalam Prabowo, Wibawa, Azmi (2020) dikenal istilah perlindungan data (data protection). Definisi perlindungan data adalah sebuah aturan hukum yang bertujuan untuk memberikan perlindungan terhadap data pribadi yang dimiliki oleh seseorang. Bagi masyarakat modern, melindungi data dari penyalahgunaan adalah sangat penting. Itu sebabnya diperlukan hukum perlindungan data yang mengatur perusahaan dan pemerintah karena dua entitas ini memiliki peran yang signifikan untuk mencegah adanya penyelewengan oleh oknum yang tidak bisa dipertanggung jawabkan tindakannya. Jika tidak ada aturan hukum, banyak pihak akandimudahkan dalam upayanya melakukan eksploitasi data. Globalisasi berjalan dengan sangat cepat dalam berbagai hal, termasuk pada aspek teknologi informasi yang didalamnya terkait dengan keamanan siber dan kedaulatan data. Perkembangan media sosial yang begitu masif sudah tidak dapat dipisahkan dari perilaku keseharian setiap warga negara. Dalam setiap aplikasi baik media sosial maupun aplikasi lainnya di ruang siber mengandung begitu banyak data yang harusnya terjamin keamanannya. Apabila hal ini disalahgunakan dapat menguntungkan kelompok tertentu dan merugikan sebagian kelompok lainnya.

Di Indonesia, kesadaran akan perlunya perlindungan data pribadi telah semakin meningkat, terutama seiring dengan pertumbuhan penggunaan internet dan aplikasi berbasis teknologi. Hak membela diri merupakan salah satu hak hukum yang digariskan dalam UUD 1945. Menurut Pasal 28G Ayat (1), warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta miliknya. Namun demikian, dengan kemajuan teknologi informasi dan komunikasi, hak pribadi seharusnya tidak hanya dipahami sebagai hak milik sebagaimana diatur dalam pasal tersebut. Hak privasi harus menjadi salah satu yang mendasar. Karena berurusan dengan informasi pribadi atau identitas seseorang, hak privasi lebih sensitif dan dapat dilihat sebagai hak pribadi. Tetapi contoh kebocoran data pribadi baru-baru ini telah menjadi masalah yang parah. Beberapa di antaranya terdiri dari:

1. Kasus Tokopedia (2020): Pada awal 2020, platform e-commerce besar di Indonesia, Tokopedia, dilaporkan mengalami pelanggaran keamanan yang mengakibatkan informasi pribadi dari jutaan pengguna bocor. Data yang dikompromikan meliputi nama, alamat, nomor telepon, alamat email, dan kata sandi terenkripsi.
2. Kasus Bukalapak (2021): Bukalapak, platform e-commerce lainnya di Indonesia, juga dilaporkan mengalami pelanggaran data pada tahun 2021. Lebih dari 13 juta akun pengguna dilaporkan terdampak, dengan data seperti nama pengguna, alamat email, nomor telepon, dan kata sandi bocor.
3. Kasus TokoTalk (2021): Pada tahun 2021, aplikasi pesan instan asal Indonesia, TokoTalk, juga dilaporkan mengalami kebocoran data. Lebih dari 91 juta akunpengguna terdampak, dan informasi yang bocor termasuk nama, nomor telepon, alamat email, dan salinan kartu identitas.

Kebocoran data pribadi adalah masalah serius yang dapat menyebabkan kerugian finansial, identitas palsu, dan bahkan penyalahgunaan data yang lebih lanjut. Pemerintah, perusahaan, dan individu perlu meningkatkan kesadaran tentang keamanan data dan mengambil langkah-langkah pencegahan yang tepat untuk melindungi data pribadi. Penting untuk terus mengikuti berita terkini untuk memahami perkembangan terbaru tentang masalah keamanan data di Indonesia atau di negara manapun.

Meskipun tersebar di berbagai undang-undang, perlindungan perlindungan data pribadi ada di Indonesia. RUU Perlindungan Data Pribadi (RUU PDT) yang dimiliki Indonesia saat ini perlu dikaji lebih detail karena regulasinya masih perlu penyempurnaan. Setidaknya Indonesia bisa disandingkan dengan undang-undang perlindungan data pribadi negara lain, seperti di Hong Kong, Malaysia, Singapura, dan Korea Selatan. Perlindungan hukum atas data pribadi sudah dijamin oleh undangundang khusus di beberapa negara tersebut, namun dalam penelitian ini, kami akan membandingkan undang-undang perlindungan data pribadi Malaysia dengan RUU PDT Indonesia. Rancangan

Undang-Undang (RUU) Perlindungan Data Pribadi memiliki tujuan dan manfaat yang penting dalam konteks perlindungan privasi dan penggunaan data pribadi di Indonesia, dan bertujuan untuk menciptakan lingkungan digital yang lebih aman, terpercaya, dan menghormati privasi individu, sambil tetap memungkinkan pertumbuhan ekonomi dan inovasi di era digital.

II. METODE PENELITIAN

Pada Artikel ini menggunakan Jenis penelitian yang digunakan adalah studi literatur. Metode studi literatur adalah serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat, serta mengelolah bahan penelitian (Zed, 2008:3).

Penelitian ini menggunakan bentuk analisis deskriptif dengan metodologi kualitatif guna menjelaskan sesuatu secara intuitif dan sistematis. Penelitian ini bersifat kualitatif, dimana peneliti kualitatif berusaha mencari arti, pemahaman, definisi tentang suatu fenomena, kejadian melalui keterlibatan langsung maupun tidak langsung dalam obyek yang diteliti. Penelitian kualitatif adalah cara yang memfokuskan untuk mendapatkan makna, definisi, konsep, karakteristik, dan sebagainya termasuk deskripsi mengenai fenomena tertentu yang memiliki sifat alami dan menyeluruh yang disajikan secara narratif. Penelitian kualitatif merupakan mekanisme pencarian dan pengumpulan, termasuk analisis dan interpretasi secara komprehensif untuk menghasilkan pemahaman mengenai permasalahan yang menarik. Penekanan analisis dekskriptif digunakan dalam penelitian ini untuk menganalisis dan memberikan pemahaman.

Jenis data dalam penelitian ini yaitu primer dan sekunder. Tekhnik pengumpulan data primer diperoleh dari studi literatur melalui buku dan artikel jurnal dimana memiliki keterkaitan terhadap keamanan siber dan kedaulatan data. Di sisi lain, data sekunder dalam penelitian ini didapatkan melalui media online dan sumber-sumber lainnya, serta digunakan sebagai data pendukung yang memiliki keterkaitan terhadap masalah penelitian. Dengan penggunaan studi pustaka, peneliti akan menjabarkan dan menganalisis sesuai dengan data dan informasi yang dikumpulkan terkait penelitian ini.

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Data Pribadi" merupakan suatu konsep yang menggambarkan proses atau upaya menggabungkan pengaturan-pengaturan mengenai privasi dan data pribadi yang tersebar di berbagai instrumen hukum ke dalam satu instrumen hukum tersendiri. Dengan demikian perlindungan privasi dan data pribadi memiliki tempat yang sui generis. Keadaan pengaturan mengenai privasi dan data pribadi di Indonesia, saat ini tengah berada dalam keadaan yang divergen, sebagai lawan dari istilah konvergen.

Prinsip hak privasi terhadap data pribadi merupakan aspek kritis dalam era digital yang semakin maju ini. Setiap harinya, kita berinteraksi dengan teknologi dan memberikan data pribadi secara online. Data pribadi merujuk pada informasi apa pun yang dapat mengidentifikasi secara langsung atau tidak langsung seseorang. Ini termasuk, namun tidak terbatas pada, nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi, data keuangan, dan informasi medis. Namun, dengan memberikan informasi ini, kita juga membuka peluang bagi potensi penyalahgunaan data dan pelanggaran privasi. Hak privasi terhadap data pribadi mencakup hak setiap individu untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang mengaksesnya, untuk tujuan apa data tersebut digunakan, dan bagaimana data tersebut diolah dan disimpan. Lebih dari itu, prinsip ini juga melibatkan hak untuk memberikan izin atau persetujuan atas penggunaan data pribadi tersebut, serta hak untuk meminta penghapusan data (right to be forgotten) atau koreksi jika data tersebut tidak akurat. Prinsip hak privasi terhadap data pribadi bertujuan untuk melindungi hak asasi manusia dan martabat individu, serta untuk memastikan bahwa data pribadi digunakan dengan etika dan kejujuran. Hal ini tidak hanya relevan bagi perusahaan yang mengumpulkan data, tetapi juga bagi pemerintah dan entitas lain yang terlibat dalam pengumpulan, pemrosesan, dan penggunaan data pribadi.

Beberapa contoh kasus hak privasi yang dilanggar atau dianggap dilanggar yang pernah ada di Indonesia adalah bocornya data pribadi pada layanan BPJS kesehatan pada tahun 2021, Pada tahun 2020, terjadi pelanggaran data di platform e-commerce Tokopedia. Data pribadi dari puluhan juta pengguna, termasuk nama, alamat email, nomor telepon, dan informasi lainnya, dan yang hingga saat ini belum jelas kebenarannya adalah data pribadi pengguna aplikasi

transportasi online seperti Gojek atau Grab telah bocor akibat pelanggaran keamanan. Hak atas privasi, terkadang dikenal sebagai hak untuk tidak diganggu, diciptakan oleh Warren dan Brandheis dan diterbitkan dalam sebuah manuskrip berjudul "The Right to Privacy" di jurnal ilmiah Harvard University Law School. Menurut Warren dan Brandheis dalam jurnal tersebut, tumbuh dan berkembangnya teknologi telah menimbulkan kesadaran masyarakat yang menimbulkan kesadaran bahwa setiap orang berhak untuk menikmati hidup.

B. Pembahasan

1. Bentuk Perlindungan Data Pribadi di Media Sosial

Sejalan dengan diaturnya perlindungan terhadap data pribadi dalam satu undang-undang khusus yaitu Undang-Undang RI No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, maka dapat diamati bahwa terdapat beberapa progresifitas perihal data pribadi di Indonesia. Dapat dilihat dari segi politik hukum, pengertian, informasi, prosesor data pribadi, pengendali data pribadi, serta subyek data pribadi yang bukan hanya orang namun pula perusahaan/ badan hukum. Sehingga politik hukum dalam pengaturan ini terlihat dalam peran aktif pemerintah mulai dari pengaturan, penyimpanan, pengolahan, pen-transferan, hingga pada penanggulangan baik secara preventif maupun represif (pengenaan sanksi). Dapat diperhatikan pula bahwa ini merupakan pengaturan mengenai perlin-dungan data pribadi yang diatur dalam tingkat undang-undang, sehingga tentu layak untuk segera diupayakan peraturan pelaksanaannya sehingga mekanisme perlindungannya menjadi efisien. Secara substansi, sedikit hal yang perlu diperhatikan adalah pengenaan sanksi terhadap beberapa bentuk kegiatan yang dianggap melanggar hak seseorang atas perlindungan data pribadinya. Hal ini tertuang dalam Bab XIII Undang-Undang Perlindungan Data Pribadi. Namun jika diamati belum dicantumkan jenis (delik) tindak pidana dalam sanksi tersebut, delik biasa atau delik aduan. Hal ini sangat logis untuk diatur secara eksplisit atau pada undang-undang ataupun peraturan pelak-sanaannya, sehingga Lembaga penegak hukum tidak bingung nanti dalam penerapannya. Tentu dapat diperhatikan bahwa hal ini terkait erat dengan bagian struktur hukum yang akan dibahas pada bagian berikutnya. Delik aduan atau delik biasa layak untuk diatur mengingat data pribadi cenderung bersifat privacy jadi akan bersifat riskan jika diatur sama sebagai delik biasa pada subyek berupa perorangan maupun subyek hukum berupa perusahaan.

Setelah secara substansi, pengaturan perihal perlindungan data pribadi ini telah terbentuk, namun hal lain sebagai penguat konstruksi perlindungan data pribadi perlu pula diperhatikan. Struktur memegang peranan yang sangat penting dalam pengaturan sebuah esensi. Betapa tidak, mengingat struktur merupakan dapat diibaratkan tembok yang harus dipasang setelah pondasi (substansi) yang kokoh. Pada substansi memang tereksplisit diatur pada bagian Bab IX yang mengatur tentang kelembagaan yang terkait dalam perlindungan data pribadi hingga Bab X yang mengatur tentang hubungan internasional yang tentu saja dilakukan oleh kelembagaan internasional yang terkait dengan perlindungan data pribadi. Maka sebuah urgensi untuk diterbitkan berbagai peraturan pelaksanaan yang terkait dengan kelembagaan sebagai pelaksana atas undang-undang ini, selama kurun waktu 2 (dua) tahun masa peralihan sebagaimana tertuang dalam Bab XV Undang- Undang Perlindungan Data Pribadi. Tentu saja bukan hanya pengaturan, namun serangkaian upaya dengan tujuan memberikan pemahaman agar dalam penegakan hukum atas undang-undang ini tidak menjadi keliru dalam berfikir (fallacy mind) bahkan bertindak.

Pengaturan mengenai klasifikasi data pribadi, diatur dalam Pasal 4 Undang-Undang Nomor 27 Tahun 2022. Merujuk pada aturan tersebut, klasifikasi data pribadi terdiri atas:

a) Data pribadi yang bersifat spesifik.
b) Data pribadi yang bersifat umum.

Data Pribadi yang bersifat spesifik merupakan Data Pribadi yang apabila dalam pemrosesnya dapat mengakibatkan dampak lebih besar kepada Subjek Data Pribadi, antara lain tindakan diskriminasi dan kerugian yang lebih besar Subjek Data

Pribadi. Adapun klasifikasi data pribadi yang bersifat spesifik meliputi:

a) Data dan informasi kesehatan;
b) Data biometrik;
c) Data genetika;
d) catatan kejahatan;
e) Data anak;
f) Data keterangan pribadi; dan
g) Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

Sementara itu, Data Pribadi yang bersifat umum meliputi:

a) Nama Lengkap;
b) Jenis Kelamin;
c) Kewarganegaraan;
d) Agama;
e) Status Perkawinan; Dan
f) Data Pribadi Yang Dikombinasikan Untuk Mengidentifikasi Seseorang Antara Lain Nomor Telepon Seluler Dan IP Address.

2. Implementasi perlindungan data pribadi di media sosial

Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu meminimalisasi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk mengamankan data pribadi sesorang pada central data atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi sesorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini. Sistem IDPS ini dilekatkan kepada Kementerian Komunikasi dan Informatika (Kominfo) yang dimana IDPS mempunyai dua unsur yang sangat penting atau urgent, yaitu central data atau data authority serta data officer. Central data atau data authority fungsinya adalah untuk mengumpulkan dan mengamankan setiap data dan informasi pribadi yang masuk dari data officer, maka dari itu data officer ditempatkan pada seluruh perusahaan dan instansi pemerintahan yang melakukan pengelolaan data dan informasi pribadi agar lebih mudah untuk melakukan koordinasi terkait dengan data dan infromasi pribadi yang dimiliki seseorang. Central data atau data authority merupakan tempat ataupun pusat penyimpanan data dan hanya dikelola oleh orang yang memiliki kewenangan untuk melakukan pengelolaan data dan informasi pribadi tersebut, central data juga harus memiliki kemanan yang sangat ketat karena merupakan tempat utama penyimpanan data.

Data officer merupakan orang-orang yang mempunyai kewenangan dan keahlian yang ditunjuk oleh central data atau data authority untuk melakukan pengelolaan data dan informasi pribadi pada setiap perusahaan dan instansi pemerintah, yang kemudian dalam pekerjaannya ini harus melakukan koordinasi tentang pengelolaan data dan informasi pribadi yang dikelola sekali dalam 24 jam, agar central data mempunyai informasi yang up to date terhadap pengelolaan data pribadi oleh perusahaan dan instansi pemerintah. Melihat pekerjaan yang sangat sulit oleh seseorang data officer, maka dari itu harus memiliki kualifikasi tersendiri agar sumber daya manusia yang bekerja sebagai data officer adalah orang-orang yang berkompeten dan seseorang yang professional, orang-orang yang bekerja dalam bidang privasi dan perlindungan data harus memiliki keahlian yang sama baik dalam hukum dan teknologi keamanan siber untuk membantu perusahaan dan instansi pemerintah mengatur penyimpanan, pemrosesan, serta perlindungan data digital yang sesuai dengan undang-undang.

IDPS sebagai sebuah sistem yang dilekatkan pada Kominfo, untuk mendukung kinerja dari sistem ini juga perlu adanya kerjasama terhadap badan atau pun tim yang sudah dibentuk oleh pemerintah sebelumnya, kerjasama ini dilakukan untuk mewujudkan adanya cyber surveillance dan perlindungan data terhadap data dan informasi seseorang yang sedang diproses, fungsi dari adanya kerjasama ini adalah untuk lebih meningkatkan ketahanan dari IDPS itu sendiri yang nantinya akan menjadi pusat pengelolaan data pribadi dan sebagai pusat kontrol data pribadi seseorang yang dilaporkan oleh data officer Kerjasama Kominfo sebagai implementasi dari sistem IDPS ini sangat diperlukan agar IDPS dalam implementasinya menjadi sebuah sistem yang kuat dan kokoh terhadap berbagai ancaman. ID-SIRTII, ID-CERT, Direktorat Tindak Pidana

Siber Bareskrim Polri, BSSN, dan satuan siber TNI, merupakan wujud nyata pemerintah dalam menyikapi tantangan

cybercrime yang terjadi di Indonesia, namun kelima lembaga tersebut masih belum menjangkau sepenuhnya terkait dengan data protection dan data surveillance, proteksi data yang dimaksud adalah proteksi data dan informasi yang dimiliki oleh seseorang, keempat lembaga ini hanya fokus pada penanggulangan, dan deteksi dini, dan tidak memperhatikan bagaimana sebenarnya pengelolaan data dan informasi seseorang itu, apakah data dan informasi pribadi seseorang sudah dikelola secara tepat dan baik, dengan adanya kerjasama ini juga sekaligus lembaga yang bertugas melakukan pengawasan terhadap kinerja oleh data officer. Kerjasama yang dilakukan kominfo oleh keempat lembaga ini adalah untuk meningkatkan keamanan siber dibidang pengelolaan data dan informasi pribadi. Sistem IDPS juga mampu mengatasi dan meminimalisir banyaknya kejahatan-kejahatan di bidang pengelolaan data dan informasi pribadi, yang diketahui bersama kejahatan tehadap pengelolaan data pribadi ini akan semakin meningkat seiring perkembangan teknologi yang begitu pesat, dan diperburuk dengan belum adanya regulasi yang mengatur mengenai perlindungan data pribadi dan kejahatan siber itu sendiri. Permasalahan yang tekait dengan keamanan data dan informasi seseorang adalah data pribadi seseorang biasanya langsung diberikan oleh pihak pengelola data tanpa sepengetahuan pemilik data pribadi tersebut, dengan adanya IDPS ini jika sebuah perusahaan maupun instansi pemerintah ingin menggunakan data dan informasi seseorang maka harus dilaporkan terlebih dahulu dan memiliki jangka waktu selambat-lambatnya 60 menit dan paling lambat 3 x 24 jam untuk melakukan konfirmasi, jika lewat dari jangka waktu tersebut atau pemilik data mengabaikan-nya maka perusahaan dan instansi terkait berhak diberikan data dengan pemberian-nya disertai dengan pengawasan.

Indonesia sendiri telah memiliki aturan perlindungan privasi dan data pribadi yang tersebar di berbagai peraturan perundang-undangan, misalnya Undang - Undang No. 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, sedangkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur privasi dan data pribadi menge-nai nasabah penyimpan dan simpanannya. Selain itu pengaturan perlindungan privasi dan data pribadi juga terdapat dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan telah diubah dengan Undang-Undang No. 24 Tahun 2013) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (telah diubah dengan Undang-Undang Nomor 19 Tahun 2016), serta berbagai peraturan lainnya. Indonesia juga telah memiliki Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi yang kini masih dalam tahap pembahasan intra Kementerian dan diharapkan dapat segera diusulkan dalam prolegnas 2018.

Konvergensi Perlindungan Data Pribadi penting bagi Indonesia belum terlaksana, padahal konvergensi tersebut penting untuk memberikan perlindungan privasi dan data pribadi yang setara dengan negara-negara lain. Pengaturan yang akan disusun dalam Rancangan Undang-Undang diharapkan akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai perlindungan privasi dan data pribadi. Sampai saat ini masih terjadi ketidakpastian perlindungan privasi dan data pribadi, karena Indonesia belum memiliki instrumen hukum yang responsif terhadap adanya kebutuhan masyarakat untuk memperoleh perlindungan yang lebih kuat. Instrumen hukum yang ada di era ekonomi digital. Suatu instrumen hukum perlindungan privasi dan data pribadi di era ekonomi digital setidaknya harus memenuhi 3 kriteria: (1) memiliki karakter internasional; dan (2) merupakan elemen perekat individu dan masyarakat ekonomi. Karakteristik Pertama, perlindungan privasi dan data pribadi harus juga ditunjang dengan pengaturan-pengaturan yang sifatnya lintas batas negara. Aturan semacam ini diantaranya adalah aturan bahwa transfer privasi dan data pribadi ke luar wilayah negara harus memerlukan persetujuan khusus, dan hanya dapat dilakukan ke negara yang memiliki perlindungan privasi dan data

pribadi setara. Karakteristik Kedua, dalam konteks Era Ekonomi Digital, perlindungan privasi dan data pribadi harus juga mencakup perlindungan hak personal. Dengan kata lain selain harus merupakan hak-hak negatif yang menuntut negara tidak melakukan sesuatu agar hak tersebut terpenuhi, juga harus merupakan hak-hak positif yang pemenuhan hak nya hanya bias dilakukan dengan peran aktif dari negara. Era Ekonomi digital dengan segala karakteristik khusus dan perkembangan pesatnya tidak bisa menuntut negara untuk hanya diam, namun melakukan sesuatu yang lebih. Karakteristik Ketiga, perlindungan privasi dan data pribadi dapat meningkatkan kepercayaan.

3. Undang-Undang Perlindungan Data Pribadi di Indonesia

Indonesia saat ini telah memiliki beberapa peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, sebagai berikut:

a) Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan Frasa "rahasia bank" diartikan sebagai "segala sesuatu yang berkaitan dengan penabung dan simpanannya" dalam Pasal 1 Ayat (28) UUD. Ini mengklarifikasi bahwa setiap informasi terkait pelanggan di bank adalah masalah yang sensitif dan pribadi. Kecuali dalam keadaan sebagaimana dimaksud dalam Pasal 41, 41A, 42, 44, dan 44A, bank diharapkan menjaga kerahasiaan informasi yang disimpan nasabah penyimpan dan simpanannya, sesuai dengan Pasal 40 Ayat (1). Menurut pasal ini, bank wajib mengamankan semua data nasabah.

b) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi Perlindungan data pribadi secara umum diatur oleh Undang-Undang Telekomunikasi, meskipun tidak secara khusus terkait dengan data pribadi. “Penyelenggara jasa telekomunikasi wajib merahasia-kan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomu-nikasi melalui jaringan telekomunikasi dan/atau jasa telekomunikasi yang diselenggarakannya,” bunyi Pasal 42 ayat 1 UU Telekomunikasi.

Hal ini menjadi dasar kewajiban penyelenggara jasa untuk menjamin keamanan setiap data yang akan dikirim melalui jaringan telekomunikasi atau diterima melalui jasa telekomunikasi. Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomuni-kasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi dan dapat memberikan informasi yang diperlukan atas:

1) Permintaan tertulis dari Kejaksaan Agung dan/atau Kepala Kepolisian Negara Republik Indonesia. Republik Indonesia untuk tindak pidana tertentu;
2) Permintaan tertulis dari Jaksa Agung dan/atau Kepala Kepolisian Republik Indonesia;

Menurut Pasal 57 UU Telekomunikasi, “Penyelenggara jasa telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp200.000.000,00 (dua ratus juta rupiah)." Undang-Undang Telekomunikasi juga mengatur tentang sanksi mengenai tindak pidana terhadap keamanan informasi tersebut.

c) Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM)

Aturan perundang-undangan yang mengatur hak asasi seseorang adalah Hukum Hak Asasi Manusia. Setiap orang berhak untuk berkomunikasi dan meng-akses pengetahuan yang diperlukan untuk mengembangkan kepribadian dan lingkungan sosialnya, sesuai dengan Pasal 14 Ayat 1 UUD. Pasal ini menegaskan bahwa setiap orang berhak untuk mengakses pengetahuan yang mereka butuhkan untuk kehidupan sehari-hari guna memajukan partum-buhan mereka sendiri dan kualitas lingkungan tempat mereka tinggal. Dalam Pasal 29 Ayat (1) UU HAM disebutkan bahwa “Setiap orang berhak melindungi diri sendiri, keluarga, kehormatan, martabat, dan hak milik”. Pasal ini mengatur tentang hak atas

perlindungan pribadi yang dijamin oleh Pasal 28 Huruf G Ayat (1) UUDNRI 1945. Menurut Pasal 32 UU

HAM, yang menyatakan bahwa "Kemerdekaan dan kerahasiaan dalam hubungan korespondensi, termasuk hubungan komunikasi dengan sarana elektronik, tidak boleh diganggu, kecuali atas perintah hakim atau pejabat lain yang sah sesuai dengan ketentuan Undang-undang Hak Asasi Manusia. undang-undang," ada juga tambahan baru pada undang-undang yang berkaitan dengan perlindungan data pribadi.

d) Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Satu-satunya pasal yang secara tegas menjamin perlindungan data pribadi setelah diproses adalah Pasal 26 Ayat 1. UU ITE, khususnya Pasal 27 hingga 37, mengatur kegiatan ilegal di bidang informasi elektronik yang tidak secara khusus berkaitan dengan data pribadi. Pasal-pasal tersebut pada umumnya melarang perbuatan yang melanggar hak dan penyalahgunaan informasi elektronik dengan sengaja yang dapat merugikan orang lain, terutama pemilik informasi.

IV. SIMPULAN DAN SARAN

A. Simpulan

Pengaturan mengenai perlindungan data pribadi yang diatur dalam tingkat undang-undang, sehingga tentu layak untuk segera diupayakan peraturan pelaksanaannya sehingga mekanisme perlindungannya menjadi efisien. Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu meminimalisasi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk mengamankan data pribadi sesorang pada central data atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi sesorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini.

Siber Bareskrim Polri, BSSN, dan satuan siber TNI, merupakan wujud nyata pemerintah dalam menyikapi tantangan cybercrime yang terjadi di Indonesia, Kerjasama yang dilakukan kominfo oleh keempat lembaga ini adalah untuk meningkatkan keamanan siber dibidang pengelolaan data dan informasi pribadi. Indonesia sendiri telah memiliki aturan perlindungan privasi dan data pribadi yang tersebar di berbagai peraturan perundang-undangan, misalnya Undang - Undang No. 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, sedangkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur privasi dan data pribadi mengenai nasabah penyimpan dan simpanannya.

Perlindungan data menjadi semakin penting dalam era digital yang terus berkembang, mengingat volume dan nilai data yang terus meningkat. Evaluasi terhadap kerangka kerja kebijakan yang ada menyoroti kebutuhan untuk peningkatan dalam aspek perlindungan data, termasuk kepatuhan terhadap regulasi dan standar keamanan yang relevan. Faktor-faktor seperti perubahan teknologi, ancaman yang berkembang, dan keterbatasan sumber daya mempengaruhi implementasi kebijakan keamanan cyber dalam perlindungan data. Meskipun tantangan yang dihadapi dalam melindungi data semakin kompleks, studi literatur menunjukkan adanya peluang untuk meningkatkan kebijakan keamanan cyber melalui pendekatan kolaboratif antara pemerintah, industri, dan masyarakat. Rekomendasi berdasarkan temuan penelitian literatur mencakup peningkatan kesadaran akan risiko keamanan cyber, investasi dalam teknologi keamanan yang canggih, dan peningkatan kerjasama lintas sektor untuk menghadapi ancaman cyber dengan lebih efektif.

B. Saran

Saran yang dapat diambil dari penelitian analisis kebijakan keamanan cyber dengan fokus pada implementasi perlindungan data di era digital meliputi:

1. Penguatan Kerjasama: Mendorong kerjasama lintas sektor antara pemerintah, industri, dan masyarakat untuk mengatasi tantangan keamanan cyber secara efektif. Ini dapat melibatkan pertukaran informasi, pembentukan standar keamanan bersama, dan kolaborasi dalam mengembangkan solusi keamanan yang inovatif.
2. Peningkatan Kesadaran: Mengedukasi pemangku kepentingan tentang risiko keamanan cyber dan pentingnya

melindungi data sensitif. Ini dapat dilakukan melalui kampanye penyuluhan, pelatihan keamanan cyber, dan penyediaan sumber daya untuk memperkuat kesadaran akan ancaman cyber.

3. Investasi Teknologi: Mengalokasikan sumber daya yang memadai untuk mengadopsi teknologi keamanan yang canggih guna melindungi data secara efektif. Ini termasuk penggunaan sistem deteksi intrusi, enkripsi data, pemantauan keamanan yang terus-menerus, dan implementasi solusi keamanan berbasis kecerdasan buatan.
4. Kepatuhan Regulasi: Memastikan kepatuhan penuh terhadap regulasi dan standar keamanan yang relevan untuk melindungi data. Ini mencakup peninjauan dan pembaruan terhadap kebijakan keamanan cyber secara berkala sesuai dengan perkembangan teknologi dan ancaman yang muncul.
5. Evaluasi Terus-Menerus: Melakukan evaluasi rutin terhadap implementasi kebijakan keamanan cyber untuk mengidentifikasi kelemahan dan memperbaiki kebijakan yang ada. Ini dapat dilakukan melalui audit keamanan, penilaian risiko secara teratur, dan pembelajaran dari insiden keamanan cyber yang terjadi.

Dengan mengambil saran-saran ini sebagai pedoman, organisasi dan pemerintah dapat meningkatkan upaya mereka dalam melindungi data sensitif dan mengurangi risiko keamanan cyber di era digital yang terus berubah.

DAFTAR RUJUKAN

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222-238.

Al Fahri, S. M. *Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce Ditinjau dari UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Lazada)* (Bachelor's thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta).

Arham, M. R. H., & Risal, M. C. (2023). Perlindungan Data Pribadi bagi Pengguna Media Sosial. *JURNAL AL TASYRI'IYYAH*, 109-119.

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). Perlindungan data dan informasi pribadi melalui Indonesian Data Protection System (IDPS). *Jurnal Legislatif*, 167-190.

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218-239.

Republik Indonesia, Undang-undang RI Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pasal 1

Republik Indonesia, Undang-undang RI Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pasal 4.

Rosadi, S. D., & Pratama, G. G. (2018). Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, *4*(1), 88-110.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285-299.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132-142.

snilam Syafitri, E. R. (2020). Studi Kepustakaan Teori Konseling "Dialectical Behavior Therapy".

Undang-undang Republik Indonesia Nomor 27 Tahun 2022 Tentang perlindungan data pribadi

Undang –Undang Dasar Negara Republik Indonesia Tahun 1945

Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang – Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang – Undang Nomor 36 Tahun 2009 tentang Kesehatan

Undang – Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Undang – Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang – Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia