Jurnal Multidisiplin Indonesia
Journal homepage: https://jmi.rivierapublishing.id/
ISSN 2963-2900 E-ISSN 2964-9048

TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DARI ASPEK PENGAMANAN DATA DAN KEAMANAN SIBER

Cindy Vania[1], Markoni[2], Horadin Saragih[3], Joko Widarto[4]
Universitas Esa Unggul, Jakarta, Indonesia
cindyvanialie1974@gmail.com[1], sh.markoni@gmail.com[2], joko.widarto@esaunggul.ac.id[3], horadin.saragih@esaunggul.ac.id[4]

Riwayat Artikel:
Received: 11-03-2023
Revised: 21-03-2023
Accepted: 31-03-2023

Keywords: *personal data protection, data security, cyber security*

Kata Kunci: perlindungan data pribadi, pengamanan data, keamanan siber

Abstract
The era of digitalization, the development of information technology, as well as cases of misuse of personal data including data leaks in Indonesia which are increasing has made the government realize that legal protection is needed which can provide legal certainty regarding the protection of personal data. Legal protection in the form of personal data protection regulations is equivalent to the law which also serves as a guideline for organizations, especially controllers of personal data and processors of personal data and the public to manage their personal data. Indonesia now officially has a Personal Data Protection Law, namely Law No. 27 of 2022 Concerning Personal Data Protection. Protection of personal data is closely related to data security and cybersecurity. In relation to cyber security, Indonesia already has various regulations such as the Law on Information and Electronic Transactions, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Minister of Communication and Informatics Regulation Number 20 of 2016 concerning Protection of Personal Data in the System Electronics to other sectoral regulations that regulate the obligations of cyber security organizations, including data security. In implementing the Personal Data Protection Law, it is still necessary to appoint an authorized institution to regulate personal data protection appointed by the government, along with derivative regulations from the Personal Data Protection Law. Organizations may also work with third parties (consultants) in developing cybersecurity programs including personal data protection in order to comply with the requirements of personal data protection regulations.

Abstrak
Era digitalisasi, perkembangan informasi teknologi, dan juga kasus penyalahgunaan data pribadi termasuk kebocoran data di Indonesia yang kian meningkat membuat pemerintah menyadari bahwa diperlukan perlindungan hukum yang dapat memberikan kepastian hukum terkait perlindungan data pribadi. Perlindungan hukum berupa peraturan perlindungan data pribadi setara dengan Undang-Undang yang turut menjadi pedoman bagi organisasi khususnya

pengendali data pribadi dan prosesor data pribadi serta masyarakat untuk mengelola data pribadi yang dimiliki. Indonesia kini telah resmi memiliki Undang-Undang Perlindungan Data Pribadi yaitu Undang-Undang No 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Perlindungan data pribadi sangat erat kaitannya dengan pengamanan data dan juga keamanan siber. Dalam kaitannya dengan keamanan siber, Indonesia telah memiliki berbagai peraturan seperti Undang-Undang Tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik hingga peraturan sektoral lainnya yang mengatur mengenai kewajiban organisasi keamanan siber, termasuk pengamanan data. Dalam implementasi Undang-Undang Perlindungan Data Pribadi, masih dibutuhkan penunjukan lembaga yang berwenang untuk mengatur mengenai perlindungan data pribadi yang ditunjuk oleh pemerintah, berikut dengan peraturan turunan dari Undang-Undang Perlindungan Data Pribadi. Organisasi juga dapat bekerja sama dengan pihak ketiga (konsultan) dalam mengembangkan program keamanan siber termasuk perlindungan data pribadi agar dapat memenuhi persyaratan peraturan perlindungan data pribadi.

Corresponding Author: Cindy Vania
E-mail: cindyvanialie1974@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade membuat adanya perubahan dan tantangan dalam menjaga privasi yang ada pada setiap individu maupun organisasi. Dengan adanya digitalisasi, setiap individu atau organisasi dapat melakukan inovasi baru dalam bentuk pemrosesan informasi termasuk data. Seiring dengan adanya digitalisasi serta kemajuan teknologi informasi, dan komunikasi, beberapa informasi yang tidak seharusnya dipublikasi, ternyata dipublikasikan tanpa adanya kesadaran dan persetujuan dari pihak yang berkaitan yang menyebabkan adanya penyalahgunaan data dan kebocoran data. Hal ini tentunya akan merugikan pihak yang berkaitan, terlebih jika informasi yang dipublikasi adalah merupakan data pribadi. Secara umum, data pribadi merupakan data yang dapat memberikan informasi mengenai ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, serta dapat mengidentifikasi seseorang, yang tentunya bersifat rahasia. Data yang jika dikombinasikan dapat mengidentifikasi seseorang juga termasuk data pribadi. Hal ini dapat mencakup kode, angka, simbol, huruf yang dapat menjadi kriteria personal bagi individu. Data pribadi perlu diberikan pengamanan yang tepat dikarenakan jika disalahgunakan akan merugikan individu sebagai subyek data pribadi dan juga organisasi yang melakukan pemrosesan data pribadi, baik kerugian yang bersifat materil dan immateril.

Setiap individu memiliki hak asasi manusia yang termasuk hak privasi, dimana hak privasi merupakan hal yang lebih sensitif dan dapat mewakili esensi dari hak pribadi tersebut

yang tentunya dilindungi oleh negara. Pada Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia Pasal 29 Ayat (1) menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya. Undang-Undang tersebut juga menjelaskan mengenai financial privacy secara eksplisit. Begitu pula, setiap warga negara juga memiliki hak konstitusional yang diatur dalam Undang-Undang Dasar Republik Indonesia Tahun 1945. Hak konstitusional yang dimaksud di Indonesia mencakup 40 hak warga negara termasuk hak atas perlindungan data pribadi. Menurut Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, berbunyi 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." Pada pasal tersebut, mengikuti perkembangan teknologi informasi, dan komunikasi maka dapat diasumsikan bahwa hak pribadi adalah hak privasi.

Secara internasional, perlindungan data pribadi sebagai hak asasi manusia juga terdapat pada Universal Declaration of Human Rights (UDHR). Pada Pasal 12 Universal Declaration of Human Rights (UDHR) menjelaskan bahwa "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to protection of the law against such interview or attacks." Pasal tersebut menjelaskan bahwa data atau informasi yang berkaitan dengan kehidupan individu selaku subyek data pribadi perlu dilindungi dan dijaga oleh peraturan perundang-undangan untuk menciptakan keadilan, keamanan, kenyamanan, manfaat, dan juga kepastian hukum. Individu sebagai subyek data pribadi memiliki hak untuk tidak diganggu atas kehidupan pribadinya dan hak tersebut tentunya harus dilindungi.

Keamanan data atau data security merupakan prosedur untuk melakukan perlindungan terhadap data dari kerusakan data baik secara disengaja ataupun tidak disengaja, modifikasi data yang tidak dilakukan oleh pihak yang memiliki wewenang dan kepentingan serta penyebaran data tanpa persetujuan pemilik data dalam kondisi apapun, baik sengaja ataupun tidak disengaja, dengan mempertimbangkan peraturan dan regulasi yang berlaku. Secara sederhana, keamanan data merupakan sistem yang diperlukan untuk menjaga dan melindungi data yang terdapat pada suatu organisasi. Pada umumnya, keamanan data termasuk keamanan fisik perangkat keras, keamanan aplikasi atau sistem perangkat lunak, kontrol keamanan data secara administratif serta kontrol akses. Saat keamanan data diterapkan dengan tepat, strategi keamanan data yang baik akan dapat melindungi aset data termasuk asset kritikal organisasi, dan informasi bisnis dari aktivitas kejahatan siber, ancaman orang dalam, serta dapat meminimalisir kerugian yang disebabkan oleh kesalahan manusia. Dalam menjaga keamanan data juga harus memperhatikan aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Keamanan data sangat erat kaitannya dengan keamanan siber. Jika organisasi melakukan penerapan keamanan siber yang mumpuni, maka kemungkinan besar keamanan data nya juga sudah sesuai dengan standar. Dalam implementasinya, terdapat berbagai macam jenis keamanan data yang dapat diterapkan untuk melindungi data atau informasi yang rahasia dan sensitif, termasuk data pribadi. Secara definisi, keamanan Siber (cyber security) merupakan upaya yang dilakukan oleh organisasi untuk melindungi sistem teknologi informasi dari berbagai ancaman dan serangan yang bersifat ilegal termasuk akses

ilegal. Cakupan keamanan siber dapat meliputi alat, kebijakan, dan konsep keamanan yang dapat digunakan untuk melindungi seluruh aset organisasi dan pengguna. Dengan menerapkan keamanan siber yang tepat maka organisasi dapat meminimalisir masuknya risiko ancaman ke dalam sistem teknologi informasi yang dapat merugikan organisasi dan pihak yang terlibat di dalamnya, termasuk subyek data pribadi.

METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan metode penelitian yang bersifat yuridis normatif dengan menggunakan studi kepustakaan (library research) yang mengacu kepada peraturan-peraturan yang tertulis atau hukum positif serta bahan-bahan hukum lain, yang berkaitan dengan perlindungan data pribadi. Penelitian penulis dilakukan secara yuridis dikarenakan penelitian menggunakan kaidah hukum, khususnya ilmu hukum terkait dengan informasi elektronik dan data pribadi. Sedangkan, secara normatif dikarenakan penelitian ini bertujuan untuk memperoleh data mengenai implikasi hukum terhadap perlindungan data pribadi menurut Undang-Undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi, dan orientasi kajiannya yang menitikberatkan pada aspek perlakuan norma-norma yakni perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. Dengan penelitian yang bersifat normatif ini, penulis menggunakan data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier dalam melakukan analisis, dengan pendukung berupa data primer yang berfungsi untuk menunjang hasil penelitian. Dalam hal data primer yang dikumpulkan, penulis melakukan wawancara kepada konsultan-konsultan yang merupakan praktisi dan memiliki pengalaman bekerja di perusahaan konsultansi swasta dengan inisial PT. DKI yang andal dalam bidang konsultasi teknologi strategi siber dan privasi data untuk menambah nilai dari penelitian ini. Adapun penulis membatasi aspek pengamanan data dan keamanan siber hanya meliputi industri yang erat kaitannya dengan teknologi dan data pribadi seperti industri telekomunikasi, industri perbankan, serta organisasi yang juga melakukan pemrosesan data pribadi seperti Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil).

Penelitian ini menggunakan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan merupakan pendekatan yang dilakukan dengan melakukan analisis terhadap aturan dan regulasi yang berkaitan dengan penelitian penulis terkait perlindungan data pribadi dan pendekatan konseptual yang lebih menekankan terhadap pandangan yang berkembang dalam ilmu hukum.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi pada era digital menyebabkan munculnya tren, budaya, dan juga perilaku yang baru di masyarakat, baik hal yang positif dan membangun ataupun hal yang negatif. Hal yang dapat dilakukan dari sisi pengguna teknologi adalah bersifat cermat. Jika diperhatikan, banyak pengguna media sosial yang baik secara sengaja maupun tidak sengaja melakukan penyebaran atas informasi atau data pribadi miliknya ke media sosial, yang tentunya dapat meningkatkan risiko kerugian secara finansial ataupun non finansial. Pada umumnya, masyarakat belum mengetahui dampak penyalahgunaan informasi

sehingga menyebabkan rendahnya kesadaran masyarakat tentang perlindungan data pribadi. Meskipun begitu, pemerintah telah mengambil tindakan awal atas perlindungan data pribadi dengan melakukan pengesahan atas Undang-Undang Perlindungan Data Pribadi sehingga pada kedepannya diharapkan Undang-Undang tersebut dapat memberikan perlindungan hukum terhadap subyek data pribadi. Tindakan awal tersebut sangatlah penting mengingat pengungkapan data pribadi tanpa kendali dapat menimbulkan banyak risiko terhadap subyek data pribadi serta organisasi serta meningkatkan kemungkinan tindak kriminalitas, mulai dari ancaman, perundungan, penipuan hingga pembobolan akun yang dimiliki oleh subyek data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang telah disahkan pada 17 Oktober 2022 lahir dari adanya pertimbangan yang tertera pada Undang-Undang Republik Indonesia Tahun 1945. Pada pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dinyatakan bahwa, "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Hal ini menegaskan bahwa seluruh warga Negara tanpa terkecuali berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya. Hak atas data pribadi merupakan hak milik yang melekat pada setiap individu sebagai subyek data pribadi. Perlindungan data pribadi berlaku bagi setiap indvidu baik warga negara Indonesia maupuan warga negara asing yang ada di Indonesia berkaitan dengan seluruh pemrosesan data pribadi yang meliputi pengumpulan, penggunaan, penyimpanan, pengiriman, hingga penghapusan.

Dengan pengesahan Undang-Undang tentang Perlindungan Data Pribadi, diharapkan dapat melindungi hak-hak dasar dan kebebasan warga negara yang berkenaan dengan perlindungan data pribadi, meningkatkan perlindungan hukum terkait data pribadi, memberikan kepastian hukum jika terjadi pelanggaran atas penggunaan data pribadi, memastikan kepatuhan organisasi terutama untuk sektor bisnis atau industri yang banyak melakukan pemrosesan data pribadi. Sebelum Undang-Undang tentang Perlindungan Data Pribadi disahkan, sudah terdapat beberapa peraturan sektoral yang mengatur terkait perlindungan data pribadi namun masih secara eksplisit dan parsial. Hal ini tentunya membuat peraturan sektoral belum dapat secara optimal memberikan perlindungan hukum dan kepastian hukum terhadap perlindungan data pribadi. Peraturan sektoral tersebut antara lain seperti Undang-Undang Nomor 7 Tahun 1971 tentang Ketentuan-Ketentuan Pokok Kearsipan, Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana Telah Diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, dan peraturan lainnya seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan

Data Pribadi dalam Sistem Elektronik. Bahkan saat ini, sudah ada pula Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan yang juga bertujuan untuk memperkuat perlindungan atas data pribadi nasabah pada sektor keuangan.

Tanpa disadari, pertumbuhan industri teknologi, informasi, dan komunikasi juga dipengaruhi oleh adanya Undang-Undang tentang Perlindungan Data Pribadi. Hal ini dikarenakan dengan adanya Undang-Undang tentang Perlindungan Data Pribadi, pengguna produk yang dirancang oleh industri teknologi, informasi, dan komunikasi merasa lebih aman dikarenakan sudah ada peraturan yang menjaga hak privasinya dan menjamin dari segi perlindungan serta kepastian hukum. Selain itu, jika dilihat dari sudut pandang yang lebih besar, negara yang telah memiliki peraturan perlindungan data pribadi akan lebih dipercaya untuk berbisnis ketimbang negara yang belum memiliki Undang-Undang tentang Perlindungan Data Pribadi. Hal ini dikarenakan berdasarkan peraturan perlindungan data pribadi internasional, disarankan untuk melakukan pengiriman data ke luar negeri ke negara yang sudah memiliki Undang-Undang tentang Perlindungan Data Pribadi yang setara dengan negara tersebut atau lebih tinggi perihal kecakapan pada Undang-Undang tentang Perlindungan Data Pribadi yang dimiliki.

Adapun, Undang-Undang tentang Perlindungan Data Pribadi juga berlaku pada lembaga-lembaga publik seperti penegak hukum dan badan-badan intelijen namun belum secara jelas diatur mengenai pengecualian terhadap penegak hukum dan badan-badan intelijen. Hal ini perlu diperjelas mengenai pengecualian agar tidak terjadi pelanggaran hak privasi dan data pribadi warga negara saat penegak hukum dan badan-badan intelijen melakukan tugas serta wewenangnya. Saat ini, Undang-Undang tentang Perlindungan Data Pribadi telah mengatur mengenai upaya perlindungan data pribadi, meliputi definisi data pribadi, jenis data pribadi, hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali dan prosesor data pribadi, larangan hingga sanksi, baik dalam bentuk administratif maupun pidana, bagi setiap pihak yang melakukan pelanggaran terhadap upaya perlindungan data pribadi. Penyelenggaraan perlindungan data pribadi dilaksanakan lembaga independen yang dibentuk dan ditunjuk oleh presiden serta bertanggung jawab secara langsung kepada presiden. Hanya saja, belum dilakukan penunjukan terkait lembaga independen tersebut sehingga tanggung jawab serta wewenang dari lembaga tersebut belum jelas.

Berdasarkan hasil wawancara penulis dengan beberapa konsultan teknologi strategi siber dan privasi data, dapat disimpulkan bahwa perlindungan data pribadi merupakan hal yang penting dan merupakan bagian dari Hak Asasi Manusia sehingga diperlukan perlindungan dan kepastian hukum. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang disahkan pada Oktober tahun 2022 merupakan langkah awal yang diambil oleh Pemerintah Indonesia untuk memberikan perlindungan dan kepastian hukum, serta secara tidak langsung melindungi warga negara Nya dari penggunaan data pribadi tidak sah yang dapat menyebabkan kerugian secara finansial hingga mempengaruhi reputasi. Sebelum disahkan Undang-Undang tentang Perlindungan Data Pribadi, Indonesia telah memiliki berbagai peraturan sektoral yang mengatur mengenai perlindungan data pribadi, antara lain dalam segi sektor perbankan dan telekomunikasi, sudah ada Undang-Undang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun

2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, POJK 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, lalu juga ada POJK 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Untuk sektor kependudukan bisa mengacu pada Undang -Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, terdapat beberapa pasal-pasal yang mengacu pada perlindungan data pribadi.

Keberhasilan akan upaya perlindungan data pribadi tidak terlepas dari implementasi dalam aspek pengamanan data dan keamanan siber yang tepat dan mumpuni. Pengamanan data dan keamanan siber merupakan salah satu aspek penting yang perlu diperhatikan dari suatu sistem informasi dimana jika tidak dilakukan implementasi dan pemeliharaan dengan baik, tentu dapat menyebabkan kerugian finansial ataupun secara non finansial bagi organisasi yang pihak yang terlibat di dalamnya. Jika sebuah organisasi dapat melakukan pengamanan data dengan tepat, baik secara fisik maupun non fisik, ketiga aspek penting dalam pengamanan data seharusnya tercukupi, dimana data terjaga kerahasiaan, integritas, dan ketersediaannya. Perlindungan data pribadi dari aspek pengamanan data dan keamanan siber tertuang pada Undang-Undang Perlindungan Data Pribadi secara eksplisit namun jika secara implementasi, aspek-aspek tersebut tertuang pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Pada Peraturan Pemerintah tentang Penyelenggara Sistem dan Transaksi Elektronik, Penyelenggara Sistem Elektronik Pasal 18 dan Pasal 69 diwajibkan untuk dilakukan audit siber secara berkala. Pada Pasal 65 hingga Pasal 72 juga dijelaskan mengenai lembaga sertifikasi keandalan yang erat kaitannya dengan keamanan siber. Sertifikat keandalan perlu diterbitkan oleh lembaga sertifikasi keandalan untuk memastikan standar operasional yang dilakukan oleh penyelenggara sistem elektronik sudah sesuai dengan peraturan yang berlaku di Indonesia dan juga sesuai dengan best practice pada industri tersebut. Selanjutnya, pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, juga ditegaskan mengenai kewajiban penyelenggara sistem elektronik untuk melengkapi dirinya dengan aturan internal perlindungan data pribadi guna mencegah terjadinya kegagalan dalam perlindungan data pribadi yang dikelolanya. Aturan internal perlindungan data pribadi dapat disebut juga internal privacy policy. Pada umumnya, sebuah penyelenggara sistem elektronik yang merupakan pengendali data pribadi perlu memiliki internal privacy policy dan external privacy policy (privacy notice).

Dalam melakukan pemrosesan data pribadi, pada Peraturan Menteri Komunikasi dan Informatika tersebut mewajibkan penyelenggara sistem elektronik untuk melakukan pemberitahuan dan juga permintaan persetujuan sesuai dengan tujuan kepada subyek data pribadi serta menentukan dasar hukum (legal basis) pemrosesan data pribadi, terutama pada saat pengumpulan data pribadi. Selanjutnya, jika dilakukan pengolahan atau analisis juga perlu dilakukan sesuai dengan persetujuan. Lalu perihal dengan dilakukannya pengiriman data pribadi juga harus dipertimbangkan cara pengiriman, tujuan pengiriman, akurasi data, dan juga

persetujuan. Data yang dikirimkan harus terverifikasi keakuratannya dan sesuai dengan persetujuan pemilik data pribadi. Selain itu juga perlu menerapkan ketentuan peraturan perundang-undangan mengenai pertukaran data pribadi lintas batas negara. Dalam hal penyimpanan, data yang termasuk data pribadi perlu dilakukan enkripsi dan diperlakukan sesuai dengan klasifikasi data yang telah ditentukan pada kebijakan manajemen data atau kebijakan privasi yang terdapat pada kebijakan yang dimiliki oleh penyelenggara sistem elektronik. Terakhir, mengenai pemusnahan, penyelenggara sistem elektronik perlu menetapkan jadwal retensi, menentukan prosedur dan pihak yang bertanggung jawab perihal retensi agar bisa melakukan retensi data secara berkala sesuai dengan kebijakan yang telah ditentukan.

Berdasarkan Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik juga mengatur mengenai kewajiban Penyelenggara Sistem Elektronik, terdapat beberapa kewajiban yang berkaitan dengan pengamanan data dan keamanan siber yaitu setiap Penyelenggara Sistem Elektronik wajib melakukan sertifikasi untuk keandalan atau uji kelayakan sistem elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan, Penyelenggara Sistem Elektronik wajib memiliki aturan internal yang mengatur mengenai perlindungan data pribadi atau dapat disebut juga kebijakan perlindungan data pribadi (privacy policy), Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan sistem elektronik yang dikelolanya. Dari sisi implementasi, konsultan memang menyarankan organisasi mengetahui aset-aset kritikal (crown jewel) dimana aset ini bisa termasuk data rahasia, data pribadi baik jenis umum maupun spesifik. Dengan mengetahui aset-aset kritikal, organisasi akan dapat menerapkan teknis pengamanan data dan keamanan siber yang tepar. Cara penentuan aset kritikal dapat dilakukan sesuai Pasal 31 pada Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, yaitu dengan melakukan aktivitas perekaman pemrosesan data. Penyelenggara Sistem Elektronik juga wajib menyediakan narahubung yang mudah dihubungi oleh subyek data pribadi terkait pengelolaan data pribadinya atau dapat disebut juga Data Protection Officer (DPO).

Berdasarkan wawancara dengan konsultan teknologi strategi siber dan privasi data yang telah menjalankan berbagai implementasi di sektor perbankan hingga telekomunikasi, baik swasta maupun non swasta, konsultan menyampaikan bahwa pengamanan data dan keamanan siber yang mumpuni akan memiliki dampak positif untuk perlindungan data pribadi. Pengamanan data merupakan bagian kecil dari keamanan siber yang saling memiliki keterkaitan. Permasalahan mengenai masalah kelemahan atau kerentanan atas kontrol keamanan informasi yang berkaitan dengan pengamanan data dan keamanan siber tidak hanya dialami oleh negara berkembang seperti Indonesia namun juga oleh negara yang maju. Maka dari itu, diperlukan perlindungan dan kepastian hukum agar memastikan bahwa organisasi atau dalam hal ini dapat disebut juga pengendali data pribadi serta prosesor data pribadi dapat menerapkan pengamanan data dan keamanan siber yang sesuai dengan peraturan yang berlaku serta juga menerapkan best practice seperti yang dihimbau pada ISO 27001, ISO 27701.

Narasumber selaku konsultan teknologi strategi siber dan privasi data juga menjelaskan bahwa secara implementasi, dapat dilakukan beberapa hal untuk meningkatkan

pengamanan data dan keamanan siber, antara lain pengamanan data menggunakan user access control. Pada Undang-Undang tentang Perlindungan Data Pribadi di Indonesia menjelaskan terkait kewajiban untuk melakukan pencegahan atau pengamanan data dari akses yang tidak sah. Penggunaan user access control yang merupakan manajemen akses dapat membantu organisasi untuk melakukan pengecekan user access yang juga disebut dengan user access review hingga melakukan kontrol terhadap user access tersebut. Lalu selain itu juga terdapat data loss prevention (DLP) dimana dengan adanya DLP akan mengurangi kemungkinan data dikirim ke pihak yang tidak berwenang, terlebih untuk data rahasia perusahaan, termasuk data pribadi, baik data pribadi milik konsumen, karyawan, hingga pihak ketiga.

Narasumber juga menambahkan perihal penanganan insiden, juga dapat dibantu dengan adanya system incident event monitoring (SIEM). Dengan adanya SIEM, organisasi dapat melakukan deteksi insiden dan melakukan investigas terkait insiden tersebut. Mengingat bahwa menurut Undang-Undang tentang Perlindungan Data Pribadi Nomor 27 Tahun 2022, jika terjadi insiden penyalahgunaan data termasuk kebocoran data maka harus melakukan pelaporan ke subjek data pribadi dan lembaga pengawas, maka sebaiknya organisasi memiliki prosedur atau dapat disebut juga playbook sebagai panduan jika terjadi insiden kebocoran data pribadi. Saat ini, belum ada ketetapan mengenai lembaga pengawas, sehingga masing-masing sektor dapat melakukan pelaporan sesuai lembaga yang mengatur mengenai sektor tersebut. Mengingat bahwa setiap organisasi memiliki sistem dan proses yang beragam, maka sebaiknya organisasi dapat melakukan uji kelayakan sistem informasi terlebih dahulu agar dapat menerapkan pengamanan data dan keamanan siber yang tepat dan efektif.

Narasumber juga menjelaskan bahwa sebenarnya setiap sektor akan memiliki implementasi pengamanan data dan keamanan siber yang berbeda dikarenakan adanya perbedaan pada kebutuhan dan tujuan hingga area of concern. Sebagai konsultan, narasumber menyarankan organisasi sebagai pengendali data pribadi atau prosesor data pribadi untuk melakukan penilaian kesenjangan (gap assessment) agar perusahaan mengetahui kondisi serta security posture yang dimiliki oleh organisasi tersebut. Setelah itu, organisasi dapat membuat roadmap implementasi data privasi. Roadmap tersebut dapat berisi penerapan consent management, praktik records of processing activities (ROPA)/perekaman aktivitas pemrosesan data pribadi, praktik data protection impact assessment (DPIA)/penilaian dampak privasi, pembuatan privacy notice atau privacy policy, penunjukkan data protection officer (DPO)/pejabat perlindungan data pribadi. Biasanya roadmap dibuat untuk kurun waktu 2 (dua) hingga 5 (lima) tahun, sesuai dengan permintaan dan kesanggupan dari organisasi.

Mengenai keterkaitan dengan aspek pengamanan data dan keamanan siber, seluruh narasumber setuju bahwa pengamanan data dan keamanan siber yang baik dapat meningkatkan dampak positif terhadap perlindungan data pribadi. Hal ini tentunya harus didasari dengan implementasi yang tepat pada organisasi, sehingga tepat sasaran.

KESIMPULAN

Berdasarkan hasil penelitian, maka dapat dirumuskan sebagai berikut: 1.) Sebelum disahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi pada Oktober 2022 sebenarnya sudah terdapat peraturan-peraturan sektoral yang mengatur mengenai perlindungan data pribadi. Pada umumnya, Undang-Undang Perlindungan Data

Pribadi dibuat dengan tujuan adanya perlindungan dan kepastian hukum atas kasus-kasus penyalahgunaan data pribadi termasuk kebocoran data yang sering terjadi di Indonesia. Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi tentu akan lebih mudah jika sudah dibuatkan peraturan turunan atau peraturan pelaksana berupa Peraturan Pemerintah. Hal ini dikarenakan Undang-Undang tentang Perlindungan Data Pribadi di Indonesia belum mengatur secara rinci mengenai penerapan perlindungan data pribadi yang pada kedepannya akan disusun oleh lembaga independen yang berwenang dan ditunjuk oleh Presiden. 2.) Perlindungan hukum data pribadi dari aspek pengamanan data dan keamanan siber juga tersampaikan pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Pada peraturan tersebut, dapat disimpulkan bahwa organisasi perlu menjaga keamanan data dan juga keamanan siber yang dimiliki oleh sebuah organisasi, baik organisasi tersebut sebagai pengendali data pribadi ataupun prosesor data pribadi. Organisasi bahkan wajib untuk audit berkala, sertifikasi keandalan oleh pihak ketiga atau konsultan untuk memastikan bahwa sistem informasi yang dimiliki masih dalam kategori aman. Menurut Pasal 31 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, juga dijelaskan mengenai aktivitas perekaman pemrosesan data pribadi. Hal ini untuk memastikan aset kritikal yang perlu dijaga oleh organisasi dan juga melakukan penerapan keamanan data serta siber yang tepat. Perlindungan hukum data pribadi dari aspek pengamanan data dan keamanan siber yang sudah ada di peraturan, harus didukung dengan penerapan yang tepat. Untuk hal ini, organisasi sebagai pengendali data pribadi atau prosesor data pribadi disarankan untuk menggunakan jasa konsultasi siber dan data privasi agar dapat mengetahui apa saja yang dibutuhkan oleh organisasi agar dapat patuh terhadap peraturan yang berlaku dan menerapkan keamanan data serta siber yang sesuai dengan kondisi, tujuan hingga kebutuhan dari perusahaan.

DAFTAR PUSTAKA

Anindia, Islamia Ayu. Perlindungan Hukum terhadap Perdagangan Anak dengan Modus Pernikahan dalam Perspektif Viktimologis. Jurnal Litigasi. Vol. 19, No.1 (2018).

Ardiyanti, Handrini. Cyber Security dan Tantangan Pengembangannya di Indonesia. Jurnal Politica. Vol. 5 No.1 (2014).

Anggraeni, S.F. Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum Di Indonesia. Jurnal Hukum & Pembangunan. Vol. 48. No. 4 (2018).

Arifin, Syamsul. 2012. Pengantar Hukum Indonesia. (Medan: Penerbit Medan Area University Press).

Azra, Azyumardi. 2003. Demokrasi, Hak Asasi Manusia dan Masyarakat Madani. (Jakarta: Tim ICCE UIN).

Cameron G. Shilling. Privacy and Data Security: New Challenges of the Digital Age, Hampshire Bar Journal. (2011).

Danrivanto Budhijanto. The Present and Future of Communication and Information Privacy in Indonesia. Jurnal Hukum Internasional, Vol. 2 No. 2 (2003).

Dewi, Shinta. 2009. Perlindungan Privasi atas Informasi Pribadi dalam E- Commerce menurut Hukum Internasional. (Bandung: Penerbit Widya Padjajaran).

Graham Greenleaf. 2014. Asian Data Privacy Laws: Trade and Human Rights Perspectives.(Oxford: University Press).

Hanifan N. Perlindungan Data Pribadi Sebagai Bagian Hak Asasi Manusia Atas Perlindungan Diri pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundangundangan Di Negara Lain. Jurnal Selisik. Vol.6. No.1 (2020).

Herdiansyah, Haris. 2010. Metode Penelitian Kualitatif untuk Ilmu-ilmu Sosial. (Jakarta: Penerbit Salemba Humanika).

Jerry Kang. Information Privacy in Cyberspace Transaction. Stanford Law Review Vol 50 (1998).

Khansa, F. N. Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Perlindungan Data Pribadi di Indonesia. Jurnal Hukum Lex Generalis. Vol.2. No.8 (2021).

Kurniawan, I Gede Hartadi, dkk. Penyuluhan Aspek Hukum Perlindungan Privasi dan Data Pribadi, Jurnal Abdimas, Vol. 8, No.5 (2022).

Mahira, D.F., Emilda Y Lisa NA. Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. Jurnal Legislatif. Vol.3. No.2 (2020).

Natamiharja. R.N. Rudi, M. Stefany. Perlindungan Hukum Atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Selular). Prodigy Jurnal Perundang-Undangan Vol.7. No.2 (2019).

Napitulu, Sarwin Kiko, dkk. 2017. Perlindungan Konsumen pada Fintech – Kajian Perlindungan Konsumen Sektor Jasa Keuangan. (Jakarta: Penerbit Otoritas Jasa Keuangan).

Nasution, Adnan Buyung. 1983. Bantuan Hukum Di Indonesia. (Jakarta: Penerbit: LP3ES Press).

Moleong, Lexy. 2010. Metode Penelitian Kualitatif. (Bandung: Penerbit Remaja Rosda Karya).

Masyhur, Effendi. 1994. Dinamika Hak Asasi Manusia dalam Hukum Nasional dan Internasional. (Jakarta: Ghalia Indonesia).

M. Nazir. 2003. Metode Penelitian. (Jakarta: Penerbit Ghalia Indonesia).

Pelealu, Andrew. Perlindungan Hukum atas Data Pribadi Konsumen dalam Transaksi E-Commerce. Jurnal UAJY. (2018).

Philipus M. Hadjon. 1987. Perlindungan Hukum bagi Rakyat Indonesia. (Surabaya: Bina Ilmu)

Prosser, William L. 1960. Privacy: A Legal Analysis. (California: Law Review).

Purwanto. Penelitian tentang Perlindungan Hukum Data Digital Laporan Penelitian. Badan Pembinaan Hukum Nasional. (2007).

Radian Adi Nugraha. Analisa Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik. Universitas Indonesia. (2012).

Raharjdo, Satjipto. 2014. Ilmu Hukum. (Bandung: Citra Aditya Bakti).

Rahardjo, Satjipto. 2003. Sisi – Sisi Lain dari Hukum di Indonesia. (Jakarta: Kompas).

Rizal, MS. Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. Jurnal Cakrawala Hukum. (2019).

Rosadi, S.D. 2015. Cyber Law Aspek Data Privasi Menurut Hukum Internasional. (Jakarta: Penerbit Refika Aditama).

Rosadi, S.D. Implikasi Penerapan program E-Health Dihubungkan Dengan Perlindungan Data Pribadi. Jurnal Arena Hukum. Vol.9. No.3 (2017).

Rosadi, S.D., Garry Gumelar Pratama. Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia. Jurnal Veritas et Justitia.Vol.4. No.1 (2018).

Salim HS & Erlies Septiana Nurbani. 2014. Penerapan Teori Hukum pada Disertasi dan Tesis. (Jakarta: Penerbit Raja Grafindo Persada).

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

Setiono. 2004. Rule of Law (Supremasi Hukum). (Surakarta: Penerbit Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret).

Shinta Dewi. 2009. Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut

Hukum Internasional. (Bandung: Widya Padjajaran).

Soerjono Soekanto & Sri Mamudji. 2004. Penelitian Hukum Normatif. (Jakarta: PT Raja Grafindo Persada).

Soekanto, Soerjono. 1986. Pengantar Penelitian Hukum. (Jakarta: Penerbit UI-Press).

Sudjatmoko, Andrey. 2015. Hukum HAM dan Hukum Humaniter. (Jakarta: Grafindo Persada).

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

Syukri Akub dan Baharudin Baharu. 2012. Wawasan Due Process of Law dalam Sistem Peradilan Pidana. (Yogyakarta: Rangkang Education).

Waluyo, Bambang. 2008. Penelitian Hukum dalam Praktek. (Jakarta: Penerbit Sinar Grafika).

Wirartha, I Made. 2006. Metodologi Penelitian Sosial Ekonomi. (Yogyakarta: Penerbit CV. Andi Offset).

Westin, A.F. 1967. Privacy and Freedom. (New York: Atheneum).

Yuniarti, S. Perlindungan Hukum Data Pribadi Di Indonesia. Jurnal Becoss, Vol. 1. No.1 (2019).