KEPANITERAAN DAN SEKRETARIAT JENDERAL

MAHKAMAH KONSTITUSI

HASIL PENELITIAN

Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital

Oleh:

KETUA : ANANTHIA AYU D. (19850906201402 2001)

ANGGOTA : 1. TITIS ANINDYAJATI (19850907201012 2001)

2. ABDUL GHOFFAR (19800701200712 1001)

PUSAT PENELITIAN DAN PENGKAJIAN PERKARA, DAN PENGELOLAAN PERPUSTAKAAN

KEPANITERAAN DAN SEKRETARIAT JENDERAL

MAHKAMAH KONSTITUSI

JAKARTA

2019

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

A. Latar Belakang

Dewasa ini telah nyata terlihat bahwa informasi memiliki posisi penting dalam ekonomi, sosial dan juga sebagai pertimbangan pengambilan keputusan politik. Francis Bacon yang merupakan filsuf ternama dalam transisi *Reinasance* ke dalam era modern, menyatakan bahwa pengetahuan itu sendiri merupakan kekuatan yang besar. Terminologi pengetahuan sendiri dapat ditarik di kompetensi yang lebih luas dimana seseorang yang memiliki informasi lebih dari orang di sekitarnya. di satu sisi, skala besar investasi dan teknologi aplikasi dapat diwujudkan dengan informasi industri dalam dekade terakhir, tergantung pada informasi yang didapat yang mengarah pada ide bahwa pemrosesan data merupakan aktivitas yang tidak tergantikan dalam kesuksesan industri dan teknologi.[1]

Teknologi informasi telah mengubah pola hidup masyarakat dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung dengan signifikan.Hal ini pada akhirnya juga mengakibatkan terciptanya suatu pasar baru yang telah mendorong perkembangan sistem ekonomi masyarakat, dari ekonomi tradisional yang berbasiskan industri manufaktur ke arah *digital economy* atau ekonomi digital. Ekonomi digital lahir

[1] Iike Gursel, dalam *Protection of Personal Data in International of Data in International Law and The General Aspect of The Turkish Data Protection Law,"The Right to Data Protection of the Employee*" dipresentasikan pada *the 1st International Scientific Researches Humanity and Social Sciences Conference* (May 19-22, 2016, Madrid, Spanyol).

dan berkembang seiring penggunaan teknologi informasi dan komunikasi yang juga semakin mengglobal di dunia.

Sebagai negara terpadat di Asia Tenggara dengan populasi 262 juta dengan 140 juta terhubung internet, sekitar 28 juta orang (13% growth YoY) aktif melakukan transaksi online. Kapasitas Indonesia dengan sekitar 49 juta UMKM (SME's) membuat pemerintah Indonesia bertekad menjadi negara dengan digital ekonomi terbesar di Asia Tenggara dimana pada tahun 2020 menyakini akan mampu akan menyerap 26 juta lebih tenaga kerja.[2]

Saat ini pemerintah sedang mencanangkan Indonesia sebagai kekuatan ekonomi digital terbesar di Asia Tenggara pada tahun 2020. Salah satu landasan pembangunan nasional dalam pencanangan ini adalah sektor digital. Pemerintah menargetkan transaksi *ecommerce* mencapai senilai US$ 130 miliar dan menciptakan 1000 teknopreneur dengan nilai bisnis US$ 10 miliar pada tahun 2020.[3]

Indonesia menjadi tempat yang menjanjikan untuk pasar ekonomi digital. Hal itu dapat diketahui dari total populasi Indonesia sebesar 265,4 juta penduduk yang 50 persennya yaitu 132,7 juta penduduk sudah menggunakan internet. Dari jumlah tersebut, pengguna perangkat seluler mencapai 177,9 juta penduduk dan

[2] Lahirnya 4 unicorn Indonesia, Gojek (transportasi dan lintas sektor), Traveloka (ticket and travel), Tokopedia dan Bukalapak (market place) terjadi setelah mendapatkan suntikan dana dari investor global atau pemain retailer besar dunia atau kapital player yang menginvest untuk dijual kembali. Keempatnya merupakan usaha yang dimulai dari bawah dan dengan kerjakeras yang baik namun ketergantungan terhadap modal begitu tinggi agar bisa berkembang. Masuknya pemain besar global membuat usaha online ini semakin terintegerasi dengan pemain global yang telah mendominasi banyak negara. Olisias Gultom, Katrin Schneider, dan Lea Mareen Preis, Ekonomi Digital, Harapan, dan Ancaman Belajar dari Indonesia, diunduh melalui http://igj.or.id/wp-content/uploads/2018/11/Industrial-Revolution-4_IGJ_AEPF12_Ind-1.pdf

[3] Tim Peneliti Badan Penelitian dan Pengembangan SDM, Kementerian Komunikasi dan Informatika, Studi Ekonomi Digital di Indonesia sebagai Pendorong Utama Pembentukan Industri Digital Masa Depan, diunduh melalui https://balitbangsdm.kominfo.go.id/?mod=publikasi... pada tanggal 2 April 2019

pengguna media sosial (medsos) seluler aktif sebesar 120 juta penduduk. Hasil riset Google dan Temasek pada 2018, diprediksi Market Size Ekonomi Digital Indonesia mencapai USD 100 Miliar pada tahun 2025.

Perkembangan teknologi informasi dan potensi ekonomi digital yang cukup besar juga diiringi oleh beberapa dampak negatif antara lain ancaman terhadap hak atas privasi dan data diri warga negara. Hak atas privasi atau *privacy right* merupakan salah satu hak dalam *fundamental right*.[4] Hak atas privasi walaupun bukan hak asasi yang absolut akan tetapi perlindungan hukum akan hak privasi tetap sangat krusial di era ekonomi digital ini.

Penggunaan teknologi internet yang meluas di dunia merupakan faktor substansi yang memberikan kontribusi atas meningkatnya pemrosesan data. Hal tersebut tidak diragukan bahwa internet menjadikan pertukaran informasi antar individu lebih mudah dan dan lebih masif. Sirkulasi secara berkelanjutan informasi individu melalui fasilitas internet yang tidak sah oleh karena itu terdapat alasan yang fokus kepada aktifitas pemrosesan data yang tidak adil antara konsumen pengguna internet dengan perusahaan yang melakukan pemrosesan data.[5]

Satu hal yang perlu diperhatikan bahwa sekali kita menggunakan internet, maka seluruh aktivitas yang kita lakukan atau situs yang pernah kita kunjungi akan terekan dan seluruh informasi tersebut menjadi jejak digital yang sudah terekam. Oleh karena itu, perlindungan data terhadap penyalahgunaan oleh pihak

[4] Lihat Piagam Hak Fundamental Uni Eropa (*Charter of Fundamental Rights of The Eropean Union*) (2012/C 326/02) Pasal 8

[5] Lihat Jacqueline Klosek, *Data Privacy in the Information Age*, Greenwood Publishing Amerika Serikat 2000, hal. 1 dan Ulrich Sieber, *The Emergence of Information Law: Object and Characteristics of a New Legal Area", Law, Information and Information Technology*, (Ed. Eli Ledermen/Ron Shapira), Kluwer Law International, Denhaag 2001, hal. 8.

ketiga memang menjadi masalah yang sensitif dan tidak mudah untuk diselesaikan. Perkembangan beserta permasalahan yang disebutkan di atas mendorong negara dan lembaga internasional untuk menguraikan masalah ini dan menetapkan kerangka hukum terkait pemrosesan data.

Perusahaan *e-commerce* harus melindungi data pribadi konsumennya. Kontroversi juga terjadi dalam praktik permintaan data kartu keluarga dalam pendaftaran kartu prabayar. Masalah serius muncul ketika praktik semacam ini dihadapkan dengan isu privasi dan perlindungan data pribadi konsumen.

Amerika Serikat juga mengalami permasalahan pelanggaran hak atas privasi dan data diri. Kasus kebocoran data pertama kali diungkapkan oleh *The Guardian*, media ternama di Inggris pada 26 Maret 2018. Di media tersebut, menengarai *Cambridge Analytica* yang merupakan perusahaan analisis data telah menggunakan informasi pribadi yang diambil dari *Facebook* tanpa izin untuk membangun sistem yang dapat menargetkan pemilih Amerika Serikat dengan iklan politik yang dipersonalisasi berdasarkan profil psikologis mereka. Hal tersebut terungkap ketika Christopher Wylie, mantan kontraktor *Cambridge Analytica* menguraikan bagaimana dengan data tersebut dibangun algoritma. Contoh kasus pelanggaran hak ats privasi dan data diri di Amerika Serikat dapat menjadi preseden buruk sisi lain dari perkembangan teknologi informasi.[6]

Pada konteks ekonomi digital, pelaku usaha seperti mekanisme dagang dengan *e-commerce* dan transaksi menggunakan *e-banking* menyimpan data pribadi konsumen seperti nama, alamat rumah atau kantor, alamat email bahkan

[6]Handrini Ardiyanti, *Big Data* Di Media Sosial, Alogaritma dan Pemilu., Kajian Singkat Terhadap Isu Aktual dan Strategis, Pusat Penelitian Badan Keahlian DPR RI, Bidang Pemerintahan Dalam Negeri, Vol. X, No. 09/I/Puslit/Mei/2018

sampai ke data nomor rekening bank milik konsumen. Ketika melakukan transaksi e-commerce, konsumen tidak hanya terekam nomor rekening saja namun untuk konsumen yang menggunakan kartu kredit maka akan terekam pula data kartu kreditnya di situs *e-commerce* tempat konsumen melakukan transaksi.

Berita mengenai maraknya penipuan menggunakan situs *e-commerce* (perdagangan elekrtorik) merupakan hal yang sering dijumpai di tanah air.Masyarakat yang sadar akan hal ini enggan atau khawatir menggunakan kartu kredit yang melibatkan privasi dan data pribadi. Seiring banyaknya situs *e-commerce* Indonesia memerlukan akan adanya jaminan perlindungan privasi dan data pribadinya. Kini, penipuan yang tumbuh subur dengan memanfaatkan media sosial seperti facebook dan Instagram.[7]

Tidak sedikit masyarakat Indonesia yang mengeluhkan aktivitas telemarketing yang masuk ke dalam kategori *direct marketing*, yaitu menawarkan secara langsung produk-produk keuangan seperti asuransi dan pinjaman tanpa agunan. Masalah yang ada dalam praktik semacam ini salah satunya adalah perpindahan data pribadi nasabah atau masyarakat yang tidak sesuai dengan prinsip etika. Data pribadi yang nasabah beredar luas di kalangan perusahaan yang menggunakan cara *direct marketing* menggunakan telepon. Apabila masalah semacam ini timbul, maka Otoritas Jasa Keuangan dapat menjadi lembaga pengaduan yang dapat digunakan oleh masyarakat. Namun demikian, praktik telemarketing tanpa persetujuan masyarakat terlebih dahulu tetap saja marak di Indonesia.

[7]Sinta Dewi, Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional, Refika, Bandung, 2015, hlm 91

Kontroversi juga terjadi dalam praktik permintaan data kartu keluarga dalam pendaftaran kartu prabayar. Masalah serius muncul ketika praktik semacam ini dihadapkan dengan isu privasi dan perlindungan data pribadi konsumen. Operator telepon seluler dalam hal ini menjadi pengumpul, pengolah sekaligus pemroses data pribadi yang secara masif diserahkan beramai-ramai oleh masyarakat karena didorong oleh kebijakan pemerintah. Kedua hal di atas mencerminkan adanya masalah sistemis dalam faktor kesadaran hukum masyarakat, faktor kurang efektifnya regulasi dan penegakan hukum.

Terdapat tiga pendekatan dalam perlindungan hak privasi warga negara dalam era ekonomi digital ini, pendekatan tersebut antara lain aspek hukum, aspek teknologi dan aspek etika. Khusus untuk penelitian ini, aspek yang digunakan adalah aspek hukum. Penelitian ini juga menggunakan studi komparasi dengan perlindungan terhadap privasi warga negara di Uni Eropa.

European Charter of Human Rights (ECHR,2000) dan *ASEAN Human Rights Declaration* (AHRD,2012) telah mengakui Hak atas perlindungan data pribad sebagai jenis Hak Asasi Manusia. Hak atas perlindungan data pribadi merupakan suatu hak hasil bentukan dari irisan penggabungan hak atas informasi dan hak atas privasi yang telah melalui evolusi yang panjang sejak diakuinya hak asasi manusia dalam *the Universal Declaration of Human Rights* (UDHR, 1948).

Data pribadi merupakan keterangan yang benar dan nyata yang melekat pada diri seseorang, sehingga dapat mengidentifikasikan orang tersebut. Pentingnya perlindungan data pribadi adalah untuk memastikan bahwa data pribadi seseorang yang terkumpul digunakan sesuai dengan tujuan pengumpulan, sehingga tidak terjadi penyalahgunaan data.

Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut *the right to private life*. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi.[8] Privasi memang tidak dicantumkan secara eksplisit di dalam Undang-Undang Dasar 1945. Namun, secara implisit hak atas privasi terkandung di dalam Pasal 28G ayat (1) UUD NRI 1945 sebagai berikut:

> "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".

Jaminan terhadap hak atas privasi juga termaktub dalam undang-undang lain yaitu Pasal 29 ayat (1) dan Pasal 30 Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia. Data Pribadi merupakan suatu konsep yang menggambarkan proses atau upaya menggabungkan pengaturan-pengaturan mengenai privasi dan data pribadi yang tersebar di berbagai instrumen hukum ke dalam satu instrumen hukum tersendiri. Dengan demikian perlindungan privasi dan data pribadi memiliki tempat yang *sui generis.*

Uni Eropa telah memiliki *The European Union DP Directive* (*Directive*) diperkenalkan tahun 1995 dengan tujuan untuk mengharmonisasi peraturan nasional di antara negara-negara anggota EU. *Directive* tersebut dianggap sebagai satu di antara rezim yang paling kuat. Regulasi terkini di Uni Eropa terkait Hak atas privasi pada data pribadi ada dalam *General Data Protection Regulation* (GDPR).

[8]*European Union Agency for Fundamental Rights and Council of Europe*, Supra no 5,. hlm. 37.

Di Asia sendiri, beberapa negara telah memiliki regulasi terkait perlindungan hak atas privasi. Hong Kong telah memiliki *Personal Data Privacy Ordinance* of 1995 (PDPO) sebagai peraturan perundang-undangan nasional pertama yang mengatur masalah privasi dan data pribadi data secara komprehensif. Privasi atas data pribadi Malaysia dilindungi melalui *The Personal Data Protection Act* No. 709 of 2010 (PDPA Malaysia). Sedangkan, Privasi dan data pribadi di Singapura dilindungi secara sektoral oleh *The Personal Data Protection Act No. 26 of 2012 Singapore* (PDPA 2012 Singapura).

Indonesia saat ini sedang melalui proses pembahasan perlindungan privasi dan data pribadi karena Indonesia telah memiliki RUU Perlindungan Data Pribadi. Fakta bahwa para ilmuwan tidak tahu aturan yang menentukan bidang permainan mereka sambil mempertahankan bahwa mereka dibatasi oleh mereka adalah masalah. Sebagai permulaan, *ignorantia juris non excusat* ("ketidaktahuan hukum tidak memaafkan"), dan kedua, hukum memiliki kekuatan normatif, aturan seharusnya dipatuhi.

Rancangan Undang-Undang tersebut bertujuan untuk menggabungkan pengaturan-pengaturan privasi atas data pribadi yang tersebar, ke dalam suatu undang-undang tersendiri. Perancangan Naskah Akademik sebagai fase awal proses konvergensi tersebut telah dirampungkan pada bulan Oktober 2015. Indonesia cukup tertinggal dalam menyelesaikan isu terkait perlindungan hak atas privasi terutama jika melihat kerangka legislasi dari perlindungan hak atas privasi, baik dari segi waktu maupun variasi perlindungannya**.**

Perlindungan hukum merupakan salah satu cara terbaik untuk memproteksi suatu subjek hukum dari kesewenangan yang diterapkan.

Perlindungan hukum mencangkup secara luas dalam segi tatanan hukumnya.Informasi adalah sumber utama. Di bidang ekonomi, dan memang untuk beberapa waktu sekarang, informasi telah dianggap sebagai barang yang sangat berbeda. Ini diperlukan untuk setiap transaksi (mis., Untuk setiap pembelian di pasar) dan biayanya mahal (setidaknya dalam bentuk biaya pencarian dan waktu). Bahkan, informasi telah menjadi salah satu komponen kunci dari teori ekonomi dan bidang utama penelitian ekonomi.

Walaupun perkembangan teknologi informasi dan ekonomi digital sangat pesat namun penelitian terkait hukum dan teknologi secara umum dan perlindungan hak privasi belum terlalu banyak. Disamping itu, peneliti merupakan generasi yang banyak terpapar oleh dunia teknologi informasi dan ekonomi digital dan memiliki minat untuk mengkaji studi teknologi informasi yang dihubungkan dengan perlindungan hak-hak warga negara. Oleh karenanya, Peneliti memiliki ketertarikan untuk mengkaji lebih lanjut dalam sebuah penelitan terkait permasalahan perlindungan hak atas privasi warga Negara.

B. Rumusan Masalah

Untuk membatasi ruang lingkup masalah pada penelitian ini, terdapat permasalahan yaitu;

1. Bagaimana pengaturan hak atas privasi atas data diri di Indonesia dan Jerman?
2. Bagaimana Perlindungan Hukum Hak Atas Privasi dan Data Diri di era ekonomi digital?

C. Tujuan

Berdasarkan rumusan masalah yang diajukan, maka penelitian ini bertujuan untuk:

1. Mengetahui dan menganalisis pengertian, batasan, dan ruang lingkup hak atas privasi dan data diri.
2. Mengetahui dan menganalisis perlindungan hukum hak atas privasi dan data diri di era digital.

D. Manfaat

Dengan dicapainya tujuan di atas, diharapkan hasil penelitian ini dapat memberikan kontribusi sebagai berikut:

1. Penelitian ini dapat dijadikan referensi pembuat kebijakan dalam menyusun produk hukum yang berkaitan dengan perlindungan hak atas privasi dan data diri.
2. Penelitian ini juga dapat dijadikan referensi atau pengkayaan khazanah penelitian di bidang hukum dan teknologi.

BAB II

Hak Privasi dan Konsep Data Diri

A. Hak Privasi

Banyak ahli hukum yang mencoba mendefinisikant privasi. Namun beberapa teori privasi hanya mengulas dasar-dasar teori privasi secara terbatas dan tidak aplikatif. Oleh karenanya untuk saat ini belum ada definisi yang jelas dan tajam terkait privasi.[9] Terdapat interaksi irisan antara inovasi atau pengembangan teknologi dengan norma dan regulasi seperti masalah hak privasi. Norma dan regulasi dapat diadaptasi berdasarkan pengembangan teknologi. Misalnya interaksi sosial melalui *Facebook* yang didefinisikan secara online tampaknya telah memengaruhi cara seseorang menghargai privasi. Perspektif saling membentuk yang tersirat dalam model ini, berangkat dari asumsi bahwa ada saling ketergantungan mendasar antara transformasi sosial, teknologi, dan normatif. Saling ketergantungan ini ada dalam proses perubahan sosial-teknologi yang dinamis dan terbuka, dan yang terjadi dalam konteks waktu dan tempat tertentu.

Jaringan media sosial (*social network*) adalah platform multi-sisi tertentu di mana pengguna biasanya memberikan data untuk menerima layanan jaringan sosial. Platform ini menyediakan layanan kepada kelompok pengguna pertama,

[9] Thomas D.C. Bennett, Triangulating Intrusion in Privacy Law, Oxford Journal of Legal Studies, Vol. 39, No. 4 (2019), pp. 751–778 July 10, 2019

menganalisis data, dan memproses data ini untuk menawarkan layanan iklan kepada kelompok pengguna lain.[10]

Hal tersebut memungkinkan untuk mengidentifikasi jenis kedua dari platform dengan banyak model yang melayani kelompok pelanggan yang berbeda tetapi menggunakan model bisnis yang berbeda, bukan berdasarkan iklan. Kita dapat menggunakan istilah "platform perantara" (*intermediary platform*) untuk mendefinisikan platform pasar multi-sisi yang memungkinkan pertemuan antara penjual dan pembeli barang dan jasa: misalnya Traveloka, Airbnb, Tiket.com, tetapi juga Amazon (saat perusahaan bukan penjual secara langsung tetapi hanya *market place*).

Dalam kasus ini platform dan media, melalui penggunaan analisis data dan algoritma, memungkinkan pertemuan antara dua atau lebih kelompok pengguna sekaligus menawarkan fasilitas lain yang memungkinkan pengurangan biaya transaksi. Peran mendasar platform ini adalah untuk "memungkinkan pihak untuk merealisasikan keuntungan dari perdagangan atau interaksi lainnya dengan mengurangi biaya transaksi untuk saling menemukan dan berinteraksi. [11]

Schrems memperkenalkan privasi sebagai konsep yang sangat bergantung pada konteks kultural dan sosial negara tertentu. Pendekatan atas konsep privasi di Eropa berbeda dengan konsep privasi di Amerika Serikat. Sistem hukum Amerika Serikat mengacu pada limitasi privas (*a reasonable expectation of privacy*) yang

[10] Graef I (2015) *Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. Telecomm Policy* Hal. 39:502–514 Graef I (2016) *Blurring boundaries of consumer welfare How to create synergies between competition, consumer and data protection law. In: Personal Data in Competition, Consumer Protection and IP Law: Towards a Holistic Approach?* diunduh melalui https://ssrn.com/ abstract=2881969 Graef I, Verschakelen J, Valcke P (2014) Putting the right to data portability into a competition law perspective. Retrieved from https://ssrn.com/abstract=2416537

[11] Evans et al. 2011.

wajar dan tidak sesuai dengan definisi yang diadopsi oleh pengadilan Eropa. Bergantung pada bentuk dari privasi, konsep tersebut dipersepsikan berbeda. Oleh karena itu, konsep privasi tidak dapat ditentukan secara tegas hitam dan putih akan nilai benar dan salahnya tetapi juga tidak dapat didasarkan pada logika sajya. Misalnya dalam budaya yang berbeda, terkait agama dapat dianggap suatu privasi sedangkan di budaya yang berbeda bukan dianggap sebagai privasi.[12]

Menurut Westin, kebutuhan akan privasi mungkin sama tuanya dengan umat manusia itu sendiri.[13]Berdasarkan kajian antropologis, biologis, dan sosiologis menunjukkan bahwa dalam masyarakat primitif sekalipun, setiap individu selalu memiliki keinginan untuk semacam privasi.[14] Oleh karenanya, hampir semua masyarakat, baik yang primitif maupun modern, memilikiteknik untuk mengatur jarak dan menghindari kontak dengan orang lain untukmenetapkan batasan fisik dengan tujuan menjaga privasi.[15]Biasanya cara orang memandang dan menghargai privasi sebagian besar ditentukan oleh sudut pandang budaya, filosofis, dan politik pada orang tersebut. Westin menyebutkan setidaknya ada 5 konsepsi privasi sebagai berikut.[16]

---

[12] The Max Schrems Litigation: A Personal Account Mohini Mann dalam Elaine Fahey Editor Institutionalisation beyond the Nation State Transatlantic Relations: Data, Privacy and Trade Law Studies in European Economic Law and Regulation Volume 10 hal. 76

[13] Dalam buku yang lain, Westin juga menggunakan kata "mimpi"dalam menngungkapkan perkembangan teknologi baru. Memulai prolog dalam buku tersebut, ia menyampaikan, The dream that a new technology might liberate man from both the tyranny of nature and the fruits of his own folly is as old as Western civilization." Lihat Alan F. Westin, Prologue: Of Technological Visions and Democratic Politics, dalam buku Alan F. Westin (Editor),Information Technology in a Democracy, (Massachusetts: Harvard University Press, 1971), hlm. 1.

[14]Alan F. Westin, *The Origins of Modern Claims to Privacy*, dalam buku: Philosophical Dimensions of Privacy: an Anthology (ed. Schoeman, F. D.), (Cambridge: Cambridge University Press, 1984). Hlm. 56-74

[15]J. Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, (Ithaca: Cornell University Press, 1997), hlm. 12.

[16]A. F. Westin, The Origins of Modern… Op Cit., hlm. 56.

1. Otonomi Pribadi

Otonomi pribadi menjadi konsep yang paling mendasar, dan memiliki dasar pemikiran dalam individualisme. Konsepsi ini,dalam masyarakat demokratis dipercaya bahwa tiap individu memiliki keunikan, martabat dasar, dan nilaisebagai manusia. Untuk melindungi otonomi pribadi dan individualitas, seseorang harus diberi ruang pribadi yang bebas dari pengaruh luar. Kebijakan privasi adalah melindungi garais perbatasan yang melindungi individu dari pandangan ingin tahu pihak ketiga. Aspek penting dari martabat manusia adalah hak untuk kebebasan individu.

Secara sederhana bisa difahami bahwa semakin banyak seseorang mengetahui pribadi orang (individu) lainnya, maka seseorang itu akan dengan mudah mengontrol orang lain tersebut. Oleh karenanya, konsep privasi menempatkan batasan pada apa yang negara dan pihak lain boleh dapatkan atau ketahui dan apa yang tidak boleh diketahui dari individu-individu tersebutdengan menciptakan "wilayah pribadi."Di dalam privasi ini bertindak sebagai batas terhadap kekuasaan yang dapat dilaksanakan atas individu oleh pihak ketiga, khususnya oleh pemerintah. Dengan demikian privasi dapat dilihat sebagai kekuatan penyeimbang melawan kekuasaan.[17]

2. Pelepasan Emosional

Persepsi kondisional tentang privasi ini adalah bahwa kebebasan pribadi memungkinkan untuk mengalami pelepasan emosional. Hal yang

[17]Bart Willem Schermer, *Software agents, surveillance, and the right to privacy: a legislative framework for agentenabled surveillance,* (Leiden: Leiden University Press, 2007), hlm. 73

patut disadari adalah hampir setiap individu ada perbedaan antara diri pribadinya dan dirinya di depan umum. Oleh karenanya, penggunakan istilah banyak diri dari diri sendiri dalam kehidupan publik biasanya lazim difahami dalam satu konteksi sosial ke konteks lainnya.

Dalam arti tertentu, disadari atau tidak, seseorang(individu) sering atau bahkan terus menerus memerankan berbagai peran dan menampilkan berbagai bagian kepribadian yang berbeda, tergantung pada audiens dan situasi yang dihadapi kala itu. Misalnya, bagaimana ia berperilaku di hadapan keluarga atau teman sebayanya mungkin sama sekali berbeda dari perilaku yang ia perlihatkan dalam kehidupan profesionalnya. Sama pentingnya dengan 'topeng' dalam sebuah interaksi sosial, sangat penting bagi kesehatan mentalnya untuk tidak mengecewakan orang lain, kemudian menjadi dirinya sendiri sepenuhnya, termasuk semua pandangan yang tidak jelas tentang kepribadiannya secara pribadi bersembunyi dari dunia luar. Menurut Westin, privasi dapat dikeluarkan untuk mengalami pelepasan emosional, untuk istirahat dari tugas berat dari interaksi sosial. Sebagai gantinya, penting untuk memahami konsepsi tentang privasi, yang memungkinkan terciptanya batas-batas sosial.[18]

Pendapat lain disampaikan oleh Rosen yang mendefinisikan privasi sebagai klaim terhadap batas sosial yang melindungi seseorang dari penyederhanaan, obyektifikasi, dan penilaian di luar konteks. Informasi pribadi yang melintasi batas sosial dari domain pribadi ke domain publik (atau dari satu konteks sosial ke orang lain) tanpa sepengetahuan yang

[18]Lihat juga E. Goffman, *The Presentation of Self in Everyday Life,*(New York: Doubleday, 1959), hlm. 55-57.

bersangkutan, dapat dengan mudah dipindahkan keluar dari konteks, yang mengarah ke penilaian karakter dirinya yang kemungkinan besar tidak akurat.[19]

3. Komunikasi Terbatas dan Terlindungi

Konsepsi hak privasi ini adalah hak privasi sebagai cara membatasi dan melindungi komunikasi. Umumnya orang akan menyampaikan apa yang dipikirkannya atau apa yang dirasakannya. Namun apabila ia menyampaikan perasaan itu dengan cara-cara yang tidak memperhatikan perasaan orang lain, maka hal demikian juga juga akan merusak hubungan interaksi sosial yang sepatutnya.

Oleh karenanya, tidak dibenarkan juga apabila seseorang menyampaikan semua hal tentang apa yang pikirkannya, dan apa yang dirasakan terhadap orang lain secara vulgar. Karena jika itu ia lakukan, akan dipastikan orang yang menjadi lawan bicara atau yang menjadi obyek pembicaraan tersebut akan merasa sakit dengannya. Termasuk dalam hal apabila ia berbicara tentang orang lain disaat orang lain itu tidak ada. Padahal, sebagai seorang manusia, ada kalanya ia juga butuh untuk melampiaaskan kemaran terhadap orang lain itu secara tersembunyi dan seorang diri.

Hak Privasi menawarkan jaminan yang diperlukan untuk berterus terang tentang perasaan dirinya sendiri tanpa harus takut bahwa ia mungkin menyinggung seseorang. Jika tidak melakukan perlindungan

[19]Bart Willem Schermer, Software agents…Op Cit, hlm. 74.

komunikasi seperti itu, mustahil akan muncul pemikiran-pemikiran bebas tanpat dihantui perasaan takut untuk dituntut akibat karena ucapan atau teks-teks yang mungkin dikemudian hari dinilai mencemarkan nama baik orang lain.[20]

4. Evaluasi Diri

Setiap individu perlu mengelompokkan pengalamannya ke dalam pola yang penuh arti dan mengerahkan individualitasnya pada berbagai peristiwa. Semua orang perlu waktu untuk memikirkan semuanya dan itu bisa dilakukan dengan sangat baik ketika ia sendirian dengan pikirannya sendiri. Hak Privasi menawarkan pengasingan individu yang diperlukan untuk evaluasi diri dan introspeksi diri. Hanya ketika ia benar-benar sendirian maka akan dapat merenungkan:(1) perilakunya dan orang lain, (2) peristiwa yang telah terjadi, dan (3) pikiran yang ia miliki. Tanpa hak privasi, ia tidak akan punya waktu untuk memproses semua informasi yang disajikan kepadanya. Aspek penting kedua dari evaluasi diri ini yang dimungkinkan oleh hak privasi adalah waktu yang diperlukan untuk membentuk, menyusun, dan mengevaluasi pendapat dan argumen dirinya. Argumen, pendapat, dan kerja kreatif perlu waktu cukup dan tanpa hak privasi rasanya akan menjadi sangat mustahil.[21]

5. Meminimalkan Beban

Konsepsi terakhir hak privasi adalah hak ini sebagai cara untuk meminimalkan beban. Kehidupan pribadi kita sering kali terganggu oleh

[20]*Ibid.*
[21]*Ibid.*

pengaruh luar. Gangguan-gangguan yang terjadi dapat menyebabkan ketidaksiapan dan itu sangat mengganggu jika sering terjadi. Karena itu, gangguan ke dalam kehidupan pribadi seseorang harus dijaga seminimal mungkin. Hak privasi memberi seseorang cara untuk melindungi diri dari gangguan yang tidak diinginkan dan memberatkan ini. Ketika gangguan yang sah terjadi, beban yang mereka tempatkan pada individu harus dijaga seminimal mungkin. Sebagai contoh, misalnya untuk menggambarkan konsepsi hak privasi ini adalah email komersial yang tidak diminta, atau '*spam*'. Di beberapa Negara, sepertidi Belanda maupun di Amerika Serikat, kebijakan perundang-undangan digunakan untuk melindungi individu dari email komersial yang tidak diminta karena gangguan yang tidak diinginkan yang disebabkan oleh spam menempatkan beban yang tidak perlu pada individu tersebut.[22]

B. Sumirnya Batasan Privasi

Dalam berbagai peraturan, privasi merujuk pada situasi di mana ruang pribadi individu tersebut dihormati. Namun sebenarny aapa yang diharapkan dari "pribadi-pribadi" di sini tidak sepenuhnya jelas. Apa yang bisa diharapkan dari istilah luas seperti itu? Pendekatan umum untuk memecahkan masalah menggambarkan ruang pribadi secara akurat adalah menentukan dimensi berbeda yang dicakupnya. Meskipun pendekatan semacam itu tidak dapat sepenuhnya menangkap esensi privasi, atau memberikan kesatuan konseptual, namun itu akan membantu dalam

[22]*Ibid.*

membangun kerangka berpikir yang relevan dengan definisi dalam persoalan ini.

Menurut Schermer, setidaknya ada tujuh dimensi paling umum dalam wacana hukum untuk mengetahui hak privasi yaitu:

1. tubuh
2. pikiran
3. rumah
4. perilaku intim
5. korespondensi
6. kehidupan keluarga
7. personal data.

Untuk lebih jelasnya akan diterangkan berikut ini.[23]

1. Tubuh

Di banyak masyarakat, setidaknya di masyarakat barat, orang ingin menyembunyikan bagian tubuh mereka dari pandangan orang lain. Hak untuk melindungi tubuh telanjang kita dari pandangan seseorang adalah kebebasan pribadi yang terlindungi. Integrasi tubuh manusia adalah elemen lain dari dimensi privasi ini. Ini merujuk pada fakta bahwa tubuh manusia tidak boleh dikenai pemeriksaan yang tidak diinginkan dalam bentuk pencarian atau penghapusan tubuh lahiriah.[24]

2. Pikiran

Terkait erat dengan integritas tubuh manusia adalah pikiran. Analog dengan hak integritas tubuh manusia, dapat dikatakan bahwa ada

[23]*Ibid.*
[24]*Ibid.*

hak atas integritas jiwa manusia. Integritas pikiran manusia, seperti halnya dimensi lain dari hak privasi, penting untuk hak asasi manusia atas penentuan nasib sendiri. Dengan menjaga pikiran kita dari pengawasan dan pengaruh luar, kita memastikan bahwa pikiran kita berkembang lebih cepat.[25]

3. Rumah

Hak Privasi rumah adalah hak untuk melindungi ruang fisik rumah seseorang dari pengaruh orang luar. Kesucian rumah adalah salah satu dimensi tertua dari hak privasi. Hampir setiap masyarakat modern dilindungi dari intrusi, penggeledahan, dan penyitaan yang melanggar hukum oleh pemerintah.[26]

4. Perilaku Intim

Kita semua ingin menjaga beberapa bagian dari hidup kita untuk diri kita sendiri. Hak untuk menjaga perilaku fisik kita (sebut saja misalnya, kehidupan seks) tersembunyi dari dunia luar adalah salah satu elemen dari hak ini, yang lain adalah pikiran kita dan dengan siapa kita berbagi.[27]

5. Korespondensi

Hak untuk menjaga agar perilaku intim kita terlindung dari dunia luar meluas hingga ke pengekspresian pikiran kita melalui komunikasi.

[25]*Ibid.*
[26]*Ibid.*
[27]*Ibid.*

Apa batas-batas hak privasi korespondensi masih belum jelas. Apabila privasi korespondensi diasumsikan sebagai hak penuh, maka penyelidikan apa pun dalam korespondensi seseorang dianggap melanggar hukum. Pandangan yang lebih terbatas adalah bahwa hanya investigasi percakapan pribadi (sehingga mengecualikan korespondensi profesional) dilindungi.[28]

6. Kehidupan Keluarga

Hak atas kehidupan keluarga yang tidak terganggu termasuk kebebasan untuk membentuk keluarga, untuk menikmati kehadiran satu sama lain, dan untuk hidup bersama diantaramereka.[29]

7. Data Pribadi

Dalam beberapa dekade terakhir perlindungan hak privasi telah berkembang untuk memasukkan perlindungan data pribadi. Pentingnya data pribadi sebagai dimensi ruang privat adalah akibat langsung dari menjamurnya teknologi informasi dan komunikasi. Sering kali hal ini meningkatkan kategori untuk menindaklanjuti tiga 'ruang privasi' yaitu Privasi Jasmani, Privasi Relasional, dan Privasi Informasi. Privasi Jasmani mencakup privasi dari (1) tubuh, (2) pikiran, dan (3) perilaku intim. Privasi Relasional meliputi privasi dari (3) perilaku intim, (4) rumah, (5) korespondensi, dan (6) kehidupan keluarga. Sedangkan Privasi Informasi terdiri dari (7) data pribadi, dan (5) korespondensi.[30]

[28] *Ibid.*
[29] *Ibid.*
[30] *Ibid.*

A. Hak Individu

Sebelum memahami hak privasi secara komprehensif, perlu difahami terlebih dahulu mengenai hak individu. Mengapa harus demikian? Secara singkat bisa dijelaskan bahwa hak privasi pada umumnya juga dianggap sebagai hak individu. Oleh karenanya, dalam tulisan ini juga akan menerangkanmengenai hak individu dan varian-varian yang terkandung di dalamnya, seperti tanggung jawab, kontrol personaldata, struktur kekuasaan, dan individu *versus* masyarakat, yang akan dijelaskan sebagai berikut:[31]

1. Tanggung Jawab

Sebagian besar sistem hukum menempatkan tanggung jawab untuk perlindungan privasi di tangan individu. Terserah individu tersebut untuk membuat pilihan kapan harus mengungkapkan apa kepada siapa. Secara khusus, dalam undang-undang perlindungan data, yang sangat dipengaruhi oleh konsep privasi informasi, tanggung jawab pribadi masing-masing dimiliki secara kritis. Seperti yang telah kita lihat di bagian sebelumnya, individu sering mendasarkan keputusannya terhadap perlindungan privasi mereka pada informasi yang tidak jelas, dan tidak lengkap. [32]

Selain itu, fakta bahwa apabilamasing-masing bertanggung jawab atas data pribadinya, dapat mengarah pada situasi di mana hak untuk privasi berubah menjadi berbeda karena diminta oleh banyak pelanggan. Konsumen memberikan informasi tentang perilaku belanja mereka di bursa, sebelum mendapatkan keuntungan, seperti harga yang lebih rendah, hadiah gratis atau layanan yang

[31] *Ibid.*
[32] *Ibid.*

lebih baik. Meskipun layanan yang dibuat khusus tidak selalu menjadi masalah dan menawarkan manfaat yang jelas bagi konsumen. Undang-undang perlindungan data tidak mengurangi kemungkinan dampak negatif dari hak privasi ini sebagai hak individu.

The European Data Protection Directive (95/46/EC), misalnya baru memperoses lebih lanjut subjek data pribadi setelah mendapat persetujuan lebih lanjut untuk pemrosesan data pribadi tersebut. Menurut Schermer, ketentuan ini masih dianggap sebagai kelemahan dari *The European Data Protection Directive* karena kategori tertentu dari konsumen yang kurang mampu sampai batas tertentu 'dipaksa' untuk membocorkan informasi pribadi mereka dengan imbalan barang dan jasa yang lebih murah. Meskipun secara teori seseorang harus selalu memiliki pilihan bebas, tetapi praktik menunjukkan bahwa pilihan yang benar-benar bebas jarang tersedia, karena alternatif yang lebih 'ramah privasi' hampir selalu lebih mahal atau kurang nyaman.

Sementara itu, informasi data pribadi warga Negara yang dikeluarkan oleh lembaga pemerintah juga dapat digunakan untuk pengawasan disipliner oleh pemerintah. Cara yang paling jelas di mana pemerintah dapat menggunakan basis data sektor swasta adalah untuk keperluan investigasi kriminal. Cara kedua di mana pemerintah dapat menggunakan basis data sektor swasta adalah untuk melakukan pengawasan terhadap kaum miskin.[33]

2. Pengendalian Data Pribadi

Dalam konsep privasi informasi dan penentuan nasib sendiri dalam informasi akan sulit diterapkan ketika individu tidak mengetahui hal-hal yang telah

[33]*Ibid.*

diberikan kepada data personal. Konsep informasi sendiri penentuan nasib sendiri hanya layak apabila terdapat pengetahuan penuh tentang jumlah dan jenis informasi yang dikumpulkan dan diproses tersedia kepada semua individu. Tanpa pengetahuan ini, penentuan nasib sendiri informasi dan hak atas privasi informasi, tidak lebih seperti hanya harimau kertas.

Sementara teknologi pengawasan secara bertahap menjadi semakin luar biasa dan meluas, dengan penempatan kamera yang berada di mana-mana, dengan jaringan yang konrehensif, maka pengetahuan tentang apa yang dilakukan dengan data pribadi akan semakin sulit didapat. Sebagai contoh, RFID memungkinkan pengumpul data untuk mengumpulkan data (pribadi) secara diam-diam dari subjek data yang membawa tag-RFID, agen perangkat lunak dapat mengumpulkan data pribadi subjek data dari berbagai sumber, dan kamera CCTV dapat mengidentifikasi dan mengikuti subjek data dari jarak jauh. Memperoleh pengetahuan tentang bagaimana, kapan, dan seseorang melakukan apa akan mudah dihimpun akan menjadi semakin sulit untuk meminta data subjek di masa depan jika tidak tersedia alat pembanding yang membantu para individu tersebut untuk mengetahui kemana larinya data-data mereka tersebut.[34]

3. Struktur Kekuasaan

Pelaksanaan kekuasaan tidak dibuat secara individual. Karena itu, hak privasi seringkali tidak responsif terhadap struktur kekuasaan yang diciptakan melalui penggunaan informasi. Banyak bentuk kontrol tidak perlu dibedakan di tingkat pribadi. Jenis panoptik, misalnya, beroperasi (sebagian karena informasi yang tidak lengkap) pada klasifikasi dan penilaian kategori (konsumen). Individu

[34]*Ibid.*

ditugaskan ke kategori tertentu dan diperlakukan berdasarkan informasi terbatas tanpa batas. Fakta bahwa individu memiliki usia, jenis kelamin, atau etnis tertentu sudah cukup untuk menempatkan individu ke kategori tertentu.[35]

Selain itu, informasi tambahan tentang kategori ini tidak perlu diberikan oleh individu jika orang lain yang termasuk dalam kategori yang sama telah selesai. Kategorisasi semacam ini berdasarkan profil umum dapat memengaruhi kebebasan negatif dan positif individu, tetapi tidak jelas. Bagaimana hak atas privasi dapat melawan efek negatif dari penggunaan informasi jenis ini.[36]

4. Individu *versus* Masyarakat.

Masalah terakhir dengan privasi sebagai hak individu adalah fakta yang sering ditempatkan terhadap kepentingan masyarakat secara mendalam. Oleh karenanya, khusus soal ini akan dikaji lebih di bawah ini.

B. Publik *versus* Pribadi[37]

Menurut Schermer, saat ini, perdebatan soal public vs. pribadi semakin mencuat seiring dengan dampak dari teknologi. Teknologi memiliki dampak mendalam pada cara membangun masyarakat. Dampak yang dimiliki teknologi informasi dan komunikasi terhadap masyarakat tercermin dalam gagasan tentang privasi dan kebebasan. Warren dan Brandeis, misalnya, menulis artikel seminar mereka pada akhir abad ke-19 ketika perkembangan media massa dan fotografi terjadi. Contoh-contoh penting lainnya yang membuat ruang privasi dikembangkan untuk komunikasi nirkabel adalah menghentikan percakapan telepon, penggunaan computer dan basis data, serta penggunaan kamera CCTV.

[35]*Ibid.*
[36]*Ibid.*
[37]*Ibid.*hlm. 125-126.

Schermer menyatakan bahwa menurut definisinya, hak atas privasi didasarkan pada perbedaan antara publik dan privat. Apa yang menjadi milik ruang privat berhak untuk dilindungi oleh hak privasi. Tetapi untuk dapat menetapkan perbedaan antara ruang publik dan ruang pribadi menjadi semakin sulit sebagai akibat dari kemajuan teknologi dan perubahan sosial yang menyertainya. Oleh karena itu area yang tetap bebas dari gangguan luar menjadi sama sulitnya, jika bukan tidak mungkin untuk dibedakan.

Pada abad ke-18, ke-19, dan bagian yang lebih baik dari abad ke-20, batas-batas fisik seperti dinding rumah kita memberikan batas yang jelas antara publik dan privat. Namun, kemajuan teknologi informasi dan komunikasi terus mengaburkan perbatasan dalam membuat keputusan tentang apa yang pribadi (privasi) dan apa yang public. Kerangka hukum yang ada saat ini dalam rangka perlindungan hak privasi, yang memiliki dasar dalam paradigma kerahasiaan dan membuat perbedaan yang jelas antara publik dan privat, akan menghadapi kesulitan yang semakin besar di masa depan pada saat akan melindungi kebebasan.[38]

Menurut Solove, sejak hukum privasi telah berkembang terutama dengan paradigma kerahasiaan dalam pikiran (terutama di Amerika Serikat), informasi yang tidak dianggap rahasia atau bagian dari ruang pribadi sering dikecualikan dari perlindungan konstitusional privasi.[39] Contoh untuk menggambarkan hal ini adalah pengawasan otomatis melalui pemasangan Kamera CCTV dengan

[38]*Ibid.*

[39]Solove,D.J.(2001).Privacy and Power:Computer Data bases and Metaphors for Information Privacy, in: Stanford Law Review, vol. 53, pp. 1393.

kemampuan pengenal wajah sekaligus memindainya dalam upaya untuk mengidentifikasi teroris yang dicurigai.

Di sini bisa dilihat bahwa teknologi telah menciptakan situasi baru yang sulit diatasi dengan menggunakan ide klasik tentang privasi. Seperti pemasangan kamaera CCTV di atas, yang memungkinkan untuk mengidentifikasi secara individu menggunakan teknologi kecerdasan buatan melalui kamera tersebut yang tentunya akan sangat berpotensi mengancam "individu-individu." Di sini muncul perdebatan, apakah hal tindakan tersebut telah mengamcam hak privasi individu? Di Amerika Serikat, kebebasan individu tidak dilindungi oleh hak privasi. Hal ini berdasarkan putusan Mahkamah Agung amerika serikat dalam perkara Amerika Serikat v. Dionisio yang mana Mahkamah Agung menyatakan bahwa karakteristik fisik suara, tulisan tangan, atau karakteristik wajah seseorang, yang terus-menerus diekspos ke ruang publik, tidak berada dalam perlindungan Amandemen Keempat Konstitusi.[40]

Oleh karena itu, penggunaan teknologi pengenalan wajah (*facial-recognition technology*) berada diluar lingkup perlindungan yang diberikan oleh hak privasi di Amerika Serikat. Di sini bisa dilihat bahwa teknologi telah menciptakan situasi baru yang sulit diatasi dengan menggunakan ide klasik tentang privasi. Seperti yang diperlihatkan dalam contoh yang mana sangat dimungkinkan untuk mengidentifikasi seseorang secara unik menggunakan teknologi kecerdasan buatan dan CCT yang berpotensi berpotensi menimbulkan ancaman bagi individu. [41]

[40]Bart Willem Schermer, *Software agents…*Op Cit, Hlm. 126.
[41]*Ibid.*

Pertanyaannya adalah apakah kita harus mengubah hak privasi dan memperluasnya ke ruang publik (yang akan menjadi hak privasi). Jika tidak, apakah kita kemudian harus menemukan mekanisme lain untuk memastikan perlindungan kebebasan konstitusional? Pengadilan Eropa untuk Hak Asasi Manusia (*The European Court of Human Rights*) mengambil pendekatan yang berbeda untuk masalah ini. Dalam perkara Halford v.the United Kingdom yang menyatakan bahwa Pengadilan mengakui bahwa seseorang mungkin memiliki harapan subjektif tentang privasi di ruang publik, itu tidak selalu merupakan faktor konklusif dalam menentukan apakah hak atas privasi dapat diterapkan. Lebih lanjut dikatakan sebagai berikut:[42]

"There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly orintentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (forexample, a security guard viewing through closed-circuit television) is of a similar character."

Selain itu, Pemgadilan juga menyatakan:

"Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method."[43]

[42]*Ibid.*,hlm. 126.

[43]Perkara P.G. and J.H. v. the United Kingdom, application no. 44787/98, 25 September 2001.

C. Hak Privasi dalam Kovenan Sipil dan Politik

Selama dekade terakhir, ICCPR telah menjadi sumber utama yang banyak dikutip terkait hak atas privasi. Terutama pada tahun 2014, Human Right Commision (HRC) membuat laporan terkait hak atas privasi di era digital sebagai respon untuk permintaan Dewan Umum PBB dalam Resolusi 68/ 167.[44] Tetapi bahkan sebelum itu, pada tahun 1988, HRC mengklarifikasi secara luas yang mana hak privasi yang dijamin oleh Pasal 17 Komentar Umum Nomor 16. Dalam perkembangan terakhir, di tahun 2016, Dewan Umum PBB mengadopsi perubahan hak atas privasi di era digital, secara eksplisit dan secara langsung mengkonstruksikan pengintaian masal dan diskriminasi sebagai praktik pelanggaran pasal 17 Kovenan Hak Sipil Politik dan Pasal 12 Piagam Hak Asasi Manusia. Pasal 17 Kovenan Hak Sipil dan Politik Pasal 17 mengatur bahwa Tidak seorangpun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri urusan-urusan pribadinya, keluarga, rumah atau hubungan surat menyurat atau secara tidak sah diserang kehormatan dan nama baiknya.

Oleh karena berdasarkan isi pasal tersebut, untuk dianggap sebagai pelanggaran Pasal 17, memiliki unsur sebagai berikut: (1) gangguan terhadap privasi, (2) yang sewenang-wenang atau melanggar hukum, dan (3) tidak dicakup oleh Pasal 4 terkait pengecualian keamanan nasional.[45] Namun, karena ICCPR

[44] Benjamin G. Waters, *An International Right To Privacy: Israeli intelligence Collection In The Occupied Palestinian Territories*, Georgetown Journal of International Law Volume 50 Tahun 2018-2019

[45] Pasal 4 Kovenan Hak Sipil Politik "Dalam keadaan darurat yang mengancam kehidupan negara dan keberadaannya yang telah diumumkan secara resmi, Negara-negara Pihak pada Kovenan ini dapat mengambil langkah-langkah yang mengurangi kewajiban-kewajiban mereka berdasarkan Kovenan ini, sejauh yang benar-benar dibutuhkan dalam situasi tersebut, asalkan langkah termaksud tidak bertentangan dengan kewajibankewajiban mereka lainnya yang diatur oleh hukum intemasional dan tidak mengandung diskriminasi yang semata-mata berdasarkan ras, warna kulit, jenis kelamin, bahasa atau asal-usul sosial".

dan Komentar Umum No. 16 dirancang jauh sebelum era internet, Kovenan tersebut tidak secara eksplisit menyebutkan pelanggaran jenis-jenis gangguan di era digital ini.

Komisi Hak Asasi manusia mendefinisikan secara luas "*interference*" atau gangguan pada konteks Pasal 17, tetapi definisi yang tepat ada dalam kasus contohnya Toonen v. Australia. Pengadilan HAM Eropa menganalisa bahwa Konvensi Eropa Hak Asasi manusia Pasal 8 menganalogikan dengan Pasal 17 telah secara eksplisit menyatakan bahwa pengawasan elektroik telah melanggar hak atas privasi. Dalam kasus Toonen, kriminalisasi teknis atas tindakan pribadi, tidak ada penuntutan atau campur tangan nyata pada privasi individu, dapat ditemukan sebagai "gangguan" yang tidak diizinkan berdasarkan Pasal 17. Seharusnya Pasal 17 Kovenan Hak Sipol mengiterpretasikan gangguan atau campur tangan dalam privasi ketika negara melakukan pengintaian elektronik kepada warga negaranya.

Pasal 17 Kovenan Hak Sipil dan Politik melarang dua bentuk pencampuran privasi yaitu sewenang-wenang dan tidak sah.[46] Sebagaimana yang didefinisikan oleh Komentar Umum Nomor 16 "tidak sah" tidak berarti secara sederhana karena bertentangan dengan undang-undang tetapi lebih kepada tidak ada pelanggaran terhadap privasi yang terjadi kecuali diatur oleh undang-undang.[47] Apabila tidak ada afirmasi dari otorisasi produk legislasi negara yang pada gilirannya bertindak seperti Kovenan Hak Sipol, maka campur tangan dengan hak individu untuk privasi dilarang. Selain itu, seperti yang diilustrasikan oleh praktik Komisi Hak Asasi Manusia dan penerapan Pengadilan HAM Eropa

[46] ICCPR, supra note 15, Pasal 17.
[47] General Comment No. 16, supra note 58, 3.

yang sebanding, undang-undang yang mengesahkan gangguan tersebut harus dapat diduga secara wajar oleh orang yang bersangkutan serta tepat dan jelas

Karena itu tidak ada otorisasi afirmatif oleh undang-undang suatu negara, yang pada gilirannya harus melakukan aksi seperti Kovenan Hak Sipil dan Politik, maka campur tangan dengan hak individu untuk privasi dilarang. Selain itu, seperti yang diilustrasikan oleh praktik Komisi Hak Asasi Manusia dan penerapan Komisi Hak Asasi Manusia Eropa yang sebanding, undang-undang dalam negeri yang mengesahkan interferensi tersebut harus dapat diramalkan secara wajar oleh orang yang bersangkutan serta tepat dan jelas.[48]

D. Ekonomi Digital

Konsep ekonomi digital pertama kali diperkenalkan oleh Don Tapscott sebagai sebuah sosiopolitik dan sistem ekonomi yang mempunyai karakteristik sebuah ruang intelijen, meliputi informasi, berbagai akses instrumen, kapasitas, dan pemrosesan informasi. Komponen ekonomi digital yang berhasil diidentifikasi pertama kalinya yaitu industri teknologi, informasi, dan komunikasi (TIK), aktivitas *e-commerce,* serta distribusi digital barang dan jasa.[49]

Era Ekonomi Digital didefinisikan oleh Atkinson dan sebagai berikut:[50]

---

[48] ACLU PROPOSAL, supra note 61, at 21. See also General Comment No. 16, supra note 58, 3.

[49] Don Tapscott menggambarkan "Age of Network Intelligence"sebagai semua dan mencakup semuamerevolusi fenomena yang dipicu oleh konvergensi kemajuan manusiakomunikasi, komputasi (komputer, perangkat lunak, layanan) dan konten (penerbitan,penyedia hiburan dan informasi), untuk membuat multimedia interaktif danjalan raya informasi. Zaman baru ini secara bertahap memaksa kita untuk memikirkan kembali cara kitamelihat definisi tradisional ekonomi, penciptaan kekayaan, organisasi bisnisdan struktur kelembagaan lainnya. Pergeseran dalam hubungan ekonomi dan sosial seperti itu memiliki peluang dan tantangan tersendiri. Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, New York: McGraw-Hill,1995, hlm 2

[50] Atkinson, R.D. and McKay, A.S., Digital Prosperity: understanding the economic benefits of the information technology revolution, Information Technology and Innovation Foundation, Washington, DC, 2007, hlm 7. dalam Sinta Dewi Rosadi dan Garry Gumelar Pratama,

"*The digital economy represents the pervasive use of IT (hardware, software, applications and telecommunications) in all aspects of the economy, including internal operations of organizations (business, government and non-profit*)…"

Berdasarkan definisi terebut maka ekonomi digital merupakan ekonomi yang didasarkan pada barang elektronik dan jasa yang dihasilkan oleh bisnis elektronik dan diperdagangkan melalui perdagangan elektronik. Artinya, bisnis dengan produksi elektronik dan proses manajemen dan yang berinteraksi dengan mitra dan pelanggan dan melakukan transaksi melalui Internet dan Web teknologi.

Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia, Jurnal Ilmu Hukum Veritas Et Justitia, Volume 4 No. 1 Juni 2018., hlm. 91

BAB III

METODE PENELITIAN

1. Jenis Penelitian

Penelitian ini termasuk penelitian hukum normatif atau sering disebut dengan penelitian doktrinal dengan obyek atau sasaran penelitian berupa peraturan, perundang-undangan dan bahan hukum lainnya.[51] Penelitian normatif pada umumnya meneliti bahan pustaka atau bahan sekunder yang melingkupi bahan hukum primer, sekunder dan tertier. Penelitian ini fokus pada perlindungan hukum hak atas privasi dan data diri di era digital termasuk bagaimana definisi, klasifikasi dan ruang lingkup hak atas privasi dan data diri itu sendiri. Selain itu, penelitian ini terdiri dari beberapa tahapan, yaitu: *Pertama,* penyusunan dan penyampaian proposal; *Kedua,* proposal akan disampaikan dan direview, kemudian setelah direview dilanjutkan dengan pengumpulan dan pengolahan data serta terakhir berupa penyusunan dan penyampaian hasil akhir penelitian ini.

2. Jenis dan Teknik Pengumpulan Data

Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang dapat dikelompokkan menjadi bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang sesuai dengan objek penelitian. Untuk mendapatkan data sekunder akan dilakukan melalui penelitian kepustakaan (*library research*) dengan menggunakan studi dokumenter

[51]Johny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia, 2005, hlm. 302.

terhadap referensi-referensi yang relevan dengan objek penelitian yang didapatkan dari peraturan perundang-undangan, buku dan artikel jurnal ilmiah serta dalam kamus dan ensiklopedia.

Bahan hukum primer penelitian ini adalah bahan-bahan hukum yang mengikat yang dalam hal ini berkaitan dengan masalah yang akan dibahas dalam penelitian ini seperti UUD 1945, Undang-Undang, Putusan MK, peraturan perundang-undangan lainnya. Peneliti juga menggunakan GDPR (*General Data Protection Regulation*) yang merupakan sumber hukum terkait hak atas privasi dan data diri khusus untuk wilayah Uni Eropa. Sementara, bahan hukum sekunder dalam penelitian ini adalah bahan-bahan yang erat hubungannya dengan bahan hukum primer dan dapat membantu menganalisis dan memahami bahan hukum primer yang berupa buku-buku pegangan, majalah hukum, jurnal hukum dan suratkabar, hasil karya ilmiah penelitian yang ditulis. Sedangkan bahan hukum tersier merupakan bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder yang berupa kamus-kamus hukum dan ensiklopedia.[52]

Data sekunder berupa undang-undang atau norma lain yang terkait hak atas privasi dan ekonomi digital. Data sekunder adalah bahan-bahan hukum yang diperoleh melalui studi pustaka antara lain peraturan perundang-undangan yang terkait atas hak privasi, buku, penelitian terdahulu, dan artikel-artikel ilmiah yang mengkaji hak privasi di era ekonomi digital. Dalam penelitian hukum normatif ini, metode yang

[52] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, Jakarta: Rajawali Press, 2003, h. 29.

digunakan dalam pengumpulan bahan hukum adalah studi kepustakaan atau studi dokumen (*documentary study*).[53]

3. Metode Pendekatan dan Analisis Data

Data penelitian ini diperoleh dari bahan sekunder kemudian dianalisa dengan menggunakan beberapa metode pendekatan yang pada akhirnya diambil kesimpulan untuk menjawab permasalahan dalam penelitian ini. Oleh karena penelitian ini merupakan penelitian doktrinal, maka pendekatan yang digunakan yaitu pendekatan perundang-undangan, pendekatan analitis serta pendekatan perbandingan atau komparatif terhadap segala jenis bahan hukum. Untuk itu, penelitian ini berpijak pada peraturan perundang-undangan untuk melihat bagaimana perlindungan yang diberikan terhadap warga negara Indonesia atas hak privasi dan data diri serta penelitian analitis dan komparatif untuk mengetahui bagaimana negara Jerman yang digunakan sebagai perbandingan karena Jerman merupakan salah satu negara yang pertama kali mencetuskan adanya pengaturan terhadap hak atas privasi dan data diri terhadap warga negaranya.

4. Jadwal Penelitian

Penelitian ini dilaksanakan dalam bulan Agustus-Desember 2019. Adapun rencana pelaksanaan seperti pada tabel-tabel berikutini:

[53]Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, Jakarta: Sinar Grafika, 2002, h. 18-19.

Tabel

Jadwal Penelitian

Kegiatan	2019																			
	Agustus				September				Oktober				November				Desember			
	I				II				III				IV				V			
	1	2	3	4	1	2	3	4	4	1	2	3	4	1	2	3	4	1	2	3	4
Penyusunan Proposal	x	x																			
Pengumpulan Data			x	x																	
Pengolahan Data				x																	
Analisis Data																					
PenyusunanHasilPenelitian																					
PenyampaianHasilPenelitian									x	x											
PerbaikanHasil Penelitian										x	x										
PenyampaianLaporan														X						X	X

5. Organisasi Penelitian

Pengarah : M. Guntur Hamzah

Penanggung Jawab : Wiryanto

Koordinator : Yuni Sandrawati

Peneliti : 1. Ananthia Ayu Devitasari

2. Titis Anindyajati

3. Abdul Ghoffar

6. Sistematika Pembahasan

Penelitian ini disusun dan dibagi ke dalam 4 (empat) bab. Bab pertama adalah bab pendahuluan yang berisi tentang latar belakang penelitian, rumusan permasalahan, tujuan dan manfaat penelitian.

Bab dua adalah bab yang membahas tentang tinjauan pustaka dimana terbagi menjadi 3 (tiga) sub bag, yaitu: Definisi Privasi dan Data Pribadi, Hak Atas Privasi dan Ekonomi Digital.

Bab tiga merupakan metode penelitian dimana dijabarkan bagaimana penelitian ini dilaksanakan. Dalam bab metode penelitian dijelaskan bagaimana klasifikasi penelitian ini/Jenis Penelitian, Jenis dan teknik Pengumpulan data serta metode pendekatana dan metode analisis data.

Bab empat adalah bab hasil penelitian yang berisi analisis untuk menjawab permasalahan penelitian. Oleh karena penelitian ini merupakan penelitian komparasi, maka analisa terbagi menjadi 2 (dua) bagian besar yakni Pengaturan hak Privasi di Jerman dan di Indonesia. Bagian pertama, Pengaturan Hak Privasi di Jerman meliputi penjelasan asal mula pengaturan hak privasi di Jerman, standar dan pengaturan privasi dan

proteksi data berdasarkan peraturan perundang-undangan (misalnya GDPR), pelaksanaan The German Federal Data Protection Act (BDSG) serta bagaimana Mahkamah Konstitusi Jerman bersikap terhadap pengaturan terkait hak atas privasi di Jerman. Bagian besar lainnya yaitu Pengaturan Hak Privasi di Indonesia dimana belum adanya UU yang mengatur secara tegas terkait perlindungan hukum hak atas privasi dan data diri sehingga masih menggunakan Peraturan setingkat Menteri dalam hal ini Peraturan Kementerian Komunikasi dan Informasi.

Bab lima adalah penutup yang berisi kesimpulan dan saran. Kesimpulan di dapatkan dari hasil analisis yang dilakukanpada bab empat. Saran berisi rekomendasi baik berupa rekomendasi aturan maupun rekomendasi untuk penelitian lebih lanjut.

BAB IV

Hak Privasi atas Data Diri di Jerman Dan Indonesia

Pada bab IV ini, Peneliti akan menganalisa pengaturan hak privasi atas Data Diri di Jerman. Seperti yang sudah diuraikan dalam bab sebelumnya, Jerman menjadi negara *benchmark* karena Jermanlah yang membuat aturan cikal bakal lahirnya proteksi data dan hak privasi. Dalam bab ini juga dibagi menjadi beberapa sub bab. Masing-masing sub bab akan membedah sejarah perkembangan pengaturan hak privasi di Jerman, perngaturan hak privasi terkait Data Diri, implementasi dan tantangan Jerman dalam melakukan proteksi hak privasi. Hasil penelitian akan pengaturan hak privasi atas data diri di Jerman kemudian akan dibandingkan dengan pengaturan yang ada di Indonesia.

I. Perlidungan Data di Jerman

A. Perlindungan Data di Eropa

Sebelum masuk ke dalam pengaturan perlindungan data di Jerman, peneliti akan memberikan konteks perlindungan data di Uni Eropa terlebih dahulu. Hal tersebut dikarenakan Jerman merupakan negara anggota Uni Eropa dan tunduk pada peraturan yang ada di Uni Eropa termasuk aturan terkait perlindungan data.

Perlindungan data merupakan hak fundamental yang diatur dalam Pasal 8 Piagam Hak Fundamental Uni Eropa pada Pasal 16 dan Perjanjian Lisbon yang secara legal mengikat negara anggota Uni Eropa ketika mengembangkan kebijakan secara domestik dan internasional. Setiap individu di Uni Eropa tidak bergantuk nasionalitas dan kewarganegaraannya merupakan subjek dari hak ini. Pembatasan dari hak ini harus memenuhi konteks yang sangat mengikat dan

secara proporsional yang menjadi batasan dari hukum terkait tujuan murni dari kepentingan umum publik.[54]

Independensi publik secara otoritas diletakkan di luar cabang eksekutif untuk memastikan sudut pandang dan pelengkap dari prinsip proteksi data. Hal ini melengkapi pemrosesan data dari berbagai tujuan (hukum perdagangan dan penegakan hukum), dengan pengecualian keamanan negara yang mana di luar kewenangan dari Uni Eropa. Kasus hukum yang secara konstan dan konsisten di Pengadilan Eropa telah mendefinisikan kompetensi dari uni Eropa. Legislasi dari perlindungan data mengimplementasikan haknya.

Reformasi perlindungan data akan menentukan kerangka hukum baru dan mutakhir dalam pemrosesan data di Uni Eropa. Reformasi ini akan memperbaruhi sistem perlindungan data di Uni Eropa untuk mengatasi tantangan terkait kominikasi elektronik, penegakan hukum dan teknik komputer yang lebih sederhana. Sistem baru menyederhanakan pengkontrol data dan beban pemrosesan administrasi dan meraih tujuan hak subjek data. Transfer data internasional merupakan bagian utama dari kerangka hukum ini. Secara khusus, pengkontrol data akan bekerja sama dengan Otoritas Perlindungan Data Uni Eropa.

Kerangka hukum terkait privasi di Uni Eropa terdiri dari aturan perlindungan data di tingkat primer dan sekunder serta mekanisme yang kuat untuk memastikan penegakan hukum privasi tersebut independen dan kelalaian. Hukum tingkat primer di Uni Eropa salah satunya adalah dalam perjanjian

[54] Claude Moraes dalam Elaine Fahey (Editor), *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* Volume 10 hal. 35

internasional Uni Eropa dan Piagam Hak Fundamental Uni Eropa. Hak atas perlindungan data diatur dalam Pasal 16 dalam *Treaty on the Functioning of the European Union* dan Pasal 39 dalam *Treaty on European Union* dan diakui sebagai hak fundamental dalam Piagam Hak Fundamental Uni Eropa. Dalam Piagam tersebut pasal 7 yang mengatur hak privasi[55] berurutan secara sistematik sebelum Pasal 8 yang mengatur mengenai Perlindungan Data. Hukum primer tersebut kemudian dilengkapi oleh hukum sekunder yaitu *Directive* 95/46/EC (*the Data Protection Directive*), yang menjadi instrumen hukum utama dalam perlindungan data selama 20 tahun sebelum diperbarui dan digantikan oleh GDPR[56]. Peraturan GDPR diberlakukan pada bulan Mei tahun 2016 dan diaplikasikan ke negara anggota pada tanggal 25 Mei 2018.

Kedua instrumen meletakkan beberapa asas dan prinsip terkait perlindungan data pribadi individu. Prinsip tersebut antara lain keabsahan (*lawfulness*), keadilan (*fairness*), transparansi (*transparency*), batasan tujuan (*purpose limitation*), minimalisasi data (*data minimisation*), akurasi (*accuracy*), integritas (*integrity*), kerahasiaan (*confidentiality*), keamanan data (*data security*)[57] dan menciptakan kewajiban yang bersamaan untuk 'pengontrol' data pribadi, dipahami sebagai orang yang, sendirian atau bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan data pribadi.[58] Mereka memberi subjek data beberapa hak prosedural, seperti hak atas informasi, hak atas akses,

[55] Article 7 *Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications.* Lihat *EU Charter of Fundamental Rights*
[56] 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 Data Protection Regulation) [2016] OJ L 119/1.
[57] Pasal 5 GDPR.
[58] Pasal 4 (7) GDPR

hak untuk perbaikan, hak untuk menghapus, hak untuk pembatasan pemrosesan, hak untuk portabilitas data dan hak untuk menolak.

Kepatuhan terhadap peraturan perlindungan data Uni Eropa dijamin oleh Otoritas Perlindungan Data Nasional (NDPA), pengadilan domestik dan akhirnya Pengadilan Uni Eropa. Badan Penasihat Independen tentang perlindungan data pribadi didirikan atas mandat dari GDPR ('Dewan Perlindungan Data Eropa'). Selain undang-undang omnibus ini, aturan perlindungan data lebih lanjut dimasukkan dalam instrumen hukum khusus sektor-sektor tertentu. Legislasi perlindungan data pribadi bahkan di luar batas wilayah Uni Eropa, sebagai sebuah aturan umum, perpindahan data dari negara ketiga akan diperbolehkan jika ada jaminan level perlindungan yang memadai dari data pribadi. Batas dan standart "memadai" dijelaskan lebih lanjut oleh *Court of Justice of the European Union* (CJEU).[59]

Implementasi hak atas privasi membutuhkan tingkat perlindungan hak-hak dasar dan kebebasan yang 'pada dasarnya setara' dengan yang ada di Uni Eropa. Ini didasarkan pada premis bahwa perlindungan data sekarang merupakan hak mendasar dalam tatanan hukum UE yang tidak dapat dielakkan dengan transfer data pribadi ke negara ketiga. Karenanya, aliran data Transborder merupakan bagian dari tugas perlindungan hak fundamental lembaga Uni Eropa, dan argumen yang valid dapat dibuat untuk mendukung ekstrateritorialtermasuk penerapan transatlantik dari standar privasi data Uni Eropa.

[59] Maria Tzanou The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation? hal. 58 The EU Data Privacy Regimes

Penegakan GDPR adalah hak prerogatif regulator perlindungan data, yang dikenal sebagai otoritas pengawas (misalnya, Cnil di Perancis atau ICO di Inggris). Dewan Perlindungan Data Eropa (penggantian untuk apa yang disebut sebagai Partai Kerja)[60] terdiri dari delegasi dari otoritas pengawas, dan memantau penerapan GDPR di seluruh Uni Eropa, mengeluarkan pedoman untuk mendorong interpretasi yang konsisten dari Peraturan. GDPR menciptakan konsep "otoritas pengawas memimpin". Di mana ada pemrosesan lintas-batas data pribadi (yaitu, pemrosesan dilakukan di tempat pengontrol atau prosesor di beberapa Negara Anggota, atau berlangsung di satu tempat pengontrol atau pengolah tetapi memengaruhi subjek data di banyak Negara Anggota), maka titik awal untuk penegakannya adalah bahwa pengontrol dan prosesor diatur oleh dan menjawab otoritas pengawas untuk pendirian utama atau tunggal mereka, yang disebut "otoritas pengawas memimpin".[61] Namun, otoritas pengawas utama diharuskan untuk bekerja sama dengan semua otoritas "terkait" lainnya, dan otoritas pengawas di Negara Anggota lain dapat memberlakukan di mana pelanggaran terjadi di wilayahnya atau secara substansial mempengaruhi subyek data hanya di wilayahnya.[62] Oleh karena itu, konsep otoritas pengawas memimpin agak terbatas untuk multinasional. Oleh karena itu, konsep otoritas pengawas memimpin merupakan bantuan terbatas bagi perusahaan multinasional.

[60] Lihat Pasal 29 GDPR
[61] Pasal 56 (1)) GDPR
[62] Pasal 56 (2) GDPR

B. Sejarah Perkembangan Pengaturan Hak Privasi di Jerman

Pada akhir tahun 1960-an, kemajuan teknologi dan modernisasi yang disebabkan oleh pemrosesan data secara otomatis mengakibatkan peningkatan kesadaran akan risiko terkait dengan produk teknologi dan informatika. Selain itu, kesadaran masyarakat Jerman akan hak-hak sipil dan tumbuhnya kecurigaan terhadap pemerintah dan programnya menghasilkan kebutuhan warga Jerman untuk membatasi kekuatan pemerintah dalam hal mengumpulkan informasi tentang warganya.

Pada tahun 1970, negara bagian Jerman di Hesse memberlakukan UU Perlindungan Data pertama di dunia. Negara bagian Jerman di Hesse memberlakukan undang-undang federal pertama di dunia yang mengatur perlindungan data warga negara. Undang-undang ini menetapkan prinsip dasar undang-undang perlindungan data, seperti persyaratan izin hukum atau pe`rsetujuan subjek data untuk setiap pemrosesan data pribadi.[63]Undang-undang awal ini difokuskan pada pencegahan penyalahgunaan data pribadi warga negara oleh pemerintah. Pemahaman Jerman saat ini tentang subjek data yang memiliki hak untuk menentukan sendiri informasi terkaitdirinya serta penanganan dan penutupan data pribadinya tidak ada pada saat itu..

Selanjutnya pada 1 Januari 1978, Undang-Undang Perlindungan Data Federal Jerman (BDSG) mulai berlaku. Undang-undang ini menetapkan prinsip dasar perlindungan data, seperti persyaratan izin hukum atau persetujuan subjek data untuk setiap pemrosesan data pribadi. Pada tahun 1983, Pengadilan Konstitusi Federal Jerman menyatakan bahwa individu tersebut bahkan memiliki

[63]Lihat bagian 4, Paragraf 1 BDSG.

hak konstitusional untuk 'penentuan nasib sendiri informasional (informational self-determination)'.[64]

Latar belakang putusan *landmark* ini adalah sensus yang direncanakan untuk tahun 1983, yang pada dasarnya berfokus pada sensus seluruh penduduk Jerman dengan cara pemrosesan data elektronik. Rakyat Jerman menyambut dengan baikputusan Mahkamah Konstitusi Jerman ini dan sebagai konsekuensinya, lebih dari 1.600 pengaduan diajukan di Mahkamah Konstitusi Federal terhadap Undang-Undang Sensus yang secara khusus diadopsi untuk sensus oleh parlemen Jerman. Akhirnya, pada bulan Desember 1983, Pengadilan Konstitusi Federal Jerman menyatakan ketentuan-ketentuan tertentu dari Undang-Undang Sensus sebagai inkonstitusional.

Pada tahun 1990, amandemen BDSG memasukkan persyaratan yang ditetapkan oleh Mahkamah Konstitusi Federal. Pada saat itu, BDSG bertujuan untuk melindungi warga negara dari penyalahgunaan pemrosesan data oleh pemerintah. Sehingga MK Federal Jerman mensyaratkan pemrosesan data didasarkan pada undang-undang yang spesifik. Di sisi lain, persetujuan individu pada umumnya diperlukan untuk mengizinkan pemrosesan data di sektor privat. Pengadilan umum di Jerman juga berkontribusi pada interpretasi undang-undang perlindungan data. Hakim pengadilan umum sering diminta untuk menerapkan prinsip proporsionalitas untuk menyeimbangkan gesekan kepentingan yang timbul dalam isu privasi data. Masalah gesekan kepentingan tersebut antara lainseperti privasi versus kelayakan teknis atau kebebasan berekspresi. Di pengadilan umum

[64]Olga Stepanova, Alan Charles Raul (Editor), *Privacy, Data Protection and Cybersecurity Law Review Fifth Edition* (Law Business Research Ltd, London, 2018). hal. 146

sendiri telah banyak kasus yang terkait pembatasan dari hak determinasi memberikan informasi (*right to informational self determination*).

Undang-undang Uni Eropa tentang perlindungan data telah berlaku sejak 1995. Instruksi Perlindungan Data menjamin perlindungan efektif terhadap hak fundamental dalam hal perlindungan data. Namun permasalahan timbul ketika masing-masing Negara Anggota menerapkan secara berbeda undang-undang tersebut. Implementasi yang berbeda tersebut telah menyebabkan inkonsistensi dan menciptakan kompleksitas, ketidakpastian hukum dan biaya administrasi. Permasalahan tersebut memengaruhi kepercayaanindividu dan daya saing ekonomi di Uni Eropa.

Selain itu, aturan tersebut juga perlu dimodernisasi karena aturan tersebut diperkenalkan pada saat servis online saat dan tantangan dunia digital terkait perlindungan data belum ada. Dengan situs jejaring sosial, *cloud computing*, layanan berbasis lokasi pengguna seperti *google maps*, dan *smart card*, maka pemrosesan data pribadi telah tumbuh secara eksponensial. Oleh karenanya, dibutuhkan seperangkat aturan yang kuat untuk memastikan hak orang atas perlindungan data pribadi.[65]

Seiring perkembangan zaman, Undang-Undang Perlindungan Data Federal Jerman kemudian diubah untuk memenuhi kebutuhan terkait pemrosesan data pribadi yang semakin berkembang. Apalagi ditambah dengan era digitalisasi yang menimbulkan banyak isu hukum yang harus diselesaikan, oleh karenanya Badan Legislatif mengeluarkan Undang-Undang Telemedia Jerman (TMA) pada tahun 2007. Undang-Undang ini yang menetapkan tujuan untuk melindungi

[65]Lihat Pasal 8 Piagam Hak-Hak Fundamental Uni Eropa

perlindungan data selama pengoperasian layanan telemedia. Namun, karena undang-undang perlindungan data dan hukum telemedia semakin bersinggungan dengan internet, maka dibutuhkan regulasi baru yang mengintegerasikan kedua isu tersebut.

Badan Legislatif Uni Eropa kemudian merencanakan peraturan privasi dalam dunia digital yang akan mulai berlaku pada saat yang sama dengan Peraturan Perlindungan Data Umum (GDPR). GDPR mulai berlaku pada tanggal 25 Mei 2018 sesuai jadwal. Regulasi *ePrivacy* masih tunduk pada negosiasi tripartit dan mungkin akan berlaku pada tahun 2020.

Sebagai peraturan, kerangka kerja GDPR tidak harus ditransformasikan ke dalam undang-undang domestik negara-negara di Eropa, tetapi GDPR harus secara langsung berlaku di semua Negara Anggota Uni Eropa. Namun, peraturan ini juga berisi 'klausul pembuka' yang memberikan diskresi kepada Negara-negara Uni Eropa untuk memperkenalkan ketentuan domestik tambahan untuk mengkonkretkan dan selanjutnya menentukan penerapan GDPR untuk masalah-masalah spesifik di masing-masing negara. Untuk itu, parlemen Jerman mengeluarkan versi baru Undang-Undang Perlindungan Data Federal Jerman (BDSG) pada bulan April 2017. Serangkaian peraturan baru ini, GDPR dan BDSG Jerman yang baru berlaku efektif pada Mei 2018.

Pertama dan terpenting, GDPR memperluas ruang lingkup teritorialnya, yang berarti bahwa perusahaan-perusahaan non-Eropa juga dapat masuk dalam ruang lingkupnya, menjadikannya undang-undang perlindungan data pertama di seluruh dunia dalam sudut pandang globalisasi. GDPR berlaku untuk:

1) semua perusahaan di seluruh dunia yang menargetkan pasar Eropa dan dalam konteks ini memproses data pribadi warga negara Uni Eropa (terlepas dari di mana pemrosesan berlangsung) dan
2) perusahaan yang memproses data warga Eropa dalam konteks perusahaan Eropa mereka. GDPR memperketat aturan untuk mendapatkan persetujuan yang sah untuk memproses informasi pribadi. Namun, persetujuan yang sah adalah salah satu dari dua kemungkinan untuk membenarkan pemrosesan data, opsi lainnya adalah pembenaran hukum.

Oleh karena itu Perusahaan harus menilai proses mereka untuk memastikan mereka memproses data pribadi secara sah, dan untuk meninjau apakah disarankan untuk menahan diri dari mencari persetujuan tetapi untuk beralih ke pembenaran hukum dengan lebih sedikit prasyarat dan tidak ada kemungkinan dicabut kapan saja.

Akibatnya, atas permintaan otoritas perlindungan data, perusahaan harus membuktikan bahwa mereka memenuhi kewajiban mereka berdasarkan GDPR. Pihak berwenang tidak perlu lagi menyelidiki dan membuktikan pelanggaran itu sendiri. GDPR juga memperkenalkan penilaian dampak privasi wajib (*Privacy Impact Assessments*(PIA)). Ini membutuhkan pengontrol data untuk melakukan PIA di mana risiko pelanggaran privasi tinggi untuk meminimalkan risiko pada subjek data.

Hal tersebut berarti bahwa sebelum suatu organisasi atau badan hukum dapat memulai kegiatan yang melibatkan data pribadi tertentu, seperti data terkait kesehatan, mereka harus melakukan PIA dan bekerja dengan kantor perlindungan data untuk memastikan mereka mematuhi undang-undang perlindungan data saat

proyek berlangsung. Selain itu, GDPR memperluas tanggung jawab di luar pengontrol data. Di masa lalu, hanya pengontrol data yang dianggap bertanggung jawab atas kegiatan pemrosesan data, tetapi GDPR memperpanjang tanggung jawab kepada semua organisasi yang memproses data pribadi. GDPR juga mencakup organisasi apa pun yang menyediakan layanan pemrosesan data ke pengontrol data, yang berarti bahwa bahkan organisasi yang murni penyedia layanan yang bekerja dengan data pribadi perlu mematuhi aturan seperti minimalisasi data.

C. Standart dan Legislasi Terkait Privasi dan Proteksi Data

Sebelum GDPR berlaku, hak privasi terkait data pribadi diatur oleh BDSG. Dalam undang-undang tersebut, BDSG mendefinisikan personal data sebagai bagian dari informasi individual terkait personal atau keadaan faktual yang dapat digunakan untuk mengidentifikasi seseorang.[66]

GDPR mendefinisikan data pribadi sebagai 'informasi apa pun yang berkaitan dengan orang alami yang diidentifikasi atau dapat diidentifikasi'. Definisi ini berlaku untuk semua data pribadi yang ditangani oleh penyedia layanan informasi dan komunikasi (telemedia) elektronik.[67] Namun, semua data ini sekarang tunduk pada GDPR, karena Konferensi Perlindungan Data Jerman mempresentasikan makalah pada tanggal 26 April 2018, yang menyatakan bahwa Pasal 95 GDPR harus ditafsirkan sedemikian rupa sehingga ketentuan TMA yang mengatur perlindungan data harus tidak berlaku lagi. Mengikuti pendapat ini,

[66]Data pribadi sebagai bagian informasi individu tentang keadaan pribadi atau faktual tentang manusia yang diidentifikasi atau diidentifikasi"

[67]informasi apa pun yang berkaitan dengan orang alami yang diidentifikasi atau dapat diidentifikasi '. Definisi ini berlaku untuk semua data pribadi yang ditangani oleh penyedia layanan informasi dan komunikasi (telemedia) elektronik.

tidak ada penanganan istimewa untuk pengumpulan data melalui telemedia lagi, sehingga pengendali harus mematuhi aturan ketat yang ditentukan oleh GDPR mulai sekarang.[68]

Parlemen Uni Eropa dan Konsil Eropa telah mencapai kesepakatan tentang reformasi perlindungan data yang diusulkan oleh Komisi. Reformasi ini merupakan langkah penting untuk memperkuat hak-hak dasar warga negara di era digital sekaligusmemfasilitasi perusahaan dengan menyederhanakan aturan untuk perusahaan di pasar digital tunggal (*digital single market*).[69]

Selama masa tahun 1960an, baik sektor publik maupun sektor privat mempertimbangkan bahwa untuk meraik efesiensi dibutuhkan pemrosesan data secara otomatis dan semakin penting dari seluruh masalah privasi di era baru teknologi yang telah diciptakan.[70] Bundestag bagaimanapun telah mengambil alih proses proteksi data dalam parlemen

D. Kerangka Hukum GDPR dalam Perlindungan Data Pribadi

GDPR memiliki cakupan luas dan dalam menggunakan definisi terkait Data Pribadi. GDPR mendefinisikan "Data pribadi" sebagai segala informasi yang terkait dengan identifikasi individu yang masih hidup (subjek data) seperti nama, alamat email, nomor ID pajak, pengenal online, dll. Sedangkan konsep

[68]The data protection reform package includes the General Data Protection Regulation ("Regulation") and the Data Protection Directive for the police and criminal justice sector.
[69]Perlindungan data berlaku lebih kuat karena Uni Eropa mengadopsi paket reformasi perlindungan
[70] J Lee Riccardi, The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?, Boston College International and Comparative Law Review, Volume 6 | Issue 1, hal.246

Pemrosesan Data mencakup tindakan seperti mengumpulkan, merekam, menyimpan dan mentransfer data.[71]

Perusahaan yang tidak didirikan di Uni Eropa mungkin harus mematuhi Peraturan saat memproses data pribadi penduduk Uni Eropa dan EEA[72] (negara-negara EEA adalah Norwegia, Lichtenstein dan Swiss). Di bawah ini adalah kualifikasi suatu perusahaan dapat menjadi subjek GDPR walau tidak berada di negara Uni Eropa antara lain:

a) Jika perusahaan menawarkan barang atau jasa ke subjek data di Uni Eropa.
b) Jika perusahaan memantau perilaku subjek data yang terjadi di Uni Eropa.

Aksesibilitas semata-mata dari situs web perusahaan di UE tidak cukup untuk membuat perusahaan tunduk pada GDPR, tetapi bukti lain dari motivasi untuk menawarkan barang atau jasa di Uni Eropa akan relevan untuk dijadikan landasan suatu perusahaan harus tunduk pada aturan GDPR.

Sebagai norma utama, perusahaan yang tidak didirikan di Uni Eropa tetapi tunduk pada GDPR harus menunjuk secara tertulis perwakilan di negara Uni Eropa untuk tujuan kepatuhan GDPR. Ada pengecualian terhadap peraturan ini untuk perusahaan dengan skala kecil yang mengolah data yang tidak sensitif.

[71]GDPR merupakan ruang lingkup yang lebih besar dan memiliki definisi yang lebih luas terkait data pribadi. Secara pokok data pribadi adalah segala hal yang dapat mengidentifikasi seseorang.
[72]Wilayah Ekonomi Eropa atau Area Ekonomi Eropa(EEA) adalah wilayah di mana Perjanjian mengenai EEA memperbolehkan pergerakan bebas manusia, barang, jasa, dan modal dalam Pasar Tunggal Eropa, termasuk kebebasan memilih tempat tinggal di setiap negara dalam area ini. EEA didirikan pada 1 Januari 1994 saat mulai berlakunya Persetujuan EEA. Lihat Perjanjian Aerea Ekonomi Uni Eropa. *European Free Trade Association*. 19 August 2016.

Apabila ada ketidakpatuhan terhadap aturan pengelolaan data pribadi, maka perusahaan tersebut akan diberikan denda. Denda jika terjadi ketidakpatuhan dapat mencapai hingga 4% dari pendapatan tahunan di seluruh dunia atau 20 juta euro yang mana lebih tinggi. Perusahaan dari semua sektor dan berbagai skala harus mempertimbangkan GDPR sebagai bagian dari upaya kepatuhan perusahaan terhadap perlindung hak privasi.[73]

Komisi Eropa dan Otoritas Perlindungan Data merilis pedoman resmi untuk membantu perusahaan untuk melaksanakan aturan dalam GDPR. Pedoman yang dikeluarkan Komisi Eropa dan Otoritas Perlindungan Data ini terkait, misalnya, dengan peran petugas perlindungan data, pemberitahuan pelanggaran data pribadi, penilaian dampak perlindungan data. Saat ini Uni Eropa sedang melakukan pembaharuan legislasi e-privacy mengatur kerahasiaan komunikasi. Instrumen legislatif ini setelah diberlakukan akan menambah beberapa persyaratan dalam GDPR.

Terminologi data pribadi (*personal data*) adalah pintu masuk aplikasi *General Data Protection Regulation* (GDPR). Aplikasi aturan tersebut hanya berlaku jika terdapat pemrosesan data terkait data pribadi. Frasa data pribadi didefinisikan melalui Pasal 4 ayat (1) bahwa Data pribadi merupakan seluruh informasi yang terkait identifikasi seseorang. Subjek data dapat diidentifikasi jika secara langsung atau tidak langsung, merujuk pada pengidentifikasi seperti nama, nomor identifikasi kependudukan, data lokasi, pengenal seperti karakter, fisik, fisiologis, genetik , ekonomi, sosial, dan budaya atau sosial perseorangan. Dalam

[73]Chapter 8 Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and "Porting Rights"

praktiknya, data pribadi dalam GDPR juga mencakup semua data yang dapat atau dapat diberikan kepada seseorang dengan cara apa pun, misalnya telepon, kartu kredit atau nomor personel seseorang, data akun, plat nomor, penampilan, nomor pelanggan, atau alamat adalah data pribadi.

Dengan berdasar pada pasal 4 ayat (1) GDPR, bahwa definisi data pribadi terkait seluruh infoemasi maka dapat diasumsikan bahwa terminologi tersebut dapat diinterpretasikan seluas mungkin. Interpretasi ini juga digunakan dalam kasus di Eropean Court of Justice yang juga mempertimbangkan informasi yang sangat implisit seperti pencatatan waktu bekerja yang termasuk informasi tentang kapan seorang pegawai memulai bekerja dan mengakhiri waktu bekerjanya sebagai "Data Pribadi".[74]

Hal yang sama juga berlaku pada alamat IP (*IP addresses*). Jika pengendali data memiliki opsi hukum untuk mewajibkan pengguna menyerahkan data atau informasi tambahan yang dapat membantu identifikasi *IP address* maka data tersebut merupakan data pribadi pula. Interpretasi secara meluas ini juga berlaku jika pengontrol memiliki opsi hukum untuk mewajibkan penyedia untuk menyerahkan informasi tambahan yang memungkinkannya mengidentifikasi pengguna di belakang alamat IP, ini juga merupakan data pribadi.

Selain itu, dalam GDPR harus dicatat bahwa data pribadi tidak perlu objektif. Informasi subyektif seperti pendapat, penilaian atau perkiraan dapat berupa data pribadi. Dengan demikian, ini termasuk penilaian kelayakan kredit seseorang atau perkiraan kinerja kerja oleh pemberi kerja.

[74] https://gdpr-info.eu/issues/personal-data/

a) Subjek data GDPR

GDPR mengatur informasi terkait data pribadi hanya merujuk pada subjek perseorangan. Dengan kata lain, perlindungan data tidak diaplikasikan pada informasi terkait badan hukum seperti perusahaan, yayasan dan lembaga. Pada dasarnya, seseorang memperoleh kapasitas ini setelah kelahirannya, dan kehilangannya setelah kematiannya. Oleh karena itu, data harus diberikan kepada orang yang teridentifikasi atau dapat diidentifikasi untuk dianggap pribadi.

Selain data pribadi secara umum, pemerintah harus memperhatikan secara khusus data pribadi sensitif yang sangat relevan karena mereka tunduk pada tingkat perlindungan yang lebih tinggi. Data ini termasuk data genetik, biometrik dan kesehatan, serta data pribadi yang mengungkapkan asal ras dan etnis, pendapat politik, keyakinan agama atau ideologis atau keanggotaan serikat pekerja.

1) Pengertian Data Pribadi Suatu data adalah data pribadi apabila data tersebut berhubungan dengan seseorang, sehingga dapat digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data[75]

Di dalam Pasal 2 (a) Data Protection Directive "personal data" adalah:

"any information relating to an identified 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".

[75] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Belgium, 2014, hlm. 36.

b) Ruang Lingkup dan Subjek dari GDPR

Regulasi ini mengatur perlindungan terkait pemrosesan data pribadi dan aturan terkait perpindahan dari data pribadi tersebut. GDPR melindungi hak fundamental dan kebebasan manusia dan secara khusus hak atas perlindungan data pribadi. Kebebasan pergerakan data dalam negara Uni Eropa seharusnya dibatasi oleh perlindungan data pribadi.[76]

Subjek perlindungan data pribadi hanya orang atau natural person bukan legal entity atau badan hukum. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut the right to private life. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi[77]

Penjelasan mengenai definisi data pribadi adalah hal penting untuk menjamin perlindungan data tersebut. Sejauh ini dalam beberapa instrumen internasional dan regional seperti dalam European Union Data Protection Directive, European Union Data Protection Convention, dan the OECD Guidelines yang dimaksud dengan "data pribadi" adalah semua data yang berhubungan dengan orang-perorangan yang teridentifikasi dan dapat diidentifikasi (information relating to an identified or identifiable natural person). Yang masih menjadi perdebatan semenjak peraturan-peraturan tersebut.

[76] Pasal. 1 GDPR
[77] *European Union Agency for Fundamental Rights and Council of Europe*, Op.Cit. hlm. 37.

c) Prinsip-prinsip pengolahan Data dalam GDPR

GDPR mengatur bahwa dalam mengolah data pribadi konsumen, perusahaan haru mengikuti prinsip-prinsip sebagai berikut:

1. diproses secara sah, adil, dan transparan dalam kaitannya dengan subjek data ('keabsahan, keadilan, dan transparansi')
2. dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah serta tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut; pemrosesan lebih lanjut untuk keperluan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistik harus, sesuai dengan Pasal 89 (1), tidak dianggap tidak sesuai dengan tujuan awal (batasan tujuan);
3. Pengolahan data harus memadai, relevan dan terbatas pada apa yang diperlukan sehubungan dengan tujuan untuk mana data tersebut diproses (minimalisasi data);
4. Pengolahan data harus dilakukan secara akurat dan jika perlu, terus diperbarui; setiap langkah harus diambil untuk memastikan bahwa data pribadi yang tidak akurat, sehubungan dengan tujuan pengolahannya, dihapus atau diperbaiki tanpa penundaan ('akurasi');
5. Data pribadi disimpan dalam bentuk yang memungkinkan identifikasi subyek data tidak lebih dari yang diperlukan untuk keperluan data pribadi tersebut diproses; data pribadi dapat disimpan untuk waktu yang lebih lama sejauh data pribadi akan diproses semata-mata untuk keperluan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistik sesuai dengan Pasal 89 (1) tunduk pada

implementasi teknis dan organisasi yang sesuai langkah-langkah yang diperlukan oleh Peraturan ini untuk melindungi hak dan kebebasan dari subjek data (batasan penyimpanan);

6. Data pribadi diproses dengan cara yang memastikan keamanan data pribadi yang tepat, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan terhadap kehilangan, kerusakan, atau kerusakan yang tidak disengaja, menggunakan tindakan teknis atau organisasi yang sesuai (‘integritas dan kerahasiaan’).

Keabsahan pemrosesan data bergantung atas implementasi prinsip di bawah ini:

a. subjek data telah memberikan persetujuan untuk pemrosesan data pribadinya untuk tujuan tertentu.
b. pemrosesan diperlukan untuk pelaksanaan kontrak dimana subjek data menjadi pihak atau untuk mengambil langkah-langkah sesuai permintaan subjek data sebelum masuk ke dalam kontrak
c. pemrosesan diperlukan untuk kepatuhan dengan kewajiban hukum yang harus dikontrol oleh pengontrol
d. pemrosesan diperlukan untuk melindungi kepentingan vital subjek data atau orang perorangan lainnya
e. pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali
f. pemrosesan diperlukan untuk tujuan kepentingan sah yang dilakukan oleh pengontrol atau oleh pihak ketiga, kecuali jika kepentingan tersebut

dikesampingkan oleh kepentingan atau hak dasar dan kebebasan dari subjek data yang memerlukan perlindungan data pribadi, khususnya di mana data tersebut subjek adalah seorang anak.

Butir (f) huruf pertama tidak berlaku untuk pemrosesan yang dilakukan oleh otoritas publik dalam melaksanakan tugasnya.

d) Data sensitif

Dalam hukum perlindungan data seperi *European Union Data Protection Directive* (EU DP Directive) membedakan data berdasarkan tingkat bahaya yang akan dirasakan kepada individu jika terjadi pengolahan data yang tanpa persetujuan ke dalam kelompok "data sensitif" dan "data nonsensitif". Data "sensitif" biasanya mendapatkan perlindungan hukum yang lebih besar, misalnya persetujuan harus secara eksplisit melalui pernyataan tertulis.[78] *European Union Data Protection Directive* melarang pengolahan data sensitif kecuali jika telah mendapatkan persetujuan yang jelas dari pemilik data. Data tersebut di antaranya informasi yang menyangkut etnis, pendapat politik, agama, dan kepercayaan, keanggotaan dari organisasi perdagangan termasuk juga data yang berhubungan dengan kesehatan dan kehidupan seks seseorang.

Data pribadi secara alami terutama yang sensitif terkait hak fundamental dan kebebasan adalah konteks dari pemrosesan data yang dapat mewujudkan resiko signifikan untuk hak fundamental dan kebebasan. Data pribadi sensitif

[78] Direktif Parlemen dan Dewan Konsil Eropa Nomor 2016/680 pada tanggal 27 April 2016 terkait perlindungan orang perorangan sehubungan dengan pemrosesan data pribadi oleh pihak yang berwenang untuk tujuan pencegahan, investigasi, deteksi atau penuntutan pelanggaran pidana atau eksekusi hukuman pidana, dan pada pergerakan bebas dari data tersebut, dan Dewan pengulang Keputusan Kerangka Kerja

meliputi data terkait ras dan etnis, oleh karenanya terminologi yang digunakan adalah frasa "asal ras atau *racial origin*" dalam peraturan Direktiv ini tidak menyiratkan sebuah penerimaan Uni Eropa terkait teori yang mencoba untuk mendeterminasi eksistensi dari ras manusia secara terpisah.

Data pribadi sensitif tidak dapat diproses, kecuali jika pemrosesan tunduk pada perlindungan yang sesuai untuk hak dan kebebasan dari subjek data yang ditetapkan oleh hukum dan diizinkan dalam kasus yang disahkan oleh hukum; jika belum disahkan oleh undang-undang semacam itu, pemrosesan diperlukan untuk melindungi kepentingan vital subjek data atau orang lain; atau pemrosesan terkait dengan data yang secara nyata diumumkan kepada publik oleh subjek data. Perlindungan yang sesuai untuk hak dan kebebasan subjek data dapat mencakup kemungkinan untuk mengumpulkan data hanya dalam kaitannya dengan data lain tentang orang alami yang bersangkutan, kemungkinan untuk mengamankan data yang dikumpulkan secara memadai, aturan yang lebih ketat tentang akses staf yang kompeten. wewenang untuk data dan larangan pengiriman data tersebut.

Pemrosesan data tersebut juga harus diizinkan oleh undang-undang di mana subjek data telah secara eksplisit menyetujui pemrosesan yang sangat mengganggu baginya. Namun, persetujuan subjek data tidak boleh dengan sendirinya memberikan dasar hukum untuk memproses data pribadi sensitif tersebut oleh pihak yang berwenang.

Subjek data harus memiliki hak untuk tidak tunduk pada keputusan yang mengevaluasi aspek-aspek pribadi yang berkaitan dengannya yang semata-mata didasarkan pada pemrosesan otomatis dan yang menghasilkan efek hukum yang merugikan terkait, atau secara signifikan mempengaruhi, dirinya. Dalam kasus

apa pun, pemrosesan tersebut harus tunduk pada perlindungan yang sesuai, termasuk penyediaan informasi spesifik pada subjek data dan hak untuk mendapatkan intervensi manusia, khususnya untuk mengekspresikan sudut pandangnya, untuk mendapatkan penjelasan tentang keputusan yang dicapai. setelah penilaian tersebut atau untuk menantang keputusan. Pembuatan profil yang menghasilkan diskriminasi terhadap orang per orang berdasarkan data pribadi yang sifatnya sangat sensitif terkait dengan hak dan kebebasan mendasar harus dilarang berdasarkan ketentuan yang diatur dalam Pasal 21 dan 52 Piagam.

e) Proteksi Data di Bidang Telekomunikasi dan Telemedia

Pada akhir tahun 2015, undang-undang tentang pengenalan kewajiban untuk melestarikan dan periode waktu maksimum retensi data menggantikan undang-undang tentang pelestarian data yang sebelumnya dianggap tidak konstitusional oleh pengadilan Konstitusi Federal, meskipun meskipun ada kritik luas dari pemegang rahasia profesional dan hak istimewa, dan tanpa menunggu peraturan masing-masing. Data telekomunikasi, termasuk data lokasi dan alamat IP, harus disimpan oleh penyedia untuk memungkinkan pihak penegak hukum mengaksesnya ketika menyelidiki kejahatan berat dan terorisme. Oleh karenanya masih harus dilihat apakah hukum akan menahan pengaduan konstitusional yang telah diajukan terhadapnya.

Pada tanggal 6 November 2015, Bundesrat Jerman menyetujui rancangan undang-undang tentang pengenalan Undang-Undang Retensi Data nasional ("DRA"). Setelah persetujuan Bundesrat, RUU ini sekarang dikirim ke Presiden

Federal yang kemungkinan besar akan menandatanganinya. Oleh karena itu, DRA kemungkinan akan mulai berlaku sebelum akhir November. DRA memperkenalkan kewajiban penyimpanan data untuk penyedia layanan telekomunikasi yang tersedia untuk umum (PECS).[79]

Namun, kewajiban penyimpanan bervariasi tergantung pada layanan yang disediakan: Penyedia layanan telepon yang tersedia untuk umum (PATS) harus menyimpan data lalu lintas tertentu selama 10 minggu. Ini termasuk:

- nomor telepon atau pengidentifikasi lain dari semua pihak yang terlibat:
- tanggal dan waktu awal dan akhir panggilan termasuk zona waktu
- informasi tentang layanan yang digunakan jika PATS memungkinkan penggunaan berbagai layanan;
- dalam hal layanan ponsel:
  - pengidentifikasi internasional pihak pemanggil dan yang dipanggil
  - pengidentifikasi internasional perangkat pemanggil dan yang dipanggil, dan
  - tanggal dan waktu termasuk zona waktu aktivasi pertama layanan pra-bayar
- dalam hal telepon internet juga alamat IP dari panggilan dan pihak yang dipanggil termasuk pengidentifikasi pengguna yang dialokasikan.

[79] Baker&McKenzie, German Parliament approves national Data Retention Act, diunduh melalui https://www.bakermckenzie.com/-/media/files/insight/publications/2015/11/german-parliament-approves/al_germany_dataretentionact_nov15.pdf?la=en pada tanggal 2 November 2019

Penyedia layanan akses internet ("ISP") yang tersedia untuk umum harus menyimpan data lalu lintas tertentu selama 10 minggu. Ini termasuk: alamat IP yang dialokasikan untuk pelanggan:[80]

- pengidentifikasi unik dari koneksi internet yang digunakan serta
- pengidentifikasi pengguna yang dialokasikan; tanggal dan waktu awal dan akhir akses internet di bawah
- alamat IP yang dialokasikan termasuk zona waktu.

Selain itu, penyedia harus menyimpan data lokasi yang dihasilkan oleh penggunaan layanan ponsel selama 4 minggu. Jika penyedia tidak menghasilkan atau memproses data masing-masing, itu harus dipastikan bahwa data disimpan dengan benar oleh pihak ketiga. Atas permintaan, itu juga harus segera beri tahu Federal Network Agency ("FNA") tentang identitas pemroses data.

f) Kewajiban Utama untuk Pemegang data

Ketentuan privasi GDPR ditujukan untuk pengontrol data (data controllers). Sehingga objek atau addresat ketentuan privasi adalah pihak yang mengontrol data pribadi. Pengontrol data ini adalah pihak yang memproses data pribadi atas nama mereka sendiri atau menugaskan pihak untuk melakukan hal yang sama. Penyedia layanan Telemedia sebagai pengumpul data dapat mengumpulkan dan menggunakan data pribadi hanya sejauh hukum secara khusus mengizinkan, atau jika subjek data telah memberikan persetujuannya.[81] Selain itu, sejauh undang-undang mengizinkan pengumpulan data untuk tujuan tertentu, data

[80] *Ibid.*
[81] Pasal 6 GDPR

ini tidak dapat digunakan untuk tujuan lain, kecuali jika subjek data telah menyetujui penggunaan lainnya.

Menurut Pasal 13 dan 14 GDPR, pengontrol harus, antara lain, menginformasikan pengguna tentang tingkat dan tujuan pemrosesan data pribadi agar persetujuan apa pun berlaku. Persetujuan dapat diberikan secara elektronik, asalkan pengontrol data memastikan bahwa pengguna layanan menyatakan persetujuannya secara sadar dan tidak ambigu, persetujuan dicatat, pengguna dapat melihat deklarasi persetujuannya kapan saja dan pengguna dapat mencabut persetujuannya di setiap saat dengan efek untuk masa depan. Prinsip-prinsip ini sesuai dengan Pasal 7 GDPR, yang mengharuskan persetujuan didasarkan pada keputusan sukarela dan berdasarkan informasi dari subjek data.

Namun, persetujuan tidak selalu diperlukan. Sebelumnya, banyak pengecualian menurut undang-undang mengizinkan penggunaan data tanpa persetujuan, untuk berbagai tujuan yang terkait dengan bisnis. Meskipun demikian, mengikuti makalah yang disebutkan di atas, pengendali tidak dapat menggunakannya sejak 25 Mei 2018. Oleh karena itu, pengendali sekarang dipaksa untuk menemukan cara baru untuk menjamin pemrosesan yang sah sambil mengumpulkan data melalui situs web, aplikasi dan melalui komunikasi elektronik. Ini juga sejalan dengan penilaian yang tepat dari prosedur pemrosesan data sebelumnya dan dapat menyebabkan peningkatan pergeseran penyedia layanan yang tidak mampu atau tidak mau mematuhi standar GDPR yang tinggi.

Namun, persetujuan tidak selalu diperlukan. Sebelumnya, banyak pengecualian menurut undang-undang mengizinkan penggunaan data tanpa persetujuan, untuk berbagai tujuan yang terkait dengan bisnis atau perdagangan.

Meskipun demikian, perusahaan pengendali data tidak dapat menggunakan pengecualian tersebut sejak 25 Mei 2018. Oleh karena itu, pengendali sekarang dipaksa untuk menemukan cara baru untuk menjamin pemrosesan data pribadi yang sah dan tidak melawan hukum sambil mengumpulkan data melalui situs web, aplikasi dan melalui komunikasi elektronik. Ini juga sejalan dengan penilaian yang tepat dari prosedur pemrosesan data sebelumnya dan dapat menyebabkan peningkatan pergeseran penyedia layanan yang tidak mampu atau tidak mau mematuhi standar GDPR yang tinggi.

g). Inovasi teknologi dan hukum privasi

Cookies

Menurut undang-undang perlindungan data, penggunaan cookie hanya relevan jika informasi yang disimpan dalam cookie dianggap sebagai data pribadi. Cookie adalah sepotong teks yang disimpan di komputer pengguna oleh situs pengeksplor webnya. *Cookie* dapat digunakan untuk otentikasi, menyimpan preferensi situs, pengidentifikasi untuk sesi berbasis server, isi keranjang belanja atau apa pun yang dapat dicapai melalui penyimpanan data teks. *Cookie* dianggap sebagai data pribadi jika mengandung data yang memungkinkan pengontrol mengidentifikasi subjek data. Namun, sebelum GDPR mulai berlaku, dan selama bagian TMA yang relevan masih berlaku, *cookie* dapat digunakan di Jerman selama pengguna memiliki opsi untuk menolak (menyisih).

Setelah berlakunya GDPR, tidak ada perlakuan istimewa seperti itu lagi karena persyaratan mengenai pemrosesan data yang sah dan tidak melawan

hukum juga berlaku untuk *cookie*. Satu-satunya pertanyaan yang tidak dijawab sejauh ini oleh Pengadilan Eropa (*European Court of Justice*) adalah apakah penggunaan cookie harus berdasarkan pada persetujuan individu yang menjadi subjek data (Pasal 6 (1) (a) GDPR) atau apakah cukup ketika pengontrol menyatakan bahwa penggunaan ini diperlukan untuk tujuan kepentingannya yang sah (Pasal 6 (1) (f) GDPR). Dalam kasus manapun, menurut Konferensi Perlindungan Data Jerman, persetujuan sebelumnya diperlukan untuk penggunaan mekanisme pelacakan (tracking system)[82], yang mengejar perilaku orang-orang yang terkena dampak di internet dan membuat profil pengguna. Itu berarti, bahwa persetujuan berdasarkan informasi dalam arti GDPR diperlukan dalam bentuk pernyataan atau tindakan konfirmasi lainnya yang diambil sebelum pemrosesan data (mis., Sebelum cookie ditempatkan pada perangkat pengguna).

E. Pelaksanaan *The German Federal Data Protection Act* (BDSG)

The German Federal Data Protection Act memiliki pemisahan pengaturan pemrosesan data di sektor publik dan sektor privat. Sebagai tambahan, Jerman memiliki pengaturan khusus untuk informasi elektronik dan pelayanan komunikasi (telemedia) dan selain itu juga terdapat aturan privasi untuk pelayanan provider yang melakukan transmisi sinyal elektronik. Semua undang-undang ini diaplikasikan ke beberapa provider pelayanan online. Melalui undang-undang ini, Jerman mengadopsi Peraturan Uni Eropa 95/46/EC dan 2002/58/EC, dengan pendekatan yang sangat kompleks dan spesifik.

[82]Sistem *tracking* adalah komponen yang salingberinteraksi yang bertujuan untuk melacak atau memantau suatu objek. Jogiyanto H, Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur teori dan Praktik Aplikasi Bisnis, Yogyakarta: Andi Offset, 2005

Di Jerman, proteksi data memiliki dimensi konstitusional yang berangkat dari perlindungan martabat kemanusiaan. Berangkat dari perlindungan hak tersebut, Mahkamah Konstitusi Federal memformulasikan hak untuk memberikan informasi (*informational self-determination right*) yang memberikan izin untuk melakukan pemrosesan data personal hanya jika disahkan oleh undang-undang atau dengan persetujuan subyek data yang bersangkutan. Pada tahun 2008, Pengadilan mengekspansi prinsip ini dengan mengartikulasikan perlindungan konstitusi atas integritas dan kerahasiaan sistem informasi teknologi. Pada tahun 2010, Mahkamah Konstitusi membatalkan pengaturan terkait transposisi data dalam *the EU Data Retention Directive* karena melanggar prinsip proporsionalitas dan hak kepribadian individu.

Tidak ada sistem registrasi atau pemberitahuan di seluruh Uni Eropa dan Pasal 89 dari GDPR berupaya untuk melarang kewajiban pemberitahuan umum tanpa pandang bulu. Namun, Negara-negara Anggota dapat mengenakan kewajiban pemberitahuan untuk kegiatan tertentu (misalnya, pemrosesan data pribadi yang berkaitan dengan hukuman dan pelanggaran pidana). Persyaratan untuk berkonsultasi dengan otoritas pengawas dalam kasus-kasus tertentu setelah penilaian dampak perlindungan data[83] merupakan persyaratan pemberitahuan. Selain itu, setiap pengontrol atau prosesor harus mengomunikasikan perincian petugas perlindungan datanya (jika diperlukan untuk menunjuk satu) kepada otoritas pengawasnya.[84] Dalam banyak hal, akuntabilitas eksternal kepada otoritas pengawas melalui registrasi atau pemberitahuan digantikan dalam GDPR oleh tuntutan keras untuk akuntabilitas internal. Khususnya, pengontrol dan prosesor

[83] Pasal 36 GDPR
[84] Pasal 37 (7) GDPR

diharuskan untuk melengkapi dan memelihara catatan komprehensif dari kegiatan pemrosesan data mereka,[85] yang harus berisi rincian spesifik tentang pemrosesan data pribadi yang dilakukan dalam suatu organisasi dan harus diberikan kepada otoritas pengawas atas permintaan. Ini adalah usaha operasional yang cukup besar.

Petugas Perlindungan Data (Data Protection Officer)

GDPR telah menetapkan Petugas Perlindungan Data (DPO) di Eropa. Berlawanan dengan kepercayaan umum, yang menentukan kewajiban hukum untuk menunjuk Petugas Perlindungan Data bukanlah ukuran perusahaan tetapi aktivitas pemrosesan inti yang didefinisikan sebagai hal yang esensial untuk mencapai tujuan perusahaan. Jika kegiatan inti ini terdiri dari pemrosesan data pribadi yang sensitif dalam skala besar atau suatu bentuk pemrosesan data yang sangat jauh menjangkau hak-hak subyek data, perusahaan harus menunjuk DPO.

Setiap pengontrol atau prosesor diharuskan untuk menunjuk petugas perlindungan data jika memenuhi satu atau lebih memiliki kualifikasi sebagai berikut:[86]

- otoritas publik;
- Kegiatan intinya terdiri dari operasi pemrosesan yang, berdasarkan sifatnya, ruang lingkup atau tujuannya, membutuhkan pemantauan berkala dan sistemik terhadap subyek data dalam skala besar;

[85] Pasal 30 GDPR
[86] Pasal 37 GDPR

- atau kegiatan intinya terdiri dari pemrosesan data pribadi yang sensitif dalam skala besar.

Badan publik di sisi lain selalu harus menunjuk DPO, dengan pengecualian pengadilan yang bertindak dalam kapasitas yudisial mereka. Selain itu, norma hukum untuk menunjuk Petugas Perlindungan Data memiliki klausul fleksibilitas untuk Negara-negara Anggota Uni Eropa. Negara Uni Eropa bebas untuk memutuskan apakah perusahaan harus menunjuk Petugas Perlindungan Data berdasarkan persyaratan yang lebih ketat.[87] Jika kewajiban semacam itu ada di bawah Peraturan Perlindungan Data Umum atau hukum nasional yang lebih spesifik, perusahaan juga dapat menunjuk seorang Petugas Perlindungan Data tunggal. Jika kelompok memutuskan untuk melakukannya, ia harus mudah diakses oleh otoritas pengawas, karyawan, dan subjek data eksternal. Jika tidak ada kewajiban hukum, perusahaan dapat menunjuk DPO atas dasar sukarela untuk membantu kepatuhan perlindungan data.

Perusahaan memiliki dua kemungkinan untuk memenuhi kewajiban mereka untuk menunjuk Petugas Perlindungan Data. Kemungkinan pertama adalah menunjuk karyawan sebagai Petugas Perlindungan Data internal, atau perusahaan menunjuk Petugas Perlindungan Data eksternal. Dalam memilih orang seperti itu, mereka harus memastikan bahwa Petugas Perlindungan Data internal tidak mengalami konflik kepentingan karena pekerjaannya di Departemen Teknologi Informasi, Departemen SDM atau Manajer, di mana ia harus mengawasi dirinya sendiri. Terlepas dari opsi mana yang dipilih, Petugas Perlindungan Data harus memiliki pengetahuan dalam undang-undang

[87] Pasal 38 Undang-Undang Perlindungan Data Federal Jerman

perlindungan data dan menguasai keamanan teknologi informasi, ruang lingkup tergantung pada kompleksitas pemrosesan data dan ukuran perusahaan.

Tugas seorang Petugas Perlindungan Data meliputi: Bekerja menuju kepatuhan dengan semua undang-undang perlindungan data yang relevan, memantau proses spesifik, seperti penilaian dampak perlindungan data, meningkatkan kesadaran karyawan untuk perlindungan data dan melatihnya, serta bekerja sama dengan otoritas pengawas. Oleh karena itu, karyawan yang bertindak sebagai Petugas Perlindungan Data tidak boleh diberhentikan atau dihukum karena pemenuhan tugasnya.[88] Meskipun fungsinya pemantauan, perusahaan itu sendiri tetap bertanggung jawab untuk mematuhi undang-undang perlindungan data. Oleh karena itu harus melibatkan Petugas Perlindungan Data dalam semua masalah yang terkait dengan perlindungan data pribadi "dengan benar dan tepat waktu". Ketika Petugas Perlindungan Data diangkat, atasannya harus mempublikasikan data kontaknya, dan mengomunikasikan penunjukan dan data kontaknya ke otoritas pengawas perlindungan data. Jika perusahaan secara sukarela menunjuk DPO, mereka juga harus mematuhi kriteria dan ketentuan yang disebutkan di atas. Juga perhatikan bahwa kegagalan yang disengaja atau lalai untuk menunjuk Petugas Perlindungan Data meskipun kewajiban hukum merupakan pelanggaran yang dikenakan denda.

Tugas seorang Petugas Perlindungan Data meliputi: Bekerja menuju kepatuhan dengan semua undang-undang perlindungan data yang relevan, memantau proses spesifik, seperti penilaian dampak perlindungan data,

[88] Pasal 39 GDPR

meningkatkan kesadaran karyawan untuk perlindungan data dan melatihnya, serta bekerja sama dengan otoritas pengawas.[89]

Oleh karena itu, pegawai yang bertindak sebagai Petugas Perlindungan Data tidak boleh diberhentikan atau dihukum karena pemenuhan tugasnya. Meskipun fungsinya pemantauan, perusahaan itu sendiri tetap bertanggung jawab untuk mematuhi undang-undang perlindungan data. Oleh karena itu harus melibatkan Petugas Perlindungan Data dalam semua masalah yang terkait dengan perlindungan data pribadi "dengan benar dan tepat waktu". Ketika Petugas Perlindungan Data diangkat, atasannya harus mempublikasikan data kontaknya, dan mengomunikasikan penunjukan dan data kontaknya ke otoritas pengawas perlindungan data. Jika perusahaan secara sukarela menunjuk DPO, mereka juga harus mematuhi kriteria dan ketentuan yang disebutkan di atas. Juga perhatikan bahwa kegagalan yang disengaja atau lalai untuk menunjuk Petugas Perlindungan Data meskipun kewajiban hukum merupakan pelanggaran yang dikenakan denda.[90]

Dewan Perlindungan Data Eropa (*The European Data Protection Board*)

Dewan Perlindungan Data Eropa ini dibangun sebagai badan bagian dari Uni Eropa dan memiliki kekuatan sebagai badan hukum. Dewan ini direpresentasikan oleh pimpinan dewan. Anggota Dewan terdiri dari salah satu supervisor otoritas tiap negara anggota Uni Eropa dan representasinya.[91] Tiap negara anggota memiliki lebih dari satu otoritas supervisi yang bertanggung jawab

[89] Pasal 39 ayat (1) GDPR
[90] https://gdpr-info.eu/issues/data-protection-officer/
[91] Lihat Pasal 68 GDPR

untuk memonitoring aplikasi norma dalam GDPR serta representasi bersama yang ditunjuk sesuai dengan undang-undang domestik negara anggota. Komisi harus memiliki hak untuk berpartisipasi dalam aktivitas dan rapat Dewan tanpa memiliki hak voting. Komisi Eropa harus mendesain representatif. Ketua Dewan harus berkomunikasi dengan Komisi terkait aktivitas Dewan. Supervisor Perlindungan Data Eropa harus memiliki hak voting hanya untuk keputusan yang tekait prinsip dan aturan aplikasi kepada institusi Uni Eropa, badan, kantor, dan agensi yang berkorespondensi dengan regulasi ini.

II. Pengaturan Hak Privasi di Indonesia

Teknologi pemrosesan data modern telah mimiliki banyak keunggulan di atas metode manual lain yang lebih lambat, akan tetapi kemajuan teknologi tersebut tentunya tidak lepas dari beberapa persoalan. Salah satu persoalan tersebut antara lain fakta bahwa pemrosesan data dapat mengancam hak individu atas privasi. Data pribadi sekarang dapat dikombinasikan dan disimpan tanpa adanya batasan dan juga sangat dapat diakses daripada era sebelum kemajuan teknologi ini. Data personal dapat disebarkan dan dimanipulasi informasinya dalam setiap bidang dan serngnya tanpa sepengetahuan pemilik data. Apalagi terdapat kemungkinan bahwa pemerintah dan perusahaan bisnis mengumpulkan informasi dari warga negara yang berpotensi mengancam kebebasan individu.[92]

Sampai saat ini tidak ada undang-undang khusus terkait perlindungan data Namun, ada peraturan tertentu tentang penggunaan data elektronik. Sumber utama

[92] J Lee Riccardi, The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?, Boston College International and Comparative Law Review, Volume 6 | Issue 1, hal.24

hukum terkait pengelolaan informasi dan transaksi elektronik adalah Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah oleh UU No. 19 tahun 2016 tentang Perubahan UU ITE, Peraturan Pemerintah No. 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Reg. 82) dan peraturan pelaksanaannya, Peraturan Menteri Komunikasi & Informatika No. 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.[93]

Indonesia memiliki aturan soal perlindungan data pribadi di era digital.Aturan itu dituangkan dalam bentuk Peraturan Menteri (Permen) No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) ditetapkan 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016. Peraturan Menteri ini adalah satu dari 21 Permen yang merupakan turunan dari Peraturan Pemerintah (PP) No 82 / 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang diundangkan dan berlaku sejak 15 Oktober 2012.

Data Pribadi yang disimpan dalam Sistem Elektronik harus Data Pribadi yang telah diverifikasi keakuratannya. Data Pribadi yang disimpan dalam Sistem Elektronik harus dalam bentuk data terenkripsi. Data Pribadi wajib disimpan dalam Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan yang mengatur kewajiban jangka waktu penyimpanan Data Pribadi pada masing-masing Instansi Pengawas dan Pengatur Sektor atau paling singkat lima tahun, jika belum terdapat ketentuan peraturan perundang-undangan yang secara khusus mengatur untuk itu.

[93]Data Protection Laws of The World, Full Handbook, DLA Piper, diunduh melalui https://www.finalcrypt.org/data-protection-full.pdf pada tanggal 3 November 2019

A. Aturan Pusat Data.

Hal yang menarik di aturan ini adalah ketentuan Pusat data(*data center*) dan pusat pemulihan bencana (*disaster recovery center*) Penyelenggara Sistem Elektronik untuk pelayanan publik yang digunakan untuk proses perlindungan wajib ditempatkan dalam wilayah negara Republik Indonesia.

Penyelenggara sistem Elektronik wajib memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing Instansi Pengawas dan Pengatur Sektor untuk itu; dan menyediakan narahubung (*contact person*) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pengelolaan Data Pribadinya.

Apabila pemilik data pribadi merupakan kategori anak-anak, pemberian persetujuan sebagaimana yang di maksud dalam permen ini dilakukan oleh orang tua atau wali anak yang bersangkutan. Untuk penyelenggara sistem elektronik yang telah menyediakan, menyimpan, dan mengelola data pribadi sebelum Permen ini berlaku, wajib tetap menjaga kerahasiaan data pribadi yang telah ada. Bagi yang melanggar aturan hanya dikenai sangsi administratif berupa: (a) peringatan lisan; (b) Peringatan Tertulis; (c) Penghentian semetara kegiatan dan / atau; pengumuman di situs dalam jaringan, yang tata caranya akan diatur dengan Peraturan Menteri.

Rancangan Undang-Undang baru tentang Perlindungan Data Pribadi Pribadi sedang dibahas namun sampai saat ini belum disahkan oleh DPR. Meskipun tanggal pastinya tetap tidak pasti dan RUU ini masih harus dipertimbangkan oleh Dewan Perwakilan Rakyat, jika disahkan, ini akan menjadi hukum komprehensif pertama di Indonesia yang secara khusus menangani masalah privasi data. Selain ketentuan dalam UU ITE, PP 82 dan Peraturan Kemenkoinfo No. 20/2016, terdapat serangkaian peraturan yang juga mencakup ketentuan tertentu terkait perlindungan data sebagai berikut:

A. Sektor Telekomunikasi

Dalam undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi Pasal 40 menyebutkan bahwa "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun". Sedangkan dalam Pasal 42 disebutkan bahwa "Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya".

B. Sektor Informasi Publik

Pada Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 6 ayat (1) menyatakan bahwa "Badan Publik berhak menolak memberikan informasi yang dikecualikan sesuai dengan ketentuan peraturan perundang-undangan". Dan pada Pasal 6 ayat (2) menyatakan "Badan Publik berhak menolak memberikan Informasi Publik apabila tidak sesuai dengan

ketentuan peraturan perundang-undangan". Sedangkan pada Pasal 17 bersama dengan undang-undang lain, melarang pengungkapan informasi pribadi siapa pun, terutama yang menyangkut sejarah keluarga, riwayat medis dan psikologis, informasi keuangan (termasuk aset, pendapatan dan catatan bank) dan catatan evaluasi mengenai kemampuan seseorang, rekomendasi, catatan pendidikan intelektual, formal, atau informal.

C. Perbankan dan Pasar Modal

Sektor Privasi data di sektor ini diatur berdasarkan Undang-Undang 7 tahun 1992 sebagaimana telah diubah dengan Undang-Undang 10 tahun 1998 tentang Perbankan dan UU 8 tahun 1995 tentang Pasar Modal (UU Pasar Modal). Peraturan tersebut berlaku untuk data individu dan perusahaan. Peraturan Bank Indonesia No. 9/15 / PBI / 2007 tentang Penerapan Manajemen Risiko dalam Pemanfaatan Teknologi Informasi oleh Bank menetapkan bahwa transfer data pelanggan bank (dengan cara membangun data pusat atau pemrosesan data di luar wilayah Indonesia) memerlukan persetujuan terlebih dahulu yang diperoleh dari Bank Indonesia. Pasal 18

Penggunaan pihak penyedia jasa Teknologi Informasi hanya dapat dilakukan sepanjang Bank dan pihak penyedia jasa Teknologi Informasi memenuhi persyaratan sebagai berikut: bagi pihak penyedia jasa Teknologi Informasi sebagai pihak terafiliasi, pihak penyedia jasa harus menjamin keamanan seluruh informasi termasuk rahasia Bank dan data pribadi nasabah.

B. Definisi Data Pribadi

Definisi Data Pribadi dalam Pasal 1 angka 27 UU ITE Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permen Kominfo Nomor 20 Tahun 2016) adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.[94] Sedangkan Data Perseorangan Tertentu adalah "setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan".Pemilik Data Pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu.[95] Terkait definisi data personal sensitif, Pemerintah Indonesia belum memberikan definisi spesifik dan khusus terkait data pribadi yang sensitif dalam undang-undang maupun regulasi teknis dibawah undang-undang.

Menurut GDPR, Data pribadi adalah informasi apapun yang terkait dengan orang perorang atau "subjek data" yang bisa digunakan untuk mengidentifikasi seseorang secara langsung atau tidak langsung. Data yang dimaksud bisa berupa nama, foto, informasi, alamat protokol Internet (IP Address), pengidentifikasi online seperti fisik, fisiologis, genetis, mental, ekonomi, budaya, atau identitas sosial seseorang[96].

Pengaturan data pribadi secara tidak langsung diatur dalam ketentuan UU No.39 Tahun 1999 tentang Hak Asasi Manusia, sebagai berikut:

---

[94] Lihat Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik Nomor 20 Tahun 2016 Pasal 1 angka 1, 2, dan 3

[95]Lihat Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik Pasal 1 Angka 1

[96] Wahyudi Djafar,dkk, Hak Atas Penghapusan Informasi di Indonesia:Orisinalitas dan tantangan dan penerapannya, 2018, Jakarta, LBG Pers, hal.25.

a. Pasal 29 ayat (1) mengatur perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya;
b. Pasal 30 mengatur perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu.
c. Pasal 31 mengatur bahwa tempat kediaman siapapun tidak boleh diganggu, menginjak atau memasuki suatu pekarangan tempat kediaman atau memasuki suatu rumah yang bertentangan dengan kehendak orang yang mendiaminya,hanya diperbolehkan dalam hal-hal yang telah ditetapkan dengan undang-undang.
d. Pasal 32 mengatur bahwa kemerdekaan dan rahasia dalam hubungan surat menyurat termasuk hubungan komunikasi surat menyurat termasuk hubungan komunikasi sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yanng sah sesuai dengan ketentuan peraturan perundang-undangan.

Dengan demikian, cakupan hak pribadi di Indonesia antara lain meliputi:

a. sesuatu yang menyangkut diri pribadi seseorang, keluarga, barang pribadi dan reputasinya;
b. berbuat dan tidak berbuat sesuatu;
c. kediaman pribadi;
d. komunikasi pribadi.

Sementaratu, diharapkan sejumlah undang-undang pada beberapa sektor mengatur perihal keharusan untuk melindungi hak-hak pribadi seseorang, seperti adanya aturan yang melarang intersepsi komunikasi secara legal, serta kewajiban bagi pengumpul data untuk melindungi kerahasiaan data pribadiyang

dikumpulkannya. Bahkan secara khusus dalam ketentuan Pasal 26 UU Informasi dan Transaksi Elektronik diatur bahwa data pribadi seseorang tidak boleh dipindah tangankan secara semena mana tanpa persetujuan dari pemilik data. Setidaknya terdapat 32 undang-undang yang materinya memiliki konten yang terkait dengan pengaturan data pribadi warga negara. Mayoritas dari 32 undang-undang tersebut materinya terkait dengan pemberian kewenangan baik bagi otoritas publik (pemerintah) maupun privat (swasta) untuk melakukan pengumpulan dan pengelolaan data pribadi warga negara, termasuk wewenang untuk melakukan intrusi dengan beberapa pengecualian. Sektor yang diatur beragam, mulai dari telekomunikasi, keuangandan perbankan, perpajakan, kependudukan, kearsipan, penegakanhukum, keamanan, hingga sektor kesehatan.[97]

Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:[98]

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan (Orang lain tanpa tindakan memata-matai).
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

[97] *Ibid*, hal.49.
[98] Lihat Pada Penjelasan Pasal 25 ayat 1 UU ITE,

Kewajiban Penyelenggara Sistem Elektronik

Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.[99]

Penyelenggara Sistem Elektronik wajib:[100]

a. menjaga rahasia, keutuhan, dan ketersediaan Data Pribadi yang dikelolanya;
b. menjamin bahwa perolehan, penggunaan, dan pemanfaatan Data Pribadi berdasarkan persetujuan pemilik Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
c. menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik Data Pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik Data Pribadi pada saat perolehan data.

Jika terjadi kegagalan dalam perlindungan rahasia Data Pribadi yang dikelolanya, Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut. Penyelenggara Sistem Elektronik wajib menyampaikan informasi kepada Pengguna Sistem Elektronik paling sedikit mengenai jaminan privasi dan/atau perlindungan Data Pribadi.[101] Perlindungan

[99] Pasal 1 angka 2 Peraturan Kemenkoinfo 4/2016
[100] Pasal 15 (1) Peraturan Pemerintah Nomor 82/2012
[101] Pasal 25 ayat (1) Peraturan Pemerintah Nomor 82/2012

terhadap kerahasiaan Data Pribadi Pengguna Sistem Elektronik juga harus dipenuhi dalam hal penyelenggara menggunakan jasa pihak lain (outsourcing).[102]

Pengamanan terhadap kerahasiaan Data Pribadi (privacy seal) merupakan Sertifikat Keandalan yang jaminan keandalannya adalah memberikan kepastian bahwa Data Pribadi konsumen dilindungi kerahasiaannya sebagaimana mestinya.

C. Otoritas Perlindungan Data Nasional (*National Data Protection Authority*)

Di Indonesia tidak ada otoritas perlindungan data nasional khusus untuk privasi data. Sebagai contoh, Otoritas Jasa Keuangan Indonesia (OJK) memiliki wewenang untuk bertindak sebagai regulator privasi data di sektor pasar modal (sejak 31 Desember 2012) dan berkaitan dengan masalah privasi data pelanggan bank (sejak 31 Desember 2013). Namun, dapat dicatat bahwa pasal 65 Peraturan Pemerintah Nomor 82 Tahun 2012 menyatakan bahwa pelaku bisnis yang mengoperasikan transaksi elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan (Kompetensi Sertifikasi) dari internal Indonesia atau badan sertifikasi kompetensi asing. Walau sampai saat ini lembaga tersebut belum ada.

Undang-undang ITE mengatur bahwa 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. Oleh karenanya setiap orang yang dilanggar haknya dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.[103]

---

[102] lihat Penjelasan 25 ayat (1) Peraturan Pemerintah Nomor 82/2012
[103] Pasal 26 (1) Undang-Undang ITE

4. Registrasi

Peraturan Kemenkoinfo Nomor 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik membedakan penyelenggaraan sistem elektronik menjadi dua jenis yaitu Penyelenggara Sistem Elektronik untuk Pelayanan Publik dan Penyelenggara Sistem Elektronik untuk non Pelayanan Publik. Penyedia sistem elektronik untuk layanan publik harus melakukan registrasi, sementara penyedia sistem elektronik untuk layanan non-publik dapat melakukan registrasi, yang menunjukkan bahwa registrasi tidak wajib untuk penyedia sistem elektronik untuk layanan non-publik).[104]

Peraturan Kemenkoinfo 36/2014 secara khusus menyatakan bahwa penyedia sistem elektronik untuk layanan publik adalah badan hukum yang terkait dengan pemerintah, misalnya lembaga negara, lembaga pemerintah, perusahaan dalam bentuk badan usaha milik negara, badan usaha milik daerah, atau badan hukum lain yang berkaitan dengan misi negara.[105] Penyedia sistem elektronik untuk layanan non-publik tidak secara khusus didefinisikan dalam Peraturan Kemenkoinfo No. 4/2016, tetapi secara umum badan hukum lain yang tidak terkait dengan pemerintah, seperti perusahaan swasta, dapat diklasifikasikan sebagai penyedia sistem elektronik untuk layanan non-publik.

Namun, pemerintah menafsirkan 'pelayanan publik' dalam hal penyedia sistem elektronik sesuai dengan Peraturan Pemerintah No. 96 tahun 2012 tentang Implementasi Undang-Undang No. 25 tahun 2009 tentang Pelayanan Publik mendefinisikan Pelayanan Publik sebagai kegiatan atau rangkaian kegiatan dalam

[104] Lihat Pasal 3 ayat (1) dan ayat (2) Peraturan Kemenkoinfo Nomor 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik
[105] Lihat Pasal 4 Peraturan Kemenkoinfo Nomor 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik

rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundangundangan bagi setiap warga negara dan penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.[106]

Peraturan Pemerintah ini lebih lanjut mendefinisikan Penyelenggara Pelayanan Publik yang selanjutnya disebut Penyelenggara adalah setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan Undang-Undang untuk kegiatan pelayanan publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik.[107]

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik mengatur bahwa ruang lingkup barang dan jasa publik serta pelayanan administrasi. Pasal 5 ayat (2) lebih jauh mengatur ruang lingkup pelayanan publik meliputi pendidikan, pengajaran, pekerjaan dan usaha, tempat tinggal, komunikasi dan informasi, lingkungan hidup, kesehatan, jaminan sosial, energi, perbankan, perhubungan, sumber daya alarn, pariwisata, dan sektor strategis lainnya. Sehubungan dengan hal di atas, penyedia sistem elektronik untuk layanan non-publik berada di bawah korporasi (badan hukum terkait non-pemerintah), menyediakan layanan untuk setiap warga negara / individu.

Oleh karena itu, penyedia sistem elektronik untuk layanan non-publik juga dianggap sebagai layanan publik sesuai dengan PP 96. Akibatnya, semua penyedia sistem elektronik, baik untuk layanan publik atau layanan non-publik, harus melakukan registrasi. Pasal 4 Peraturan Menteri Komunikasi dan

[106] Lihat Peraturan Pemerintah Nomor 96 Tahun 2012 Pasal 1 Angka 1
[107] Lihat Peraturan Pemerintah Nomor 96 tahun 2012 Pasal 1 Angka 2

Informatika No. 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Peraturan Kemenkoinfo No. 4/2016) menetapkan bahwa ada tiga kategori sistem elektronik:

1) Sistem Elektronik strategis merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.
2) Sistem Elektronik tinggi merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.
3) Sistem Elektronik rendah merupakan Sistem Elektronik lainnya yang tidak termasuk pada Sistem Elektronik strategis dan Sistem Elektronik tinggi.

Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi.[108] Sementara Penyelenggara Sistem Elektronik rendah dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi dalam memberikan layanan kepada warga negara.[109]

Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya. Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi harus menerapkan standar SNI ISO/IEC 27001. Penyelenggara Sistem

[108] Lihat Peraturan Kemenkoinfo No. 4/2016 Pasal 10 ayat (1)
[109] Lihat Pasal 10 ayat (2) Peraturan Kemenkoinfo No. 4/2016

Elektronik yang menyelenggarakan Sistem Elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi. Ketentuan mengenai pedoman Indeks Keamanan Informasi diatur dalam Peraturan Menteri.[110]

Dalam penerapan standar dan pedoman sebagaimana dimaksud di atas, Penyelenggara Sistem Elektronik dapat menggunakan Tenaga Ahli internal dan/atau Tenaga Ahli eksternal. Dalam hal penerapan standar terhadap Sistem Elektronik strategis, Penyelenggara Sistem Elektronik harus menggunakan Tenaga Ahli berkewarganegaraan Indonesia.

Setelah akurasi dan kompatibilitasnya dengan tujuan memperoleh dan mengumpulkan Data Pribadi tersebut diverifikasi Pasal 22 (1) Peraturan Kemenkoinfo No. 4/2016 menyatakan bahwa mentransfer Data Pribadi yang dikelola oleh operator sistem elektronik di pemerintah dan lembaga pemerintah daerah termasuk masyarakat atau sektor swasta yang berdomisili di wilayah Indonesia untuk [pihak] di luar wilayah Indonesia harus: Berkoordinasi dengan Peraturan Kemenkoinfo No. 4/2016 atau pejabat atau lembaga yang berwenang untuk tujuan tersebut, dan Menerapkan undang-undang dan peraturan tentang pertukaran lintas batas Data Pribadi. Implementasi dari koordinasi sebagaimana diatur dalam Pasal 22 (1) (a) Peraturan Peraturan Kemenkoinfo No. 4/2016 adalah: Untuk melaporkan rencana implementasi transfer Data Pribadi, paling sedikit memuat nama yang jelas, negara yang ditunjuk, nama subjek penerima, tanggal pelaksanaan, dan alasan / tujuan dari transfer Untuk meminta advokasi, jika perlu melaporkan hasil implementasi kegiatan.

[110] Lihat Pasal 7 ayat (1), (2), (3) Peraturan Kemenkoinfo No. 4/2016

Setelah akurasi dan kompatibilitasnya dengan tujuan untuk memperoleh dan mengumpulkan Data Pribadi tersebut diverifikasi Pasal 22 (1) Peraturan Kemenkoinfo No. 4/2016 menyatakan bahwa mentransfer Data Pribadi yang dikelola oleh operator sistem elektronik di pemerintah dan lembaga pemerintah daerah termasuk masyarakat atau sektor swasta yang berdomisili di wilayah Indonesia untuk [pihak] di luar wilayah Indonesia harus: Berkoordinasi dengan Peraturan Kemenkoinfo No. 4/2016 atau pejabat atau lembaga yang berwenang untuk tujuan tersebut, dan Menerapkan undang-undang dan peraturan tentang pertukaran lintas batas Data Pribadi. Implementasi dari koordinasi sebagaimana diatur dalam Pasal 22 (1) (a) Peraturan Peraturan Kemenkoinfo No.. 4/2016 adalah: Untuk melaporkan rencana implementasi transfer Data Pribadi, paling sedikit memuat nama yang jelas, negara yang ditunjuk, nama subjek penerima, tanggal pelaksanaan, dan alasan / tujuan dari transfer Untuk meminta advokasi, jika perlu melaporkan hasil implementasi kegiatan.

Lembaga Sertifikasi Sistem Manajemen Pengamanan Informasi

Lembaga Sertifikasi adalah lembaga yang menerbitkan Sertifikat Sistem Manajemen Pengamanan Informasi. Sertifikat Sistem Manajemen Pengamanan Informasi adalah bukti tertulis yang diberikan oleh Lembaga Sertifikasi kepada Penyelenggara Sistem Elektronik yang telah memenuhi persyaratan. Penilaian Mandiri adalah mekanisme evaluasi kategori Sistem Elektronik yang dilakukan secara mandiri (*self assessment*) oleh Penyelenggara Sistem Elektronik berdasarkan kriteria tertentu.

Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi. Penyelenggara Sistem Elektronik rendah dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi. Sertifikasi Sistem Manajemen Pengamanan Informasi dilakukan oleh Lembaga Sertifikasi yang diakui oleh Menteri.

Lembaga Sertifikasi harus memenuhi syarat sebagai berikut:

a. berbentuk badan hukum Indonesia;
b. berdomisili di Indonesia;
c. terakreditasi oleh Komite Akreditasi Nasional;
d. memiliki tim Auditor yang beranggotakan paling sedikit 1 (satu) Auditor Permanen;
e. memiliki tim pengambil keputusan sertifikasi.

Tim Auditor dan tim pengambil keputusan sertifikasi yang melakukan sertifikasi Sistem Elektronik strategis harus berkewarganegaraan Indonesia. Sertifikasi Sistem Manajemen Pengamanan Informasi harus dilakukan sesuai dengan proses Penyelenggaraan Sistem Elektronik dengan memperhatikan tingkat Risiko.[111] Lembaga Sertifikasi menugaskan tim Auditor untuk melakukan audit Sistem Manajemen Pengamanan Informasi terhadap Penyelenggara Sistem Elektronik. Tim Auditor melaporkan hasil audit pada Lembaga Sertifikasi yang menugaskan.

[111] Pasal 16

D. Keamanan Data Pribadi

Kewajiban dari penyedia sistem elektronik diatur dalam diatur dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Kemenkoinfo No. 4/2016 sebagai berikut:

a. melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik yang melakukan Transaksi Elektronik;
b. memiliki dan melaksanakan kebijakan dan prosedur untuk mengambil tindakan jika terdapat indikasi terjadi pencurian data;
c. memastikan pengendalian terhadap otorisasi dan hak akses terhadap sistem, database, dan aplikasi Transaksi Elektronik;
d. menyusun dan melaksanakan metode dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Transaksi Elektronik;
e. memiliki dan melaksanakan standar dan pengendalian atas penggunaan dan perlindungan data jika pihak penyedia jasa memiliki akses terhadap data tersebut;
f. memiliki rencana keberlangsungan bisnis termasuk rencana kontingensi yang efektif untuk memastikan tersedianya sistem dan jasa Transaksi Elektronik secara berkesinambungan; dan
g. memiliki prosedur penanganan kejadian tak terduga yang cepat dan tepat untuk mengurangi dampak suatu insiden, penipuan, dan kegagalan Sistem Elektronik.

Selain kewajiban yang secara eksplisit diatur, jika kita membaca Peraturan Pemerintah Nomor 82 Tahun 2012 dan Peraturan Kemenkoinfo No. 4/2016 kita dapat melihat kewajiban lainnya yaitu:

- Memastikan perjanjian tentang tingkat layanan minimum dan keamanan informasi terhadap layanan teknologi informasi yang digunakan serta keamanan dan fasilitas keamanan komunikasi internal yang diterapkannya
- Melindungi dan memastikan privasi dan perlindungan data pribadi pengguna
- Memastikan penggunaan yang sah dan pengungkapan data pribadi
- Menyediakan pusat data dan pusat pemulihan bencana (untuk Penyedia Sistem Elektronik untuk layanan publik)
- Memberikan catatan audit tentang semua Penyediaan kegiatan Sistem Elektronik. Memberikan informasi dalam Sistem Elektronik berdasarkan permintaan yang sah dari penyidik untuk kejahatan tertentu
- Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang diproses sehingga [Data Pribadi] dapat atau tidak dapat digunakan atau ditampilkan oleh pihak ketiga berdasarkan Persetujuan selama itu terkait dengan tujuan untuk memperoleh dan mengumpulkan Data Pribadi
- Memberikan akses atau peluang kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadi mereka tanpa mengganggu manajemen sistem Data Pribadi, kecuali jika sebaliknya diatur oleh undang-undang dan peraturan.
- Menghapus Data Pribadi jika:

1) telah mencapai periode maksimum menyimpan Data Pribadi (paling singkat lima tahun atau berdasarkan peraturan yang berlaku / peraturan sektoral tertentu); atau
2) atas permintaan dari Pemilik Data Pribadi, kecuali jika sebaliknya diatur oleh hukum dan peraturan, dan
3) Memberikan orang yang mudah dihubungi oleh Pemilik Data Pribadi sehubungan dengan Data Pribadi mereka

Di sektor telekomunikasi, Pasal 19 Peraturan Menteri Komunikasi dan Informatika No. 26 / PER / M.KOMINFO / 05/2007 tentang Keamanan dan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet (sebagaimana diamandemen) (MR 26/2007) juga menyediakan bahwa penyedia layanan telekomunikasi bertanggung jawab atas penyimpanan data karena kewajibannya untuk mencatat file log-nya setidaknya selama tiga bulan.

Pemberitahuan Pelanggaran

Pasal 15 (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan bahwa penyedia Sistem Elektronik harus memberikan pemberitahuan tertulis kepada pemilik data pribadi setelah kegagalannya melindungi data pribadi. Pasal 20 (3) PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan bahwa penyedia Sistem Elektronik harus melakukan upaya terbaik untuk melindungi data pribadi dan untuk segera melaporkan kegagalan atau gangguan sistem serius atau gangguan kepada pejabat penegak hukum atau Otoritas Pengawas dan Pengatur sektor terkait. Pasal 25 ayat 2 Peraturan Kemenkoinfo No. 4/2016 Peraturan mengatur bahwa pemberitahuan tertulis

kepada Pemilik Data Pribadi diperlukan jika ada kegagalan dalam melindungi kerahasiaan Data Pribadi dalam Sistem Elektronik.

Ketentuan pemberitahuan pelanggaran harus memberikan alasan atau penyebab terjadinya kegagalan dalam melindungi kerahasiaan Data Pribadi. Ini dapat diberikan secara elektronik, jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu pada saat memperoleh dan mengumpulkan Data Pribadi mereka Harus memastikan bahwa pemberitahuan tersebut telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian pada Data Pribadi yang relevan Pemilik, dan Pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi selambat-lambatnya 14 hari setelah kegagalan ditemukan

E. Pelaksanaan Perlindungan Data

Di Indonesia, sanksi untuk pelanggaran privasi data ditemukan di bawah undang-undang yang relevan dan pada dasarnya adalah denda. Penjara dapat dijatuhkan dalam kasus yang berat, seperti dalam hal terjadi pelanggaran yang disengaja.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur pelanggaran privasi pada Pasal 30 ayat (1), (2), dan (3).[112] Sedangkan sanksi pidana untuk pelanggaran pada Pasal 30 ayat (1), (2), (3) terdapat pada pasal 46 ayat (1), (2), dan (3).

UU ITE dan Amandemen UU ITE memberikan hukuman pidana mulai dari: denda Rp 600 juta hingga Rp 800 juta dan hukuman penjara enam hingga

[112] Lihat Pasal 30 ayat 1, 2, dan 3 UU ITE

delapan tahun untuk akses tidak sah, denda Rp800 juta dan hukuman penjara 10 tahun karena intersepsi atau penyadapan transmisi. Sedangkan denda Rp2 miliar hingga Rp5 miliar dan 8 hingga 8 tahun. 10 tahun penjara karena perubahan, penambahan, pengurangan, transmisi, gangguan, penghapusan, memindahkan atau menyembunyikan Informasi Elektronik atau Kegagalan Arsip Elektronik untuk mematuhi Reg. 82 dikenai sanksi administratif (yang tidak menghilangkan tanggung jawab perdata dan pidana).

Sanksi administrasi ini adalah dalam bentuk: Peringatan tertulis Denda administratif Pengusiran sementara dari daftar pendaftaran (sebagaimana disyaratkan dalam peraturan) Kegagalan untuk mematuhi PERATURAN KEMENKOINFO NO. 4/2016 Peraturan tunduk pada sanksi administratif dalam bentuk: Peringatan lisan Peringatan tertulis Pemberhentian sementara kegiatan Pengumuman di situs web online Hukum Perbankan Menurut Pasal 47 UU Perbankan, komisaris, direktur atau karyawan bank atau afiliasinya yang dengan sengaja memberikan informasi yang harus dirahasiakan dapat dijatuhi hukuman penjara tidak kurang dari 2 tahun tetapi tidak lebih dari 4 tahun, dan didenda setidaknya Rp4 miliar tetapi tidak lebih dari Rp8 miliar.

Pasar modal

Undang-Undang Berdasarkan UU Pasar Modal, Otoritas Jasa Keuangan (Sebelumnya BAPEPAM LK) diberdayakan untuk menjatuhkan sanksi administratif berikut untuk pelanggaran ketentuan yang berkaitan dengan perlindungan data). Sanksi tersebut meliputi: Pengingat tertulis Denda pembatasan bisnis Penangguhan pencabutan izin usaha Pembatalan persetujuan Pembatalan pendaftaran.

Lokasi Data dan Pengaturan Cookies

Saat ini tidak ada undang-undang dan peraturan tentang cookie dan data lokasi. Namun, jika data yang dikumpulkan oleh cookie atau data lokasi diperoleh oleh akses ilegal informasi elektronik pihak lain, ini dikenakan hukuman penjara enam hingga delapan tahun dan / atau denda Rp600 juta hingga Rp800 juta.

BAB V

Kesimpulan dan Saran

A. Kesimpulan

Berdasarkan pemaparan hasil penelitian sebelumnya, dapat dilihat bahwa Jerman telah memiliki sejarah panjang terkait perlindungan data, bahkan hukum perlindungan data Jerman telah dimulai jauh sebelum GDPR berlaku di Uni Eropa. Melalui Bundestag atau BDSG, Jerman memiliki rezim perlindungan privasi dan perlindungan data pribadi. Oleh karenanya, sistem perlindungan privasi di Jerman sudah mapan baik tatanan hukum dan implementasinya.

Saat ini rezim perlindungan data di Jerman berada di bawah GDPR dan BDSG sebagai undang-undang domestik Jerman selain GDPR yang merupakan payung undang-undang perlindungan data di Uni Eropa. Setelah GDPR dibentuk pada tahun 2016, Jerman mengeluarkan Undang-undang perlindungan data dalam BDSG yang dibentuk pada tahun 2017. Undang-undang ini melengkapi area yang tidak diatur oleh GDPR.

Definisi Data Pribadi dalam Peraturan Menteri Komunikasi dan InformatikaNomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permen Kominfo Nomor 20 Tahun 2016) adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Sedangkan Data Perseorangan Tertentu adalah “setiap keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi, baik langsung maupun tidak langsung, pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan”.

Pemilik Data Pribadi adalah individu yang padanya melekat Data Perseorangan Tertentu. Terkait definisi data personal sensitif, Pemerintah Indonesia belum memberikan definisi spesifik dan khusus terkait data pribadi yang sensitif dalam undang-undang maupun regulasi teknis dibawah undang-undang.

Dari segi organ atau institusi pengawas perlindungan data, Jerman memiliki badan terpusat terkait perlindungan data. Walau demikian, badan perlindungan data Jerman, tersebar di 16 negara bagian Jerman. Namun konteks perlindungan privasi di Jerman dapat berbeda dengan Indonesia. Terkait perlindungan data, banyak hal yang perlu dibenahi. Saat ini belum ada satu kesatuan peraturan yang secara komprehensif mengatur perlindungan data baik perlindungan data konsumen secara khusus maupun perlindungan data secara umum seperti data diri dan kependudukan.

Peraturan perlindungan data di Indonesia masih tersebar di undang-undang sektoral seperti UU ITE, UU Perbankan, UU Pasar Modal berikut Peraturan Pemerintah dan Peraturan Menteri maupun badan yang terkait langsung dengan perlindungan data seperti Otoritas Jasa Keuangan dan Bank Indonesia.

B. Saran

Berdasarkan penelitian yang kami lakukan, saran dan rekomendasi kepada pembuat kebijakan antara lain sebagai berikut:

1. Segera mengesahkan RUU Perlindungan Data yang sifatnya komprehensif.
2. Di dalam RUU tersebut seharusnya memuat pengaturan terkait data sensitif dan non-sensitif.

3. Adanya otoritas perlindungan data nasional yang sifatnya mengawasi dan menindak pelanggaran perlindungan data.

DAFTAR PUSTAKA

Buku

Alan F. Westin (Editor), 1971, *Information Technology in a Democracy*, Massachusetts: Harvard University Press,

Alan F. Westin,1984, *The Origins of Modern Claims to Privacy*, dalam buku: Philosophical Dimensions of Privacy: an Anthology (ed. Schoeman, F. D.), Cambridge: Cambridge University Press

Bambang Waluyo, 2002, *Penelitian Hukum Dalam Praktek*, Jakarta: Sinar Grafika

Bart Willem Schermer, 2007, *Software agents, surveillance, and the right to privacy: a legislative framework for agentenabled surveillance,*Leiden: Leiden University Press

Council of Europe Conference of Ministers responsible for Spatial/Regional Planning (CEMAT), 2010, *Basic text 1970-2010,Territory and landscape*.Strasbourg : Council of Europe Publishing,

Don Tapscott, 1995, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence,* New York: McGraw-Hill,

Goffman, 1959,*The Presentation of Self in Everyday Life,*New York: Doubleday

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

Jacqueline Klosek, 2000, *Data Privacy in the Information Age*, United States: Greenwood Publishing

Jogiyanto H, 2005, *AnalisisdanDesainSistemInformasi: PendekatanTerstrukturteoridanPraktikAplikasiBisnis*, Yogyakarta: Andi Offset

J. Wagner DeCew,1997, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, Ithaca: Cornell University Press

Johny Ibrahim, 2005, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia,

Olga Stepanova dan Alan Charles Raul, 2018, *Privacy, Data Protection and Cybersecurity Law Review Fifth Edition*London : Law Business Research Ltd

Sinta Dewi, 2015, *Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional,*Bandung: Refika Aditama

Soerjono Soekanto dan Sri Mamudji,2003, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat),* Jakarta: Rajawali Press

Wahyudi Djafar,dkk, 2018, *Hak Atas Penghapusan Informasi di Indonesia:Orisinalitas dan tantangan dan penerapannya,*Jakarta : LBH Pers

Jurnal

Benjamin G. Waters, "An International Right To Privacy: Israeli Intelligence Collection In The Occupied Palestinian Territories", *Georgetown Journal Of International Law,* Volume 50 2018-2019

Handrini Ardiyanti, 2018, "Big Data Di Media Sosial, Alogaritma dan Pemilu", *Jurnal Kajian Singkat Terhadap Isu Aktual dan Strategis, Pusat Penelitian Badan Keahlian DPR RI, Bidang Pemerintahan Dalam Negeri,* Vol. X, No. 09/I/Puslit/Mei/2018.

Iike Gursel," Protection of Personal Data in International of Data in International Law and The General Aspect of The Turkish Data Protection Law,*"TheRight to Data Protection of the Employee*" to be presented at the 1st International Scientific Researches Humanity and Social Sciences Conference (May 19-22, 2016, Madrid, Spain).

J Lee Riccardi, 1983, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", *Boston College International and Comparative Law Review,* Volume 6 | Issue 1, hal.24

Sinta Dewi Rosadi dan Garry Gumelar Pratama, 2018, "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia", *Jurnal Ilmu Hukum Veritas Et Justitia,* Volume 4 No. 1 Juni 2018., hlm. 91

Solove,D.J. 2001, "Privacy and Power: Computer Database and Metaphors for Information Privacy", *Stanford Law Review,* vol. 53, pp. 1393.

Internet

Data Protection Laws of The World, Full Handbook, DLA Piper, diunduh melalui https://www.finalcrypt.org/data-protection-full.pdf pada tanggal 3 November 2019

Perkara P.G. and J.H. v. the United Kingdom, application no. 44787/98, 25 September 2001., diunduh melalui https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]},pada tanggal 5 April 2019

Olisias Gultom,dkk, *Ekonomi Digital, Harapan, dan Ancaman Belajar dari Indonesia*, diunduh melalui http://igj.or.id/wp-content/uploads/2018/11/Industrial-Revolution-4_IGJ_AEPF12_Ind-1.pdf, pada tanggal 2 April 2019

Tim Peneliti Badan Penelitian dan Pengembangan SDM, Kementerian Komunikasi dan Informatika, *Studi Ekonomi Digital di Indonesia sebagai Pendorong Utama Pembentukan Industri Digital Masa Depan*, diunduh melalui https://balitbangsdm.kominfo.go.id/?mod=publikasi... pada tanggal 2 April 2019

Peraturan Perundang-undangan

Undang-undang Dasar negara Republik Indonesia Tahun 1945

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia,

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik

Charter of Fundamental Rights of The Eropean Union (2012/C 326/02)

Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik Nomor 20 Tahun 2016

Peraturan Kemenkoinfo Nomor 36 Tahun 2014 tentang Tata Cara Pendaftaran Penyelenggaraan Sistem Elektronik