JURNAL BECOSS
(Business Economic, Communication, and Social Sciences), Vol.1, No.1 September 2019: 147-154 e-ISSN: 2686-2557

PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA

Siti Yuniarti

Business Law Program, Law Department, Faculty of Humanities, Bina Nusantara University
Jakarta, Indonesia 11480
yuniarti@binus.ac.id

ABSTRACT

Attention to the protection of personal data increases with the development of technology, information and communication (ICT). Collecting, managing and storing personal data is increasingly easy to do by using the technology. These conditions are vulnerable to individual privacy. Privacy is recognized as a human right that required s a legal protection of personal data. As a legal state, Indonesia provides legal protection of human rights as stated firmly on UUD 1945. On the other hand, Indonesia is open to utilization of information and communication technology, including the internet. As consequences, Indonesia has to ensure that data protection has been covered by law. Therefore, using a normative juridical research method, this paper seeks to describe legal protection for personal data in Indonesia today. It shows that legal protection of personal data only accommodated on sectoral regulation that acquired a specific comprehensive act.

ABSTRAK

Perhatian terhadap perlindungan data pribadi meningkat dengan perkembangan teknologi, informasi dan komunikasi (TIK). Mengumpulkan, mengelola, dan menyimpan data pribadi semakin mudah dilakukan dengan menggunakan teknologi. Kondisi ini rentan terhadap privasi individu. Privasi diakui sebagai hak asasi manusia yang membutuhkan perlindungan hukum terhadap data pribadi. Sebagai negara hukum, Indonesia memberikan perlindungan hukum terhadap hak asasi manusia sebagaimana dinyatakan dengan tegas pada UUD 1945. Di sisi lain, Indonesia terbuka untuk pemanfaatan teknologi informasi dan komunikasi, termasuk internet. Sebagai konsekuensinya, Indonesia harus memastikan bahwa perlindungan data telah dilindungi oleh undang-undang. Oleh karena itu, dengan menggunakan metode penelitian yuridis normatif, makalah ini berupaya menggambarkan perlindungan hukum untuk data pribadi di Indonesia saat ini. Ini menunjukkan bahwa perlindungan hukum terhadap data pribadi baru diakomodasi pada peraturan sektoral yang memerlukan suatu undang-undang spesifik yang komprehensif.

Keyword: *Privasi, data pribadi, perlindungan hukum*

PENDAHULUAN

Perkembangan teknologi, informasi dan komunikasi memungkinkan distribusi informasi dan data secara cepat. Internet yang semula hanya untuk mempublikasikan informasi (satu arah) kemudian berubah menjadi pola yang lebih interaktif dan selanjutnya menjadi sarana untuk bertransaksi (Makarim, 2014). Pertukaran informasi menggunakan arsitektur open network memungkinkan dilakukan pertukaran melewati batas territorial negara

(cross border). Perkembangan sistem komputer dan internet membuat informasi menjadi mudah untuk dicari dan dibagi (Rosadi, 2015).

Manfaat dan nilai ekonomis data membuat kegiatan pengumpulan dan pengolahan data pribadi menjadi semakin masif. Informasi mempunyai nilai ekonomi yang tinggi karena tidak semua pihak mampu untuk memproses dari suatu data yang mentah menjadi suatu informasi sesuai kebutuhannya (Makarim, 2003) sehingga data menghasilkan keunggulan kompetitif yang esensial bagi siapapun (Djafar, 2017). Tak heran apabila data dianggap sebagai new oil (Economist, 2017). Olehkarenanya, era ekonomi industry pada abad ke-21 ini tergantung pada data (Taylor-Sakyi, 2016).

Walaupun demikian, pengumpulan dan pengolahan data rentan menimbulkan intervensi terhadap privasi. Data pribadi seseorang mudah terpapar dan dipindahtangankan secara semena-mena, tanpa kontrol dari pemilik data. Terlebih dimungkinkannya aliran data (data flow) yang melibatkan lebih dari satu yurisdiksi menjadi perhatian, terutama dalam perspektif keamanan nasional. Mempertimbangkan globalisasi dan perkembangan teknologi yang cepat, pengaturan di level nasional saja tidak cukup, namun juga memerlukan pengaturan di level internasional(Lukacs, 2017).

Pembahasan mengenai perlindungan data pribadi terus meningkat, baik di tingkat internasional, regional maupun nasional. Organisasi-organisasi internasional maupun regional menerbitkan rekomendasi yang dapat dijadikan pedoman (guideline) bagi negara-negara anggota. Rekomendasi tersebut turut berpengaruh terhadap pembentukan regulasi perlindungan data pribadi pada masing-masing negara. Diantaranya adalah The OECD Privacy Framework yang diterbitkan oleh Organization for Economic Co-Operation and Development (OECD) tahun 1980 sebagaimana telah direvisi pada tahun 2013. Dalam level regional di ASEAN diterbitkan Framework on Personal Data Protection yang disepakati dalam ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin).

Terkait dengan penggunaan data pribadi, pelaku bisnis pada sektor privat bukan merupakan satu-satunya pihak yang melakukan pengumpulan dan pengolahan data pribadi. Dalam kerangka negara hukum kesejahteraan (welfare state), negara memiliki keterlibatan dalam aspek kehidupan masyarakat. Guna peningkatan fungsi negara, negara secara langsung maupun tidak langsung melakuan aktivitas pengumpulan, pengolahan dan penyimpanan data pribadi warga negara. Melalui konsep e-government, teknologi menjadi mediator hubungan antara negara dan warga negara. Konsep smart city dalam pengelolaan wilayah urban yang memanfaatkan teknologi memunculkan isu terkait kebijakan distribusi informasi dan perlindungan hukum(Su, Li, & Fu, 2011).

Di Indonesia pelanggaran terhadap penggunaan data pribadi kerap terjadi. Pada praktik perbankan, pertukaran data pribadi dilakukan melalui sistem sharing yaitu bertukar informasi tentang data pribadi nasabah di antara sesama card center, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjualbelikan di antara bank sendiri ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjualbelikan data pribadi nasabah (Rosadi, 2017b). Dalam sektor kesehatan, data pasien diperjual belikan atau diungkap untuk keperluan asuransi, kesempatan kerja, mendapatkan program bantuan pemerintah tanpa sepengetahuan pasien (Rosadi, 2017a). Pada platform transportasi online, data telepon konsumen digunakan bukan untuk tujuan awal pengumpulan data tersebut, bahkan digunakan untuk mengancam konsumen tersebut karena penilaian buruk yang diberikan penumpang(Geistiar Yoga Pratama*, 2016) atau menganggu kenyamanan dari konsumen dalam bentuk mengirimkan pesan-pesan pribadi yang tidak ada kaitannya dengan penggunaan transportasi online (Kumparan, 2017) . Pada transaksi belanja melalui online marketplace, penggunaan teknologi cookies berpotensi memanfaatkan data pribadi diantaranya pelacakan transaksi daring dimana didalamnya terdapat preferensi belanja, lokasi belanja, data komunikasi, hingga alamat seorang konsumen (Indriyani et al., 2017).

Variasi dan jumlah pelanggaran atas data pribadi dimungkinkan meningkat di masa akan datang seiring dengan semakin meningkatnya jumlah pengguna internet di Indonesia. Pada tahun 2018, Asosiasi Penyelenggara Jasa Internet Indonesia menyebutkan jumlah pengguna internet di Indonesia tahun 2018 adalah 64,8% dari jumlah penduduk Indonesia. Jumlah tersebut mengalami peningkatan dibandingkan tahun 2017 yakni 54,68% (Asosiasi Jasa Penyelenggara Internet Indonesia, 2018). Seiring dengan pembangunan jaringan (network) oleh Pemerintah guna membuka akses lebih luas terhadap internet, jumlah pengguna internet tentunya akan semakin meningkat pada masa mendatang.

Sebagai negara hukum, Indonesia menjamin perlindungan atas hak asasi manusia dalam konstitusi negara. Merujuk pada meningkatnya penggunaan teknologi informasi dan komunikasi pada berbagai aktivitas individu memunculkan potensi meningkatnya pelanggaran data pribadi. Di latar belakangi potensi pelanggaran data pribadi di Indonesia, tulisan ini bertujuan memberikan gambaran mengenai perlindungan data pribadi dalam tataran regulasi.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan menggunakan data kualitatif. Sumber data yang digunakan merupakan data sekunder yang berasal dari bahan hukum premier yang diperoleh dari peraturan perundang-undangan terkait dengan perlindungan data pribadi di Indonesia. Bahan hukum sekunder terutama jurnal, pedoman yang diterbitkan oleh organisasi internasional digunakan untuk memberikan pemahaman mengenai konsep privasi sebagai dasar dari perlindungan data pribadi. Bahan tersier berupa index digunakan untuk memberikan gambaran mengenai penggunaan internet di Indonesia sebagai salah satu alasan urgenitas legalitas perlindungan data pribadi di Indonesia.

HASIL DAN PEMBAHASAN

Pembahasan mengenai perlindungan data pribadi tidak bisa dilepaskan dari konsep privasi. Hukum telah mengenal konsep privasi dalam kaitannya dengan gangguan secara fisik berupa trespass (memasuki pekarangan orang lain tanpa ijin) yang dikenal dalam hukum pidana. Dalam perkembangannya, hukum memberikan pula perlindungan terhadap emosional dan intelektual manusia. Samuel D. Warren dan Louis D. Brandeis (1890) mengemukan bahwa privasi merupakan pengembangan perlindungan hukum terhadap emosi manusia.

Lebih lanjut, menurut Holvast (2008), privasi identik dengan kebebasan (freedom), kontrol dan self-determination (menentukan nasib sendiri). Namun demikian, sampai dengan saat ini belum ada kesatuan pendapat mengenai makna definitif dari privasi. Solove (2002) mengemukan setidaknya ada 6 (enam) rumusan privasi, yakni: :(1) the right to be let alone (hak untuk menyendiri); (2) limited access to the self (hak untuk menutup diri dari orang lain); (3) secrecy (hak untuk menutup hal-hal tertentu dari orang lain); (4) control over the personal information (hak untuk mengendalikan informasi pribadi); (5) personhood (hak untuk melindungi kepribadian); dan (6) intimacy (hak untuk berhubungan dengan orang lain).

Dilatarbelakangi inovasi dan perkembangan model bisnis, Warren dan Brandeis menyusun tulisan dengan judul "The Right to Privacy" pada tahun 1890 yang memberikan pengaruh terhadap pembahasan mengenai konsep privasi. Merujuk pada pendapat Hakim Thomas Colley, Warren dan Brandeis (1890) mengartikan privasi sebagai right to be let alone. Setelah perang dunia kedua, konsep privasi kembali menjadi pembahasan di Amerika Serikat seiring dengan perkembangan komputer. Berbagai pembahasan dilakukan untuk merumuskan konsep privasi dan perkembangan pelanggaran privasi. Puncaknya adalah proyek The Impact of Science and Technology on Privacy yang dilaksanakan pada tahun 1962-1966 oleh Special Committee on Science and Law of the Association of the Bar of the City of New York. Hasil penelitian dituangkan dalam buku berjudul Privacy and Freedom oleh Alan Westin (Holvast, 2008).

Alan Westin memberikan pengertian privasi sebagai "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (privasi adalah klaim individu, kelompok, atau institusi untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain)"(Cate, 2000). Definisi yang dikemukakan oleh Westin disebut sebagai information privacy karena menyangkut informasi pribadi (Rosadi & Gumelar Pratama, 2018).

Konsep privasi sebagai suatu hak asasi manusia yang harus dilindungi diakui dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia (1948), yang menyatakan bahwa: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack (Tidak ada seorang pun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan surat menyuratnya, juga tidak diperkenakan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran itu)". Ketentuan tersebut selanjutnya dipertegas dalam Pasal 17 Konvenan Internasional Tentang Hak -hak Sipil dan Politik (1966), yang menyatakan bahwa: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation; (2) Everyone has the right to protection of the law against such interference or attack ((1) Tidak boleh seorangpun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya;(2) Setiap

orang berhak atas perlindungan hukum terhadap campur tangan atau serangan seperti tersebut di atas)".

Walaupun privasi menjadi bagian dari hak asasi manusia, privasi memiliki beberapa pengecualian atau dengan kata lain, privasi tidak bersifat absolut. Merujuk pada keberlakuan pedoman perlindungan data pribadi yang diterbitkan OECD, pengecualian penerapan pedoman perlindungan data pribadi tersebut dimungkinkan atas kedaulatan nasional, keamanan nasional, dan kebijakan publik sepanjang dilakukan sesedikit mungkin dan harus diketahui oleh publik (OECD, 2013). Pembatasan privasi juga diberikan oleh Warren dan Brandeis mengungkapkan bahwa privasi tidak bersifat absolut, akan tetapi ada batasnya, yaitu: (1) tidak menutup kemungkinan untuk mempublikasikan informasi pribadi seseorang untuk kepentingan publik; (2) tidak ada perlindungan privasi apabila tidak ada kerugian yang diderita; (3) tidak ada privasi apabila orang yang bersangkutan telah menyatakan persetujuan bahwa informasi pribadinya akan disebarkan kepada umum; (4) persetujuan dan privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Karena menyangkut mental seseorang maka kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik karena telah menganggu kehidupan pribadi (Warren Samuel D, 1890).

Lebih lanjut, menurut General Assembly United Nation dalam The Right of Privacy in the Digital Age mengakui bahwa perkembangan teknologi komunikasi membuat orang dapat terkoneksi ke seluruh dunia, namun di sisi lain perkembangan tersebut juga meningkatkan kemampuan pemerintah, perusahaan-perusahaan dan individu-indivu untuk melakukan pengawasan (surveillance), penyadapan dan pengumpulan data yang berpotensi mengancam hak asasi manusia. Olehkarenanya, diperlukan perlindungan privasi baik terhadap aktivitas secara online maupun offline (UN, 2016).

Secara harfiah, data merupakan bentuk jamak dari kata "datum" yang dalam Bahasa Latin bermakna sebagai bagian dari informasi. Dalam Knowledge Hierarchy yang disusun oleh Russell L.Ackoff (1919-2009), data didefinisikan sebagai symbols that are properties of observables (simbol yang dimiliki oleh obyek yang diamati), sedangkan informasi didefinisikan sebagai deskripsi. Perbedaan diantara keduanya bersifat fungsional yang mana informasi disimpulkan dari data (Dammann, 2018).

Gambar 1. *Knowledge Hierarchy*

Dalam konteks perlindungan data pribadi, terminologi yang kerap digunakan adalah "informasi pribadi" dan "data pribadi". Amerika Serikat menggunakan istilah informasi pribadi (personally identifiable information), sedangkan Eropa menggunakan istilah data pribadi (personal data). Dalam regulasi yang ada di Indonesia saat ini, terminologi yang digunakan adalah data pribadi.

Data pribadi atau personal data diartikan sebagai "any information relating to an identified or identifiable individual (data subject)"(setiap informasi yang mengidentifikasikan atau dapat mengindentifikasikan individu (subyek data) (OECD, 2013). General Data Protection Regulation (GDPR) menjabarkan secara spesifik lingkup dari data pribadi, yakni diantaranya nama, nomor identitas, data lokasi, online identifier, atau satu atau lebih komponen spesifik terkait fisik, physiological, genetik, mental, ekonomi, budaya atau sosial dari seseorang. Lebih lanjut, termasuk dalam lingkup data yang mengindentifikasikan diri pribadi dalam GDPR adalah data yang tidak diketahui (pseudonymization) namun dengan menggunakan informasi tambahan, mampu mengindentifikasikan seseorang(GDPR, 2016).

Batasan mengenai informasi yang termasuk dalam informasi pribadi (personal information) dan bukan informasi pribadi (no- personal information) dikemukan oleh Jerry Kang. Diklasifikasikan sebagai personal information adalah informasi yang dapat mengidentifikasikan seseorang melalui 3 (tiga) cara, yakni dapat menunjukan (1) hubungan kepemilikan (authorship) dengan individu; (2) mendeskripsikan ciri-ciri individu yang permanen; atau (3) informasi yang dapat dijadikan instrumen untuk mendeskripsikan seseorang(Kang, 2006). Adapun dimaksud dengan non-personal information adalah apabila informasi tersebut bukan merupakan data terkait

dengan privasi individu, yakni informasi yang bukan mengenai seseorang, informasi mengenai seseorang tetapi bersifat anonimus sehingga tidak dapat merujuk pada individu tertentu, informasi merujuk secara langsung pada kelompok dan tidak secara langsung merujuk pada individu yang merupakan bagian dari kelompok (Kang, 2006).

Dalam pembahasan mengenai perlindungan data pribadi dikenal pula pengelompokan berdasarkan sensitifitas data atau disebut data sensitif. Klasifikasi data sensitif dapat berbeda-beda di setiap negara. Secara khusus, GDPR memberikan perlindungan khusus terhadap beberapa jenis data pribadi yang dianggap sensitif berupa informasi terkait etnis, pilihan politik, agama atau kepercayaan atau keanggotaan pada organisasi perdagangan, data biometrik untuk tujuan mengidentifikasi seseorang, data kesehatan atau kehidupan sex atau orientasi sexual. Terhadap data sensitif tersebut dilarang untuk diproses kecuali memenuhi serangkaian persyaratan yang dicantumkan secara eksplisit dalam GDPR, antara lain persetujuan tertulis dari pemilik data dan pengumpulan data dibatasi hanya pada tujuan-tujuan yang telah tercantum secara definitif dalam GDPR (GDPR, 2016).

Walaupun pengaturan perlindungan data pribadi pada setiap negara dapat berbeda, pada umumnya pengaturan merujuk pada prinsip-prinsip perlindungan data yang serupa. Pada umumnya rezim perlindungan data terinsipirasi dari OECD tahun 1980 tentang Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data yang menerapkan prinsip-prinsip pertama privasi yang diakui secara internasional(OECD, 2013). Berikut adalah prinsip perlindungan data pribadi menurut OECD (OECD, 2013):

Tabel 1. Prinsip Perlindungan Data

Prinsip	Penjelasan
Prinsip Pembatasan Pengumpulan *Collection Limitation Principle*	Harus ada batasan untuk pengumpulan data pribadi dan data semacam itu harus diperoleh dengan cara yang sah dan adil dan dengan sepengetahuan atau persetujuan dari subjek data.
Prinsip Kualitas Data *Data Quality Principle*	Data pribadi harus relevan dengan tujuan penggunaannya, dan sejauh yang diperlukan untuk tujuan tersebut, harus akurat, lengkap, dan terus diperbarui.
Prinsip Spesifikasi Tujuan *Purpose Specification Principle*	Tujuan pengumpulan data pribadi harus ditentukan selambat-lambatnya pada saat pengumpulan data dan penggunaan selanjutnya terbatas pada pemenuhan tujuan tersebut atau tujuan lainnya yang tidak sesuai dan ditentukan untuk setiap perubahan tujuan.
Prinsip Pembatasan Penggunaan *Use Limitation Principle*	Data pribadi tidak boleh diungkapkan, tersedia atau digunakan untuk tujuan selain yang ditentukan kecuali: (a) dengan persetujuan subjek data; atau (b) oleh otoritas hukum.
Prinsip Perlindungan Keamanan *Security Safeguards Principle*	Data pribadi harus dilindungi oleh perlindungan keamanan yang wajar terhadap risiko seperti kehilangan atau akses tidak sah, perusakan, penggunaan, modifikasi atau pengungkapan data.
Prinsip Keterbukaan *Openness Principle*	Adanya kebijakan keterbukaan tentang perkembangan, praktik, dan *policy* berkenaan dengan data pribadi. Sarana tersebut harus tersedia untuk menetapkan keberadaan dan sifat data pribadi, dan tujuan utama penggunaannya, serta identitas dan lokasi pengontrol data (*data controller*).
Prinsip Partisipasi Individu *Individual Participation Principle*	Individu berhak: a. untuk memperoleh dari pengontrol data (*data controller*), atau konfirmasi, apakah pengontrol data memiliki data terkait atau tidak; b. untuk berkomunikasi dengan mereka, data yang berkaitan dengan mereka: (i) dalam waktu yang wajar;(ii) dengan biaya, jika ada;(iii) alasan yang cukup; dan (iv) diberikan dalam bentuk yang dapat dipahami. c. Diberikan alasan jika permintaan dibuat berdasarkan huruf (a) dan (b) di tolak, dan dapat diargumentasikan penolakan tersebut; d. Untuk melawan data terkait mereka, dan seandainya perlawanan tersebut benar, untuk menghapus data, memperbaiki, melengkapi atau mengubah.
Prinsip Akuntabilitas *Accountability Principle*	Pengontrol data (*data controller*) harus bertanggung jawab untuk mematuhi langkah-langkah yang berdampak pada prinsip-prinsip yang disebutkan di atas.

Dalam hal perlindungan data pribadi, dikenal dua metode untuk melindungi suatu data pribadi, yakni pengamanan terhadap fisik data pribadi itu sendiri dan melalui regulasi yang bertujuan untuk memberi jaminan privasi terhadap penggunaan data pribadi tersebut (Djafar Wahyudi, Sumigar Bernhard Ruben Fritz, 2016). Dalam tataran regulasi, saat ini setidaknya 107 negara telah memiliki undang-undang perlindungan data pribadi (UNCTAD, 2019).

J.B.J.M ten Berge menyebutkan bahwa salah satu prinsip negara hukum adalah perlindungan terhadap hak asasi (Ridwan, 2011). Arief Shidarta merumuskan salah satu unsur dari negara hukum adalah pengakuan, penghormatan, dan perlindungan Hak Asasi Manusia yang berakar dalam penghormatan atas martabat manusia (human dignity) (Kusniati Retno, 2011). Sebagai negara hukum, Indonesia meletakan perlindungan hak asasi manusia dalam konstitusi, melalui penambahan Bab XA Hak Asasi Manusia pada Perubahan Kedua UUD 1945. Ketentuan dalam Pasal 28 huruf G UUD 1945 yang berbunyi sebagai berikut: " Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaanya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi", dianggap sebagai dasar konstitusional perlunya perlindungan data pribadi. Menurut Sinta Dewi Rosadi bahwa Pasal 28 huruf G tersebut tidak secara eksplisit menyebut mengeni privasi dan perlindungan data privasi (Rosadi, 2015).

Terkait dengan perlindungan data pribadi, Indonesia belum memiliki aturan khusus mengenai perlindungan data pribadi pada level undang-undang. Walaupun demikian, berdasarkan penelitian yang dilakukan oleh Lembaga Studi dan Advokasi Masyarakat (ELSAM) setidaknya terdapat 30 (tiga puluh) ketentuan perundang-undangan yang mengatur mengenai kewajiban untuk memberikan perlindungan data pribadi di Indonesia(Djafar Wahyudi, Sumigar Bernhard Ruben Fritz, 2016). Undang-undang Administrasi Kependudukan merupakan salah satu ketentuan yang telah mengatur secara lebih spesifik mengenai klasifikasi data pribadi. Semula lingkup data pribadi menurut Undang-Undang No.23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dalam Undang-Undang No. 24 Tahun 2013 (UU Administrasi Kependudukan) adalah: (a) Nomor Kartu Keluarga; (b) Nomor Induk Kependudukan; (c) tanggal/bulan/tahun/lahir;(d) keterangan tentang kecacatan fisik dan/atau mental; (e) Nomor Induk Kependudukan Ibu kandung; (f) Nomor Induk Kependudukan ayah; dan (g) beberapa isi catatan peristiwa penting. Lebih lanjut, UU Administrasi Kependudukan mengubah lingkup data pribadi menjadi: (a) keterangan tentang cacat fisik dan/atau mental; (b) sidik jari; (c) iris mata; (d) tanda tangan; dan (e) elemen data lainnya yang merupakan aib seseorang. Namun demikian, UU Administrasi Kependudukan hanya sebatas mengatur mengenai Dengan kata lain, UU Administrasi Kependudukan tidak mengatur secara detail mengenai perolehan, pemrosesan dan penyimpanan data pribadi.

Regulasi yang secara lebih spesifik meletakan hak pemilik data adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam Undang-Undang No. 19 Tahun 2016 (UU ITE). UU ITE memberikan landasan perlindungan data pribadi yang diperoleh dengan menggunakan sistem elektronik sebagaimana dinyatakan dalam Pasal 26 UU ITE. Persetujuan pemilik data merupakan kata kunci dalam penggunaan data pribadi seseorang sebagaimana dinyatakan dalam Pasal 26 ayat (1) UU ITE yang mana pelanggaran terhadap hal tersebut menyebabkan timbulnya hak hukum keperdataan bagi pihak yang digunakan datanya untuk mengajukan gugatan sebagaimana dinyatakan dalam Pasal 26 ayat (2) UU ITE. UU ITE mengakomodir pula konsep right to be forgotten melalui ketentuan dalam Pasal 26 ayat (3) yang memberikan hak kepada pemilik data untuk meminta penghapusan data pribadi yang tidak relevan kepada penyelenggara sistem elektronik.

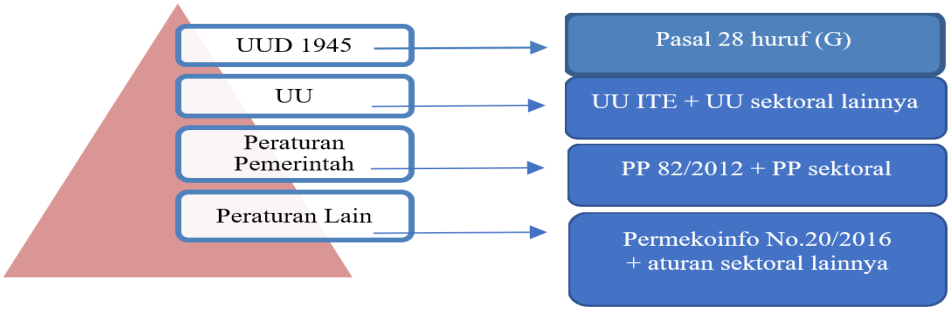
Walaupun UU ITE mengatur mengenai data pribadi, namun UU ITE tidak memberikan definisi dari data pribadi itu sendiri. Terminologi data pribadi diberikan dalam peraturan di bawah undang-undang di antaranya Peraturan Pemerintah No. 18 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 18/2012), Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkoinfo 20/2016). Termasuk pula aturan pelaksanaan yang bersifat sektoral seperti Surat Edaran OJK No.014/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Pribadi Konsumen (SEOJK 014/2014).

Tabel 2. Pengertian Data Pribadi

PP 18/2012 Permenkoinfo 20/2016	SEOJK No.014/2014
Data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya	Data dan/atau Informasi Pribadi Konsumen adalah data dan/atau informasi yang mencakup sebagai berikut: a. Perorangan: nama, alamat, tanggal lahir dan/ atau umur, nomor telepon dan/atau nama ibu kandung. b. Korporasi:nama, alamat, nomor telephon, susunan direksi dan komisaris termasuk dokumen identitas berupa KTP/paspor/ijin tinggal; dan/atau susunan pemegang saham

Sebagai salah satu aturan pelaksana yang diamanatkan dalam UU ITE, PP No.82/2012 membebankan tanggung jawab kepada penyelenggara sistem elektronik untuk menjaga keutuhan data pribadi serta mensyaratkan persetujuan pemilik data terhadap setiap perolehan, penggunaan, pemanfaatan dan pengungkapan data pribadi. Namun demikian, PP No.82/2012 tidak merefleksikan prinsip-prinsip dasar perlindungan data pribadi secara lebih detail. Asas-asas perlindungan data pribadi dan pengaturan lebih komprehensif muncul pada level regulasi yang lebih rendah, yakni Permenkoinfo No. 20/2016. Lingkup perlindungan data pribadi dalam sistem elektronik dalam Permenkoninfo No.20/2016 mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Perlindungan data pribadi juga diatur pada peraturan pelaksana yang bersifat sektoral seperti perlindungan data pribadi bagi konsumen yang diatur dalam peraturan Bank Indonesia dan Otoritas Jasa Keuangan. Dengan demikian, pengaturan perlindungan data pribadi di Indonesia saat ini masih bersifat sektoral.

Berikut adalah regulasi perlindungan data pribadi di Indonesia saat ini yang disusun dengan menggunakan hirarki perundang-undangan dalam Undang-Undang No. 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan:



Gambar 2. Regulasi Perlindungan Data Pribadi Indonesia

KESIMPULAN

Indonesia mengakui bahwa perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi manusia. Pengakuan tersebut terefleksi, baik dalam konstitusi maupun beragam peraturan selevel undang- undang. Namun demikian, peraturan yang khusus mengatur mengenai perlindungan data pribadi pada level undang-undang belum dimiliki. Untuk mengisi kekosongan hukum, pengaturan detail mengenai perlindungan data pribadi diakomodir dalam peraturan pada level peraturan menteri maupun peraturan teknis sektoral. Dengan demikian, dapat disimpulkan bahwa regulasi perlindungan data pribadi di Indonesia masih bersifat sektoral. Kebutuhan pengaturan perlindungan data pribadi pada level undang-undang dibutuhkan karena perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi warga negara.

DAFTAR PUSTAKA

Asosiasi Jasa Penyelenggara Internet Indonesia, A. (2018). Laporan Survei Penetrasi & Profil Perilaku Pengguna Internet Indonesia. APJI.

Cate, F. H. (2000). Principles of Internet Privacy. Connecticut Law Review, 32(3), 877–896.

Dammann, O. (2018). Data, Information, Evidence, and Knowledge: A Proposal for Health Informatics and Data Science. Online Journal of Public Health Informatics, 10(3). https://doi.org/10.5210/ojphi.v10i3.9631

Djafar, W. (2017). Big data dan pengumpulan data skala besar di Indonesia:Pengantar untuk memahami tantangan aktual perlindungan hak atas privasi (Internet dan Hak Asasi Manusia). Jakarta.

Djafar Wahyudi, Sumigar Bernhard Ruben Fritz, S. B. L. (2016). Protection of personal data in Indonesia. Jakarta. Retrieved from http://weekly.cnbnews.com/news/article.html?no=124000

Economist, T. (2017). The worlds most valuable resource is no longer oil but data. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

GDPR. Directive 95/46/EC General Data Protection Regulation (2016).

Geistiar Yoga Pratama*, S. A. (2016). Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, 5(3), 1–19.

Holvast, J. (2008). History of Privacy *. In The Future of Identity in the information society (pp. 13–42). IFIP Advances in Information and Communication Technology.

Indriyani, M., Andaria, N., Sari, K., P, S. U. W., Hukum, F., Airlangga, U., & Surabaya, K. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. Justitia Jurnal Hukum, 1(2), 191–208.

Kang, J. (2006). Information Privacy in Cyberspace Transactions. Stanford Law Review, 50(4), 1193–1293. https://doi.org/10.2307/1229286

Kumparan. (2017). Kisah “Teror Cinta” Driver Ojek Online pada Sang Penumpang. Kumparan. Retrieved from https://kumparan.com/@kumparannews/kisah-teror-cinta-driver-ojek-online-pada-sang-penumpang

Kusniati Retno. (2011). Sejarah Perlindungan Hak Hak Asasi Manusia Dalam Kaitannya Dengan Konsepsi Negara Hukum. Inovatif Jurnal Hukum, 4(5), 79–91. https://doi.org/10.1093/oxfordhb/9780199578610.013.0012

Lukacs, A. (2017). What Is Privacy? The history and definition of privacy. University of Szeged, 256–265. https://doi.org/3188699

Makarim, E. (2003). Kompilasi hukum telematika. Jakarta: Raja Grafindo Perkasa.

Makarim, E. (2014). KERANGKA KEBIJAKAN DAN REFORMASI HUKUM UNTUK KELANCARAN PERDAGANGAN SECARA ELEKTRONIK (E-COMMERCE) DI INDONESIA. Jurnal Hukum & Pembangunan. https://doi.org/10.21143/jhp.vol44.no3.25

OECD. (2013). The OECD Privacy Framework. https://doi.org/10.1787/5kgf09z90c31-en

Ridwan, H. (2011). Hukum Administrasi Negara. Jakarta: Raja Grafindo Perkasa.

Rosadi, S. D. (2015). Cyber Law-Aspek Data Privasi Menurut Hukum Internasional,Regional dan Nasional. Refika Aditama.

Rosadi, S. D. (2017a). Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi. Arena Hukum, 9(3), 403–420. https://doi.org/10.21776/ub.arenahukum.2016.00903.6

Rosadi, S. D. (2017b). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya, 19(3), 206–212.

Rosadi, S. D., & Gumelar Pratama, G. (2018). Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia. Brawijaya Law Journal, 5(2), 143–157. https://doi.org/10.21776/ub.blj.2018.005.01.09

Solove, D. J. (2002). Conceptualizing Privacy. California Law Review, 90(4), 1087–1156. https://doi.org/10.15779/Z382H8Q

Su, K., Li, J., & Fu, H. (2011). Smart city and the applications. 2011 International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings, 1028–1031. https://doi.org/10.1109/ICECC.2011.6066743

Taylor-Sakyi, K. (2016). Big Data:Understanding big data. Research Gate, 1–9.

UN. (2016). The right to privacy in the digital age. United Nations. https://doi.org/10.1017/S0020818300024796

UNCTAD. (2019). Data Protection and Privacy Legislation Worldwide. Retrieved from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Warren Samuel D, L. D. B. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. Retrieved from https://www.jstor.org/stable/1321160