Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 8, No. 9, September 2023

MODEL PELINDUNGAN HUKUM DATA PRIBADI DI ERA DIGITAL GUNA MENJAMIN HAK WARGA NEGARA ATAS PELINDUNGAN DATA PRIBADI

Waspiah, Noveria Sekar S, Ammirah Lies S, Tegar Islami P, Setyaning Wida N, Salisa Widyaning K
Fakultas Hukum, Universitas Negeri Semarang, Semarang, Indonesia
E-mail: waspiah@mail.unnes.ac.id, noveriasekarsulistyowati@students.unnes.ac.id, ammirahlies363@students.unnes.ac.id, tegarislami44@students.unnes.ac.id, setyaningwida@students.unnes.ac.id, salisawidya039@students.unnes.ac.id

Abstrak

Era perkembangan teknologi yang pesat mengakibatkan banyak perubahan sekaligus permasalahan baru dalam kehidupan bermasyarakat. Contohnya permasalahan pelindungan hukum data pribadi yang terjadi di Indonesia. Masalah ini menjadi suatu hal yang serius karena menyangkut hak asasi manusia sekaligus hak warga negara yang harus ditegakkan oleh pemerintah. Karena itu maka penulis mengangkat topik pelindungan hukum pribadi dalam artikel ini untuk melihat apa saja permasalahan pelindungan hukum data pribadi yang terjadi dan berusaha untuk mengetahui jawaban dari masing-masing permasalahan dengan teknik penulisan yang menggunakan metode penelitian hukum normatif-empiris serta pendekatan empiris dan perbandingan. Selain itu penulis juga menggunakan beberapa teknik pengumpulan data seperti wawancara langsung, studi lapangan, dokumen, dan diskusi terfokus dengan harapan mendapatkan hasil yang konkrit. Hasil dari penelitian ini dapat diketahui bahwa ada empat permasalahan pelindungan hukum data pribadi, yakni kasus kebocoran data pribadi yang disebabkan rendahnya tingkat keamanan siber; transparansi pemerintah terkait kasus kebocoran data pribadi; urgensi regulasi mengenai pelindungan data pribadi dalam Artificial Intelligence; dan belum terciptanya lembaga penyelenggara pelindungan data pribadi yang terintegrasi. Dimana dari empat permasalahan tersebut dapat dijawab dengan melihat perlindungan privasi sebagai antisipasi kebocoran data di Singapura; keterbukaan informasi masyarakat atas penyelenggaraan pelindungan data pribadi; model regulasi pelindungan data pribadi pada penggunaan Artificial Intelligence; dan melalui model perlindungan hukum data pribadi melalui lembaga penyelenggara yang terintegrasi.

Kata Kunci: Data Pribadi; Era Digital; Hak Warga Negara; Pelindungan Hukum

Abstract

The era of rapid technological development has resulted in many changes as well as new problems in social life. For example, the problem of legal protection of

How to cite:	Waspiah, Noveria Sekar S, Ammirah Lies S, Tegar Islami P, Setyaning Wida N, Salisa Widyaning K (2023) Model Perlindungan Hukum Data Pribadi di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi, *(8) 9,* http://dx.doi.org/10.36418/syntax-literate.v6i6
E-ISSN:	2548-1398
Published by:	Ridwan Institute

personal data that occurred in Indonesia. This problem becomes a serious matter because it involves human rights as well as citizens' rights which must be upheld by the government. Because of this, the author raises the topic of personal law protection in this article to see what are the problems of personal data legal protection that occur and try to find out the answers to each problem with writing techniques that use normative-empirical legal research methods as well as empirical and comparative approaches. The results of this study show that there are four legal protection problems for personal data, namely cases of personal data leakage caused by low levels of cyber security; government transparency regarding cases of personal data leakage; the urgency of regulation regarding the protection of personal data in Artificial Intelligence; and there has not been an integrated personal data protection organizer. Which of the four problems can be answered by looking at privacy protection in anticipation of data leaks in Singapore; disclosure of public information on the implementation of personal data protection; regulation model of personal data protection on the use of Artificial Intelligence; and through a personal data legal protection model through an integrated administering agency.

Keywords: *Personal Data; Digital Era; Citizens' Rights; Legal Protection*

Pendahuluan

Dewasa ini manusia dengan sangat mudahnya dapat menjalankan berbagai kegiatan komunikasi dan informasi tanpa adanya kendala jarak, ruang, dan waktu. Hal tersebut membuktikan bahwa saat ini manusia tidak terlepas dari kebutuhan akan teknologi yang cenderung memberikan kemudahan dalam menjalan berbagai aktivitas di berbagai bidang (Himakom, 2022). Perkembangan teknologi informasi dan komunikasi terus berlangsung dan berkembang begitu cepat dan semakin canggih menjadi salah satu munculnya era digitalisasi.

Beberapa contoh transformasi teknologi yang sudah dimanfaatkan untuk kegiatan manusia, antara lain berupa transaksi digital, aktivitas digital, hingga perusahaan digital (Danuri, 2019). Indonesia dijuluki "raksasa teknologi digital Asia yang sedang tertidur" membuktikan bahwa Indonesia adalah pasar yang besar dalam pertumbuhan pengguna *smartphone*. Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2022 terdapat kurang lebih 77 persen penduduk Indonesia sudah menggunakan internet. Hal tersebut memungkinkan masyarakat dapat memanfaatkan produk inovasi dan distruksi digital (Dewi, 2022).

Timbulnya perubahan di kehidupan manusia sekaligus juga menimbulkan permasalahan baru. Salah satu contohnya adalah permasalahan keamanan data pribadi yang seringkali terjadi bagi para pengguna teknologi digital. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Data pribadi menjadi salah satu hal yang penting untuk dijaga dengan baik, karena perlindungan data pribadi dapat menghindari ancaman pelecehan seksual, mencegah pihak tidak bertanggungjawab atas potensi pencemaran nama baik, dan memberikan hak kendali atas data pribadi.

Permasalahan keamanan data pribadi telah cukup banyak terjadi di berbagai negara, yang mana hal tersebut sudah seharusnya pemerintah juga turun tangan dan

mengatur. Pada tahun 2022 tercatat indekas keamanan siber Negara Asia Tenggara, Indonesia berada pada peringkat ke-6. Kasus kebocoran data di Indonesia bukan hanya terjadi di sebuah media sosial sosial saja, mulai dari dashboard.prakerja.go.id (17.331 data), ssso.datadik.kemendikbud.go.id (15.729 data), info.gtk.kemdikbud.go.id (10.761 data), situs djponline.go.id (10.049 data), myaspk.bkn.go.id (7.0data), daftarsscasn.bkn.go.id (6.770 data), hingga ereg.pajak.go.id (5.083 data). Keamanan siber di Indonesia apabila dibandingkan dengan negara-negara Asia Tenggara lainnya mendapatkan skor 38,96 poin.

Negara Malaysia menduduki peringkat pertama dengan skor 79,22 poin. Kemudian, disusul oleh Singapura 71,43 poin, dan Thailand 69,94 poin (Alifah, 2022). Dari data tersebut terbukti bahwa kebocoran data masih masih sering terjadi dan hal ini menunjukkan hak atas privasi sangat rentan untuk disalahgunakan, sehingga berujung pada kerugian dan dampak negatif lainnya.

Jika melihat uraian di atas, maka perlindungan data pribadi menjadi hal penting untuk diperhatikan oleh pihak pengguna atau pihak terkait, hingga dari negara. Sejatinya, perlindungan data juga termasuk hak asasi manusia yang fundamental. Bahkan terdapat beberapa negara yang telah mengakui bahwa perlindungan data menjadi hak konstitusional, yang dikenal dalam bentuk "habeas data" yang berarti seseorang memiliki hak untuk mendapatkan pengamanan atas datanya dan apabila ditemukan kesalahan atas datanya maka terdapat pembenaran.

Perlindungan data dapat memiliki keterkaitan khusus dengan privasi. Menurut Allan Westin, privasi sebagai hak indivisu, grup atau lembaga dalam menentukan akan atau tidak informasi mengenai yang bersangkutan dikomunikasikan kepada pihak lain (Niffari, 2020). Dalam perspektif Hak Asasi Manusia (HAM) internasional, perlindungan data pribadi sebagai hak privasi dituangkan dalam article 12 *Universal Declaration of Human Right* (UDHR), jaminan atas hak privasi dalam article 17 International Covenant on Civil and Political Right (ICCPR), serta dalam lingkup regional mengakui hak privasi atas data pribadi dalam article 21 ASEAN *Human Rights* Declaration tahun 2012 (Zaman, 2021).

Di Indonesia sendiri, dalam Undang-Undang Dasar 1945 tidak secara tegas dicantumkan mengenai privasi. Namun, hak privasi secara implisit terkandung dalam Pasal 28G ayat (1) yang menyatakan 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".

Pemerintah Indonesia membentuk UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik jo UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, UU Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, UU Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, dan UU Nomor 23 Tahun 2006 jo UU Nomor 24 Tahun 2013 beserta beberapa pengaturan pelaksana dibawahnya terkait aktivitas digital yang dibuat oleh Pemerintah Indonesia dimulai dari pembentukan.

Dimana dalam UU tersebut juga diatur terkait data pribadi yang dalam era digital ini dianggap sebagai suatu hal yang penting karena menyangkut privasi oleh tiap individu dalam Masyarakat. Hingga pada akhirnya pemerintah mengeluarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi atau disebut dengan UU PDP. Dalam implementasinya, UU PDP masih dihadapkan beberapa tantangan salah satunya adalah banyaknya data personal penduduk yang dikelola pemerintah untuk kebutuhan

pelayanan publik dan bagaimana menjaga keamanan data personal tersebut dengan baik masih menjadi pertanyaan (Jannah, 2022).

Undang-undang perlindungan data pribadi yang baru saja disahkan akan memberikan kepastian hukum untuk setiap warga negara Indonesia, tanpa terkecuali, berdaulat atas data pribadinya. Namun, terlepas dari pentingnya dan diperlukannya aturan ini, masih ada beberapa kelemahan yang ditenggarai akan mengancam hak warga negara atas perlindungan data dirinya dan keterbukaan terhadap informasi data pribadi. Adanya UU PDP tersebut, bukan berarti perjuangan melindungi data pribadi berakhir.

Terdapat banyak hal yang masih harus dibenahi seperti pelaksanaan dan pengawasannya. Berkaca pada Singapura yang telah mengundangkan Personal Data Protection Act (PDPA) pada tahun 2012, yang merupakan dasar hukum perlindungan data pribadi di Singapura. Selain itu, Malaysia juga memiliki regulasi perlindungan data pribadi yang diundangkan pada tahun 2010, Undang-Undang Perlindungan Data Pribadi (UU PDP 2010) (Daniswara & Rahman, 2018).

Dari beberapa regulasi yang ada di beberapa negara terbukti bahwa perlindungan data pribadi sangat penting karena apabila hingga bila kasus kebocoran data terjadi, maka akan sama saja dengan tidak dipenuhinya hak asasi manusia terlebih dalam ranah privasi ini. Oleh karena itu, sangat penting untuk memastikan data pribadi seseorang yang terkumpul digunakan sesuai dengan tujuan pengumpulan, sehingga tidak terjadi penyalahgunaan data.

Dengan demikian, penelitian ini bertujuan untuk menemukan model perlindungan hukum yang tepat terkait perlindungan data pribadi. Serta berdasarkan latar belakang di atas, maka dapat dirumuskan permasalahan sebagai berikut: 1) Bagaimana permasalahan perlindungan hukum data pribadi di era digital? 2) Bagaimana model perlindungan hukum data pribadi di era digital guna menjamin hak warga negara atas perlindungan data pribadi?

Metode Penelitian

Metode penelitian hukum normatif-empiris adalah metode yang digunakan dalam penelitian ini yang merupakan penggabungan antara hukum normatif dengan adanya penambahan unsur empiris mengenai implementasi ketentuan hukum normatif (undang-undang) yang terdapat pada setiap peristiwa hukum tertentu dalam masyarakat dan dengan menggunakan pendekatan empiris dan pendekatan perbandingan *(comparative approach).*

Penyusunan penelitian ini menggunakan beberapa sumber dan jenis data, yaitu primer, sekunder, dan tersier. Sumber Data Primer, merupakan sumber data penelitian yang diperoleh secara langsung dari sumber pertama (tanpa perantara) melalui menggunakan metode wawancara maupun metode observasi dengan subjek penelitian yakni wawancara dengan pihak terkait sebagai bahan utama serta dasar dalam mengkaji penelitian ini.

Selain itu, Sumber Data Sekunder, merupakan sumber data yang diperoleh secara tidak langsung melalui media perantara (diperoleh ataupun dicatat oleh pihak lain), berupa dokumen–dokumen, teks, naskah– naskah, dan pendapat para ahli sebagai penunjang bahan utama yang memberikan penjelasan maupun teori untuk mengkaji permasalahan penelitian ini. Serta Sumber Data Tersier yang merupakan teori-teori dan konsep yang memiliki hubungan dengan permasalahan yang dikaji sebagai acuan guna penafsiran tambahan atas bahan hukum yang lainnya.

Teknik pengumpulan data yang digunakan melalui beberapa cara, antara lain wawancara langsung, studi lapangan, dokumen, dan diskusi terfokus (*focus group discussion)*. Selain itu, dalam teknik pengolahan dilakukan beberapa langkah, seperti melakukan penelitian kembali data-data yang telah didapat dan validitas data, klasifikasi data yang kemudian disesuaikan dengan permasalahan yang ada, dan melakukan pencatatan secara sistemastis yang kemudian dituangkan ke rancangan konsep yang pada akhirnya menjadi dasar utama untuk memberikan analisis sehingga adanya kesesuian data dengan analisis yang diberikan. Dalam penelitian kualitatif ini, analisis data dilakukan pada saat pengumpulan data berlangsung, dan setelah selesai pengumpulan data dalam periode tertentu.

Hasil dan Pembahasan

A. Permasalahan Pelindungan Hukum Data Pribadi Di Era Digital

Perkembangan teknologi dan internet yang pesat membuat Indonesia memasuki era digital yang merubah pola kehidupan masyarakat secara luas. Termasuk dalam hal interaksi antar masyarakat yang tak terbatas karena munculnya sosial media (Rafiq, 2020). Hingga aktivitas masyarakat yang dilakukan menjadi lebih cepat dan efisien berkat bantuan berbagai aplikasi maupun layanan berbasis online, yang makin banyak disediakan oleh pihak swasta maupun pemerintah.

Karena itu untuk memberikan perlindungan bagi masyarakat dari permasalahan yang mungkin akan muncul karena aktivitas di era digital, maka Pemerintah Indonesia membuat beberapa pengaturan seperti undang-undang yang diharapkan dapat mencegah permasalahan yang dapat terjadi.

1. Kasus Kebocoran Data Pribadi Yang disebabkan Masih Rendahnya Tingkat Keamanan Siber

Seiring dengan pembuatan beberapa pengaturan terkait pelindungan data pribadi yang dimaksudkan untuk menjaga serta melindungi data pribadi masyarakat, ternyata masih terdapat beberapa permasalahan yang kerap terjadi. Hal ini terbukti dari data Perusahaan Siber asal Belanda Surfshark, yang menyatakan bahwa Indonesia adalah negara dengan peringkat ke-3 kasus kebocoran data terbanyak pada kuartal III 2022. Dimana sebelum peringkat ini dirilis, menurut data dari Perusahaan Surfshark juga, Indonesia mengalami kenaikan sebesar 143% kasus kebocoran data pada kuartal II 2022 yakni dari sebelumnya 430,1 ribu akun yang mengalami kebocoran menjadi 1,04 juta akun yang mengalami kebocoran data (Dihni, 2022).

Padahal terjadinya kasus kebocoran data merupakan bentuk pelanggaran terhadap hak asasi manusia yakni perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasannya yang landasan hukumnya terdapat pada pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Permasalahan kebocoran data pribadi sering terjadi dikarenakan angka pengguna internet yang makin banyak tiap tahunnya, namun tidak dibarengi dengan tingkat keamanan siber yang kuat (Silalahi & Chairina, 2023). Dimana tingkat keamanan siber bila ditinjau dari sudut pandang hukum dapat dilihat pada faktor undang-undang, penegak hukum, serta sarana dan fasilitasnya. Dibutuhkan undang-undang maupun pengaturan

yang kuat dalam penanganan maupun pembentukan sistem keamanan siber yang dalam pelaksanaaannya dibutuhkan kontrol, koordinasi, dan pengawasan secara strategis dan efektif oleh penegak hukum yang ditunjuk sesuai dengan pengaturan yang berlaku.

Yang mana menurut Peraturan Presiden Nomor 53 Tahun 2017 Tentang Pembentukan Badan Siber dan Sandi Negara menegaskan bahwa tugas dari keamanan sistem informasi dipindahkan dari kominfo ke BSSN. Kemudian terkait penegak hukum selain dipegang oleh BSSN maupun Kominfo juga dapat dilakukan oleh tim maupun lembaga khusus seperti tim *siber* Polri (Chesterman, 2014).

Lalu yang terakhir terkait sarana dan fasilitas dari pencegahan kebocoran data pribadi, maka akan kembali lagi seperti diawal yakni terkait hubungan dari undang-undang maupun pengaturan yang berlaku serta peranan dari penegak hukum untuk dapat melaksanaan sesuai dengan aturan kemudian juga didukungdengan beberapa hal sebagai sarana maupun fasilitas yang dapat mewujudkan target pelindungan data pribadi terkait kebocoran data yang erat kaitannya dengan keamanan siber.

2. Transparansi Pemerintah Terkait Kasus Kebocoran Data Pribadi

Kasus kebocoran data yang terjadi di Indonesia juga tidak berhenti pada keamanan *siber* nya saja, namun juga berkaitan erat dengan transparansi dari pihak pemerintah selaku pembuat kebijakan dari pelindungan data pribadi masyarakat. Dapat diketahui bahwa selama awal tahun 2023, terjadi kurang lebih empat kasus kebocoran data (CNNIndonesia, 2022). Kasus pertama yakni kasus Bjorka yang menghebohkan masyarakat dari akhir tahun 2022 yang pada Maret 2023 juga menyatakan bahwa terjadi pencurian data pribadi dari BPJS Ketenagakerjaan sebanyak 19,5 juta data.

Dalam kasus tersebut pada akhirnya Deputi Bidang Komunikasi BPJS Ketenagakerjaan menyatakan bahwa pihak BPJS Ketenagakerjaan turut melakukan investigasi bersama dengan BSSN dan Kominfo, dengan hasil investigasi yang menyatakan bahwa dugaan sementara sumber kebocoran data tersebut bukan berasal dari BPJS Ketenagakerjaan.

Kasus kedua yakni pencurian data Bank Syariah Indonesia (BSI) yang terjadi pada bulan Mei 2023, dengan total kebocoran data sebanyak 1,5 TB, termasuk 15 juta data pengguna dan password untuk akses internal dan layanannya, data pribadi nasabah, dan informasi pinjaman. Yang ditanggapi oleh *Corporate Secretary* BSI bahwa data nasabah aman dan pihak BSI akan bekerjasama dengan otoritas dengan isu kebocoran data. Kasus ketiga yakni pencurian data paspor WNI sebanyak 34.900.867 pada Juli 2023. Dimana sempat dibantah oleh Direktur Jenderal Imigrasi Kemenkumham, namun pada akhirnya menyatakan bahwa kebocoran data itu terjadi pada Januari 2022.

Kasus keempat adalah pencurian data Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kementerian Dalam Negeri sebanyak 337 juta data yang bocor itu terdiri dari nama, Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (KK), tanggal lahir, alamat, nama ayah, nama ibu, NIK ibu, nomor akta lahir, nomor akta nikah dan lainnya. Yang pada akhirnya Dirjen Dukcapil Kemendagri menyatakan bahwa data yang bocor bukan merupakan data yang sama dengan milik lembaganya.

Sehingga berdasarkan keempat kasus tersebut dapat disimpulkan bahwa semua kasus tidak diakui atau dibantah oleh pemerintah sehingga mengakibatkan masyarakat bertanya-tanya apakah memang kasus kebocoran data yang terjadi hanya bualan saja atau benar-benar terjadi namun disembunyikan hasilnya karena bila memang terjadi kasus kebocoran data yang besar akan membuat kehebohan bahkan aksi protes pada masyarakat.

Apalagi dengan diberitakannya kasus-kasus tersebut pada banyak media sehingga masyarakat pun juga mendesak pemerintah untuk memberikan penjelasan yang pasti terkait bagaimana kronologi kasus kebocoran data, penyelidikan, hingga hasil akhir yang dapat dipertanggungjawabkan.

3. Urgensi Regulasi Mengenai Pelindungan Data Pribadi dalam Artificial Intelligence

Pesatnya teknologi saat ini yang telah mencapai fase industry 4.0 yang menggunakan komunikasi serba digital telah menemukan terobosan baru bernama AI atau Artificial Intelligence. AI adalah salah satu cabang ilmu komputer sains yang mempunyai kemampuan layaknya seorang manusia dalam penalaran, pembelajaran, perencanaan, kreativitas, dan analisis dalam bentuk kapasitas mesin (Disemadi, 2021). Beberapa manfaat yang diberikan oleh AI dalam membantu kehidupan sehari-hari adalah menyelesaikan masalah yang sulit diselesaikan secara konvensional, merangkum dan menginterpretasi informasi yang berlebihan, membantu melaksanakan pencarian data yang dengan jumlah yang sangat besar, dan dapat menjadi pengaman dengan jejak digital.

Namun, semakin canggihnya teknologi AI juga dapat menjadi boomerang bagi manusia seperti yang diucapkan oleh Guru Besar UGM, Prof. DR. Ir. Ridi Ferdiana, S.T., M.T., IPM., bahwa AI dapat menjadi bahaya ketika ada orang pintar yang paham dan dapat membuat varian baru AI yang menyalahi etika terkait privasi seperti perubahan muka dan data pribadi lainnya (Ekaptiningrum, 2023). UU PDP menjelaskan mengenai jenis data pribadi, hak pemilik data pribadi, pemrosesan data pribadi, kewajiban pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi, pemindahan data pribadi, sanksi administratif, larangan dalam penggunaan data pribadi, pembentukan pedoman perilaku pengendali data pribadi, penyelesaian sengketa dan hukum acara, Kerjasama internasional, peran pemerintah dan Masyarakat, serta ketentuan pidananya.

Dalam praktik dan pelaksanaannya, UU PDP memang dapat memberikan payung hukum bagi seseorang yang melanggar ketentuan mengenai data pribadi. Namun terdapat kelemahan UU PDP jika disandingkan dalam AI yang saat ini dan masa yang akan datang digunakan. Kelemahan yang terjadi adalah belum diaturnya regulasi mengenai AI terlebih lagi yang menjadi kunci tersimpannya data pribadi. Aplikasi maupun mesin yang menggunakan kecerdasan buatan AI harus memiliki izin dan penetapan dibawah lindungan hukum agar dapat dimintai pertanggung jawaban atas segala risiko yang akan terjadi, selain itu regulasi sangat diperlukan di kemudian hari sebagai rujukan dan pedoman yang lebih jelas.

Tak hanya sebagai rujukan dan pedoman regulasi tersebut juga sebagai asas legalitas dalam penyelesaian sengketa pelindungan data pribadi di ranah pengadilan pidana, perdata, maupun yang lainnya(Butarbutar, 2012). Oleh karenanya diperlukan regulasi tambahan guna memperjelas payung hukum sesuai kedinamisan teknologi saat ini.

3. Belum Terciptanya Lembaga Penyelenggara Pelindungan Data Pribadi yang terintegrasi

Sejak diundangkannya UU PDP pada tanggal 17 Oktober 2022 dan beradaptasi untuk diterapkan, terdapat suatu ketentuan yang terdapat dalam pasal 58-61 mengenai kelembagaan(Indonesia, 2022). Saat ini belum ada realisasi dari pasal tersebut, dari pasal tersebut juga belum menjelaskan secara lebih lanjut mengenai lembaga penyelenggara data pribadi. Alasan hingga saat ini belum terbentuknya lembaga penyelenggara

pelindungan data pribadi adalah belum ditemukannya titik temu, karena banyak lembaga yang didirikan oleh berbagai regulasi perundang-undangan tidak bekerja semaksimal mungkin, bahkan Presiden Joko Widodo membubarkan bebeapa lembaga negara yang diatur oleh PP atau Perpres seperti Dewan Buku Nasional, Komisi Hukum Nasional, Dewan Gula Nasional, dll (Doly, 2021).

Pembentukan lembaga penyelenggara pelindungan data pribadi sangat penting dilakukan karena dapat menjadi lembaga yang memastikan pelindungan data pribadi, kepatuhan pengendali dan prosesor data pribadi, baik itu secara individu, badan privat, ataupun lembaga publik terhadap UU PDP dan UU lainnya yang berkaitan dengan pelindungan data pribadi. Lembaga penyelenggara pelindungan data pribadi harus didirikan secara independent agar tidak terjadi konflik kepentingan (Doly, 2021).

Jimly Asshiddiqie menyatakan bahwa dibentuknya lembaga independent di Indonesia karena lembaga negara yang telah ada belum dapat menjadi solusi untuk menyelesaikan permasalahan yang ada. Selain itu lembaga negara independent juga dibentuk atas ketidakpercayaan publik terhadap lembaga negara yang sudah ada. Sama dengan halnya lembaga atau badan pemerintahan lain seperti kominfo yang dirasa kurang tanggap dan bisa untuk mengatasi masalah pelindungan data pribadi.

Pembentukan lembaga penyelenggara pelindungan data pribadi sebagai lembaga negera independent sudah memenuhi kriteria yang disebutkan oleh Jimly Asshiddiqie yakni, pertama tidak adanya kredibilitas lembaga negara yang mampu melakukan pelindungan data pribadi yang dibuktikan dengan masih banyaknya kasus kebocoran dan pencurian data di Indonesia. Kedua, tidak independentnya lembaga negara karena berada dibawah pengaruh kekuasaan pemerintah seperti kementerian komunikasi dan informasi yang dikhawatirkan adanya potensi konflik kepentingan.

Ketiga, adanya pengaruh secara global karena banyak dari negara-negara lain yang membentuk lembaga penyelenggara pelindungan data pribadi secara independent. Alasan yang menjadi pentingnya untuk dibentuk adalah guna memastikan aturan UU PDP, menegakkan dan mengawasi hukum pelindungan data pribadi yang masih lemah, dan masih kurangnya kesadaran Masyarakat akan pelindungan data pribadi jadi lembaga penyelenggara pelindungan data pribadi penting segera mungkin dibentuk melihat dari urgensi yang dibawanya melalui undang-undang.

B. Model Pelindungan Hukum Data Pribadi Di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi

1. Pelindungan Privasi Sebagai Antisipasi Kebocoran Data di Singapura

Singapura menjadi negara yang cukup memberikan perlindungan data pribadi dengan baik. Perlindungan data pribadi di negara ini diatur dalam Singapore’s Personal Data Protection Act 2012 (PDPA 2012) dan telah berlaku sejak tahun 2014 yang kemudian dijalankan oleh Personal Data Protection Commission Singapore (Setiawati, Hakim, & Yoga, 2020). Melalui pembentukan PDPA, pengalaman Singapura menjadi menarik setidaknya karena tiga alas an (Chesterman, 2014) Pertama, PDPA dirancang untuk populasi yang sangat terhubung antar warga dan negara dan PDPA dapat beradaptasi dengan perubahan teknologi sehingga menjadi model undang-undang yang efektif saat ini.

Kedua, memiliki tujuan legislasi yang berbeda dengan yurisdiksi negara lain, jika Uni Eropa ("UE") telah lama melakukan pendekatan terhadap perlindungan data melalui lensa hak asasi manusia secara umum dan hak privasi secara khusus, PDPA secara

eksplisit berusaha untuk menyeimbangkan antara kebutuhan bisnis yang sah dan hak-hak individu. Ketiga, lingkungan politik Singapura yang unik dan sifat hubungan antara pemerintah dan yang diperintah.

Di Singapura pada esensinya setiap institusi yang mengolah data pribadi, wajib untuk memberitahu kepada seseorang untuk mengumpulkan data pribadi dan memperoleh persetujuan orang tersebut sebelum pengumpulan, penggunaan, dan pengungkapan data pribadi seseorang tersebut. Dalam hal seseorang bersedia untuk memberikan data pribadinya untuk maksud tertentu, orang tersebut dapat juga memperbolehkan organisasi untuk mengumpulkan, menggunakan, serta mengungkapkan data pribadinya (Sugeng, 2020).

Privasi adalah suatu hak setiap orang untuk menikmati hidup dan menuntut privasinya untuk dilindungi (Rosadi, 2015). Hak privasi telah berkembang sehingga dapat digunakan untuk merumuskan hak untuk melindungi data pribadi (Priliasari, 2019). Penting untuk dicatat bahwa sebagian besar negara ASEAN memiliki privasi sebagai hak konstitusional-biasanya menjadi dasar hukum untuk memberlakukan undang-undang perlindungan data.

Akhirnya, sebagai sebuah kolektif, ASEAN mengadopsi deklarasi regional pertamanya tentang privasi melalui Deklarasi Hak Asasi Manusia tahun 2012. Pasal 21 dari instrumen tersebut menyatakan bahwa "Setiap orang berhak untuk bebas dari campur tangan sewenang-wenang terhadap privasi, keluarga, rumah, atau korespondensi, termasuk data pribadi, atau serangan terhadap kehormatan dan reputasi orang tersebut. Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan semacam itu".

Dalam klausul peraturan The Personal Data Protection Act No. 26 of 2012 Singapore (PDPA 2012). disebutkan bahwa Undang-Undang ini digunakan untuk mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi, dan untuk menetapkan Daftar Jangan Panggil dan mengatur administrasinya, serta hal-hal yang terkait dengannya. Hal ini merupakan suatu bentuk representasi perlindungan privasi.

Pada *section* 5 aturan tersebut mengenal badan yang khusus menangani privasi dalam bentuk perlindungan data pribadi yaitu Personal Data Protection Commission and Administration (PDPCA). Lembaga ini dibentuk khusus oleh Menteri dengan jumlah komisioner sebanyak tiga orang dengan maksimal tujuh belas orang. Berdasarkan *section* 6, PDPCA memiliki fungsi yaitu: 1) Mendorong kesadaran mengenai perlindungan data di Singapura; 2) Melakukan konsultasi, pendampingan hukum, administrasi, atau sejumlah pelayanan terkait dengan perlindungan data; 3) Memberikan saran kepada pengambil kebijakan terhadap setiap permasalahan yang berhubungan dengan perlindungan data; 4) Representasi Pemerintah di luar negeri yang berhubungan dengan perlindungan data pribadi; a) Melaksanakan riset, edukasi, dan mendorong aktivitas pemahaman yang berhubungan dengan perlindungan data pribadi seperti seminar, workshop, dan lokakarya terkait dengan perlindungan data pribadi dengan melibatkan lembaga lainnya; b) Berbagi informasi yang berhubungan dengan perlindungan data peribadi bersama lembaga atau organisasi lainnya; c) Menjalankan regulasi yang berkaitan dengan perlindungan data pribadi; d) Memberikan penegasan terkait fungsi atau kewenangan terhadap badan yang tercantum dalam regulasi lainnya; dan e) Terlibat dalam sejumlah aktivitas lainnya serta menjalankan tugasnya mewakili Menteri.

Sebagai model perlindungan, perlindungan privasi oleh regulasi ini juga mengenal Prinsip *Reasonableness.* Suatu organisasi dapat mengumpulkan, menggunakan atau

mengumumkan data pribadi seseorang apabila ia melakukannya dengan tujuan yang pantas dan beralasan (Setyawati Fitri Anggraeni, 2018). PDPA mengakui hak pribadi untuk melindungi data pribadi miliknya, termasuk hak untuk mengakses dan membenarkan, juga kebutuhan suatu organisasi untuk mengumpulkan, menggunakan data pribadi untuk maksud tertentu.

PDPA 2012 yang dimiliki Singapura juga mengatur mengenai sanksi baik denda maupun pidana yaitu dengan denda sampai USD 790.000 dan/atau sanksi pidana penjara sampai dengan 3 (tiga) tahun (Muin, 2023). Selain itu dalam aturan Singapura, dalam hal seseorang bersedia untuk memberikan data pribadinya untuk maksud tertentu, orang tersebut juga dapat memperbolehkan organisasi untuk mengumpulkan, menggunakan, serta mengungkapkan data pribadinya. Peraturan mengakui konsep "*deemed consent*", atau persetujuan yang diberikan secara diam-diam untuk digunakan untuk maksud dan tujuan tertentu (Setyawati Fitri Anggraeni, 2018).

2. Keterbukaan Informasi Masyarakat Atas Penyelenggaraan Pelindungan Data Pribadi

Keterbukaan dan transparansi informasi akan mampu meningkatkan kepercayaan masyarakat atau stakeholder meningkat dan pada akhirnya partisipasi stakeholder dam masyarakat meningkat. Undang-undang Keterbukaan Informasi Publik ini memberikat kebebasan masyarakat untuk mengakses informasi yang seluas-luasnya kepada masyarakat baik mengenai kebijakan Pemerintah atau Badan Publik maupun penyelenggaraan pemerintahan (Surianto, 2023). Melalui keterbukaan informasi diharapkan dapat mewujudkan kegiatan politik yang bersih, santun dan mengedepankan kepentingan publik/masyarakat karena aspek yang menjadi landasan bagi pemerintah dalam mengeluarkan kebijakan semua dapat diketahui dan laporannya transparan kepada Masyarakat (Nurdiansyah, 2016).

Pada dasarnya, salah satu elemen penting dalam era demokrasi dewasa ini berkaitan dengan penyelenggaraan pemerintah adalah hak publik (masyarakat) untuk memperoleh informasi sesuai dengan ketentuan perundang-undangan. Kebebasan dan kemudahan untuk memperoleh informasi adalah sebagai sarana kehidupan berdemokrasi (Kristiyanto, 2016). Hak atas informasi teresebut menjadi sangat penting agar masyarakat dapat melakukan pengawasan secara lebih efektif dan effisien berkaiatan dengan proses pelayanan publik dan akuntabilitas pemerintah dalam melaksanakan tugas-tugas pelayanan publik bagi masyarakat itu sendiri.

Kondisi yang demikian itu pula diharapkan dapat meningkatkan partisipasi masyarakat untuk ikut terlibat secara aktif dalam proses pengambilan keputusan publik dalam penyelenggaraan pemerintahan. Oleh karena itu partisipasi masyarakat tersebut haruslah didukung oleh askes informasi, transparasi dan akuntabilitas penyelenggara pemerintahan di daerah dengan memberikan jaminan atas keterbukaan informasi publik. Untuk menyongsong sebuah masyarakat yang demokratis memerlukan dukungan perangkat hukum dan kontrol masyarakat terhadap penyelenggara negara.

Salah satu cara memperkuat kontrol masyarakat itu adalah dengan adanya jaminan untuk memperoleh informasi trantra (Fadjar Trisakti, Adnin Dikeu Dewi Berliana, Al Bukhori, & Alya Fitr, 2022). Berdasarkan hal inilah, penting kiranya untuk dapat memberikan suatu bentuk perlindungan hukum berupa transparansi penyelenggaraan data pribadi.

3. Model Regulasi Pelindungan Data Pribadi Pada Penggunaan *Artificial Intelligence*

Kementerian Komunikasi dan Informatika bekerja sama dengan gerakan Siberkreasi dalam meningkatkan literasi dan sosialisasi kepada masyarakat sebagai upaya dalam menangani dampak negatif dari penggunaan artificial intelligence di Indonesia saat ini, akan tetapi nyatanya upaya tersebut tidak dapat mengurangi permasalahan penggunaan artificial intelligence yang kian tak terkendali. Hal ini disebabkan karna Indonesia belum memiliki kerangka strategi regulasi sebagaimana yang telah diterapkan oleh negara Malaysia dan Singapura.

Pemerintah malaysia ditahun 2020 telah menetapkan suatu kebijakan yang diberi nama Strategi Keamanan Siber Malaysia (MCSS) 2020-2024. Strategi keamanan ini memuat setidaknya lima pilar strategis yang akan mengatur seluruh aspek pengelolaan serta penerapan dari keamanan siber di Malaysia yang berakhir pada tahun 2024 (MANAGEMENT, 2021). Lima pilar tersebut mencakup tata kelola dan manajemen yang efektif bagi instansi terkait, penguatan kerangka legislatif dan penegakan hukum, mengkatalisasi inovasi, teknologi, penelitian dan pengembangan kelas dunia dan industri, peningkatan kapasitas dan kapabilitas, kesadaran dan pendidikan guna meningkatkan kesadaran masyarakat malaysia mengenai pentingnya menjaga keamanan data pribadi masing-masing, serta memperkuat kolaborasi global dengan bekerjasama dengan negara internasional yang memiliki keamanan siber diatas negara malaysia.

Pemerintah malaysia memiliki suatu klinik khusus yang bertugas dalam menangani penyelenggaraan serta pemulihan keamanan dari penggunaan artificial intelligence dan cara memitigasi ancaman online yang diberi nama Klinik MyCyberSecurity dan CyberSAFE Malaysia (Freedomhouse, 2021). Meskipun demikian hingga saat ini belum ada regulasi khusus yang diterapkan negara Malaysia mengenai penggunaan artificial intelligence.

Hal ini disampaikan langsung oleh Menteri Komunikasi dan Digital Fahmi Fadzil pada program Hari Sektor Publik Malaysia 2023. Adanya kemajuan infrastruktur negara Singapura membuatnya mampu mengatasi masalah penggunaan artificial intelligence. Guna menyesuaikan antara kepentingan pertumbuhan bisnis dengan regulasi, singapura menerapkan suatu strategi penggunaan artificial intelligence secara skalabilitas sehingga diharapkan dapat berdampak positif pada berbagai sektor di tahun 2030 mendatang.

Perlindungan terhadap data perusahaan pengguna artificial intelligence telah diatur dalam Singapore Academy of Law yang memuat pengawasan terhadap seluruh undang-undang yang berlaku pada sistem artificial intelligence serta menangani permasalahan yang berdampak pada industri artificial intelligence (Yu, 2023). Selain itu Otoritas Pengembangan Media Info-Komunikasi dan Komisi Perlindungan Data Pribadi Singapura telah bekerjasama dengan vendor cloud AS untuk menciptakan suatu AI Government Cloud Cluster yang digunakan untuk mengetahui berbagai permasalahan yang akan muncul selama penggunaan artificial intelligence generatif melalui penggunaan aplikasi yang diberi nama Dua sandbox (Chua, 2022).

4. Model Pelindungan Hukum Data Pribadi Melalui Lembaga Penyelenggara Yang Terinterasi

Kasus mengenai kebocoran data pribadi di Indonesia setiap tahunnya kian mengkhawatirkan. Berbagai upaya telah dilakukan oleh pemerintah Indonesia dalam menekan laju kasus penyalahgunaan data pribadi tersebut, salah satunya yaitu dengan

mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pada tanggal 20 September 2022.

Sebagaimana yang tersirat dalam pasal 58 ayat 2 dijelaskan bahwa pengendalian perlindungan data pribadi dilaksanakan oleh otoritas lembaga penyelenggara perlindungan data pribadi. Namun saat ini lembaga penyelenggara perlindungan data pribadi tersebut belum terbentuk secara spesifik, sehingga berdasarkan Peraturan Presiden Nomor 22 Tahun 2023 penanganan kasus kebocoran data pribadi dilimpahkan kepada Kementerian Komunikasi dan Informatika (Yudistira, 2023).

Di Singapura, dikenal lembaga bernama Personal Data Protection Comission (PDPC) yang beroperasi sejak tahun 2013 melalui PDPA. Secara umum fungsi lembaga ini yakni melakukan sosialisasi mengenai pengumpulan maupun penggunaan data, standarisasi kebijakan, dan penyelesaian masalah perlindungan data pribadi (Annur, 2019).

Peran PDPC secara khusus dijelaskan dalam section 7 PDPA (Chik, 2013) PDPC memiliki peran sebagai berikut: a) Melaksanakan wewenang untuk menyelidiki atau melakukan penyelidikan (pengawasan kepatuhan dan investigasi), wewenang untuk meninjau dan memberikan arahan (misalnya, penerbitan perintah perbaikan) dan wewenang untuk melakukan penegakan hukum (untuk memberikan kekuatan pada prinsip akuntabilitas). b) Memberikan panduan dan layanan audit (untuk kelembagaan) penerbitan pedoman dan panduan seperti konsep persetujuan, kewajaran dan kebutuhan. c) Melakukan upaya sosialisasi dan kesadaran tentang data pribadi dan privasi (untuk organisasi dan juga untuk masyarakat luas).

Kesimpulan

Kesimpulan dari penelitian ini adalah era perkembangan teknologi digital yang pesat mengakibatkan banyak perubahan sekaligus permasalahan baru dalam kehidupan bermasyarakat. Contohnya permasalahan data pribadi yang kerap terjadi karena aktivitas masyarakat yang berhubungan dengan teknologi digital. Mudahnya mengakses data secara daring dan lemahnya perlindungan data pribadi menjadikan permasalahan ini kerap terjadi dan membuat Pemerintah Indonesia akhirnya membuat pengaturan terkait data pribadi lewat Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi atau yang disebut UU PDP.

Namun sayang walau UU PDP sudah disahkan, masih kerap terjadi kasus pelanggaran data pribadi. Baik kasus yang terjadi dalam ranah privat hingga publik seperti kasus kebocoran data pelanggan lewat layanan aplikasi dan website. Selain itu juga masih terdapat beberapa pengaturan lain yang mengatur terkait perlindungan data pribadi di samping UU PDP yang dapat menimbulkan tumpang tindihnya pengaturan.

Dengan masih maraknya kasus kebocoran data dan terdapat kelemahan dalam UU PDP maka seharusnya dapat ditemukan bentuk model perlindungan terkait data pribadi khususnya untuk melindungi sekaligus menjamin hak warga negara atas perlindungan data pribadi. Perlindungan data pribadi di Indonesia sejatinya ada, akan tetapi tidak memberikan kepastian yang begitu jelas dalam memberikan perlindungan kepada masyarakat.

Bahkan regulasi mengenai data pribadi saat ini belum memiliki peraturan pelaksana serta lembaga penyelenggara khusus dibidang pengelolaan kasus kebocoran

data pribadi. Selain perlindungan yang belum dapat terpenuhi secara menyeluruh terdapat juga kelemahan lain dalam memberikan jaminan pemulihan bagi korban yang hak privasinya dilanggar. Berbeda halnya dengan Undang-Undang Perlindungan Data Pribadi Malaysia dan Singapura yang telah mengatur mengenai perlindungan data pribadi masyarakatnya dengan memberikan pilihan, pengelolaan, dan batasan terhadap data pribadi yang dikelolanya.

Bahkan dalam memberikan sanksi kepada para pelanggar data pribadi di Malaysia dan Singapura terbilang cukup tegas dan disiplin baik dalam penerapan sanksi perdata maupun sanksi pidana. Sedangkan di Indonesia dalam memberikan sanksi kepada para pelanggar data pribadi hanya berupa sanksi administratif dan sanksi pidana secara terbatas. Oleh karena itu, saat ini perlindungan data pribadi di Indonesia menjadi suatu kebutuhan yang sangat mendesak terlebih lagi dengan semakin berkembangnya teknologi informasi. Indonesia perlu segera membuat strategi khusus dalam menangani berbagai permasalahan terkait dengan kasus kebocoran data salah satunya melalui pengadopsian desain model perlindungan data pribadi dari negara Malaysia dan Singapura.

BIBLIOGRAPHY

Alifah, N. N. (2022). Keamanan Siber Negara Asia Tenggara 2022, Indonesia Peringkat Berapa? Retrieved August 16, 2023, from Good Stats website: https://goodstats.id/article/keamanan-siber-negara-asia-tenggara-2022-indonesia-peringkat-berapa-3RLgv

Annur, C. M. (2019). Contoh Singapura, Kominfo Akan Bentuk Komisi Perlindungan Data Pribadi.

Chesterman, S. (2014). Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected Alifah, N. N. (2022). Keamanan Siber Negara Asia Tenggara 2022, Indonesia Peringkat Berapa? Retrieved August 16, 2023, from Good Stats website: https://goodstats.id/article/keamanan-siber-negara-asia-tenggara-2022-indonesia-peringkat-berapa-3RLgv

Annur, C. M. (2019). Contoh Singapura, Kominfo Akan Bentuk Komisi Perlindungan Data Pribadi.

Chesterman, S. (2014). Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World (Introduction). *Academy Publishing.*, 3.

Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. . . *In Computer Law & Security Review*, *29*(5), 554–575. https://doi.org/10.26858/jiap.v7i2.4954

CNNIndonesia. (2022). *4 Kasus Kebocoran Data di Semester I 2023, Mayoritas Dibantah* (pp. 1–2). pp. 1–2.

Daniswara, F., & Rahman, F. (2018). Perlindungan Data Pribadi: Studi Komparasi terhadap Praktik di Singapura, Amerika Serikat, dan Malaysia. *Center For Digital*

Society, *31*, 24.

Danuri, M. (2019). Development and transformation of digital technology. *Infokam*, *XV*(II), 116–123.

Dewi, I. R. (2022). Data Terbaru! Berapa Pengguna Internet Indonesia 2022? Retrieved August 15, 2023, from CNBC Indonesia website: https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022

Dihni, V. A. (2022). Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022.

Fadjar Trisakti, Adnin Dikeu Dewi Berliana, Al Bukhori, & Alya Fitr. (2022). Transparansi Dan Kepentingan Umum. *Jurnal Dialektika: Jurnal Ilmu Sosial*, *19*(1), 29–38. https://doi.org/10.54783/dialektika.v19i1.61

Himakom. (2022). Perlindungan Data Pribadi di Era Digital. Retrieved August 16, 2023, from http://himakom.student.uny.ac.id/perlindungan-data-pribadi-di-era-digital/

Jannah, L. M. (2022). UU Perlindungan Data Pribadi dan Tantangan Implementasinya. Retrieved August 16, 2023, from Fakultas Ilmu Administrasi Universitas Indonesia website: https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

Kristiyanto, E. N. (2016). Urgensi Keterbukaan Informasi Dalam Penyelenggaraan Pelayanan Publik. *Jurnal Penelitian Hukum DE JURE*, *16*(2), 231–244.

Muin, I. (2023). *Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia*. *1*(2), 81–91.

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Nurdiansyah, E. (2016). KETERBUKAAN INFORMASI PUBLIK SEBAGAI UPAYA MEWUJUDKAN TRANSPARANSI BAGI MASYARAKAT. *Jurnal Bhinneka Tunggal Ika*, *3*(2), 147–151. Retrieved from https://ejournal.unsri.ac.id/index.php/jbti/article/view/4593/pdf

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending). *Majalah Hukum Nasional*, (2), 1–27. https://doi.org/10.24843/jmhu.2017.v06.i03.p03

Rafiq, A. (2020). Dampak Media Sosial Terhadap Perubahan Sosial Suatu Masyarakat. *Global Komunika*, *1*(1), 18–29.

Rosadi, S. D. (2015). *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan NasionalMetode Penelitian*. Jakarta: Refika Aditama.

Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2), 2–9. https://doi.org/10.18196/iclr.2219

Setyawati Fitri Anggraeni. (2018). Polemik pengaturan kepemilikan data pribadi: urgensi untuk harmonisasi dan reformasi hukum di indonesia. *Jurnal Hukum & Pembangunan*, *48*(4), 814 – 825.

Silalahi, P. R., & Chairina. (2023). *Ekonomi Digital: Perkembangan Bisnis Digital, Pemasaran Digital, Ecommerce, Fintech Berbasis Syariah, dan Homoislamicus dalam Perilaku Konsumen*. Medan: Merdeka Kreasi Group.

Sugeng. (2020). *Hukum Telematika*. Jakarta: Prenadamedia Group.

Surianto. (2023). Dampak Positif Dan Negatif UU KIP Bagi Pemerintah Dan Masyarakat.

Zaman, M. N. U. (2021). Perlindungan Data Pribadi: Hak Privasi Menurut Perspektif Hak Asasi Manusia. Retrieved August 16, 2023, from Heylaw Edu website: https://heylaw.id/blog/hak-privasi-menurut-perspektif-hak-asasi-manusia

Copyright holder:
Waspiah, Noveria Sekar S, Ammirah Lies S, Tegar Islami P, Setyaning Wida N, Salisa Widyaning K (2023)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under: