Al-Manhaj: Jurnal Hukum dan Pranata Sosial Islam
Vol. 4, 2 (Desember, 2022), pp. 207-2018
ISSN: 2686-1607 EISSN: 2686-4819, DOI: 10.37680/almanhaj.v4i2.1791

Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman

Namrysilia Buti Anjawai[1], F. Yudhi Priyo Amboro[2], Rufinus Hotmaulana Hutauruk[3]

[1] Universitas Internasional Batam, Indonesia; namrysiliabutianjaway@gmail.com
[2] Universitas Internasional Batam, Indonesia; yudhi.amboro@gmail.com
[3] Universitas Internasional Batam, Indonesia; rufinushotmaulanahutauruk@gmail.com

ARTICLE INFO

Keywords:

Comparison;
Protection;
Personal data

Article history:

Received 2022-04-11
Revised 2022-07-09
Accepted 2022-09-03

ABSTRACT

Protection of personal data is a human right that must be given legal protection. However, Indonesia does not yet have special rules governing the protection of personal data and the Personal Data Protection Supervisory Agency. As for when compared to Germany, which has special rules regarding the protection of personal data in full to the Institution that oversees the implementation of the rules for protecting Personal Data. The research method used by the author is a legal comparison method with the type of research being normative research. The author uses secondary data to analyze the results of the data, namely, primary materials, secondary materials, and tertiary materials. The analytical method used by the author is a qualitative method. Similarities and differences in personal data protection between Indonesia-Germany and the legal contributions of personal data protection that he can adopt or apply in Indonesia such as special arrangements for personal data protection, data classification, one of which is the deletion of personal data, and the establishment of a Personal Data Protection Supervisory Agency and the rules that govern it

Corresponding Author:
Namrysilia Buti Anjawai
Fakultas Magister Hukum Universitas Internasional Batam, Indonesia; namrysiliabutianjaway@gmail.com

1. PENDAHULUAN

Kemajuan yang pesat dari teknologi informasi dan komunikasi memunculkan berbagai peluang juga tantangan. Perkembangan teknologi informasi ini juga mempengaruhi salah satu bidang yaitu interaksi yang terjadi antar individu/orang dengan pihak layanan penyedia jasa informasi. Dalam kehidupan masyarakat, banyak yang telah menggunakan teknologi berbasis online di berbagai bidang seperti aspek perdagangan, pemerintahan, keuangan, transportasi, industri dan pariwisata. Adapun cara kerja sistem ini yang meliputi pengumpulan data, penyimpanan data, di proses, di produksi, dan pengiriman, hingga dapat dikonsumsi oleh masyarakat. Dengan teknologi semakin canggih, segala aktivitas terus diciptakan hanya dengan melalui smartphone. Bahkan internet sebagai

kebutuhan. Urusan administrasi seperti mendaftarkan identitas contohnya mendaftar diri atau pengajuan surat suatu badan resmi dengan mudah didapatkan melalui online. Dari kecanggihan tersebut, timbullah sebuah kekhawatiran dari konsumen dikarenakan keamanan data pribadi yang belum terjamin.

Peningkatan aktivitas masyarakat di ruang digital menyebabkan munculnya berbagai kasus tindak criminal yang merugikan baik secara materiil ataupun immatteriil bagi pihak yang mengalami. Jumlah pengguna yang semakin meningkat membuat kekhawatiran akan keamanan data ditambah lagi dengan kasus yang muncul perlahan menangani kebocoran data pribadi dari seseorang, penyebaran data tersebut dengan mudahnya cepat tersebar dikarenakan teknologi yang semakin canggih. Kondisi ini membuat masyakarat semakin takut dan berharap agar aktivitas dunia digital dan data yang dimiliki dapat terlindungi dari pihak yang tidak bertanggungjawab.

Menurut data dari Perusahaan Teknologi IBM, bahwa kasus kebocoran data terus mengalami peningkatan kerugian finansial. Pada tahun 2020, kerugian finansial mencapai USD 3,86 Juta dan meningkat Kembali di 2021 sebanyak USD 4,24 Juta. Apabila jumlah tersebut dirata-ratakan, kerugian yang didapat USD 2,5 Juta pada satu data masyarakat pada kasus kebocoran data. Dari Badan Siber dan Sandi Negara (BSSN) melaporkan, Untuk Indonesia sampai oktober 2021, sekitar 1 Miliar serangan terjadi. Masalah berikut 2 kali lipat dibandingkan serangan yang terjadi di tahun 2020 (Rokhayah, 2022). Sebanyak 182 kasus dilaporkan oleh masyarakat dengan laporan kasus pencurian data. Polisi Siber mencatat kasus tersebut meningkat hingga 27,3 % daripada sebelumnya, hanya 143 kasus meningkat selama 5 tahun belakangan, tercatat peningkatan sebesar 810% daripada data tahun 2016 (Jayani, 2021). Pada tahun 2015 laporan kejahatan siber tidak begitu tinggi dibandingkan dengan tahun 2020, yaitu sebanyak 4.250 laporan jika dibanding tahun 2015 yang sebesar 2.609 kasus. Kasus penipuan daring dan penyebaran konten termasuk dalam laporan kejahatan siber tersebut. Minimnya Peraturan Perlindungan Data Pribadi, mengakibatkan keamanan semakin tidak terjamin dan membuat para pengguna tidak nyaman dalam berjelajah di dunia digital. Indonesia juga memiliki aturan tersebut, namun peraturannya terdiri dengan terpisah dan hanyalah menjelaskan perlindungan data pribadi (Jayani, 2021). Peraturan yang dimiliki Indonesia secara umum mengenai perlindungan data pribadi. Salah satunya dalam UUD 1945, pada pasal 28F dan 28G berisi bahwasannya hak tiap orang mendapatkan perlindungan data diri pribadi juga untuk berkomunikasi serta memperoleh informasi. Kedua pasal tersebut menjadi dasar aturan terkait hak privasi.

Beberapa Perlindungan Data Pribadi diatur dalam UU No. 7 Tahun 1971 Tentang Ketentuan-Ketentuan Pokok Kearsipan, UU No. 10 Tahun 1998 Tentang Perubahan atas UU No. 7 Tahun 1992 Tentang Perbankan, UU No.8 Tahun 1998 Tentang Dokumen Perusahaan, UU No. 39 Tahun 1999 Tentang HAM, UU No. 8 Tahun 1999 Tentang Perlindungan Konsumen, UU No. 36 Tahun 1999 Tentang Telekomunikasi, UU No.23 Tahun 2006 Tentang Administrasi Kependudukan, UU No. 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, UU No. 36 Tahun 2009 Tentang Kesehatan, UU No. 19 Tahun 2016 Tentang Perubahan atas UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, PP No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Sehingga membuat Kementerian Perdagangan serta Kementerian Komunikasi dan Informatika memiliki kewenangan yang secara tidak langsung dalam urusan perlindungan data pribadi. Namun hal ini menimbulkan antar peraturan saling tumpang tindih serta menjadi dasar pembahasan RUU Perlindungan Data Pribadi yang bertujuan mengharmonisasikan juga singkronisasi dari Undang-Undang yang sudah berlaku.

Beberapa kasus yang muncul dalam dunia siber tidak dapat tertangani dikarenakan hukum positif Indonesia masih kekurangan peraturan mengenai perlindungan data pribadi. Keadaan ini sangat mengkhawatirkan karena banyaknya oknum yang tidak bertanggungjawab menyalahgunakan data pribadi sehingga sudah sepatutnya mendesak pemerintah untuk membuat suatu regulasi khusus. Pembahasan ini sudah pernah dilaksanakan pada tahun 2012 oleh DPR RI yang dituangkan

pada RUU Perlindungan Data Pribadi yang memuat definisi, jenis, hak, kepemilikan, proses, pengiriman, dan Lembaga hingga sanksi (Indonesia, 2021).

Namun dikarenakan peraturan terkait ini dibahas pada UU dari Kementerian Komunikasi dan Informatika dan Kementerian Kesehatan serta Kementerian Dalam Negeri, Ini menbuat tugas Kementerian Komunikasi dan Informatika untuk mengharmonisasikan antar Undang-Undang. Diketahui ada sebanyak 32 regulasi yang membahas data pribadi. Beberapa negara melakukan kesepakatan pada sidang PBB tahun 2013, negara-negara yang hadir bertanggungjawab saat membahas mengenai data pribadi diminta untuk transparan. Bahasan dari kesepakatan tersebut tertuang dalam General Data Protection Regulation atau GDPR, ialah aturan untuk perlindungan data pribadi di Uni Eropa. Aturannya tersebut berarti kewajiban perusahaan, aturan pelayan konsumen serta aturan dalam penyimpanan data pribadi konsumen. Aturan ini bersifat tegas dan ketat, termasuk aturan untuk platform seperti Google, Facebook atau Platform yang lain (Susmoro, 2019). Kasus berskala Internasional mengenai Penyalahgunaan Data Pribadi dari milik Indonesia yaitu kasus Cambridge Analytica. Sekitar 82 Juta data diambil oleh konsultan publik ialah Inggris Cambridge Analytica. Pada pemilihan presiden 2016, saat itu sebuah perusahaan melakukan perbuatan curang demi kemenangan Donald Trump dengan memanfaatkan data pribadi konsumen Facebook dan saat itu GDPR belum berlaku, sehingga kasus tersebut tidak dapat diselesaikan serta tidak dapat melindungi data Indonesia yang dapat dicari oleh perusahaan tersebut (Zaenudin & Jovankurbalija, 2018). Berlakunya GDPR, menjadi banyak kritikan serta mulai diakui menjadi aturan dalam perlindungan data pribadi. GDPR juga menjadi pedoman seluruh dunia untuk pelindungan data diri pribadi. GDPR sudah menjadi landasan untuk platform-platform seperti Google, Facebook, dan Amazon serta instansi-instansi resmi pemerintah dan non pemerintah (Sudibyo, 2019).

Tujuan penelitian yakni membandingkan pengaturan mengenai perlindungan data pribadi dari negara Indonesia dan Jerman. Rumusan masalah penelitian meliputi: (1) apakah persamaan dari peraturan perlindungan data pribadi Indonesia dan Jerman, (2) apa perbedaan yang terdapat dalam peraturan perlindungan data pribadi Indonesia dan Jerman, (3) bagaimana kontribusi negara mengenai hukum perlindungan data pribadi jerman ke dalam pengaturan data pribadi Indonesia?.

2. METODE

Penelitian merupakan penelitian normatif dengan memakai kaidah-kaidah ataupun norma hukum dalam aturan perundang-undangan yang menjadi pedomannya. Di penulisannya, penulis menggunakan pendekatan perundang-undangan, pendekatan konseptual (Marzuki, 2008). Selain itu penulis juga menggunakan pendekatan sejarah, pendekatan perbandingan, serta pendekatan kasus (Seokanto & Mamuji, 2001). Data penelitian merupakan hasil Analisa pada data sekunder dari bahan pustaka. Data sekunder berupa bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Metode analisis data yaitu metode Kualitatif, yaitu metode yang digunakan untuk menganalisa dan menjelaskan suatu peristiwa atau fenomen yang terjadi seperti wawancara, catatan lapangan, gambar, foto atau subjek lainnya (Poerwandari, 1980).

3. HASIL DAN PEMBAHASAN

Lahirnya peraturan perlindungan data pribadi pada 1960. Hingga aturan perlindungan ini diberlakukan pada 1970 di negara Hessa, Jerman. Peraturan tersebut menjadikan yang pertama diberlakukan pada saat itu. Peraturan itu menjadi hukum nasional yang diikuti Swedia tahun 1973, Jerman Barat tahun 1977, Perancis tahun 1978, Amerika Serikat tahun 1974, dan Inggris tahun 1989. Kerangka Perlindungan data ini menjadi bagian dari perlindungan privasi (A, 2013).

3.1. Persamaan dari perlindungan data pribadi Indonesia dan Jerman

Sejarah Singkat Undang-Undang Perlindungan Jerman

Konsep pengaturan data pribadi Jerman diawali terlebih dahulu dengan perlindungan data pribadi di Uni Eropa sebab Jerman menjadi anggota Uni Eropa serta wajib mengikuti peraturannya.

Pasal 8 dan pasal 16 piagam Hak Fundamental Uni Eropa serta dalam perjanjian Lisbon mengatur Hak Fundamental dari perlindungan data pribadi. Peraturan ini secara sah sudah mengikat pada negara anggota dalam Uni Eropa saat aturan ini dikembangkan di wilayah dosmetik dan internasional. Subjek dari hak ini adalah setiap individu tidak bergantung pada nasionalitas dan kewarganegaraan serta pembatasan hak yang harus dipenuhi dan terikat, sehingga menjadi Batasan hukum demi terciptanya kemurniaan dalam kepentingan public (Fahey, 2010). Demi kepentingan bersama juga dasar dari kasus hukum yang jerjadi menjadikannya ide kerangka hukum untuk perlindungan data pribadi. Reformasi perlindungan data ini bertujuan menegakkan hukum dan Teknik mengenai komunikasi elektronik. Pengolah data dan proses data bekerjasama pada Otoritas Perlindungan Data Uni Eropa.

Kerangka Hukum perlindungan data Uni Eropa berupa peraturan primer yaitu perjanjian Internasional dan Piagam Hak Fundamental Uni Eropa. Hak perlindungan data terdapat pada pasal 16 dan pasal 39 yang diakui sebagai hak fundamental serta pasal 7 dan pasal 8 di dalam Piagam Gak Fundamental mengenai hak pribadi. Tingkat sekunder, peraturan ini sebagai perlengkap peraturan tingkat primer, yakni Directive 95/46/EC. Setelah 20 tahun aturan tersebut mengalami perubahan dan pembaharuan menjadi GDPR yang berlaku Mei 2016 juga berlaku untuk negara anggota pada 25 Mei 2018 (EU), 2016). Beberapa asas dan prinsip terkandung dalam aturan GDPR menjadi dasar diantaranya, keabsahan, keadilan, transparansi, Batasan tujuan, minimalisasi data, akurasi, integritas, kerahasiaan, keamanan data serta terciptanya kewajiban Bersama sebagai "pengawas" data pribadi, sehingga dapat dipahami oleh berbagai kalangan demi tujuan Bersama. Adapun subjek data yang diberikan antara lain hak procedural yaitu hak atas informasi, hak atas akses, hak perbaikan, hak menghapus, hak pembatasan pemrosesan, hak portabilitas data, serta hak menolak.

GDPR yaitu peraturan yang dibuat untuk keamanan perlindungan data pribadi dari penyalahgunaan data oleh pihak asing maupun pihak yang berada di wilayah Eropa, aturan ini berlaku di wilayah Uni Eropa. Aturan ini mengontrol dan memberikan kewajiban bagi pelaku bisnis, instansi, dan badam-badan resmi lain untuk menggunakan metode tranparasi sebagi penerapan dalam mempraktikkan data yang dimiliki, mengatur pelaku bisnis dengan tujuan mengumpulkan, memproses, dan menyimpan data Dapat dikatakan GDPR didasari oleh pemberlakuan Undang-Undang Perlindungan Data pada tahun 1970 di Hessa, Jerman. UU berikut disahkan yang berprinsip perlindungan data atas hak dan kewajiban perizinan hukum juga persetujuan subjek data dalam pemrosesan data pribadi (Fahey, 2010). UU berikut menjadi UU Perlindungan Data pertama yang berlaku di negara Jerman. Kemudian pada tanggal 1 Januari 1978, Pemerintah Jerman memberlakukan Undang-Undang Perlindungan Data Federal Jerman (BDSG). Prinsip perlidungan data diri termasuk perizinan hukum, dan persetujuan subjek data menjadi dasar setiap proses data. Dikatakan oleh pihak Pengadilan Konstitusi Federal Jerman bahwa setiap orang mempunyai hak konstitusi sebagai acuan atau keputusan mendapatkan informasi sendiri (Informational Self Determination) (Raul & Stepanova, 2018).

3.2. Persamaan Perlindungan Data Pribadi Indonesia dan Jerman

Perlindungan Data Diri merupakan Bagian Hak Asasi Manusia

Sebelum masuk pada hakikat HAM sebagai hak fundamental, terlebih dahulu yang harus dikenalkan yaitu hak diartikan sebagai unsur normatif yang memiliki fungsi sebagai patokan dalam bertingkah laku, kebebasan, kekuasaan, serta jaminan peluang demi melindungi harkat dan martabat. Unsur-unsur yang dari yang harus diketahui, antara lain; (a) pemegang atau Pemilik Hak; (b) ruang Penerapan Hak dan (c) Penerima Hak. Tiap orang berhak sama dalam mendapatkan persamaan serta kebebasan hak. Ketiga unsur yang disebutkan sebelumnya merupakan pengeritan dasar hak yang saling menyatu dan berkaitan (Ayumardi, 2000). John Lock berpendapat bahwasannya HAM merupakan hak kodrat dari Tuhan YME. Kekuasaannya pada hak tersebut tidak dapat diganggu gugat baik dunia sekalipun. Hak ini merupakan sifat dasar bagi kehidupan manusia dan tidak dapat dilepas di kehidupan manusia (Masyhur, 1994).

Definisi HAM pada Pasal 1 UU No 39 tahun 1999 tentang HAM bahwa:

"*Hak Asasi Manusia adalah seperangkat hak yang melekat pada hakikat dari keberadaan manusia sebagai makhluk Tuhan Yang Maha Esa dan merupakan anugrah-Nya yang wajib dihormati, dijunjung tinggu, dan dilindungi oleh negara, hukum, pemerintah, dan setiap orang demi kehormatan serta perlindunga harkat dan martabat manusia*."(Undang-Undang, 1999a).

Menurut Leach Levi, seorang aktitivis HAM, konsep HAM memiliki 2 dasar sebagai pengertian. (1), HAM ialah hak yang mengikat, tidak dapat dicabut, merupakan hak moral pada diri setiap manusia dengan tujuan menjadi jaminan dalam kehidupan. (2), HAM merupakan hak berdasarkan tahap pembentukan aturan hukum yang disesuaikan dengan aturan dari masyarakat, baik secata nasional ataupun internasional (Hasan, 2001). Edmon Makarim juga menyimpulkan bahwa Hak Asasi Manusia merupakan Hak Pribadi, antara lain ; (a) Hak tidak diusil; (b) Hak merahasiakan informasi pribadi dan (c) Hak mengontrol penggunaan data pribadi dari pihak lain (Makarim, 2010).

Pada hukum Indonesia mengenai perlindungan hak-hak pribadi ada pada UUD 1945 pasal 28 F bahwa, *"Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan social, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia."*

Adapun juga dalam pasal 28 G ayat (1) dan ayat (2), bahwa *"(1). 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 manusia, (2). Setiap orang berhak untuk bebas dari penyiksaan atau perlakuan yang merendahkan derajat martabat manusia dan berhak memperoleh suaka politik dari negara lain* (Undang-Undang, n.d.) Kemudian UUD Republik Federal Jerman 1949 (Bahasa Jerman disebut Ubergangszeit) mengenai perlindungan hak pribadi tertuang dalam Art 2 atau pasal 2 bahwa; *"(1). Everyone has the right to free development of their personality, as long as the do not violate the rights of others and do not violate the constitutional order or the moral code; (2). Everyone has the right to life and physical integrity. The freedom of a person is inviolable. These rights may only be interfered with on the basic of a law."* (Ministry, 2019). Diartikan pada ayat pertamanya bahwa setiap orang berhak atas kebebasan mengembahkan kepribadiannya, selama tidak melanggar hak orang lain serta tatanan konstitusional. Ayat kedua diartikan bahwa tiap orang berhak atas kehidupan dan keutuhan fisik kebebasan seseorang tidak bisa diganggu gugat. Hak tersebut hanya bisa di ganggu atas dasar undang-undang.

Adapun ditegaskan Kembali pada act 5 atau pasal 5 ayat (1) bahwa setiap orang berhak untuk secara bebas menyatakan dan menyebarluaskan pendapatnya dalam, kata, tulisan dan gambar serta untuk memperoleh ionformasi dari sumber yang dapat diakses ecra umum tanpa hambatan, kebebasan pers dan kebebasan melaporkan melalui radio dan film dijamin sebuah sensor tidak terjadi. Pada ayat (2) menyebutkan bahwa hak-hak ini dibatasi oleh ketentuan hukum umum, ketentuan perundang-undangan untuk perlindungan orang muda dan hak atas kehormatan pribadi.

3.3. Data Pribadi sebagai Hak Privasi

Indonesia dan Jerman memiliki kesamaan dalam memahami Data Pribadi sebagai Hak Privasi dari Data Pribadi dimana harus diberikan Perlindungan Hukum. Pengertian data pribadi itu sendiri ada diatur dalam Permenkominfo Pasal 1 Angka 1 nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik ("Permenkominfo 20/2016") "**Data Pribadi** adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". Dalam KBBI bahwa "kebebasan dan keleluasaan pribadi". Maka, kesimpulannya hak privasi adalah hak setiap orang untuk kebebasan dan keleluasaan pribadi demirasa nyaman dan aman. Hak privasi dan Data Pribadi memiliki keterkaitan, hal ini dapat dilihat Pasal 28 Huruf G Ayat (1) 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" (Undang-Undang, n.d.). Juga pasal 26 ayat (1) "Kecuali ditentukan lain oleh Peraturan Perundang-undangan,

penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."(Undang-Undang, 1999a).

Pada Undang-Undang Dasar Republik Federal Jerman 1949 Article 2 atau pasal ayat 2 menyebutkan "*Everyone has the right to life and physical integrity. The freedom of a person is inviolable. These rights may only be interfered with on the basic of a law."* Diartikan dalam bahwa "Setiap orang berhak atas kehidupan dan keutuhan fisik. Kebebasan seseorang tidak dapat diganggu gugat. Hak-hak ini hanya dapat diganggu atas dasar undang-undang". Juga didalam Article 5 atau pasal 5 ayat (2) *"These rights are limited by the provisions of general law, the statutory provisions for the protection of young people and the right to personal honour."* Dapat diartikan bahwa "bahwa hak-hak ini dibatasi oleh ketentuan hukum umum, ketentuan perundang-undangan untuk perlindungan orang muda dan hak atas kehormatan pribadi." Hak yang dimaksud merupakan hak data pribadi milik individu. Maka kesimpulannya data pribadi dan hak privasi memiliki keterkaitan juga saling berhubungan yang terdapat pada hak dari setiap insan untuk bebas menyebarluaskan informasi yang dimilikinya pada pihak lain berdasarkan kebebasan milik orang itu.

Pembahasan

3.4. Perbedaan yang terdapat dalam peraturan perlindungan data pribadi Indonesia dan Jerman

Aturan Hukum mengenai Perlindungan Data Pribadi

Peraturan Perlindungan Data Pribadi Indonesia

Indonesia belum memiliki aturan khusus mengenai data pribadi namun dari beberapa peraturan perundang-undangan memiliki aspek perlindungan yang terkandung didalamnya, didasari aturan mendasar yaitu Undang-Undang Dasar Negara Republik Indonesia 1945 pasal 28 F secara indikatif , pasal 28 C juga 28 G ayat (1) mengenai kebebasan mendapatkan informasi dan perlindungan data pribadi. Beberapa peraturan perlindungan Indonesia yaitu, Undang-Undang No.39 tahun 1999 tentang Hak Asasi Manusia terdapat pada pasal 14 ayat (2) yang menjelaskan mengenai hak pengembangan dan juga penggunaaan informasi pribadi. Pasal 32 berisi kerahasiaan informasi melalu elektronik termasuk informasi pribadi. Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik, pada pasal 26 ayat (1) mengenai penggunaan informasi pribadi melalui elektronik atas persetujuan yang bersangkutan dan pada ayat (2) menjelaskan apabila melanggar akan diberikan kebebasan kepada pemilik untuk mengajukan gugatan. Secara keseluruhan pasal ini menjelaskan perizinan terlebih dahulu dari pemilik data jika diperlukan.

Undang-Undang No. 36 tahun 1999 tentang Telekomunikasi, pada pasal 22 yang berisi larangan memanipulasi jaringan telekomunikasi serta sanksi denda sebanyak Rp 600.000,00 atau sanksi penjara maksimal 6 tahun (Undang-Undang, 1999b). Undang-Undang ini didampingi oleh Peraturan Pemerintah tahun 2000 tentang penyelenggaraan telekomunikasi sebagai aturan pelaksana dari Undang-Undang No. 36 tahun 1999. Peraturan Pemerintah No. 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, pada pasal 12 ayat (1) huruf c mengenai kewajiban menjaga rahasia data pribadi yang dikelola dan jaminan sesuai pemilik data (Pemerintah, 2012). Pada pasal 22 ayat (1), pasal 38 ayat (2), pasal 39 ayat (1), pasal 55 ayat (3), pasal 68 ayat (1) memiliik kesamaan mengenai kewajiban perlindungan informasi data elektronik. Bahkan terdapat pasal 15 ayat (2) yang mengatur apabila terjadi kegagalan atau data bocor maka pihak pengelola harus segera memberikan informasi kepada pemilik data.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No.20 tahun 2016 tentang Perlindungan Data Pribadi dalam system elektronik, pasal (1) mengenai perlindungan wajib terhadap data yang disimpan. Pasal 2 (1) berisi tentang perlindungan data itu mencakup perolehan, pengumpulan, pengolahan, penganalisaan, penyampaian, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data. Tentu saja hal ini harus disesuaikan dengan asas perlindungan data sebagai betuk penghormatan data pribadi yang merupakan bagian dari hak privasi. Dalam pasal 2 (3) menjelaskan hak pemilik data dapat mengatakan apakah data tersebut bersifat rahasia atau tidak (Patent No. 20, 2016). Aturan yang terakhir adalah Naskah Akademik dari Rancangan Undang-Undang Perlindungan Data Pribadi. Namun aturan ini masih bersifat gagasan

berbentuk Rancangan yang belum diberlakukan hingga saat ini. Rancangan ini dibuat dengan dasar kondisi masyarakat yang semakin maju sangat membutuhkan perlindungan hukum juga kenyamanan dalam berselancar di media elektronik. Di dalam Rancangan tersebut mengatur secara khusus Perlindungan Data Pribadi juga hak dan kewajiban pemilik data atas data dan informasi pribadinya.

3.5. Peraturan Perlindungan Data Pribadi Jerman

Jerman merupakan bagian dari anggota Uni Eropa, sebelum GDPR berlaku Jerman memiliki Undang-Undang tersendiri mengenai perlindungan data pribadi yaitu The German Federal Data Protection Act (disebut dengan BDSG-*Bundesdatenschutzgesetz*). Aturan didalamnya terdapat pengaturan mengenai pemrosesan data secara umum dan secara rahasia. Jerman juga mempunyai peraturan khusus informasi dan pelayanan elektronik serta pelayanan provider. Aturan Uni Eropa 95/46/EC dan 2002/58/EC diadopsi oleh Jerman.

Mahkamah Konstitusi Jerman pada 1983 menetapkan hak warga negara untuk bebas menggunakan data pribadi dan menguraikan perlindungan privasi data pribadi sebagai hak konstitusional warga negara. Pemerintah Jerman memberikan perhatian secara keseluruhan dan menjadikan hal penting konstitusi terhadap perlindungan data pribadi serta rasa aman bagi setiap orang (Stepanova & Raul, 2018). Selain itu Mahkamah Konstitus memberikan bagi para pihak untuk melakukan pemrosesan data tentunya dengan persetujuan. Pada tahun 2010, aturan permutasian data dibatalkan oleh Mahkamah Konstitusi dalam the Europa Union Data Retention Directive karena dianggap melanggar hak pribadi individu dan prinsip proporsionalitas. GDPR diberlakukan tahun 2018 di Uni Eropa. GDPR mengatur hak atas perlindungan data pribadi, hak melakukan pemrosesan juga mengontrol informasi identitas diri. GDPR berlaku bukan hanya untk individu tapi juga instansi serta badan-badan resmi.

> Dalam pasal 2 (a) mengenai Data Protection Directive yang berbunyi, "*any information relating to an identified or or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*(European Union Agency for Fundamental Rights and Council of Europe, 2014).

Dalam European Union data Protection Directive, data dibedakan berdasarkan peringkat besarnya bahaya yang terjadi tanpa sepengetahuan atau persetuan pemilik data. Data dibedakan menjadi data sensitif dan data non-sensitif data sensitif diartikan sebagai data yang berhak mendapatkan perlindungan hukum lebih ketat, perizinan harus dilakukan secara tertulis. Aturan European Union Data Protection Directive mewajibkan data yang diolah harus mendapatkan perizinan oleh pemilik data terutama data sensitive yang menyangkut informasi pribadi seperti etnis, pendapat politik, agama, kepercayaan, keanggotaan organisasi dan data yangberhubungan dengan Kesehatan dari pemilik data (Direktif Parlemen dan Dewan Konsil Eropa, 2016).

3.6. Aturan Klasifikasi Data Pribadi

Dalam peraturan GDPR yang berlakukan di Jerman selain BDSG terdapat beberapa hal penting yang menjadi dasar aturan ini yang menjadi perbedaan diantaranya; pertama, peraturan mengenai penghapusan data sepeti data berupa nama, alamat IP, gambar atau foto, alamat e-mail, Alamat rumah, aktivitas social media, informasi perbankan dan Kesehatan (Eropa, 2016). Kedua, peraturan mengenai tahapan dalam penghapusan data. Ketiga, aturan mengenai pengawas dalam pengelolaan data. Keempat, adaanya penyeragaman aturan formulir Privacy Policy. Di Indonesia belum memiliki aturan klasifikasi pada data pribadi apabila dapat dilakukan penghapusan data. Belum diatur juga secara konsep dala peraturan perundang-undangan. Belum adanya tahapan notifikasi mengenai penghapusan data tersendiri, harus melalui putusan pengadilan. Ini dikarenakan belum adanya Lembaga khusus yang berwenang mengawasi penggunaan data pribadi serta tidak adanya aturan penyeragaman privacy policy.

3.7. Aturan Pelaksana Pengawas Perlindungan Data Pribadi

Pelaksana Pengawas Perlindungan Data Pribadi Indonesia

Indonesia belum ada otoritas pelindungan data nasional untuk data privasi. Contoh, pada Otoritas Jasa Keuangan Indonesia memiliki kewenangan menjadi regulator privasi data pada bidang pasar modal dan selalu berkaitan dengan permasalahan data pribadi pelanggan bank. Namun pada Peraturan Pemerintan No.82 tahun 2012 pasal 65 menyebutkan pelaku bisnis yang melakukan transaksi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan dari dalam tingkat nasional maupun internasional. Namun Lembaga tersebut belum ada di Indonesia. Lembaga yang di maksud merupakan Lembaga Sertifikasi Sistem Manajemen Pengamanan Informasi yang menerbitkan sertifikat legal Sistem Manajemen Pengamanan Informasi. Sertifikat tersebut berbentuk tertulis yang diberikan kepada penyelenggara sistem elektronik.

Pelaksana Pengawas Perlindungan Data Pribadi Jerman

Dalam pelaksanaan dan pengawasan perlindungan data pribadi, Jerman sudah memiliki beberapa pihak yang ditugaskan demi keamanan dan kenyamanan masyarakat hal ini diatur dalam GDPR. Petugas Perlindugan Data Pribadi yang ditetapkan berdasarkan aturan GDPR sebagai pengontrol untuk aktivitas pemrosesan data dengan kualifikasi sebagai berikut; (a) Otoritas publik; (b) kegiatan inti seperti operasi pemrosesan yang disesuaikan dengan sifatnya, tujuan yang membutuhkan pemantauan subjek dan (c) pengawasan pemrosesan data sensitive. Tentu saja dalam pemilihan tugas persyaratan yang dimiliki harus ketat, ditentukan pada badan-badan resmi. Tugas dari Petugas Prlindunga Data yaitu bekerja secara detai disesuaikan dengan Peraturan Perlindungan Data Pribadi, maka dari itu siapapun yang bekerja menjadi Petugas Perlindungan Data Pribadi tidak dapat diberhentikan atau dihukum karena memenuhi tugasnya (Eropa, 2016). Selain itu, Jerman memiliki Dewan Perlindungan Data Eropa yang merupakan badan resmi yang dibangung khusus wilayah Uni Eropa. Setiap negara memiliki tanggungjawab menunjuk satu supervise yang ditugaskan untuk memantau dalam mengimplementasikan norma dan peraturan dalam GDPR. Dewan Perlindungan ini juga bertanggungjawab menindaklanjuti permasalahan apabila terjadi pelanggaran dalam Perlindungan Data Pribadi.

3.8. Kontribusi hukum perlindungan data pribadi Jerman apabila dapat diadopsi ke pengaturan data pribadi Indonesia

Beberapa inti penting dapat dipelajari dan dipahami dari Peraturan Perlindungan Data Pribadi di Jerman dan dapat didaptasi oleh Indonesia. Diantaranya mengenai pemberlakuan peraturan khusus sendiri yang mengatur Perlindungan Data Pribadi, melihat Indonesia sampai saat ini belum memiliki aturan hukum terkait mengenai Data Pribadi hingga Rancangan mengenai Perlindungan Data Pribadi belum segera disahkan dan diberlakukan. Peraturan klasifikasi data pribadi dari GDPR mengenai data sensitive dan non-sensitif dapat diadaptasi di Indonesia, perbedaan tersebut sangatlah penting yang sebelumnya telah dijelaskan bahwa adanya perbedaan tersebut memudahkan pengawas mengontrol data pemilik. Aturan perizinan pemiliik data apakah data tersebut merupakan data sensitive yang dibuktikan dengan pernyataan tertulis. Dalam aturan tersebut juga mengatur tahapan penghapusan data., aturan mengenai badan resmi atau pengawas yang mengelola data serta keseragaman aturan formulir privacy policy. Di Indonesia belum memilii aturan tersebut sehingga tidak dapat menjamin kenyamanan dan keamanan data pribadi yang dimiliki, bahkan untuk tahapan penghapusan data pribadi belum diatur dan harus melalui putusan pengadilan terlebih dahulu.

Secara teknis, di Indonesia memang memiliki peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam system elektronik yang dianggap menjadi peraturan lengkap mengenai aturan data pribadi. Namun didalam peraturan tesebut tidak terdapat aturan mengenai aturan mengenai penghapusan data pribadi. Apabila dilihat dari aturan Uni Eropa yaitu, GDPR. Contohnya seperti makna, jenis data, standarisasi peraturan perusahaan serta aturan pemebritahuan setelah dihapusnya data pribadi. Hal ini membuat pengelolaan data pribadi di Indonesia tidak dapat diawasi dan dilindungi. Beberapa kasus kebocoran data pada social

media terjadi seperti Facebook, Whatsapp, Google atau social media lainnya yang korbannya merupakan warga negara Indonesia, menjadi korban tindak kejahatan penyalahgunaan data pribadi, dikarenakan peraturan di Indonesia belum ada yang mengatur secara khusus mengenai aturan pengawasan, sanksi atas penyelenggaraan data pribadi. Sehingga jika dilihat GDPR yang memiliki aturan pengelolaan data termasuk penghapusan data pribadi. Indonesia dapat mengadaptasi aturan tersebut dan cocok untuk diterapkan di Indonesia demi menjamin perlindungan data pribadi masyarakat, jadi penghapusan data tidak perlu melalui proses dan menunggu putusan pengadilan. Indonesia juga dapat mengacu pada aturan GDPR mengenai Lembaga pengawas yang bertugas untuk mengelola data. Lembaga tersebut secara khusus dibentuk untuk tujuan perlindungan data pribadi seperti yang dijelaskan sebelumnya, Jerman memiliki petugas perlindungan data pribadi dan Dewan Perlindungan Data Eropa. Tugas dari petugas perlindungan data pribadi diatur dalam Undang Undang Jerman atau BDSG pada article 7 atau pasal 7 ayat (1) yang diartikan sebagai berikut
,

a) Untuk menginformasikan dan memberi saran kepada badan public dan karyawan yang melakukan pemrosesan kewajiban mereka sesuai dengan Undang-Undang ini dan Undang-Undang perlindungan data lainnya, termasuk Undang-Undang yang diber;akukan untuk menerapkan Directive (EU) 2016/680
b) Untuk memantau kepatuhan terhadap Undang-Undang ini dan Undang-Undang perlindungan data lainnya, termasuk Undang-Undang yang diberlakukan untuk menerapkan Directive (EU) 2016/680, dan dengan kebijakan badan public terkait dengan perlindungan data pribadi termasuk penugasan tanggungjawab, peningkatan kesadaran, dan pelatihan staf yang terlibat dalam operasi pemrosesan dan audit terkait.
c) Memberikan saran mengenai penilaian dampak perlindung data dan memantau pelaksanaannya sesua dengan pasal 67 Undang-Undang ini
d) Bekerja sama dengan otoritas pengawas
e) Untuk bertindak sebagai titik kontak untuk otoritas pengawas tentang masalah yang berkaitan dengan pemrosesan, termasuk konsultasi sebelumnya yang dirujuk dalam bagian 69 Undang-Undang ini, dan untuk berkonsultasi, jika perlu, terkait dengan masalah lain (BDGS, n.d.).

Indonesia dapat mengadaptasi aturan tersebut menjadikan acuran untuk membentuk Lembaga independent yang memiliki tugas untuk mengawasi pengelolaan data pribadi dan bertindak sebagai petugas perlindungan data pribadi. Selain itu juga membentuk Dewan Perlindungan Data Pribadi apabila terjadinya kesalahan pada penerapan norma dan aturan mengenai Perlindungan Data Pribadi, dapat segera menindaklanjuti permasalahan tersebut.

4. CONCLUSION

Berdasarkan pembahasan yang telah dipaparkan, jerman memiliki sejarah terkait perlindungan data perlindungan sebelum berlakunya GDPR, yaitu BDSG yang mengatur secara khusus tentang perlindungan data pribadi. Indonesia dan Jerman memilki persamaan diantaranya yang pertama, perlindungan data pribadi yang dianggap hak asasi manusia. Perlindungan tersebut merupakan hak yang melekat pada diri setiap manusia termasuk informasi data pribadi. Hal ini diatur dalam Undang-Undang Dasar Republik Indonesia tahun 1945 pasal 28F-28G ayat (1) dan BDSG pada article 2 juga article 5 paragraph 2. Kedua, data pribadi merupakan bagian dari Hak Privasi, hal ini dibuktikan pada hak data pribadi yang seharusnya mendapatkan perlindungan data pribadi, maka data pribadi dan hak privasi saling berkaitan satu sama lain. Adapun perbedaan yang dimiliki dari peraturan perlindungan pribadi Indonesia dan Jerman yang terletak pada aturan yang mengatur. Indonesia tidak memiliki aturan khusus sendiri mengenai perlindungan data pribadi seperti Jerman, walau beberapa Undang-Undang Indonesia mengatur mengenai data pribadi namun tetap saja hal ini tidak menjadikan ketetapan hukum yang mengatur data pribadi. Indonesia juga belum mengatur klasifikasi data termasuk penghapusan data pribadi serta pembentukan otoritas pengawan perlindungan data pribadi. Dapat disimpulkan bahwasanya Indonesia dapat mengadaptasi beberapa

aturan di Jerman baik pada GDPR atau BDSG, seperti aturan khusus perlindungan data pribadi, aturan klasifikasi data termasuk penghapusan data pribadi, serta aturan pengawas perlindungan data pribadi sebelum membentuk Lembaga pengawas perlindungan data pribadi.

REFERENSI

(EU), R. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da*.

A, M. (2013). *Information Technology Law : The Lawa and Society*. Inggris: University Press.

Ayumardi, A. (2000). *Demokrasi Hak Asas Manusia dan Masyarakat Madani 2000), hal 32*. Jakarta: Tim UIM SyarifHidayatullah.

BDGS. (n.d.). *Federal Data Protection Act (BDSG), Article 7 paragraph 1*. Jerman.

Direktif Parlemen dan Dewan Konsil Eropa. *Direktif Parlemen dan Dewan Konsil Eropa No. 2016/680 tanggal 27 April 2016 yang terkait perlindungan oleh pihak individu sehubungan yang berwenang dengan tujuan pencegahan, investigasi, deteksi, atau penuntutan pelanggaran pidaha/eksekusi hukuman pidana* . , (2016). Eropa.

Eropa, U. (2016). *The General Data Protection Regulation*. *697*(1).

European Union Agency for Fundamental Rights and Council of Europe. (2014). European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law. In *Handbook on European Data Protection Law*. Belgium.

Fahey, E. (2010). Pendapat Claude Moranes di "The European Parliament and Transatlantic Relations: Personal Reflections Institutionalisation beyond the Nation State Transatlantic Relations: Data. *Privacy and Trade Law Studies in European Economic Law and Regulation*, *10*(1).

Hasan, M. T. (2001). *Perlindungan terhadap Korban Kekerasan Seksual (Advokasi atas Hak Asasi Manusia)*. Bandung: Refika.

Indonesia, N. (2021). "Menunggu UU Perlindungan Data Pribadi.

Jayani, D. H. (2021). "Pencurian Data Pribadi makin Marak kala pandemic.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2016). *Patent No. 20*. Indonesia.

Makarim, E. (2010). *Tanggungjawab Penyelenggara Sistem Elektronik*. Jakarta: Rajawali Pers.

Marzuki, P. M. (2008). *Penelitian Hukum Kasus*. Jakarta: Kencana.

Masyhur, E. (1994). *Dimensi/Dinamika Hak Aasasi Manusia dalam hukum Nasional dan Internasional*. Jakarta: Gahlia Indonesai.

Ministry, F. (2019). Federal Data Protection Act (BDSG).

Pemerintah, P. *Peraturan Pemerintah, No. 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, pada pasal 12 ayat (1) huruf c.* , (2012). Indoensia.

Poerwandari, E. K. (1980). *Pendekatan Kualitatif dalam Penelitian*. Jakarta: Lembaga dan Perjuangan Psikologi.

Raul, A. C., & Stepanova, O. (2018). *Privacy, Data Protection and Cybersecurity Law Review Fifth Edition*. London: Law Business Research Ltd.

Rokhayah, S. (2022). Marak, Waspada Pencurian Data Pribadi.

Seokanto, S., & Mamuji, S. (2001). *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. Jakarta: Rajawali Pers.

Stepanova, O., & Raul, A. C. (2018). *Privacy, Data Protection and Cybersecurity Law Review Fifth Edition*. London: Law Business Research Ltd.

Sudibyo, A. (2019). *Jagat Digital : Pembebasan dan penguasaan*. Jakarta: Kepustakaan Populer Gramedia.

Susmoro, H. (2019). *The Spearhead of Sea Power*. Yogyakarta: Pandiva Buku.

Undang-Undang. *Undang-Undang Dasar Tahun 1945, pasal 28 F dan 28 G*. Indonesia.

Undang-Undang. *Indonesia, Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia, pasal 1.* , (1999). Indonesia.

Undang-Undang. *Undang-Undang No. 36 tahun 1999 tentang Telekomunikasi, pada pasal 22.* , (1999).

Indonesia.

Wibisono, A. (2019). Kementerian Keuangan Republik Indonesia : Memahami Metode Penelitian Kualitatif.

Zaenudin, A., & Jovankurbalija. (2018). "Data warga Eropa yang disimpan di Indonesia harus dilindungi.