

## PERSPEKTIF HUKUM TERHADAP KEAMANAN DATA: TANTANGAN DAN SOLUSI DI ERA TEKNOLOGI INFORMASI

Andy Satria<sup>1)</sup>, Nadiah Puteri Hana Ulina<sup>2)\*</sup>, Putri Safira<sup>3)</sup>, Bagus Pangestu<sup>4)</sup>

1)Program Studi Teknologi Informasi, Universitas Dharmawangsa

2)3)4)Program Studi Ilmu Hukum, Universitas Medan Area

\*Corresponding Email: nadiahputeri2@gmail.com

**ABSTRAK**-Ketika data memiliki nilai, keamanan dan kerahasiaan data menjadi sangat penting. Misalnya, data pribadi warga negara harus dilindungi karena dapat dieksploitasi oleh entitas jahat untuk kegiatan kriminal. Oleh karena itu, pemilik data memikul tanggung jawab. Keamanan data mencakup berbagai aspek seperti privasi, konsistensi, keaslian, ketersediaan, dan kontrol akses (Harun Mukhtar, 2018). Menurut Pasal 28G(1), warga negara berhak atas perlindungan pribadi, keluarga, kehormatan, martabat, dan kekayaan. Namun, mengingat kemajuan teknologi informasi dan komunikasi, hak-hak individu tidak boleh hanya dipahami sebagai kepemilikan tekstual; privasi harus dianggap sebagai hak asasi manusia. Hak atas privasi lebih sensitif dan dapat dianggap sebagai hak individu karena berkaitan dengan data pribadi atau identitas individu. Rencana perlindungan data pribadi yang ada saat ini awalnya dimulai berdasarkan peraturan yang ada, khususnya Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi, yang diundangkan pada tanggal 7 November 2016 - efektif mulai tanggal 1 Desember 2016. Diusulkan sejak tahun 2014, rencana perlindungan data pribadi RUU Perlindungan Data Pribadi (RUU PDP) dinilai penting demi keselamatan masyarakat. Mengingat RUU tersebut tidak masuk dalam Program Legislatif Nasional (Prolegnas) tahun 2018, maka pembahasan RUU PDP diharapkan selesai sebelum berakhirnya masa jabatan Majelis Permusyawaratan Rakyat Indonesia (DPR-RI) 2014-2019. Pada 24 Januari 2020, Presiden Joko Widodo menandatangani RUU PDP yang selanjutnya akan dibahas di DPR. RUU PDP diusulkan dalam Program Legislatif Nasional Prioritas DPR periode 2019-2024.

**Kata Kunci: Perlindungan Data, RUU PDP, Pengujian Keamanan Transaksi Elektronik**

**ABSTRACT**- *When data holds value, the security and confidentiality of data become crucial. For instance, the personal data of citizens must be protected as it can be exploited by malicious entities for criminal activities. Therefore, data owners bear the responsibility. Data security encompasses various aspects such as privacy, consistency, authenticity, availability, and access control (Harun Mukhtar, 2018). According to Article 28G(1), citizens have the right to personal protection, family,*

*honor, dignity, and wealth. However, considering the advancements in information and communication technology, individual rights should not merely be understood as textual ownership; privacy ought to be considered a basic human right. The right to privacy is more sensitive and can be considered an individual right as it relates to personal data or individual identity. The current plan for personal data protection initially began based on existing regulations, particularly Ministerial Regulation No. 20 of 2016 on Personal Data Protection, enacted on November 7, 2016 - effective from December 1, 2016. Proposed since 2014, the Personal Data Protection Bill (RUU PDP) is considered essential for community safety. Considering the bill was not included in the National Legislative Program (Prolegnas) in 2018, it is hoped that the discussion on the RUU PDP will conclude before the end of the term of the Indonesian People's Consultative Assembly (DPR-RI) 2014-2019. On January 24, 2020, President Joko Widodo signed the RUU PDP, and it will subsequently be deliberated in the DPR. The RUU PDP is proposed in the National Legislative Program Priority of the DPR for the period 2019-2024.*

**Keywords: Data Protection, PDP Bill, Security Testing of Electronic Transactions**

## **PENDAHULUAN**

Perkembangan dan kemajuan dunia digital dapat mengubah perilaku dan dan pergeseran gaya hidup sehingga penggunaan data pribadi dan identitas seseorang sangat dibutuhkan dalam berbagai kepentingan dalam Tindakan online seperti melibatkan berbagai informasi pribadi termasuk detail tentang nama seseorang, tanggal lahir, tempat tinggal, nomor identitas, situasi keuangan, Riwayat medis, dan data sensitif lainnya (Suari dan M Sarjana, 2023). Revolusi digital telah berdampak pada berbagai aspek kehidupan, termasuk cara kita berkomunikasi, bekerja, berbelanja, dan menjalankan bisnis (Panggabea, 2022).

Sebab, digitalisasi semakin memudahkan dan mempercepat pengambilan, penyimpanan, dan pengolahan data. Di era digital, data kini menjadi asset paling berharga untuk organisasi dan individu. Data adalah sumber informasi untuk mengambil keputusan penting, menciptakan nilai tambah bagi perusahaan anda, dan mendorong inovasi. Oleh karena itu, menjaga keamanan data menjadi suatu hal yang sangat krusial dan penting dalam transformasi digital. Transformasi digital berkembang pesat di Indonesia. Pemerintah Indonesia telah meluncurkan berbagai inisiatif untuk mempercepat transformasi digital Indonesia. Namun,

meskipun transformasi digital dapat membawa banyak manfaat bagi perekonomian Indonesia, terdapat juga risiko keamanan yang perlu diatasi (Saefudin 2022). Masalah keamanan data telah menjadi isu yang sangat serius di seluruh dunia. Data dapat dilihat oleh pihak yang tidak berwenang dan digunakan untuk tujuan jahat. Contohnya termasuk pencurian identitas, penipuan, dan penggunaan data untuk melakukan kejahatan. Oleh karena itu, Anda memerlukan sistem keamanan yang kuat untuk melindungi data Anda dari risiko.

Lembaga yang melakukan perlindungan dan kerahasiaan data tidak boleh melakukan tindakan yang dapat merugikan pihak lain seperti tidak melakukan penjualan data, lemahnya sistem yang digunakan (Retas), sehingga masyarakat dan warga negara melindungi data pribadi masyarakat sebagai warga negara menjadi suatu keharusan karena ada potensi penggunaan yang tidak sah oleh pihak yang tidak berhak yang selanjutnya dapat menimbulkan tanggung jawab bagi pemilik data. Aspek-aspek keamanan data mencakup privasi (kerahasiaan), integritas (konsistensi), otentisitas (keaslian), ketersediaan (availability), dan pengendalian akses (access control) (Harun Mukhtar, 2018).

Di Indonesia, orang-orang menjadi lebih sadar akan kebutuhan untuk melindungi data pribadi, terutama mengingat meningkatnya aplikasi berbasis teknologi dan penggunaan internet. Hak untuk melindungi diri sendiri merupakan satu dari hak yang diatur dalam UUD 1945. Sesuai dengan Pasal 28G, setiap warga negara memiliki hak untuk melindungi dirinya sendiri, keluarganya, martabatnya dan harta bendanya. Tetapi, mengingat kemajuan teknologi informasi dan komunikasi, hak individu hendaknya tidak hanya dipahami sebagai hak milik dalam arti tekstual. Hak atas privasi harus menjadi hak mendasar. Karena hak atas privasi berkaitan dengan informasi atau identitas pribadi seseorang, maka hak tersebut lebih sensitif dan dapat dianggap sebagai hak individu. Namun, baru-baru ini insiden bocornya data telah menjadi isu yang signifikan. Beberapa di antaranya terdiri dari:

1. Kejadian Tokopedia (2020): Pada permulaan tahun 2020, terjadi insiden keamanan pada Tokopedia, sebuah platform e-commerce besar di Indonesia. Kejadian ini

mengakibatkan data pribadi jutaan pengguna terbocor, mencakup nama, alamat, nomor telepon, alamat email, dan kata sandi yang telah dienkripsi.

2. Insiden Bukalapak (2021): Platform e-commerce lain di Indonesia, terjadi juga pelanggaran data pada tahun 2021. Informasi termasuk nomor telepon, alamat email, kata sandi, dan nama pengguna terungkap, mempengaruhi lebih dari 13 juta pengguna.
3. Kejadian TokoTalk (2021): Pada tahun 2021, aplikasi pesan instan asal Indonesia, TokoTalk, dilaporkan mengalami kebocoran data. Lebih dari 91 juta akun pengguna terpengaruh, dan data yang terbocor mencakup nama, nomor telepon, alamat email, dan salinan kartu identitas (Mirnayanti dkk, 2023).

Peningkatan pada PC dan kerangka web telah mempermudah pencarian dan berbagi data. Sekitar tahun 1960 konsep dasar keamanan informasi pribadi pertama kali muncul. Asuransi informasi umumnya dianggap sebagai bagian dari fungsi keamanan jaminan. Sekarang, Indonesia memiliki regulasi perlindungan data pribadi melalui UU No 19 Tahun 2016 tentang pertukaran data elektronik Tahun 2007 (UU ITE) dan peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

Terjadi insiden dimana seorang peretas, umumnya dikenal sebagai hacker, berhasil mencuri data pengguna Tokopedia dan menjualnya di darkweb. Pada tahun 2021, Kementerian Komunikasi dan Informatika (kominfo) memastikan tidak ada kebocoran data BPJS kesehatan dan E-ktp, namun diduga data tersebut dijual di forum hacker "raid forums". Menghadapi berbagai permasalahan ini, pemerintah Indonesia perlu memastikan keamanan data pribadi, mengatur perlindungan data, dan menyusun berbagai bentuk perlindungan hukum. Salah satunya adalah regulasi perlindungan data. Ada RUU PDP (Perlindungan Data Pribadi), tapi belum disahkan. Oleh karena itu, adanya fenomena tersebut memerlukan penelitian ilmiah yang secara khusus mengkaji peraturan keamanan data pribadi dalam hukum domestik Indonesia dan kebijakan hukum dalam pelaksanaan PDP untuk mencapai perlindungan data pribadi warga negara hukum di Indonesia belum diratifikasi. Dalam variasi

sistem hukum ini, asas universalitas dapat dipakai secara khusus untuk kebutuhan seluruh dunia. Hal ini didasarkan pada pemikiran bahwa semua negara di dunia wajib berpartisipasi dalam pelaksanaan tatanan hukum global. Berlandaskan peristiwa diatas dan penyimpangan data privasi, peneliti terdorong untuk menelaah “Perspektif Hukum Terhadap Keamanan Data: Tantangan dan Solusi di Era Teknologi Informasi”

## **METODE PENELITIAN**

Penelitian ini menerapkan pendekatan kuantitatif deskriptif sebagai metodenya. Kajian ini dilakukan dengan menganalisis data dan informasi dari berbagai studi literatur dengan mengkaji jurnal, artikel dan sumber resmi terkait keamanan data dari sudut pandang hukum. Bahan referensi hukum yang digunakan untuk melakukan analisis penyelesaian masalah adalah bahan hukum yang penting yang melibatkan Undang-Undang Peraturan Pemerintah, dan Undang-Undang peraturan menteri terkait. Dalam penelitian ini, terdapat penggunaan beberapa teori dalam menganalisis masalah hukum, seperti teori rule of law, teori konvergensi, teori perlindungan hukum, teori hierarki hukum, serta teori keamanan siber yang terkait dengan keamanan data hukum positif di Indonesia.

## **HASIL DAN PEMBAHASAN**

### **A. Keamanan Data Terhadap Perspektif Hukum**

Pemerintah memiliki tanggung jawab hukum untuk melindungi seluruh warga Indonesia dan semua elemen masyarakat Indonesia, meningkatkan taraf hidupnya, dan ikut serta dalam perlindungan segenap bangsa, termasuk perlindungan hak-hak sipil sebagaimana yang dijelaskan dalam Pembukaan UUD 1945 Pasal 4. Prinsip perlindungan juga berlaku di era digital, karena perlindungan terhadap hak privasi mengenai data seseorang menjadi salah satu aspek penting di era digital yang semakin maju. Melakukan intraksi berkomunikasi dengan teknologi setiap hari dan menyediakan data seseorang secara online. Data perorangan merupakan data yang diberikan secara langsung atau tidak langsung yang dapat mengidentifikasi seseorang berbagai hal yang dibutuhkan termasuk, nama, tempat dan tanggal

lahir, alamat, nomor telepon, alamat surel, nomor identifikasi, data keuangan, dan informasi kesehatan (Mahira,dkk, 2020). Namun, pemberian data dan informasi juga memberikan peluang yang sangat potensi dalam penyalahgunaan dan pelanggaran data. Hak privasi terkait dengan data pribadi mencakup hak setiap individu untuk mengetahui informasi mengenai data pribadinya, siapa yang dapat mengakses data tersebut, tujuan penggunaan data, serta proses menyimpan data. Penggunaan Dana pada prinsipnya harus dapat bersetujuan dan diizinkan oleh pihak pemilik data dan apabila yang bersangkutan tidak berkenan datanya digunakan, anda, dan hak untuk meminta penghapusan (hak untuk dilupakan) atau perbaikan data Anda jika tidak akurat. Prinsip hak privasi terkait data pribadi bertujuan melindungi hak asasi manusia dan martabat individu, serta memastikan penggunaan data secara etis dan berintegritas. Prinsip kerahasiaan harus dijaga perusahaan, pemerintah, dan entitas lain yang terlibat dalam pengumpulan dan pemrosesan data (Ratumahina, RE, 2014).

Untuk menjaga hubungan dengan orang lain, pertama-tama Anda harus menyembunyikan beberapa aspek kehidupan pribadi Anda untuk mempertahankan posisi seseorang pada tingkatan tertentu. Kedua, hak independen dan privasi seseorang yang yang penggunaannya tidak bergantung pada hak orang lain. Namun hak itu bisa tidak berarti/hilang apabila seseorang membiarkan sesuatu yang bersifat pribadi tersedia untuk umum. Ketiga, sebagian orang membutuhkan privasi karena sebagian orang membutuhkan waktu dalam berbagai kegiatan. Keempat, kemampuan untuk mempertahankan ikatan rumah tangga, seperti mendukung pernikahan dan menyediakan untuk keluarga Warren termasuk dalam hak privasi, ini lebih lanjut digambarkan sebagai hak untuk berbicara. Kelima, ketidakmungkinan mengukur kerugian adalah alasan lain mengapa privasi harus dilindungi secara hukum. Karena mengganggu kehidupan pribadinya, maka korban harus diberi ganti rugi jika kerugian terjadi karena kerugian yang dirasakannya jauh lebih besar dari kerugian sebenarnya (Dewi, S, 2017).

Konstitusi dan Undang-undang peraturan terkait berfungsi sebagai dasar hukum Indonesia. Setiap individu memiliki hak untuk melindungi diri, keluarga, kehormatan, martabat, dan harta benda yang dimilikinya sesuai UUD 1945. Pasal 28 Huruf G Ayat (1) UUDNRI

Tahun 1945 menegaskan hak untuk melindungi diri sendiri, keluarga, dan properti seseorang, juga hak untuk merasa terlindungi dari kejahatan. Konsep perlindungan data memberi individu pilihan untuk memutuskan apakah akan membagikan atau mengekspos informasi pribadi mereka, dengan hak untuk menentukan persyaratan transfer data. Hak privasi, sebagai upaya melindungi data pribadi, terus berkembang (Anggraeni, SF, 2018).

Warga negara Indonesia memiliki hak konstitusional untuk melindungi privasi mereka, yang mencakup hak privasi mengenai informasi pribadi, berdasarkan dasar hukum. Hak konstitusional negara untuk secara hukum melindungi banyak aspek kehidupan masyarakat Indonesia. Hak konstitusional harus memiliki tiga tujuan hukum mencakup keadilan, kejelasan, dan kegunaan hukum. Pemerintah Indonesia telah menerapkan beberapa langkah atau inisiatif terkait perlindungan data pribadi:

- A. UU ITE Tahun 2020, Nomor 11, meskipun terfokus pada transaksi elektronik dan keamanan informasi juga mencakup ketentuan perlindungan data pribadi dalam sistem elektronik. Undang-undang ini mengharuskan proses data untuk melindungi informasi pribadi dan menetapkan sanksi untuk pelanggaran yang melanggar hak perlindungan data.
- B. Pemerintah Indonesia telah menyiapkan undang-undang yang secara khusus mengatur perlindungan data pribadi. Meskipun kabarnya RUU tersebut belum dilaksanakan, langkah ini menunjukkan upaya pemerintah untuk mengatasi perlindungan data pribadi secara lebih komprehensif.
- C. Merinci langkah-langkah pengamanan informasi pribadi dalam sistem elektronik sesuai dengan regulasi Menteri Komunikasi dan Informatika No. 20 Tahun 2016. Selain menawarkan praktik terbaik untuk mengelola data pribadi, undang-undang ini mengatur bagaimana informasi pribadi dilindungi dalam sistem elektronik.
- D. Peraturan terkait perlindungan data pribadi disektor-sektor ekonomi spesifik, seperti perbankan, perawat kesehatan, dan telekomunikasi, mencakup panduan atau kebijakan khusus untuk menjaga keamanan informasi pribadi. Sebagai contoh, Bank

Indonesia memiliki peraturan yang harus dipatuhi untuk melindungi informasi pribadi kliennya.

- E. Pengawasan dan Sanksi Pemerintah juga berperan dalam pengawasan terhadap perusahaan pengendali data pribadi. Apabila terjadi pelanggaran, sanksi dapat dikenakan kepada pihak yang bersalah melanggar aturan perlindungan data.
- F. Sebuah program untuk meningkatkan pemahaman publik tentang nilai menjaga informasi pribadi dan metode berbagi yang aman juga dilakukan oleh pemerintah.
- G. Pengembangan Kerangka Keamanan Data Pemerintah telah mengembangkan kerangka keamanan data untuk membantu organisasi dan bisnis melindungi data pribadi yang mereka simpan.
- H. Seiring dengan mematuhi norma-norma internasional yang diakui, pemerintah Indonesia juga mengambil bagian dalam kolaborasi internasional di bidang perlindungan data pribadi.

Upaya teknis pemerintah dalam melindungi data pribadi warga negara Indonesia antara lain:

- A. Meningkatkan standar keamanan yang tinggi dapat diterapkan oleh Keamanan Sistem Pemerintah ke infrastruktur dan sistem yang menangani data pribadi. Ini mencakup penyebaran firewall yang kuat, enkripsi data, dan pertahanan terhadap serangan siber.
- B. Teknologi pemantauan dapat digunakan oleh pemantauan aktivitas anomali pemerintah untuk mengidentifikasi aktivitas mencurigakan dan tidak biasa yang terjadi dalam suatu sistem dan jaringan. Ini mendukung dalam mendeteksi akses yang tidak diinginkan dan upaya peretasan.
- C. Ketika bisnis atau layanan yang menangani data pribadi menyatakan bahwa mereka mematuhi persyaratan keamanan tertentu, badan sertifikasi keamanan pemerintah dapat memberikan sertifikasi keamanan.

- D. Untuk melakukan audit berulang terhadap prosedur dan sistem yang berkaitan dengan keamanan data pribadi, auditor keamanan pemerintah dapat membuat kontrak dengan auditor keamanan independen.
- E. Menurut Peraturan Kewajiban Pelaporan Pelanggaran Perjanjian Pemerintah, Perusahaan harus memberitahu pihak berwenang yang berwenang tentang setiap pelanggaran yang melibatkan data pribadi sesegera mungkin sehingga Tindakan cepat dapat dilakukan untuk mengurangi kerugian.
- F. Pelatihan Karyawan Pemerintah dapat memotivasi perusahaan untuk memberikan pelatihan kepada anggota staf tentang prosedur keamanan data, seperti perlindungan kata sandi dan kesadaran phishing.
- G. Pemisahan Data Sensitif dimungkinkan untuk mengisolasi informasi pribadi sensitif dari jenis data lain untuk menurunkan kemungkinan akses yang tidak diinginkan.
- H. Untuk menghentikan akses ilegal ke data pribadi, keamanan akses pemerintah dapat mendukung pemasangan control akses atau sistem otentikasi ganda.
- I. Privasi dalam transit pemerintah mungkin mempromosikan penggunaan enkripsi, misalnya melalui protocol HTTPS, ketika data sedang dikirim antara pengirim dan penerima.
- J. Organisasi bisa mendapatkan saran dari Penanganan Aman Data yang tidak digunakan pemerintah tentang cara menghapus atau menghancurkan data yang tidak lagi diperlukan dengan aman. Organisasi dapat didorong untuk secara teratur melakukan tes keamanan, seperti pengujian penetrasi, untuk menemukan kelemahan dengan menggunakan pengujian keamanan pemerintah.
- K. Bekerja sama dengan sektor keamanan pemerintah, sektor perusahaan, dan pakar keamanan siber dapat lebih memahami tren ancaman saat ini dan menerapkan tindakan pencegahan.

## **B. Perspektif Politik Hukum dalam Pembentukan RUU PDP**

Politik legislatif merupakan subsistem hukum. Oleh karena itu, kebijakan legislasi dan kebijakan hukum tidak dapat dipisahkan. Pengetahuan tentang kebijakan hukum pada dasarnya berarti pengetahuan tentang kebijakan legislatif dan sebaliknya. Kebijakan legislatif diartikan sebagai “kebijaksanaan” atau (kebijakan publik) mengenai penetapan, pelaksanaan dan penegakan muatan dan materi pelajaran pendidikan.

Strategi dasar hukum komprehensif dan politik instrumen hukum terhadap pengembangan undang-undang dan pedoman. Soal implementasi hukum identik dengan bagian organisasi pemerintah di bidang hukum. Persoalan hukum untuk melaksanakan hukum diidentikkan dengan bagian yang kohesif dari kerangka nasional, misalnya ketergantungan negara pada hukum.

Fokus pasal ini adalah pada persoalan hukum dan ketertiban peraturan perundang-undangan, baik dari segi strategis dan isi undang-undang, serta pedoman yang berkaitan dengan penciptaan, pemulihan, dan pemajuan hukum. Tentang Perlindungan data berdasarkan RUU data pribadi di Indonesia. Pentingnya kebijakan dalam peraturan yang mengatur data pribadi harus menganut dan didasari untuk kepentingan masyarakat dan melindungi masyarakat dari tindakan -tindakan yang dapat merugikan masyarakat. Perlindungan merupakan perwujudan dari warga negara sejalan dengan kewajiban Negara yang tercantum dalam UUD Negara Republik Indonesia Tahun 1945 untuk menjunjung tinggi hak asasi manusia (HAM). Selain hak asasi manusia, pentingnya UU PDP terutama terletak pada memberikan keamanan dan kenyamanan kepada warga negara dalam melakukan berbagai aktivitas baik online maupun offline. Seluruh rezim perlindungan data pribadi saat ini sedang dalam proses konvergensi (Sinta Dewi Rosadi dan Gerry Gumelar Pratama)

Hal ini menggambarkan proses atau upaya untuk mengintegrasikan dan mengintegrasikan pengaturan data pribadi ke dalam berbagai instrumen hukum, inilah yang menjadi konsep dari Dokumen hukum lainnya. Oleh karena itu, perlindungan data pribadi memiliki arti penting tersendiri. Berbeda dengan istilah konvergensi, situasi regulasi terkait data pribadi di Indonesia berbeda dengan situasi saat ini (Monster Aditya).

## 1. Proses Pembentukan RUU PDP

Perencanaan perlindungan data pribadi yang ada akhir ini awalnya dimulai berdasarkan peraturan yang ada, khususnya berupa Peraturan Menteri Undang-Undang Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi diundangkan pada tanggal 7 November 2016, diundangkan dan berlaku efektif pada tanggal 1 Desember 2016. RUU PDP sangat penting dalam melindungi kepentingan masyarakat serta melindungi hak-hak masyarakat, hal ini kehadiran RUU PDP sudah diusulkan sejak tahun 2014. Mengingat RUU PDP tidak lolos dalam Rencana Legislasi Nasional (Prolegnas) 2018, Pembahasan RUU PDP diharapkan selesai sebelum masa jabatan DPR-RI 2014-2019 berakhir. Sejak 24 Januari 2020, RUU PDP ditandatangani Presiden Joko Widodo dan tengah dibahas di DPR.

RUU PDP ini diusulkan dalam Program Legislatif Nasional Prioritas DPR Tahun 2019-2024. Dalam pelaksanaan Perkembangan pembahasan RUU PDP dilaporkan dalam Siaran Pers No 231/HM/KOMINFO/07/2021. Di jelaskan bahwa (1) Tim Panitia Kerja (Panja Pemerintah yang dipimpin oleh Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, perwakilan pejabat kementerian/lembaga terkait dan Panitia Kerja Komite I DPR RI) melakukan pembahasan mengenai hal yang sama. Rancangan Undang-Undang Kebijakan Perlindungan Data (RUU PDP) telah diajukan di Jakarta sejak Selasa, 29 Juni 2021 hingga Rabu, 30 Juni 2021. (2) Panitia Kerja Pemerintah menggarisbawahi pentingnya perlindungan data pribadi dalam kerangka hukum yang kuat dan dapat di selesaikan dalam UU PDP sebagai undang-undang tentang perlindungan data pribadi. (3) Tim Panitia Kerja Pemerintah hendaknya merumuskan secara tepat dan akurat isi ketentuan-ketentuan penting RUU PDP, termasuk sistematika pelaksanaan perlindungan data pribadi, sehingga pembahasan RUU PDP dapat terlaksana dengan baik. (4) Tim Satuan Tugas Pemerintah berpendapat bahwa Perlindungan data pribadi dalam penyelenggaraannya merupakan urusan pemerintah dan pelaksanaannya didorong

oleh Departemen Komunikasi dan Informatika yang bertanggung jawab kepada Presiden Indonesia memandang bahwa: (a) Berdasarkan Undang-Undang Dasar Negara, pada saat Negara Kesatuan Republik Indonesia bersatu pada tahun 1945, pemerintah harus berperan secara tepat untuk menjamin dan mewujudkan rasa keadilan bagi seluruh masyarakat. (b) Keterlibatan Negara melalui perannya dalam penyelenggaraan perlindungan data pribadi dilakukan melalui mekanisme pengawasan DPR yang transparan dan akuntabel, sesuai dengan peraturan perundang-undangan yang berlaku. (c) Selanjutnya, diskusi mengenai masalah perlindungan data pribadi di forum internasional akan dilakukan oleh pemerintah melalui kementerian yang bertanggung jawab di bidang tata kelola data, seperti yang dilakukan di berbagai negara lainnya. (5) Pemerintah akan mengutamakan kepentingan nasional Indonesia, konsisten dalam pembahasan UU PDP, dan memperhatikan pengelolaan data pribadi untuk melindungi data pribadi warga negara, kedaulatan data, dan ketahanan nasional.

## 2. Substansi Pengaturan RUU PDP

Isi RUU Perlindungan Data Pribadi untuk perlindungan hukum memuat ketentuan mengenai hak warga negara atas datanya. Hak-hak tersebut antara lain hak untuk meminta dan memperoleh informasi mengenai kejelasan identitas, dasar kepentingan hukum, tujuan dimintanya penggunaan data pribadi, dan tanggung jawab pengguna data (dalam hal ini disebut kewenangan pengguna) Itu sudah termasuk. RUU tersebut mengatur bahwa pemilik data pribadi memiliki hak untuk menarik persetujuan atas pemrosesan data pribadi dari mereka yang telah diberikan akses untuk menggunakannya, dan bahwa pemilik data pribadi memiliki hak untuk menarik persetujuan atas pemrosesan data pribadi data dari mereka yang telah diberikan akses untuk penggunaannya, ini juga menyatakan bahwa Anda dapat menolak tindakan pembuatan profil saat menggunakan data pribadi yang dikelola oleh institusi pengguna.

Dalam konteks perlindungan data pribadi melalui RUU perlindungan data, hak hukum yang diberikan mencakup aspek manajemen data oleh entitas swasta. Jika pengelola data kependudukan berencana memberikan akses data pribadi kepada pihak ketiga seperti perusahaan swasta, persetujuan dari pemilik data diperlukan. Ini menegaskan pentingnya hak pemilik data, seperti hak untuk menolak atau menyatakan keberatan, sebagai faktor pengunci dalam menjaga keamanan data pribadi dalam pengelolaan kependudukan, terutama terkait dengan entitas komersial seperti lembaga swasta.

RUU PDP memperhitungkan hak untuk dilupakan, kecuali penerapan perlindungan data pribadi yang berkaitan dengan kepentingan pertahanan dan keamanan negara, kepentingan umum pada struktur organisasi negara, dan kepentingan pengelolaan sektor keuangan. Pengelolaan dll, uang, kerangka anggaran, kesehatan kerangka keuangan, atau nomor dimaksudkan untuk diolah untuk tujuan terukur dan penyelidikan logis terkait pengawasan pemerintah. Namun, RUU ini tidak melibatkan sistem atau batasan tertentu apa pun terkait keamanan informasi (Sinaga E.M dan M C Putri 2020).

Selanjutnya, RUU PDP tidak menawarkan dasar untuk sebuah organisasi (lembaga administratif independen) atau komisi administratif tersendiri untuk bertindak sebagai direktur, pengendali, atau pengatur keamanan informasi. Tugas ini diserahkan kepada otoritas publik sesuai bidang keahliannya, di bawah koordinasi Kementerian Komunikasi dan Informatika. Kementerian Dalam Negeri mengelola informasi individu penduduk yang teridentifikasi. OJK mempertahankan informasi identifikasi dengan uang di dekat rumah dengan mentransfernya, dan Kementerian Hukum dan Hak Asasi Manusia mengawasi informasi pribadi yang dapat diidentifikasi berdasarkan identitas, visa, dan informasi hukum lainnya. Dalam metode PDP ada empat faktor penting yang harus diperhitungkan. Pertama, disamakan dengan guncangan informasi dan keamanan informasi, bahkan informasi untuk keamanan nasional. Kedua, informasi pemilik, informasi pemilik spesifik, dan informasi eksplisit lainnya

digunakan untuk mengidentifikasinya. Yang ketiga adalah data klien, yang memerlukan konfirmasi informasi yang tepat. Keempat, penjadwalan lalu lintas data, terutama dalam hal pergerakan data lintas batas antar negara.

## **SIMPULAN**

1. Perlindungan data masih dipandang sebagai cara untuk mengamankan informasi pribadi secara legal sebagai hak privasi di Indonesia Meskipun perlindungan data pribadi belum secara khusus dicakup oleh undang-undang atau peraturan apa pun di Indonesia, Undang-undang Perlindungan Data Pribadi dibuat untuk memenuhi tanggung jawab pemerintah untuk melindungi hak-hak konstitusional warga negara Indonesia sebagaimana diuraikan dalam UUD 1945. Secara khusus, Pasal 28G ayat (1) mengatur: UU PDP khususnya mempunyai kelemahan dalam perlakuannya terhadap perlindungan data bagi anak-anak dan penyandang disabilitas yang diatur. Informasi mengenai anak-anak dan individu dengan gangguan, bagaimanapun, sering salah diterapkan. Antara lain, tidak ada Batasan usia pada kategorisasi anak dibawah umur dibawah proses “khusus” yang disebutkan dalam Undang-undang PDP. Untuk melindungi hak warga negara Indonesia atas perlindungan data, undang-undang PDP memungkinkan pemerintah untuk membentuk Lembaga kontrol data yang kuat dan independen dan menawarkan perlindungan yang ditingkatkan terhadap data milik anak-anak dan kelompok yang lebih rentan.
2. Berdasarkan peraturan yang berlaku pada saat itu rencana perlindungan data pribadi saat ini awalnya dibuat, khususnya yang disahkan dalam bentuk Undang-Undang Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi. Efektif tanggal 7 November 2016 dan efektif tanggal 1 Desember 2016. RUU PDP dinilai sangat penting dalam melindungi hak-hak masyarakat, oleh karena itu Sejak tahun 2014 RUU PDP sudah diusulkan. Mengingat RUU PDP tidak masuk dalam Rencana Legislasi Nasional (Prolegnas) 2018, maka diharapkan pembahasan RUU PDP selesai sebelum masa

jabatan DPR-RI 2014-2019 berakhir. Sejak 24 Januari 2020, RUU PDP ditandatangani Presiden Joko Widodo dan tengah dibahas di DPR. Pada Program Legislatif Nasional Prioritas DPR Tahun 2019-2024, RUU PDP diusulkan dalam program tersebut.

## **DAFTAR PUSTAKA**

- Anggraeni, SF, 2018, “Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia”, *Jurnal Hukum & Pembangunan*, Vol. 48 No. 4, 814 – 825
- Aditya Halimawan, *et al*, 2023. *Kajian Mencari Solusi Permasalahan Instrumen Hukum Perlindungan Data Pribadi di Indonesia*, Constitutional Law Society, dalam *demajusticia.org* diakses pada 24 Desember 2023, hal. 22
- Dewi, S, 2017, *Prinsip – Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya*”, *Sosiohumaniora*, Vol.19 No. 3, Hal. 206 – 212
- Elsam, *Kerentanan Perlindungan Data Pribadi dalam Pengelolaan Data Kependudukan*, URI: <https://elsam.or.id/kerentanan-perlindungan-data-pribadi-dalam-pengelolaandata-kependudukan>, 2019, Diakses pada 23 Desember 2023
- Harun Mukhtar, *Kriptografi Untuk Keamanan Data*, Penerbit Deepublish (Grup Penerbitan CV. Budi Utama), Yogyakarta, 2018, Halaman. 6
- Leski Rizkinaswara, *PSE Wajib Mengakui dan Melaporkan jika Terjadi Kebocoran Data*, diakses pada 25 Desember 2023.
- Latumahina, RE, 2014, “Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya”, *Jurnal Gema Aktualita*, Vol.3, No. 2, 11 Halaman
- Mahira, DF, Emilda Y Lisa NA, 2020, “Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept”, *Legislatif*, Vol.3 No.2, Hal.287 -302
- Mirnayanti, Judhariksawan dan Maskum, 2023. *Analisis Pengaturan Keamanan Data Pribadi di Indonesia*. *Jurnal Living Law*, Vol. 15, No. 1, 2023, Program Magister Hukum, Fakultas Hukum, Universitas Hasanuddin Makassar. 14 Halaman
- Panggabean, A. N. (2022). *Memahami Dan Mengelola Transformasi Digital*. OSF Preprints.<https://doi.org/10.31219/osf.io/s36wq>
- Rancangan Undang-undang Tentang Perlindungan Data Pribadi pasal 4-10
- Rancangan Undang-Undang Perlindungan Data Pribadi Pasal 16 ayat (1)
- Samuel A. Pangerapan, *Perkembangan Pembahasan Rancangan Undang-Undang PERLindungan Data Pribadi (RUU PDP)*, dalam *Kominfo.go.id* diakses pada 24 Desember 2023

- Saefudin. 2022. Gerakan Smart City sebagai Muara Kemajuan Transformasi Digital Indonesia. Ditjen Aptika. Retrieved Desember 23, 2023, from <https://aptika.kominfo.go.id/2023/12/gerakan-smart-city.sebagai-muara-kemajuan-transformasi-digital-indonesia>
- Sinta Dewi Rosadi dan Gerry Gumelar Pratama, Perlindungan Privasi dan Data Pribadi di Era Ekonomi Digital di Indonesia, VeJ Volume 4 Nomor 1, hlm. 99.
- Suari dan M Sarjana, 2023. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum. Fakultas Hukum Universitas Udayana. 15 halaman
- Harun Mukhtar, Kriptografi Untuk Keamanan Data, Penerbit Deepublish (Grup Penerbitan CV. Budi Utama), Yogyakarta, 2018, hal. 6
- Sinaga E.M dan M C Putri 2023. hal. 253 23 Pendapat Menteri Komunikasi dan Data

