DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, menyebutkan Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, tujuan bernegara tersebut diwujudkan dalam bentuk pelindungan data pribadi dari setiap penduduk atau warga negara Indonesia.

Sebagai suatu bentuk inovasi, teknologi informasi dan komunikasi sekarang telah mampu melakukan pengumpulan, penyimpanan, pembagian dan penganalisaan data. Aktivitas tersebut telah mengakibatkan berbagai sektor kehidupan memanfaatkan sistem teknologi informasi dan komunikasi, seperti penyelenggaraan *electronic commerce (e-commerce)* dalam sektor perdagangan/bisnis, *electronic education (e-education)* dalam bidang pendidikan, *electronic health* (*e-health)* dalam bidang kesehatan, *electronic government (e-government)* dalam bidang pemerintahan, *search engines*, *social networks*, *smartphone* dan *mobile internet* serta perkembangan industri komputasi awan atau *cloud computing.*[1]

[1] Komputasi awan adalah gabungan pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan). Saat ini, beberapa perusahaan teknologi informasi dan komunikasi terkemuka mengeluarkan aplikasi dalam menyediakan ruang penyimpanan data pengguna seperti Evernote, Dropbox, Google Drive, Sky Drive, Youtube, Scribd, iCloud, dan lain sebagainya.

Isu mengenai pentingnya pelindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.

Pelindungan data pribadi berhubungan dengan konsep privasi.[2] Konsep privasi sendiri adalah gagasan untuk menjaga integritas dan martabat pribadi.[3] Hak privasi juga merupakan kemampuan individu untuk menentukan siapa yang memegang informasi tentang mereka dan bagaimana informasi tersebut digunakan.[4]

Konsep pelindungan data mengisyaratkan bahwa individu memiliki hak untuk menentukan apakah mereka akan membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Lebih jauh, pelindungan data juga berhubungan dengan konsep hak privasi. Hak privasi telah berkembang sehingga dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.[5]

Hak privasi melalui pelindungan data merupakan elemen kunci bagi kebebasan dan harga diri individu. Pelindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual,

---

2 Kamus Besar Bahasa Indonesia memberikan pengertian privasi berarti kebebasan dan keleluasaan diri, Kamus Besar Bahasa Indonesia, Edisi 3, Departemen Pendidikan Nasional dan PT. Balai Pustaka, Jakarta 2001.

3 Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*, Elsam, Jakarta, 2014, hlm. 2

4 Lord Ester dan D, Pannick (ed.) dalam *ibid,* hlm. 6.

5 *Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (art. 17) seperti yang dikutip dalam Privacy International Report, 2013, hlm. 1-2.

keagamaan bahkan kegiatan yang bersifat privat. Hak untuk menentukan nasib sendiri, kebebasan berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.

Pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi.[6] Data pribadi merupakan suatu aset atau komoditi bernilai ekonomi tinggi.[7] Selain itu, terdapat suatu hubungan korelatif antara tingkat kepercayaan dengan pelindungan atas data tertentu dari kehidupan pribadi. Sayangnya, pelindungan terhadap data pribadi saat ini belum diatur dalam undang-undang tersendiri melainkan masih tersebar di berbagai peraturan perundang-undangan, misalnya Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya.

Ketentuan hukum terkait pelindungan data pribadi masih bersifat parsial dan sektoral, tampaknya belum bisa memberikan perlindungan yang optimal dan efektif terhadap data pribadi, sebagai bagian dari privasi.

Potensi pelanggaran hak privasi atas data pribadi tidak saja ada dalam kegiatan *on-line* tetapi juga kegiatan *off-line.* Potensi pelanggaran privasi atas data pribadi secara *on-line* misalnya terjadi

---

6 *Human Rights Committee General Comment* No. 16 (1988), *Op. Cit.*

7 Edmon Makarim, *Kompilasi Hukum Telematika,* PT. Raja Grafindo Perkasa, Jakarta 2003, hlm. 3. Lihat juga M. Arsyad Sanusi, *Teknologi Informasi & Hukum E-commerce,* PT. Dian Ariesta, Jakarta, 2004, hlm. 9. Menurut Branscomb, *Information is the Lifeblood that sustain political, social and business decision,* dalam Anne W. Branscomb, Global Governance of Global Networks: "A survey of Transborder Data Flows in Transition", *Vanderbilt Law Review,* Vol. 36, 1983, hlm. 985.

dalam kegiatan pengumpulan data pribadi secara masal (*digital dossier),* pemasaran langsung (*direct selling),* media sosial, pelaksanaan program e-KTP, pelaksanaan program *e-health* dan kegiatan komputasi awan (*cloud computing*). Khususnya di era *big data*[8], pengumpulan data secara masif lazim dilakukan, tak hanya oleh pemerintah, namun juga oleh entitas bisnis atau korporasi. Jenis data yang dikumpulkan pun beragam, mulai dari *personally identifiable information* (PII) hingga *sensitive personal information* (SPI). Perusahaan sebagai pengendali data memiliki tanggung jawab untuk menjaga data konsumen dari kebocoran data. Bocornya data pribadi konsumen merupakan sebuah bentuk pelanggaran terhadap hak atas privasi. Oleh karenanya, diperlukan peraturan hukum yang komprehensif guna melindungi data pribadi konsumen yang dikumpulkan oleh korporasi.[9] Dalam beberapa tahun terakhir secara global telah terjadi banyak kasus kebocoran data pribadi yang berimbas kepada Indonesia contohnya kasus Yahoo tahun 2014 ketika dalam proses penjualan kepemilikan pada Verizon menyatakan telah mengalami kebocoran 500 juta data pelanggan dan Yahoo menderita kerugian dengan menurunnya asset penjualan hingga 350 juta dolar [10]. Kasus lainnya kasus Equifax pada tahun 2017 dimana terjadi kebocoran data pribadi 143 juta pelanggan dan pada tahun 2018 kasus yang paling menhebohkan dunia adalah kasus Facebook dan Cambridge Analytica ketika sekitar 87 juta data pribadi

[8] Istilah *Big Data* dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik terdapat istilah *Big Data Analitics* yang diartikan sebagai teknologi analisis terhadap data yang berukuran sangat besar, tidak terstruktur, dan tidak diketahui pola, korelasi ataupun relasi antar data.

[9] http://elsam.or.id/category/publikasi/asasi/

[10] https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

pengguna Facebook dibagikan kepada pihak ketiga tanpa sepengetahuan pemilik data.[11]

Selanjutnya potensi pelanggaran pelindungan data pribadi dalam berbagai kegiatan di atas akan diuraikan satu per satu:

Digital dossier yang merupakan suatu pengumpulan data pribadi seseorang dalam jumlah banyak dengan menggunakan teknologi digital telah dimulai sejak tahun 1970 oleh pemerintah terutama di negara-negara Eropa dan Amerika Serikat. Kini, pihak swasta juga menjadi pelaku *digital dossier* dengan menggunakan teknologi internet.[12] Praktik *digital dossier* yang dilakukan oleh pihak swasta tersebut sangat berpotensi melanggar hak privasi seseorang atas data pribadinya.

Selain *digital dossier*, terdapat juga praktik *direct selling* yaitu praktik yang dilakukan para penjual untuk memasarkan barang dengan cara pemasaran langsung. Dengan berkembangnya cara pemasaran tersebut maka telah berkembang industri bank data yang khusus mengumpulkan informasi konsumen. Sampai saat ini, tercatat lebih dari 550 perusahaan pengumpul data atau kini disebut dengan bank data (*database*) yang memperjualbelikan informasi konsumen. Perusahaan yang melakukan transaksi melalui internet akan mendapatkan informasi konsumen dengan membeli informasi tersebut dari jasa perusahaan pengumpul data ini.

[11] https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

[12] Daniel J. Solove, *The Digital Person, Technology and Privacy in the Information Age,* West Group Publication, New York University Press, New York, 2004, hlm. 13-17.

Nilai transaksi penjualan data pribadi konsumen pada tahun 2006 secara global telah mencapai 3 miliar dolar Amerika.[13] Pertumbuhan industri bank data tersebut demikian pesat sehingga telah melahirkan perusahaan-perusahaan bank data yang secara global telah menempatkan mereka menjadi perusahaan-perusahaan yang memiliki pendapatan besar. Dengan demikian, informasi pribadi pelanggan telah menjadi aset yang sangat berharga bagi perusahaan-perusahaan tersebut di atas.[14] Akibatnya, berbagai cara digunakan untuk mengumpulkan data pribadi sebanyak-banyaknya dengan cara yang sering kali tidak menghargai hak privasi seseorang.

Praktik pemasaran langsung di Indonesia telah banyak terjadi terutama dalam industri keuangan, khususnya dalam pemrosesan data kartu kredit. Dalam praktik, informasi pribadi konsumen telah diperjualbelikan melalui agen-agen tanpa meminta izin terlebih dahulu dari pemilik informasi.[15] Kasus yang banyak terjadi di Indonesia adalah jual beli data konsumen. Konsumen yang datanya berhasil diperoleh menjadi target pemasaran suatu produk perusahaan atau perseorangan. Tidak sedikit pula pengguna internet menawarkan jasa jual-beli akun atau pengikut. Padahal praktik tersebut membuka ruang terjadinya penyalahgunaan data seseorang untuk melakukan kejahatan. Kasus terbaru yaitu penipuan dan penggelapan kartu kredit nasabah dengan tersangka Imam Zahali (IZ), yang menyebabkan kerugikan pihak bank sekitar Rp 250 juta setelah menggunakan kartu kredit nasabah untuk

---

[13] Marcy E.Peek, *Information Privacy and Corporate Power: Toward a Re-Imagination of Information Privacy Law, Seton Hall Law Review,* Vol 37, 2006, hlm. 6-7.

[14] Tal Z. Zarsky,*Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall solutions to the Problems of Information Privacy in the Internet Society*, University Miami Law Review, Vol 58, 2004, hlm. 991.

[15] http://rahard.worldpress.com/2009, diakses pada tanggal 30 Maret 2009.

transaksi gesek tunai. Hasil kejahatan itu kemudian digunakan untuk kepentingan dirinya, salah satunya menunaikan ibadah haji di Tanah Suci Mekah. Pelaku mendapatkan data nasabah dengan cara membelinya di internet sebesar Rp 800 ribu untuk 25 data. Dari data tersebut, pelaku kemudian menghubungi korban dengan mengaku sebagai sales kartu kredit dan menawarkan untuk menaikkan limit kartu kredit.[16]

Bentuk lain dari diabaikannya perlindungan terhadap privasi adalah munculnya sebuah pesan berisi iklan yang biasa disebut *Location-Based Messaging*. Pesan tersebut akan terkirim otomatis kepada seseorang jika ia berada di tempat tertentu. Padahal, belum tentu ia pernah menyetujui suatu perjanjian dengan sang provider dan memperbolehkan mereka merekam setiap aktivitasnya.[17]

Salah satu tujuan utama regulasi pelindungan data pribadi adalah melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. Berdasarkan kasus yang terjadi di Eropa yaitu Maximillian Schrems v. *Data Protection Commissioner* yang diputus *Court of Justice of the European Union,* 2015, perbedaan perlindungan kepentingan konsumen dapat mengancam transaksi antar dua negara atau dua regional.

Dari kasus tersebut terlihat bahwa terdapat kepentingan untuk memberikan pelindungan data pribadi yang setara dengan negara-negara lain. Pengaturan yang akan disusun dalam Rancangan Undang-Undang (RUU) diharapkan akan menempatkan Indonesia sejajar dengan negara-negara maju yang telah menerapkan hukum mengenai pelindungan data pribadi. Hal ini akan lebih mendorong dan memperkuat posisi Indonesia sebagai

[16] http://news.detik.com/berita/3158671/duh-sales-kartu-kredit-gadungan-ini-gunakan-uang- haram-buat-naik-haji, diakses pada tanggal 5 April 2016.
[17] http://aitinesia.com/3-contoh-pelanggaran-privasi-yang-terjadi-di- internet diakses pada tanggal 4 April 2016.

pusat bisnis terpercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia.

Selain itu pengaturan mengenai pelindungan data pribadi akan meminimalisasi ancaman penyalahgunaan data pribadi di industri perbankan, situs pertemanan *online* (misalnya Facebook, Twitter), program KTP elektronik (e-KTP), *e-health*. Potensi terjadinya kejahatan yang bermula dari pencarian data pribadi seseorang, penghilangan identitas atas data dari pelaku kejahatan, *search* mesin pencari (misal google.com dan bing.com), dan *cloud computing.* Dengan mempertimbangkan semua ancaman dan potensi pelanggaran di atas, pengaturan pelindungan data pribadi dimaksudkan untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia.

Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai pelindungan data pribadi. Berbagai macam permasalahan di atas menuntut pemerintah Indonesia untuk melindungi masyarakat dan mengatur masalah perlindungan atas data pribadi dan menyiapkan berbagai bentuk perlindungan hukum. Selain itu, dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang 2005-2025 juga telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus meningkatkan pemanfaatan ilmu pengetahuan dan teknologi. Salah satunya melalui peraturan yang terkait dengan privasi.[18]

B. Identifikasi Masalah

1. Permasalahan apa yang dihadapi bangsa Indonesia dengan belum terlindunginya data pribadi dalam kehidupan

[18] Rencana Pembangunan Jangka Panjang 2005-2025, hlm. 108.

bermasyarakat, berbangsa dan bernegara dan bagaimana permasalahan tersebut dapat diatasi?

2. Mengapa perlu rancangan undang-undang sebagai dasar pemecahan masalah tersebut, yang berarti membenarkan pelibatan negara dalam penyelesaian masalah tersebut?
3. Apa yang menjadi pertimbangan atau landasan filosofis, sosiologis, yuridis pembentukan RUU tentang Pelindungan Data Pribadi?
4. Apa sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan dalam pengaturan pelindungan hukum atas data pribadi?

C. Tujuan dan Kegunaan Penyusunan Naskah Akademik

1. Tujuan

a. Merumuskan permasalahan yang dihadapi bangsa Indonesia dalam kehidupan bermasyarakat, berbangsa dan bernegara terkait dengan pelindungan data pribadi serta cara mengatasi permasalahan tersebut.
b. Merumuskan permasalahan hukum yang dihadapi sebagai dasar pembentukan Rancangan Undang-Undang sebagai dasar hukum penyelesaian atau solusi permasalahan hukum dalam kehidupan bermasyarakat, berbangsa dan bernegara.
c. Merumuskan pertimbangan atau landasan filosofis, sosiologis, yuridis pembentukan RUU Pelindungan Data Pribadi.
d. Merumuskan sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan dalam RUU Pelindungan Data Pribadi.

2. Kegunaan

Kegunaan penyusunan naskah akademik adalah sebagai acuan atau referensi penyusunan dan pembahasan RUU tentang Pelindungan Data Pribadi.

D. Metode

Penyusunan naskah akademik pada dasarnya merupakan suatu kegiatan penelitian, sehingga digunakan metode penyusunan naskah akademik yang berbasiskan metode penelitian.

Dengan berbasis pada metode penelitian hukum, maka penyusunan naskah akademik RUU tentang Pelindungan Data Pribadi ini menggunakan metode yuridis normatif. Adapun langkah-langkah yang dilakukan adalah melalui studi kepustakaan *(library research)* yang menelaah (terutama) data sekunder berupa bahan hukum primer dan bahan hukum sekunder.

Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11

Tahun 2008 tentang Informasi dan Transaksi Elektronik dan perjanjian internasional yang telah disahkan serta berbagai peraturan perundang-undangan terkait lainnya.

Bahan hukum sekunder diperoleh melalui pengkajian hasil-hasil penelitian, buku-buku, jurnal ilmiah, dan yurispridensi, serta bahan pustaka lainnya yang membahas mengenai pelindungan atas data pribadi. Untuk mendapatkan pemahaman yang lebih komprehensif, dilakukan juga studi komparatif terhadap data sekunder yang berkaitan dengan pengaturan pelindungan atas data pribadi di negara-negara lain seperti Hongkong, Korea Selatan, Malaysia, dan Singapura.

Selain metode perbandingan hukum, metode hukum yang akan datang (*legal futuristic method*).[19] juga dipilih dalam penyusunan naskah akademik ini. Hal tersebut dimaksudkan untuk dapat menemukan hukum apa yang sebaiknya diciptakan untuk masa yang akan datang.

Data sekunder tersebut di atas dilengkapi dengan data primer yang diperoleh melalui pengamatan, wawancara, *focus group discussion,* dengar pendapat para ahli, diskusi publik dengan menghadirkan narasumber yang berkompeten dan penyebaran kuesioner. Hal ini ditempuh untuk mendapatkan masukan guna memenuhi persyaratan formal dan ideal penyusunan undang-undang sebagaimana disyaratkan Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan sebagaimana diubah dengan Undang-Undang Nomor 15 Tahun 2019, dan menampung kebutuhan riil masyarakat sebagaimana diharapkan.

[19] Menurut Sunaryati Hartono, Metode penelitian *futuristic* adalah metode penelitian mengenai hukum yang seyogjanya diciptakan untuk masa yang akan datang misalnya untuk menyusun suatu naskah akademik, seperti yang dikutip dalam Sunaryati Hartono, *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20*, Penerbit Alumni, Bandung, 1994, hlm. 146.

Adapun untuk menganalisis data sekunder digunakan metode kualitatif dan analisis materi muatan. Metode penelitiannya menggunakan deskriptif analitis.

BAB II
KAJIAN TEORETIS DAN PRAKTIK EMPIRIS

A. Kajian Teoretis

1. Negara Hukum dan Hak Asasi Manusia

Negara Hukum adalah negara yang penyelenggaraan kekuasaan pemerintahannya didasarkan atas hukum. Pemerintah atau lembaga-lembaga lain dalam melaksanakan tindakan apa pun harus dilandasi oleh hukum dan dapat dipertanggungjawabkan secara hukum. Dalam negara hukum, kekuasaan menjalankan pemerintahan berdasarkan kedaulatan hukum (supremasi hukum) dan bertujuan untuk menyelenggarakan ketertiban hukum.

Menurut Arief Sidharta, Scheltema merumuskan pandangannya tentang unsur-unsur dan asas-asas Negara Hukum itu secara baru, yaitu meliputi 5 (lima) hal sebagai berikut:[20]

a. Pengakuan, penghormatan, dan perlindungan hak asasi manusia yang berakar dalam penghormatan atas martabat manusia (*human dignity*).
b. Berlakunya asas kepastian hukum. Negara Hukum untuk bertujuan menjamin bahwa kepastian hukum terwujud dalam masyarakat. Hukum bertujuan untuk mewujudkan kepastian hukum dan prediktabilitas yang tinggi, sehingga dinamika kehidupan bersama dalam masyarakat bersifat *'predictable'*. Asas-asas yang terkandung dalam atau terkait dengan asas kepastian hukum tersebut yaitu

[20] B. Arief Sidharta, "Kajian Kefilsafatan tentang Negara Hukum", *Jentera (Jurnal Hukum)*, "Rule of Law", Pusat Studi Hukum dan Kebijakan (PSHK), Jakarta, edisi 3 Tahun II, November 2004, hlm.124-125.

sebagai berikut:

1) Asas legalitas, konstitusionalitas, dan supremasi hukum;
2) Asas undang-undang menetapkan berbagai perangkat peraturan tentang cara pemerintah dan para pejabatnya melakukan tindakan pemerintahan;
3) Asas non-retroaktif perundang-undangan, sebelum mengikat undang-undang harus lebih dulu diundangkan dan diumumkan secara layak;
4) Asas peradilan bebas, independen, imparsial, dan objektif, rasional, adil dan manusiawi;
5) Asas *non-liquet*, hakim tidak boleh menolak perkara karena alasan undang-undangnya tidak ada atau tidak jelas; dan
6) Hak asasi manusia harus dirumuskan dan dijamin perlindungannya dalam undang-undang atau undang-undang dasar.

c. Berlakunya persamaan (*similia similius* atau *equality before the law*), dalam negara hukum, Pemerintah tidak boleh mengistimewakan orang atau kelompok orang tertentu, atau mendiskriminasikan orang atau kelompok orang tertentu. Di dalam prinsip ini, terkandung (a) adanya jaminan persamaan bagi semua orang di hadapan hukum dan pemerintahan, dan (b) tersedianya mekanisme untuk menuntut perlakuan yang sama bagi semua warga negara.
d. Asas demokrasi, dimana setiap orang mempunyai hak dan kesempatan yang sama untuk turut serta dalam pemerintahan atau untuk mempengaruhi tindakan-tindakan pemerintahan. Untuk itu asas demokrasi itu diwujudkan melalui beberapa prinsip, yaitu:

1) adanya mekanisme pemilihan pejabat-pejabat publik tertentu yang bersifat langsung, umum, bebas, rahasia, jujur dan adil yang diselenggarakan secara berkala;
2) pemerintah bertanggung jawab dan dapat dimintai pertanggungjawaban oleh badan perwakilan rakyat;
3) semua warga Negara memiliki kemungkinan dan kesempatan yang sama untuk berpartisipasi dalam proses pengambilan keputusan politik dan mengontrol pemerintah;
4) semua tindakan pemerintahan terbuka bagi kritik dan kajian rasional oleh semua pihak;
5) kebebasan berpendapat/berkeyakinan dan menyatakan pendapat;
6) kebebasan pers dan lalu lintas informasi;
7) setiap rancangan undang-undang harus dipublikasikan untuk memungkinkan partisipasi rakyat secara efektif.

e. Pemerintah dan pejabat mengemban amanat sebagai pelayan masyarakat dalam rangka mewujudkan kesejahteraan masyarakat sesuai dengan tujuan bernegara yang bersangkutan. Dalam asas ini terkandung hal-hal sebagai berikut:
1) asas-asas umum pemerintahan yang layak;
2) syarat-syarat fundamental bagi keberadaan manusia yang bermartabat manusiawi dijamin dan dirumuskan dalam aturan perundang-undangan, khususnya dalam konstitusi;
3) pemerintah harus secara rasional menata tiap tindakannya, memiliki tujuan yang jelas dan berhasil

guna (*doelmatig*). Artinya, pemerintahan itu harus diselenggarakan secara efektif dan efisien.

Negara berdasar atas hukum menempatkan hukum sebagai hal yang tertinggi (*supreme*) sehingga ada istilah supremasi hukum. Supremasi hukum harus tidak boleh mengabaikan 3 (tiga) ide dasar hukum yaitu keadilan, kemanfaatan, dan kepastian. Apabila negara berdasar atas hukum, pemerintahan negara itu juga harus berdasar atas suatu konstitusi atau Undang-Undang Dasar sebagai landasan penyelenggaraan pemerintahan. Konstitusi dalam negara hukum adalah konstitusi yang bercirikan gagasan konstitusionalisme yaitu adanya pembatasan atas kekuasaan dan jaminan hak dasar warga negara.

Pengertian hak asasi manusia sering dipahami sebagai hak kodrati yang dibawa oleh manusia sejak manusia lahir ke dunia. Pemahaman terhadap hak asasi yang demikian ini merupakan pemahaman yang sangat umum dengan tanpa membedakan secara akademik hak-hak yang dimaksud serta tanpa mempersoalkan asal-usul atau sumber diperolehnya hak tersebut.

Pertanyaan mendasar yang dikemukakan pada bagian ini adalah apa hubungan negara hukum dengan hak asasi manusia? Jawaban atas pertanyaan ini sudah barang tentu, tidak begitu sulit mengkajinya dari sudut ilmu hukum, sebab antara negara hukum dan hak asasi manusia, tidak dapat dipisahkan satu sama lain. Argumentasi hukum yang dapat diajukan tentang hal ini, ditunjukan dengan ciri negara hukum itu sendiri, bahwa salah satu diantaranya adalah perlindungan terhadap hak asasi manusia. Dalam negara hukum, hak asasi manusia terlindungi. Jika dalam suatu negara hak asasi manusia tidak dilindungi,

negara tersebut bukan negara hukum akan tetapi negara diktator dengan pemerintahan yang otoriter. Perlindungan hak asasi manusia dalam negara hukum terwujud dalam bentuk penormaan hak tersebut dalam konstitusi, undang-undang serta untuk selanjutnya penegakannya melalui badan-badan peradilan sebagai pelaksana kekuasaan kehakiman.

Jika membicarakan peran negara hukum dan hak asasi manusia maka berarti membicarakan dimensi kehidupan manusia. Hak Asasi Manusia adalah hak-hak yang dimiliki manusia semata-mata karena ia manusia. Umat manusia memilikinya bukan karena diberikan kepadanya oleh masyarakat atau berdasarkan hukum positif, melainkan semata-mata berdasarkan martabatnya sebagai manusia. Dalam arti ini, maka meskipun setiap orang terlahir dengan warna kulit, jenis kelamin, bahasa, budaya dan kewarganegaraan yang berbeda-beda, tetapi tetap mempunyai hak-hak tersebut. Inilah sifat universal dari hak-hak tersebut. Selain bersifat universal, hak-hak itu juga tidak dapat dicabut (*inalienable*).[21]

Konsep hak asasi manusia menurut Leach Levin (aktivis HAM) memiliki dua pengertian dasar. Pertama, bahwa hak-hak yang tidak dapat dipisahkan atau dicabut adalah hak asasi manusia. Hak-hak ini adalah hak-hak moral yang berasal dari kemanusiaan setiap insan. Tujuan dari hak tersebut adalah untuk menjamin martabat setiap manusia. Kedua, adalah hak-hak menurut hukum yang dibuat sesuai dengan proses pembentukan hukum yang dibuat sesuai dengan proses

[21] Knut D. Asplund, Suparman Marzuki dan Eko Riyadi, (ed.), *Hukum Hak Asasi Manusia,* Pusat Studi Hak Asasi Manusia Universitas Islam Indonesia, PUSHAM UII, Yogyakarta, 2008, hlm.11.

pembentukan hukum dari masyarakat itu sendiri, baik secara nasional maupun internasional.[22]

Asas perlindungan dalam negara hukum tampak antara lain dalam *Declaration of Independent*, deklarasi tersebut mengandung asas bahwa orang yang hidup di dunia ini, sebenarnya telah diciptakan merdeka oleh Tuhan, dengan dikaruniai beberapa hak yang tidak dapat dirampas atau dimusnahkan, hak tersebut mendapat perlindungan secara tegas dalam negara hukum. Peradilan tidak semata-mata melindungi hak asasi perorangan, melainkan fungsinya adalah untuk mengayomi masyarakat sebagai totalitas agar supaya cita-cita luhur bangsa tercapai dan terpelihara.

Terkait hak pribadi sebagai hak asasi manusia dijelaskan Danrivanto Budhijanto, bahwa "Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah."[23]

Edmon Makarim berpendapat dari beberapa pendapat ahli menyimpulkan bahwa ada 3 (tiga) prinsip penting tentang hak pribadi, yakni:[24]

a. hak untuk tidak diusik oleh orang lain kehidupan pribadinya;

---

[22] Muhammad Tholhah Hasan, *Perlindungan Terhadap Korban Kekerasan Seksual (Advokasi atas Hak Asasi Perempuan)*, PT. Refika Aditama, Bandung, 2001, hlm. xii.

[23] Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi, PT. Refika Aditama, Bandung, 2010, hlm. 4.

[24] Edmon Makarim, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Rajawali Pers, Jakarta, 2010, hlm. 298-299.

b. hak untuk merahasiakan informasi-informasi yang bersifat sensitif yang menyangkut dirinya; dan
c. hak untuk mengontrol penggunaan data pribadinya oleh pihak-pihak lain.

Dalam amandemen keempat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, penuangan pasal-pasal hak asasi manusia (HAM) sebagai wujud jaminan atas perlindungannya dituangkan dalam bab tersendiri, yaitu pada Bab XA dengan judul "Hak Asasi Manusia", yang di dalamnya terdapat 10 (sepuluh) pasal tentang HAM ditambah 1 pasal (Pasal 28) dari bab sebelumnya (Bab X) tentang "Warga Negara dan Penduduk", sehingga ada 11 (sebelas) pasal tentang HAM, mulai dari Pasal 28, 28A sampai dengan Pasal 28J. Terkait perlindungan hak-hak pribadi diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28G ayat (1), yang menyatakan bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Dalam Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan International *Covenant on Civil and Political Rights* (Konvenan Internasional tentang Hak-hak Sipil dan Politik) diatur mengenai pembatasan kewenangan petugas penegak hukum untuk melakukan pengawasan rahasia terhadap individu (warga negara), antara lain sebagaimana tersebut dalam Pasal 17, yang menyatakan bahwa:

> (1) Tidak boleh seorang pun yang dengan sewenang-wenang atau secara tidak sah dicampuri masalah pribadi, keluarga, rumah atau korespondensinya, atau secara tidak sah diserang kehormatan dan nama baiknya. (2) Setiap orang

berhak atas perlindungan hukum terhadap campur tangan atau serangan tersebut.[25]

Dari uraian di atas, terlihat jelas hubungan antara negara hukum dan hak asasi manusia, hubungannya bukan hanya dalam bentuk formal semata-mata, dalam arti bahwa perlindungan hak asasi manusia merupakan ciri utama konsep negara hukum, tapi juga hubungan tersebut dilihat secara materiil. Hubungan secara materiil ini digambarkan dengan setiap sikap tindak penyelenggara negara harus bertumpu pada aturan hukum sebagai asas legalitas. Konstruksi yang demikian ini menunjukan pada hakikatnya semua kebijakan dan sikap tindak penguasa bertujuan untuk melindungi hak asasi manusia. Pada sisi lain, kekuasaan kehakiman yang bebas dan merdeka tanpa dipengaruhi oleh kekuasaan manapun, merupakan wujud perlindungan dan penghormatan terhadap hak asasi manusia dalam negara hukum.

2. Data Pribadi sebagai Hak Asasi Manusia

a. Pengertian Dasar

1) Pengertian Data Pribadi

Suatu data adalah data pribadi apabila data tersebut berhubungan dengan seseorang, sehingga dapat

[25] Adnan Buyung Nasution & A. Patra M. Zen, *Instrumen Internasional Pokok Hak Asasi Manusia*, ed.III., Yayasan Obor Indonesia, Yayasan Lembaga Bantuan Hukum Indonesia dan Kelompok Kerja Ake Arif, Jakarta, 2006, hlm. 162. Adapun bunyi asli *Article* 17 ICCPR: "(1) *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks."* Ketentuan ini menekankan pada pembatasan kewenangan petugas penegak hukum untuk melakukan pengawasan rahasia terhadap individu (warga negara). Lihat Komentar Umum Nomor 16 yang disepakati oleh Komite Hak Asasi Manusia Perserikatan Bangsa-Bangsa pada persidangan ke 23 (dua puluh tiga) tahun 1998, yang memberikan komentar terhadap materi muatan Pasal 17 Kovenan Internasional Hak Sipil dan Politik.

digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data.[26] Sebagai contoh, nomor telepon di dalam secarik kertas kosong adalah data. Berbeda halnya apabila di dalam secarik kertas tersebut tertulis sebuah nomor telepon dan nama pemilik nomor telepon tersebut, data tersebut adalah data pribadi. Nomor telepon di dalam secarik kertas kosong bukan data pribadi karena data tersebut tidak dapat digunakan untuk mengidentifikasi pemiliknya, sedangkan data nomor telepon dan nama pemiliknya dapat digunakan untuk mengidentifikasi pemilik data tersebut, oleh karena itu dapat disebut sebagai data pribadi.

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".*

Dari pengertian data pribadi di atas, dapat terlihat bahwa seseorang yang dapat diidentifikasi adalah seseorang yang dapat dikenali/diidentifikasi secara langsung maupun tidak langsung berdasarkan nomor tanda pengenal atau berdasarkan satu atau lebih faktor spesifik dari identifikasi fisik, psikologi, mental, budaya atau sosial.

Entitas yang dilindungi dalam mekanisme pelindungan data pribadi adalah "orang perorangan"

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

(*natural person*) bukan "badan hukum" (*legal person*).[27] Hak pelindungan 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 pelindungan data pribadi.[28]

Penjelasan mengenai definisi data pribadi adalah hal penting untuk menjamin pelindungan 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 diberlakukan adalah jenis data yang dapat dikategorikan sebagai data pribadi. Otoritas pelindungan data yang diatur dalam *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* telah memberikan interpretasi yang berbeda namun pada intinya data itu berhubungan dengan individu walaupun

---

[27] Mengenai istilah "badan hukum", Pasal 1653 Kitab Undang-Undang Hukum Perdata menyatakan:
"Selain perseroan perdata sejati, perhimpunan orang-orang sebagai badan hukum juga diakui undang-undang, entah badan hukum itu diadakan oleh kekuasaan umum atau diakuinya sebagai demikian, entah pula badan hukum itu diterima sebagai yang diperkenankan atau telah didirikan untuk suatu maksud tertentu yang tidak bertentangan dengan undang-undang atau kesusilaan."

[28] European Union Agency for Fundamental Rights and Council of Europe, *Op.Cit.* hlm. 37.

informasi yang teridentifikasi telah terpisah akan tetapi mendapatkan perlindungan mengingat data tersebut tidak dianggap sebagai data yang tidak bernama.[29]

2) Prinsip-prinsip *anonymity/pseudonymity*

Perkembangan media, baik media komunikasi maupun media elektronik sangat berkembang pesat, bahkan terkadang data di media tersebut tidak mempunyai nama.

Melihat perkembangan media, komunikasi dan teknologi dapat bersatu menjadi sebuah entitas yang besar.[30] yang memiliki puluhan bahkan ratusan layanan jasa dan produk. Media tersebut memiliki kemampuan untuk melacak perilaku online para penggunanya atau bahkan menghubungkannya dengan identitas *offline* penggunanya. Terdapat beberapa kasus di mana data yang tanpa nama telah berhasil untuk di re-identifikasi.[31] *Pseudonymity* yaitu memisahkan data dengan identitas namun dalam keadaan tertentu memungkinkan data tersebut untuk disatukan, dapat menjadi alat yang berguna namun juga dapat melemahkan data-data yang

---

[29] Mark F. Kightlinger, E. Jason Albert, and Daniel P. Cooper, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* of 28 January 1981, dapat diakses di: http://conventions.coe.int/treaty/EN/Treaties/HTML/108.htm.

[30] http://www.businessweek.com/technology/content/apr2007/tc20070414 _ 675511.htm. diakses pada januari 2015.

[31] Lihat Kasus Netflix di Artikel Berita, "Researchers reverse Netflix anonymization", 14 Desember 2007, http://www.securityfocus.com/ news/11497, diakses pada Januari 2015 Pukul 17.00 WIB. Lihat Juga Artikel Berita Forbes Tech, "Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study", 25 April 2013, http://www.forbes.com/sites/ adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous volunteers-in-dna-study/, diakses pada Januari 2015 Pukul 17.00 WIB.

tanpa nama karena dapat digunakan sebagai alat untuk membuka privasi.

Dengan demikian, perlu ditinjau kembali definisi data pribadi untuk menjamin apakah definisi tersebut sudah memberikan perlindungan yang sama, terlepas dari data tersebut mempunyai nama atau tanpa nama. Tentu saja hukum tentang data pertama kali memberikan langkah-langkah perlindungan bagi semua informasi yang berhubungan dengan "orang yang teridentifikasi atau yang dapat teridentifikasi". Hal tersebut merupakan hal yang rumit tetapi tetap perlu diatur sebelum ada ketentuan yang dapat mencakup seutuhnya aturan hukum tentang pelindungan data modern dan teknologi privasi yang ramah.

3) Data sensitif

Dalam hukum pelindungan data seperti *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. *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.

Jika dalam peraturan perundang-undangan daftar data yang dikategorikan sebagai data sensitif diatur secara eksplisit (*rigid*), kekosongan pasti akan selalu muncul di masa mendatang seiring dengan kemajuan teknologi. Sebagai contoh, data sensitif dalam *EU DP Directive* tidak mencakup data keuangan atau lokasi, yang keduanya merupakan kunci dari kehidupan privat yang modern. Beberapa data geolocation diatur secara terpisah oleh EC Directive 2002/58/EC (the e-Privacy Directive), yang berlaku bagi pengolahan "*base station data*" oleh operator telekomunikasi termasuk aturan mengenai WiFi hotspots. E-Privacy Directive berlaku secara eksklusif bagi penyedia jasa telekomunikasi sehingga tidak mengatur tingkah laku entitas lain dalam hal pengumpulan dan pengolahan data geolocation misalnya penyedia aplikasi data geolocation, pengembang dari sistem pengoperasian pengguna smart mobile devices, situs sosial media, dan lain-lain. Pasal 29 dari Working Party (WP), sebuah badan penasihat independen yang terdiri dari perwakilan semua otoritas EU DP, telah menyatakan keprihatinannya mengenai persetujuan (*consent*) dalam konteks jasa lokasi. Mereka menegaskan bahwa ketersediaan pengaturan mengenai informasi tentang tujuan pengumpulan dan penggunaan data geolocation yang jelas, komprehensif dan mudah dimengerti adalah penting untuk mendapatkan persetujuan yang valid. (Pasal 2(h)).[32]

[32] EC Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 16 Mei 2011, Dapat diunduh di:

Hukum sektor privasi di Kanada juga memiliki persyaratan yang ketat mengenai pengolahan data yang sensitif, namun tidak seperti *DP Directive*, hukum ini tidak memiliki daftar kategori yang *rigid*.[33] Hukum ini menjelaskan bahwa organisasi perdagangan sebelumnya harus mendapatkan persetujuan yang nyata ketika informasi cenderung merupakan informasi yang sensitif, mengingat fakta bahwa semua informasi dapat menjadi sensitif tergantung dari konteksnya. Sifat dari pengamanan yang diperlukan sangat tergantung dari sensitifitas informasi yang telah dikumpulkan tersebut, jumlah distribusi dan format serta penyimpanan dari informasi tersebut. Semakin sensitif suatu informasi, maka penjagaannya harus dilakukan dengan perlindungan tingkat tinggi.[34]

b. Privasi sebagai suatu Hak

Dalam sejarah perkembangannya, privasi merupakan suatu konsep yang bersifat universal dan dikenal di berbagai negara baik tertulis dalam bentuk undang-undang maupun tidak tertulis dalam bentuk aturan moral.[35] Contohnya: privasi di negara-negara yang menganut *civil law*, seperti

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, diakses pada tanggal 14 Oktober 2014 Pukul 20.00 WIB.

33 *Personal Information Protection and Electronic Documents Act Canada* (S.C.2000,c.5), diakses di http://laws-lois.justice.gc.ca/eng/acts/P-8.6/, pada tanggal 11 September 2014 Pukul 2014 Pukul 10.00 WIB.

34 *Ibid.*

35 http://www.privacyinternational.org.Countries.index.html, diakses pada tanggal 10 Januari, 2007. Lihat juga Banisar, *Privacy & Human Rights,An International Survey of Privacy Laws and Developments,* Electronic *Privacy* Information Centre, Washington. D.C, 2000, hlm. 1-3. Seperti yang dikutip dalam Sinta Dewi Rosadi, *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, Widya Padjadjaran, Bandung, 2009, hlm. 45.

dignitas di Belanda yang berarti hak pribadi,[36] istilah *personlichkeitsrecht* di Jerman yang berarti hak pribadi sebagai perwujudan kepribadian seseorang dan istilah *geheimssphare* di Swiss yang berarti privasi individu ("*individual privacy*").[37] Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandeis yang menulis sebuah artikel di dalam Jurnal Ilmiah, Fakultas Hukum, Universitas Harvard yang berjudul "*The Right to Privacy*"[38]. Mereka menyatakan bahwa: "*Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition.*" Privasi adalah hak untuk menikmati hidup dan menuntut hukum untuk melindungi privasi, selanjutnya menurut Warren, karena terdapat perkembangan teknologi, ekonomi dan politik maka muncul hak baru yang belum dilindungi oleh *Common Law*.

Hak tersebut berkaitan dengan kebutuhan spiritual manusia yaitu kebutuhan untuk dihargai perasaan, pikiran dan hak untuk menikmati kehidupannya atau disebut dengan *the right to be let alone.*[39] sehingga kemudian Warren mengusulkan kepada hakim untuk mengakui privasi sebagai suatu hak yang harus dilindungi.

Alasan privasi harus dilindungi adalah:

---

[36] Nihal Jayawickrama, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence*, Cambridge University Press, United Kingdom, 2002, hlm. 599. Sinta Dewi Rosadi, Ibid.

[37] Hofstadter and Horowitz, *The Right of Privacy*, Central Book Company, New York, 1964, hlm.10-11.

[38] Samuel Warren & Louis D. Brandeis, "The Right To Privacy", *Harvard Law Review*, Volume 4, 1890, hlm. 1.

[39] Warren dan Brandheis mengikuti pendapat Hakim Cooley tentang dasar privasi yaitu hak untuk ditinggalkan sendiri atau *the right to be let alone, Loc.Cit.*

1) Dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu.
2) Seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*"solitude")* sehingga privasi sangat diperlukan oleh seseorang.
3) Privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hak ini akan hilang apabila orang tersebut memublikasikan hal-hal yang bersifat pribadi kepada umum.
4) Privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai *the right against the word*.
5) Dalam pelanggaran privasi terdapat kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya, sehingga bila terdapat kerugian yang diderita maka pihak korban wajib mendapatkan kompensasi.

Menurut Berzanson, pendapat Warren dan Brandheis tersebut merupakan suatu pendapat yang sangat penting karena untuk pertama kalinya privasi dipaparkan sebagai suatu konsep hukum yang menuntut negara dalam hal ini

pengadilan untuk menghargai hak seseorang sehingga dia dapat lebih menikmati kehidupannya.[40]

Di dalam mengemukakan konsepnya Warren juga mengemukakan privasi tidak bersifat absolut karena memiliki ada batasan yaitu:[41]

1) tidak menutupi kemungkinan untuk memublikasikan 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 memberikan bahwa informasi pribadinya akan disebarkan kepada umum;
4) persetujuan dan privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik karena telah mengganggu kehidupan pribadi.

Sebenarnya privasi tersebut di atas pada waktu itu bukan merupakan suatu hak yang asing karena sebenarnya di dalam lapangan hukum pidana telah dikenal perlindungan hak lain yang pada pengembangannya akan merujuk kepada privasi. Contohnya, pengaturan tentang *trespass* (memasuki tempat tinggal orang lain tanpa izin).

Rezim *trespass* mirip dengan privasi karena memiliki sifat yang sama dengan *trespass* yaitu orang memiliki daerah yang tidak boleh dimasuki oleh orang lain tanpa izin orang

[40] Randall P. Berzanson, "*The Right to Privacy Revisited : Privacy, News and Social Change*", California Law Review, Vol 80, 1992, hlm. 2-5.
[41] *Ibid,* hlm. 25.

yang bersangkutan. Hanya rezim *trespass* mempunyai arti fisikal sedangkan privasi mempunyai arti spiritual.[42]

Menurut Wellington pendapat Warren dan Bradheis merupakan pendapat yang sangat penting karena menjadi permulaan suatu konsep moral dan diakui menjadi suatu prinsip hukum dan prinsip dasar privasi berasal dari konsep moral.[43] Wellington menyatakan: *"This articles is an extraordinary essay by many tests, especially for its attempt to fashion a legal principle from changes in moral perception*".

Dalam konteks hukum internasional, privasi telah diatur sebagai pengaruh dari perkembangan yang terjadi terutama di Amerika Serikat dan Eropa Barat. Di dalam hukum internasional, privasi secara jelas diakui sebagai bagian dari hak dasar manusia yang patut dilindungi.[44], dan merupakan hak yang berdiri sendiri. Dasar pengaturan privasi di dalam hukum internasional muncul setelah Perang Dunia II dan dipengaruhi oleh perkembangan pengaturan nasional yang berasal dari Amerika Serikat.[45]

Menurut Komisi Hak Asasi Manusia Perserikatan Bangsa-Bangsa (PBB), alasan privasi digolongkan sebagai hak dasar manusia karena yang dilindungi adalah manusia sebagai individu yang perlu untuk mengembangkan kepribadiannya dengan memberikan zona (*space*) untuk dirinya sendiri.[46]

---

42 Ken Gormley, *One Hundred Years of Privacy*, Wisconsin Law Review, Vol 52, 1992, hlm. 3.

43 Lihat kasus Pavesich v. New England Life, Ins, Co, 1995.

44 *In international law, privacy is clearly and unambigously established as a fundamental right to be protected*, seperti yang dikutip dalam James Michael, *Privacy and Human Rights, an International and Comparative Study, with Special Reference to developments in Information Technology,* UNESCO, France, 1994, hlm. 1. Lihat Sinta Dewi Rosadi, *Praktik Negara-Negara dalam Mengatur Privasi dalam E-Commerce*, Widya Padjadjaran, Bandung, 2009, hlm. 32.

45 Nihal Jayawickrama, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence, Op.Cit,* hlm. 560.

46 *Ibid,* hlm. 605.

Dengan demikian, saat ini privasi diatur di dalam beberapa instrumen internasional, seperti:

1) Deklarasi Universal tentang Hak Asasi Manusia (*Universal Declaration of Human Rights*, 1948);
2) Kovenan Internasional tentang Hak Sipil dan Politik (International Covenant on Civil and Political Rights, 1966);
3) Konvensi Eropa tentang Hak Asasi Manusia (*European Convention for the Protection of Human Rights and Fundamental Freedoms*, 1950);
4) Konvensi Amerika tentang Perlindungan Hak Asasi Manusia (*American Convention on Human Rights*, 1979);
5) Deklarasi Kairo tentang Hak Asasi Manusia Islam (*Kairo declaration of Islamic Human Rights*, 1990).

3. Hubungan antara Privasi dan Hak Pribadi

Perkembangan sistem komputer dan internet membuat informasi menjadi mudah untuk dicari dan dibagi. Konsep dasar dari pelindungan data pribadi pertama muncul sekitar tahun 1960. Pada tahun 1970, Negara Bagian Hesse di Jerman adalah negara bagian pertama yang memberlakukan peraturan tentang pelindungan data, diikuti oleh hukum nasional di Swedia pada tahun 1973, Jerman Barat pada tahun 1977, Amerika Serikat pada tahun 1974, dan Prancis pada tahun 1978 dan Inggris pada tahun 1984.[47] Konsep pelindungan data sering diperlakukan sebagai bagian dari perlindungan privasi. Pelindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau

[47] Andrew Murray, *Information Technology Law, The Law and Society,* Oxford University Press, New York, 2010, hlm. 466.

lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi.[48]

Definisi yang dikemukakan oleh Westin tersebut, kemudian dikembangkan oleh para pakar hukum lainnya terutama dalam menyikapi perkembangan dan kemajuan teknologi informasi dan komunikasi. Melalui kemajuan teknologi maka informasi pribadi seseorang dapat diakses, diproses, dikumpulkan dan dimanipulasi secara cepat dan murah. Westin menambahkan, hak terhadap privasi tidak bersifat absolut karena ada kewajiban sosial yang harus diperhatikan yang sama pentingnya dengan privasi.[49] sehingga seseorang dituntut untuk selalu menyeimbangkan antara privasi dan kepentingan sosial yang akan selalu berproses sesuai dengan lingkungan sosial tempat dia hidup.

Melihat ruang lingkup yang sangat luas maka menurut Abu Bakar Munir privasi dapat dikategorikan menjadi 4 (empat) golongan yaitu: [50]

a. privasi atas informasi, berkaitan dengan cara pengumpulan dan pemrosesan data pribadi seperti informasi kredit dan catatan kesehatan;
b. privasi atas anggota badan, berkaitan dengan perlindungan secara fisik seseorang seperti prosedur pemeriksaan

[48] Menurut Alan Westin: *Privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to others* dalam, Allan Westin, Alan F. Westin, *Privacy and Freedom,* London, 1967, hlm. 7.

[49] *Ibid.*

[50] Abu Bakar Munir, Siti Hajar, Mohd Yasin, *Privacy and Data Protection,* Sweet & Mawell Asia, Malaysia, 2002, hlm. 2. Lihat Juga Abu Bakar Munir, Siti Hajar Mohd Yasin, *Personal data Protection in Malaysia,* Sweet & Maxwell Asia, 2010, hlm. 3.

penggunaan obat bius, pengambilan data biometrik seperti sidik jari dan retina mata;

c. privasi atas komunikasi, meliputi perlindungan atas komunikasi seseorang contohnya surat, telepon, email atau bentuk-bentuk komunikasi lainnya;
d. privasi atas teritorial contohnya privasi di lingkungan domestik atau tempat tinggal, privasi di tempat kerja.

Dalam konteks Rancangan Undang-Undang Pelindungan Data Pribadi, privasi atas data merupakan hal yang harus dilindungi. Menurut doktrin yang telah dikemukakan oleh Westin tersebut di atas, privasi atas data pribadi adalah privasi yang memberi kebebasan kepada seseorang untuk menentukan apakah data pribadinya boleh diakses oleh pihak ketiga atau tidak.

Sejumlah instrumen internasional telah mengatur prinsip-prinsip pelindungan data.[51] dan banyak aturan-aturan nasional telah memasukannya sebagai bagian dari hukum nasional. Pelindungan data juga merupakan hak asasi manusia yang fundamental, sejumlah negara.[52] telah mengakui pelindungan data sebagai hak konstitusional atau dalam bentuk '*habeas data*' yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya. Albania, Armenia, Filipina, Timor Leste, Kolombia dan Argentina adalah negara-negara dengan perbedaan

[51] Lihat *the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72*).

[52] Dalam hal ini, Pasal 35 of the 1976 *Constitution of Portugal* dapat menjadi contoh yang baik.

sejarah dan budaya yang telah mengakui peran dari pelindungan data yang dapat memfasilitasi proses demokrasi dan telah menjamin perlindungannya dalam konstitusi mereka.

ASEAN Human Rights Declaration yang baru saja diadopsi negara-negara ASEAN juga secara jelas mengakui hak privasi atas data pribadi dalam Pasal 21. Dewasa ini, telah banyak negara yang undang-undangnya mengatur tentang pelindungan data, setidaknya terdapat lebih dari 132 negara yang memiliki hukum tentang pelindungan data.[53]

B. Kajian terhadap Asas/Prinsip yang Terkait dengan Penyusunan Norma

Dalam setiap perumusan undang-undang, sebelum diformulasikan sebagai norma-norma maka terlebih dahulu perlu dilakukan eksplorasi terhadap asas-asas hukum yang relevan, baik asas-asas yang bersifat umum maupun khusus. Asas-asas hukum tersebut juga sangat diperlukan sebagai pedoman, standar dan prinsip-prinsip. Seorang ahli hukum merumuskan asas hukum sebagai*: "a standard that is to be observed...because it is a requirement of justice or fairness or some other dimension of morality".*[54] Dengan demikian, asas hukum merupakan standar yang harus diperhatikan karena merupakan persyaratan terjadinya keadilan, ketidakberpihakan dan dimensi moralitas lainnya. Di samping sebagai landasan, asas hukum ini layak disebut sebagai alasan bagi lahirnya peraturan hukum, atau merupakan *ratio legis*

[53] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (6th Ed January 2019) (February 9, 2019). (2019) Supplement to 157 Privacy Laws & Business International Report (PLBIR) 16 pgs. Available at SSRN: https://ssrn.com/abstract=3380794.

[54] Theodore M. Bendit, *Law as Rule and Principle, Problems of Legal Philosphy*, Stanford University Press, Stanford-California, 1978, hlm. 74.

dari peraturan hukum.[55] Asas hukum ini tidak akan habis kekuatannya dengan melahirkan peraturan hukum, melainkan tetap saja ada dan akan melahirkan peraturan-peraturan selanjutnya.[56] Asas hukum berfungsi sebagai suatu sarana yang membuat hukum itu hidup, tumbuh dan berkembang karena mengandung nilai-nilai dan tuntutan etis.[57] Karena asas hukum mengandung tuntutan etis, maka asas hukum merupakan jembatan antara peraturan-peraturan hukum dengan cita-cita sosial dan pandangan etis masyarakatnya. Dengan singkat dapat dikatakan, bahwa melalui asas hukum ini, peraturan-peraturan hukum berubah sifatnya menjadi suatu tatanan etis.

1. Asas Materi Muatan Peraturan Perundang-undangan

a. pengayoman, bahwa setiap materi muatan perundang-undangan harus berfungsi memberikan perlindungan dalam rangka menciptakan ketenteraman masyarakat.
b. kemanusiaan, bahwa setiap materi muatan peraturan perundang-undangan harus mencerminkan perlindungan dan penghormatan hak-hak asasi manusia serta harkat dan martabat setiap warga negara Kesatuan Republik Indonesia.
c. kebangsaan, bahwa setiap materi muatan perundang-undangan harus mencerminkan sifat dan watak warga negara yang pluralistik (heterogen) dengan tetap menjaga prinsip Negara Kesatuan Republik Indonesia.
d. kekeluargaan, bahwa setiap materi muatan perundang-undangan harus mencerminkan musyawarah untuk mufakat dalam setiap pengambilan keputusan.

---

[55] Lihat Satjipto Rahardjo, *Ilmu Hukum*, Cetakan V, Penerbit Citra Aditya Bhakti, Bandung, 2000, hlm. 45.
[56] Lihat GW Paton, *Textbook of Jurisprudence*, Oxford University Press, London, 1964, hlm. 204.
[57] *Ibid*.

e. kenusantaraan, bahwa setiap materi muatan perundang-undangan senantiasa memperhatikan kepentingan seluruh warga negara dan materi muatan peraturan perundang-undangan merupakan bagian dari sistem hukum nasional yang berdasarkan Pancasila.
f. bhinneka tunggal ika, bahwa setiap materi muatan perundang-undangan harus memperhatikan keragaman penduduk, agama, suku dan golongan, kondisi sosial dan ekonomi masyarakat, serta budaya khususnya yang menyangkut masalah-masalah sensitif dalam kehidupan bermasyarakat, berbangsa dan bernegara.
g. keadilan, bahwa setiap materi muatan peraturan perundang-undangan harus mencerminkan keadilan secara proporsional bagi setiap warga masyarakat tanpa kecuali.
h. kesamaan kedudukan dalam hukum dan pemerintahan, bahwa setiap materi muatan perundang-undangan tidak boleh berisi hal-hal yang bersifat membedakan berdasarkan latar belakang, antara lain: agama, suku, ras, golongan, gender atau status sosial.
i. ketertiban dan kepastian hukum, bahwa setiap materi muatan perundang-undangan harus dapat menimbulkan ketertiban dalam masyarakat melalui jaminan adanya kepastian hukum.
j. keseimbangan, keserasian, dan keselarasan, bahwa setiap materi muatan perundang-undangan harus mencerminkan keseimbangan, keserasian, dan keselarasan antara kepentingan individu dan masyarakat dengan kepentingan bangsa dan negara.

2. Asas-Asas di Bidang Hukum Pelindungan Data Pribadi.

Di samping asas-asas sebagaimana diuraikan di atas, perlu diperhatikan juga asas-asas yang relevan untuk dijadikan sebagai dasar dari perumusan norma dalam RUU tentang Pelindungan Data Pribadi, antara lain:

a. Asas Pelindungan

Asas pelindungan sangat relevan dengan RUU tentang Pelindungan Data Pribadi karena pada dasarnya keberadaan undang-undang ini kelak dimaksudkan untuk memberi pelindungan kepada pemilik data mengenai privasinya, mengenai data pribadinya, mengenai hak-haknya atas data agar data tersebut tidak disalahgunakan sehingga merugikan kepentingan pemilik data;

b. Asas Kepentingan Umum

Asas kepentingan umum sangat penting untuk menjadi salah satu asas dari RUU tentang Pelindungan Data Pribadi, karena kepentingan umumlah yang dapat dijadikan alasan yang sah, sesuai dengan rumusan undang-undang, sebagai alasan untuk menerobos atau alasan pengecualian terhadap perlindungan privasi atas data pribadi. Kepentingan umum tersebut meliputi, antara lain: keamanan negara, kedaulatan negara, pemberantasan korupsi dan tindak pidana lainnya.

c. Asas Keseimbangan

Asas keseimbangan juga merupakan asas penting yang perlu dipertimbangkan untuk dijadikan dasar bagi perumusan norma pada RUU tentang Pelindungan Data Pribadi, karena pengaturan dalam undang-undang ini sebenarnya mencerminkan upaya untuk

menyeimbangkan antara hak-hak privasi di satu pihak dengan hak-hak negara yang sah berdasarkan kepentingan umum.

d. Asas Pertanggungjawaban

Asas pertanggungjawaban memberi landasan bagi semua pihak yang terkait dengan pemrosesan, penyebarluasan, pengelolaan, dan pengawasan data pribadi untuk bertindak secara bertanggung jawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak yang terkait, termasuk pemilik data.

e. Asas Timbal Balik (*Resiprositas)*

Asas yang menyatakan bahwa tindakan suatu negara terhadap negara lain dapat dibalas setimpal, baik tindakan yang bersifat positif maupun negatif. Asas ini memberikan dasar terhadap negara yang melakukan perjanjian internasional untuk melaksanakan isi perjanjian dengan cara-cara yang baik sesuai dengan tujuan negaranya masing-masing tanpa mengesampingkan tujuan awal pelaksanaan perjanjian itu sendiri, sehingga balasan yang timbul dari negara pihak adalah balasan yang bersifat positif. Dalam kaitannya dengan perlindungan data pribadi dimungkinkan kerjasama internasional antara pemerintah dengan pemerintah negara lain atau organisasi internasional sehingga bentuk kerjasama tersebut harus berdasarkan prinsip atau asas timbal balik.

3. Prinsip Penyusunan Norma Pelindungan Data

1. Persetujuan pemilik data pribadi

Persetujuan adalah salah satu prinsip paling mendasar untuk sah atau tidaknya suatu data untuk dapat diproses. Untuk data pribadi yang bersifat spesifik maka persetujuan harus diungkapkan secara eksplisit. Persetujuan harus menempatkan individu sebagai pemilik data yang memiliki kontrol atas data pribadinya. Persetujuan harus diberikan secara bebas yang berarti institusi harus memberikan pilihan kepada pemilik data bagaimana pemilik data mengontrol data pribadinya.

Petunjuk memberikan persetujuan harus jelas dan diperlukan tindakan nyata dari pemilik data untuk menyatakan persetujuannya dan tidak boleh diikuti oleh oleh persyaratan dan ketentuan lain intinya harus singkat, mudah dipahami, dan mudah digunakan. Persetujuan harus secara spesifik mencakup nama pengontrol, tujuan pemrosesan dan jenis aktivitas pemrosesan.

2. Kejelasan dasar kepentingan dan tujuan permintaan pengguna data pribadi

   Singkatnya, prinsip kejelasan dasar dan kepentingan dan tujuan permintaan menyatakan bahwa data pribadi yang dikumpulkan untuk satu tujuan tidak boleh digunakan untuk tujuan lain yang tidak kompatibel.

   Dalam pertimbangannya Rec.28 dan Art.6 (1) (b) dalam EU Data Protection Directive 1996 disebutkan bahwa:

   > "Data pribadi hanya dapat dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan nya. (Pemrosesan data lebih lanjut

untuk tujuan sejarah, statistik dan penelitian ilmiah diizinkan, dengan ketentuan bahwa Negara Anggota memberikan perlindungan yang tepat)."

Penjelasan selanjutnya dapat dilihat didalam General Data Protection Regulation (GDPR) 2016, disebutkan bahwa:

"Data pribadi hanya dapat dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah dan tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan nya. (Pemrosesan lebih lanjut dari data pribadi untuk tujuan pengarsipan untuk kepentingan publik, sejarah, statistik atau tujuan penelitian ilmiah, diizinkan, sesuai dengan ketentuan Art.89 (1))."

Jika dilihat bahwa GDPR membawa sedikit perubahan terbatas pada prinsip pembatasan tujuan. Pemrosesan lebih lanjut data terkait data pribadi untuk keperluan pengarsipan, penelitian ilmiah, historis atau statistik masih diizinkan, tetapi tunduk pada perlindungan tambahan yang disediakan di Art.89 dari GDPR.

3. Keamanan data pribadi

Pengguna data (*the controller*) bertanggung jawab untuk memastikan bahwa datapribadi tetap aman, baik terhadap ancaman eksternal (misalnya, peretasan berbahaya) dan ancaman internal (misalnya, karyawan yang kurang terlatih).

Perlindungan (*secure*) dan keamanan (*protect*) data merupakan tujuan utama dari pembentukan regulasi terkait pelindungan data. Dalam EU Data Protection Directive 1996

yang tertuang dalam pertimbangan Rec.46 dan Art.17 (1) bahwa:

> "Pengguna data harus menerapkan tindakan teknis dan organisasional yang tepat untuk melindungi data pribadi dari kerusakan yang tidak disengaja atau melanggar hukum atau kehilangan yang tidak disengaja, perubahan, kebocoran atau akses yang tidak sah."

Selanjutnya ketentuan diatas adopsi kedalam General Data Protection Regulation (GDPR) 2016, GDPR memindahkan kewajiban ini ke dalam Prinsip Pelindungan Data, memperkuat gagasan bahwa keamanan data adalah kewajiban mendasar dari semua pengguna data. Namun, prinsip itu sendiri pada dasarnya tidak berubah secara subtansi.

Dalam GDPR disebutkan dalam Rec.29, 71, 156; Art.5 (1) (f), 24 (1), 25 (1) - (2), 28, 39, 32, bahwa:

> "Data pribadi harus diproses dengan cara tertentu yang memastikan keamanan yang sesuai untuk data tersebut, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan terhadap kehilangan, kehancuran atau kerusakan yang tidak disengaja, dengan menggunakan tindakan teknis atau organisasional yang tepat."

4. Akses Data Pribadi

Dalam perihal akses data pribadi, tertuang prinsip minimisasi data, yang pada dasarnya adalah gagasan guna memberikan pengecualian terbatas, pengguna data hanya dapat

memproses atau mengakses data pribadi yang sebenarnya perlu diproses untuk mencapai tujuan penggunannya.
Prinsip ini membawa persyaratan yang lebih ketat karena terkait data pribadi yang didalamnya juga ada data sensitif.

Dalam Directive termuat dalam pertimbangan Rec.28 dan Art.6 (1) (c) yang memberikan pengaturan bahwa:

> "Data pribadi harus memadai, relevan dan tidak berlebihan sehubungan dengan tujuan pengumpulan dan/atau pemrosesan data tersebut lebih lanjut."

Ada sebuah kehawatiran bahwa perlu secara hati-hati meninjau operasi pemrosesan data untuk mempertimbangkan dan memverifikasi apakah pengguna data memproses data pribadi yang tidak benar-benar diperlukan dalam kaitannya dengan relevansi tujuan awal.

Sehingga dalam GDPR Rec.39; Art.5 (1) (c) memberikan tambahan bahwa:

> "Data pribadi harus memadai, relevan dan dalam pemrosesan nya terbatas pada apa yang diperlukan sehubungan dengan tujuan yang terkait."

Kewajiban untuk memastikan bahwa data pribadi tidak berlebihan diganti dengan kewajiban yang lebih membatasi untuk memastikan bahwa data pribadi "terbatas pada apa yang diperlukan".

5. Akurasi

Ada risiko yang jelas terhadap subyek data jika data yang tidak akurat diproses. Oleh karena itu pengguna data bertanggung jawab untuk mengambil semua langkah yang wajar untuk memastikan bahwa data pribadi yang diproses memang akurat.

Art.6 (1) (d) Directive 1996 memberikan pengaturan bahwa:

> "Data pribadi harus akurat dan jika perlu terus diperbarui. Setiap langkah yang masuk akal harus diambil untuk memastikan bahwa data yang tidak akurat atau tidak lengkap harus segera dihapus atau diperbaiki."

Ketentuan yang sama diadopsi dalam Art.5 (1) (d) GDPR 2016, yang menyebutkan bahwa:

> "Data pribadi harus akurat dan jika perlu terus diperbarui. Setiap langkah yang masuk akal harus diambil untuk memastikan bahwa data pribadi yang tidak akurat dihapus atau diperbaiki tanpa penundaan."

Dapat dilihat bahwa pengaturan didalam GDPR tidak mengubah prinsip akurasi secara redaksional. GDPR menetapkan bahwa penghapusan atau perbaikan data pribadi yang tidak akurat harus dilaksanakan tanpa penundaan, tetapi persyaratan tersebut tersirat dalam susunan kata dalam ketentuan didalam Direktif.

6. Retensi

   Gagasan bahwa data pribadi tidak boleh disimpan lebih lama dari yang diperlukan sehubungan dengan tujuan pengumpulannya, atau bilamana mereka memproses lebih

lanjut, adalah kunci untuk memastikan pemrosesan data pribadi yang benar menurut hukum.

Directive Art.6 (1) (e) mengatur bahwa:

> "Data pribadi harus disimpan dalam bentuk yang memungkinkan bahwa waktu pengidentifikasian nya tidak lebih lama dari yang diperlukan dalam pengumpulan data atau bilamana mereka memproses lebih lanjut. Negara-negara Anggota wajib menerapkan perlindungan yang tepat untuk data pribadi yang disimpan atau lebih lanjut untuk waktu yang lebih lama untuk keperluan historis, statistik atau ilmiah."

Peraturan Pelindungan Data Umum GDPR 2016, yang mulai berlaku pada 25 Mei 2018, membawa persyaratan yang lebih ketat mengenai berapa lama data pribadi dapat dipertahankan. Organisasi perlu lebih dipertimbangkan dan didisiplinkan dalam retensi data pribadi individu mereka. Panduan ringkas ini dirancang untuk membantu memahami prinsip retensi.

GDPR Art.5 (1) (e) mengatur bahwa:

> "Data pribadi harus disimpan dalam bentuk yang memungkinkan bahwa waktu pengidentifikasian nya tidak lebih lama dari yang diperlukan untuk tujuan pemrosesan. Data pribadi dapat disimpan untuk periode yang lebih lama sejauh data akan diproses semata- mata untuk keperluan pengarsipan untuk kepentingan umum, atau tujuan ilmiah, historis, atau statistik sesuai dengan

Art. 89 (1) dan tunduk pada penerapan perlindungan yang tepat."

Dapat dilihat bahwasannya ada sedikit perubahan dari pengaturan Directive dan GDPR, namun prinsipnya tidak berubah, GDPR memperkenalkan dua faktor baru yang penting:

1. Ada ketentuan khusus tentang pemrosesan data pribadi untuk tujuan historis, statistik atau ilmiah.
2. Prinsip tambahan harus dibaca dalam (Art. 17 GDPR Right to erasure ('right to be forgotten')) di mana pemilik data (subject data) memiliki hak untuk menghapus data pribadi, dalam beberapa kasus lebih cepat dari akhir periode retensi maksimum.

Untuk meringkas persyaratan hukum, Pasal 5 (e) dari GDPR menyatakan data pribadi harus disimpan tidak lebih lama dari yang diperlukan untuk tujuan yang sedang diproses. Ada beberapa keadaan di mana data pribadi dapat disimpan untuk periode yang lebih lama (misalnya tujuan pengarsipan untuk kepentingan publik, tujuan penelitian ilmiah atau sejarah).

Recital 39 dari GDPR juga menyatakan bahwa periode penyimpanan data pribadi harus dibatasi pada minimum yang ketat dan batas waktu harus ditetapkan oleh pengontrol data untuk penghapusan catatan (disebut sebagai penghapusan dalam GDPR) atau untuk tinjauan berkala.
Badan pengawas karenanya harus memastikan data pribadi dibuang dengan aman ketika tidak diperlukan lagi. Ini akan

mengurangi risiko bahwa itu akan menjadi tidak akurat, ketinggalan zaman atau tidak relevan.

7. Pemberitahuan

Pada prinsipnya, memproses data pribadi itu dilarang, kecuali jika secara tegas diizinkan oleh hukum, atau setelah ada **a. Pemberitahuan kepada pemilik data** dan telah disetujui nya. **b. Pemberitahuan kepada otoritas pengawas**.

Konsideran No. 25, 49 dalam pembukaan Directive menegaskan bahwa:

> "Kewajiban dikenakan pada orang, otoritas publik, perusahaan, lembaga atau badan lain yang bertanggung jawab telah memproses data pribadi seseorang, pemberitahuan kepada otoritas pengawas, serta kepada seseorang, yang data sedang diproses, untuk diberitahu bahwa proses sedang berlangsung, dapat berkonsultasi, atau meminta koreksi dan bahkan pemilik data dapat menolak pemrosesan dalam keadaan-keadaan tertentu."

Art.12 (c); Art. 18; Art. 28 Directive memberikan pengaturan bahwa:

> "Kewajiban untuk memberi tahu otoritas pengawas dan Hukum nasional tiap-tiap negara, membentuk komisi pelindungan data pribadi yang bertanggung jawab secara khusus untuk memastikan secara independen.
>
> Dengan demikian memastikan bahwa hak dan kebebasan dari pemilik data tidak akan terpengaruh secara negatif atau di intervensi tanpa pengawasan oleh lembaga-

lembaga atau badan lain yang melaukan pemrosesan data pribadi."

Pengaturan selanjutnya dalam GDPR memperkuat hak dan kewajiban serta tanggungjawab yang lebih besar kepada komisi/ otoritas pengawas untuk bertindak terhadap aduan (complaints) yang terjadi kepada pemilik data. Otoritas pengawas juga dapat melakukan semua tindakan-tindakan lain yang mungkin diperlukan untuk menerapkan aturan GDPR dan menjalankan perintah, keputusan, termasuk pengenaan sanksi administrasi, denda, atau hukuman kepada pihak-pihak yang melakukan penyalahgunaan data pribadi seseorang yang berakibat kerugian.

Terkait dengan kegagalan pelindungan data pribadi, pengendali data pribadi memiliki kewajiban untuk memberitahu pemilik data pribadi seperti yang diatur pada GDPR Art.33 :

"1. Dalam kasus kegagalan pelindungan data pribadi, pengendali harus tanpa penundaan dan, jika memungkinkan, tidak lebih dari 72 jam setelah mengetahuinya, memberitahukan kegagalan pelindungan data pribadi kepada otoritas pengawas yang kompeten sesuai dengan Pasal 55, dikecualikan jika kegagalan pelindungan data pribadi tidak menimbulkan risiko terhadap hak dan kebebasan pemilik data pribadi."

"2. Jika pemberitahuan kepada otoritas pengawas tidak dibuat dalam waktu 72 jam, harus disertai dengan alasan penundaan."

8. Pemusnahan dan penghapusan

Pemilik data memiliki hak untuk dapat menghapus data pribadi. Hak untuk menghapus juga dikenal sebagai 'hak untuk dilupakan' (*the right to be forgotten*) sebagai pengaruh dari keputusan EUCJ (European Union Court of Justice) yang memutus kasus yang sangat penting (*landmark case*) dikenal dengan *Google Spain Case*, 2014, antara seorang warga negara Spanyol bernama Mario Costeja Gonzalez dengan Google. Individu dapat mengajukan permintaan penghapusan secara lisan atau tertulis. Dalam menerapkan hak untuk menghapus data pribadi ada beberapa persyaratan[58] :

a) data pribadi tidak lagi diperlukan untuk tujuan yang awalnya pengumpulan ;
b) ketika pemilik data menarik kembali kesepakatan/persetujuan;
c) sudah tidak ada lagi kepentingan yang sah dari pengendali dan prosesor data pribadi;
d) data pribadi sudah tidak relevan lagi dengan kondisi saat ini;
e) data pribadi yang telah menjadi *public domain* atau *public interest* tidak dapat dimintakan untuk dihapus;
f) data pribadi tentang *public figure* seperti pejabat publik, orang-orang terkenal tidak bisa dimintakan penghapusan sepanjang informasi pribadinya diperlukan untuk kepentingan publik;
g) harus dilihat apakah informasi atas data pribadi sudah diperlukan untuk kepentingan arsip, sejarah dan penelitian;

[58] Sinta Dewi, hukum online

h) kewajiban penyelenggaran sistem elektronik untuk mengeluarkan *trasparency report* yang dimuat secara online sehingga masyarakat akan mengetahui bahwa pernyelenggara sistem elekronik telah memenuhi kewajibannya.

9. Akuntabilitas

Prinsip akuntabilitas berusaha menjamin penegakan Prinsip Pelindungan Data.

Prinsip ini mengharuskan mereka untuk bisa menunjukkan, dan selalu mendokumentasikan aktivitas mereka dalam pemrosesan data pribadi apakah mematuhi hukum pelindungan data.

Tujuan sederhananya bahwa setiap kegiatan dan hasil akhir dari kegiatan pemrosessan data terkait data pribadi seseorang dapat dipertanggungjawabkan.

Directive Art.6 (2) memberikan ketentuan bahwa:

> "Pengguna data harus memastikan kepatuhannya sesuai dengan Prinsip-prinsip Pelindungan Data."

Lihat lebih lanjut tentang prinsip akuntabilitas data di bawah GDPR, ketentuan Rec.85; Art.5 (2) memberikan pengaturan yang sama, yaitu:

> "Pengguna data bertanggung jawab atas, dan harus mampu menunjukkan, sesuai dengan Prinsip Pelindungan Data."

Di bawah GDPR, pengguna data berkewajiban untuk menunjukkan bahwa kegiatan pemrosesannya sesuai

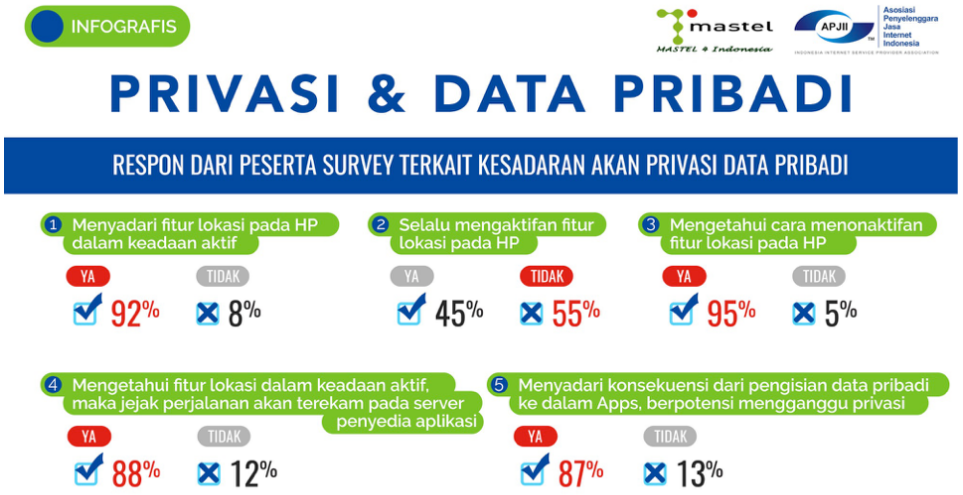
dengan Prinsip Perlindungan Data. Kewajiban ini diperluas pada (Art. 24 GDPR Responsibility of the controller), yang menetapkan kewajiban-kewajiban yang harus dipenuhi oleh pengguna data (*Controllers*).

C. Kajian terhadap Praktik Penyelenggaraan, Kondisi yang Ada, serta Permasalahan yang Dihadapi Masyarakat

1. Praktik Penyelenggaraan di Indonesia

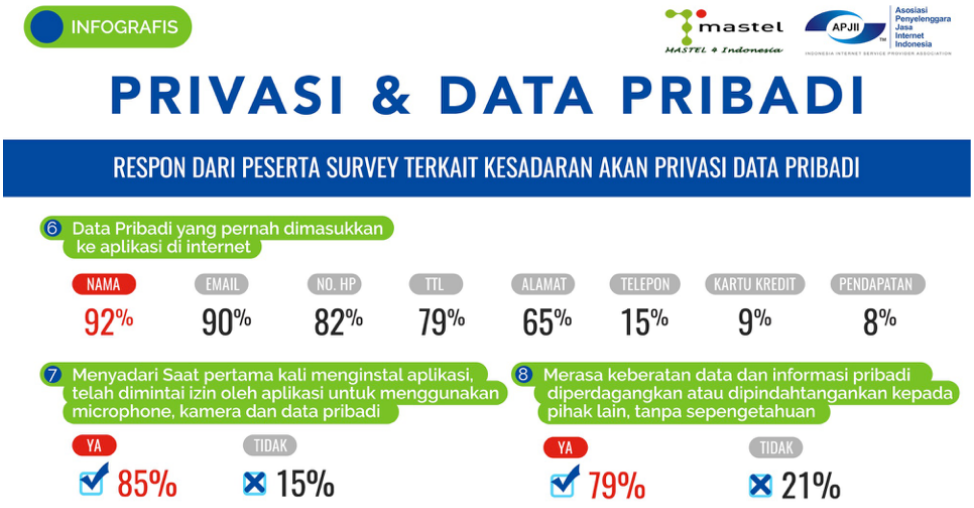
Pada rentang 20 Oktober s/d 20 November 2016, Masyarakat Telematika Indonesia (MASTEL) dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melakukan survei tentang Ekosistem DNA (Device, Network & Application) dan Awareness yang diikuti oleh 1.020 orang responden yang tersebar di berbagai daerah di Indonesia dengan komposisi 82% berumur 19-36 tahun, 15% berumur kurang dari 19 tahun dan 3% berumur diatas 37 tahun. Berdasarkan hasil survei dapat ditemukan bahwa *awareness* terhadap privasi dan data pribadi dari responden, yang didominasi generasi milenial, sudah cukup baik. Karena sebanyak 92% responden menyadari apabila fitur lokasi pada ponsel sedang dalam kondisi aktif dan 55% responden hanya mengaktifkan fitur update lokasi bila diperlukan.

Diagram 1.2
Aspek kesadaran responden terhadap fitur lokasi pada ponsel



Kemudian walau 95% mengetahui cara menonaktifkan fitur lokasi pada ponsel dan 88% responden mengetahui jejak perjalanan akan terekam pada server aplikasi apabila fitur lokasi diaktifkan, tetap saja 87% menyatakan siap menerima potensi terganggunya privasi sebagai konsekuensi karena data pribadinya sudah tersimpan di dalam aplikasi. Namun 79% responden dengan tegas menyatakan keberatan apabila informasi pribadinya diperdagangkan kepada pihak lain tanpa sepengetahuan dirinya.

Diagram 2.2
Aspek kesadaran responden terhadap data pribadi dan perijinan aplikasi



Selain itu terdapat 98% responden yang menghendaki adanya perlindungan atas data pribadi di internet dan setuju bila pemerintah mengatur perlindungan atas privasi dan data pribadi.

Diagram 3.2
Aspek kesadaran responden terhadap pentingnya perlindungan data pribadi

Kepopuleran media sosial dan situs pertemanan, misalnya situs Facebook dan Twitter telah mengakibatkan banyak terjadi kasus pelanggaran atas privasi. Data pribadi seseorang dapat dengan mudah diakses dan disebarluaskan tanpa sepengetahuan

pemilik data.[59] Masyarakat terjebak dengan *Terms of Use* dalam situs-situs tersebut sehingga tanpa sadar memberikan hak untuk menggunakan dan menyebarkan data pribadi pelanggan kepada pihak ketiga terutama untuk kepentingan pemasaran. Tak heran apabila di negara lain seperti Kanada, Inggris dan Amerika Serikat Facebook telah dituntut oleh masyarakat karena telah menyebarkan data pribadi pelanggan tanpa izin pemilik data.[60] Data statistik telah menunjukkan bahwa pengguna situs-situs tersebut bertambah contohnya hingga Oktober 2019 pengguna aktif bulanan Facebook mencapai 2,41 miliar, sedangkan situs Twitter yang muncul tahun 2006 telah memiliki pengguna aktif bulanan sebesar 330 juta.[61]

Potensi pelanggaran privasi di media sosial tidak hanya muncul karena praktik pihak swasta, lebih jauh lagi potensi pelanggaran privasi juga dapat muncul dari program yang digulirkan pemerintah dengan keterlibatan pihak swasta seperti program KTP elektronik (*e*-KTP) dan *e-health.* Padahal berdasarkan informasi kebocoran dari kawat Wikileaks, yang berisikan presentasi sebuah perusahaan Inggris ThorpeGlen (2008), metode pengamatan dapat dilakukan dengan menggunakan *e*-KTP.[62] Menurut informasi tersebut, dengan menggunakan perangkat *e*-KTP, warga negara dapat dilacak

---

[59] Lihat dalam http://watch.com/internetsehat, seorang mahasiswa yang aktif menggunakan facebook merasa dirugikan karena foto-foto pribadinya telah dicopy oleh orang yang tidak bertanggung jawab dan dimasukan ke dalam imageshack. US suatu situs foto gratis yang disebarkan secara internasional dan telah diubah fotonya sehingga telah mencemarkan nama baiknya. Diakses tanggal 1 Maret, 2009.

[60] *Canadian Internet Policy and Public Interest Clinic (CIPPIC*) v. Facebook, 2008 diakses dalam http://www.cippic.ca/uploads/newrelease, diakses 1 April, 2009. Lihat kasus Rahpael Vs Mathew Firsht yang diputuskan oleh *High Court London.*

[61] Hasil Survei *Statista* sampai dengan Oktober 2019, diakses di https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ pada 13 Januari 2020.

[62] Wahyudi Djafar dan Asep Komarudin, *Op.Cit.,* hlm. 23.

keberadaan dan aktivitasnya, sehingga dapat berpotensi terjadinya pelanggaran terhadap hak-hak warga negara.

Penyelenggaraan *e*-KTP di Indonesia juga menghadapi berbagai permasalahan. Menteri Dalam Negeri, Tjahjo Kumolo mengatakan bahwa saat itu terdapat beberapa permasalahan yang cukup serius dalam penyelenggaraan *e*-KTP, di antaranya adalah *server* yang digunakan *e*-KTP milik negara lain sehingga *data base* di dalamnya sangat rentan diakses oleh pihak tidak bertanggung jawab. Kemudian, *vendor* fisik *e*-KTP tidak menganut *open system* sehingga Kementerian Dalam Negeri tidak bisa mengutak-atik sistem tersebut. Kemudian terakhir, banyak terjadi kebocoran *data base*.[63] Dari beberapa permasalahan tersebut, terlihat bahwa perlindungan data pribadi milik masyarakat yang direkam dalam *e*-KTP sangat rentan dalam hal keamanannya.

Potensi pelanggaran dalam program *e*-KTP juga terjadi dalam program *e-health*. Di masa mendatang permasalahan pelindungan data pribadi akan menjadi bertambah rumit terutama di bidang pelayanan kesehatan dengan menerapkan *e-health* program yang sedang dirancang untuk diterapkan bersamaan dengan peluncuran *e*-KTP generasi kedua. *E*-KTP generasi kedua nantinya akan menggunakan *microchip* untuk menyimpan data pemiliknya termasuk daftar sejarah kesehatan masyarakat. KTP elektronik ini nantinya dapat merekam daftar dan sejarah kesehatan masyarakat, sehingga dapat memudahkan dokter yang memeriksa juga menguntungkan masyarakat pastinya. Namun demikian, program ini akan sangat

[63] Artikel Berita, Waspada Online, "e-ktp ternyata bermasalah", diakses melalui http://www.waspada.co.id/index.php?option=com _content&view =article&id=341427:e-ktp-ternyata-bermasalah&catid=77: fokuredaksi& Itemid=131, pada 15 November 2014 Pukul 13.00 WIB.

berbahaya apabila tidak didukung oleh regulasi yang memadai karena dikhawatirkan privasi atas data pribadi pasien tidak terlindungi sehingga dapat dikompilasi, diakses dan disebarluaskan kepada pihak lain untuk dapat dimanfaatkan secara ekonomi oleh industri penyedia jasa lainnya seperti industri obat-obatan, industri asuransi atau industri terkait lainnya. Dalam program BPJS (Badan Penyelenggara Jaminan Kesehatan) yang kemudian diintegrasikan dengan Program ASKES (Asuransi Kesehatan) yang mencakup data pribadi kesehatan seluruh Pegawai Negeri Sipil, Pemerintah memiliki data pribadi kesehatan pasien dan masyarakat tidak mengetahui bagaimana penyelenggara program BPJS akan menjaga kerahasiaan data kesehatan pasien yang merupakan data sangat sensitif.

Potensi pelanggaran secara online seperti yang terjadi dalam program *e-health* di atas ternyata terdapat juga dalam tatanan *off-line*, atau yang tidak menggunakan teknologi informasi. Pelanggaran secara *off-line* tersebut salah satunya adalah penyalahgunaan oleh perusahaan terhadap data pribadi pelanggan yang diserahkan sebagai persyaratan transaksi bisnis, ditambah munculnya potensi terjadinya kejahatan yang bermula dari pencarian data pribadi seseorang serta penghilangan identitas atas data dari pelaku kejahatan.

Potensi ancaman lainnya muncul dari fungsi *search engines* (mesin pencari) di internet. Mesin pencari sudah sejak lama digunakan untuk membantu para pengguna internet dengan memberikan informasi seluas-luasnya mengenai data yang tersedia di dalam jaringan. Mesin pencari di internet sering memperluas layanan mereka dengan mencakup layanan *email*, penyimpanan foto atau bahkan penyimpanan data. Dengan

demikian terdapat ancaman bahwa layanan tambahan tersebut memungkinkan mesin pencari untuk menyebrang informasi yang diberikan pengguna saat registrasi penggunaan layanan.[64]

Salah satu teknologi komunikasi dan informasi yang berkembang pesat saat ini adalah teknologi komputasi awan atau *cloud computing*. Komputasi awan adalah gabungan pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan). Saat ini, beberapa perusahaan teknologi informasi dan komunikasi terkemuka mengeluarkan aplikasi dalam menyediakan ruang penyimpanan data pengguna seperti Evernote, Dropbox, Google Drive, Sky Drive, Youtube, Scribd, iCloud, dan lain sebagainya.

Perkembangan pemanfaatan teknologi tersebut menimbulkan potensi pelanggaran serius. Contoh pelanggaran terbaru adalah bobolnya data pengguna iCloud (komputasi awan yang disediakan oleh Apple) yang kemudian menyebar di beberapa media massa. Kasus ini mendapat banyak perhatian publik karena pemilik data merupakan beberapa selebritis terkenal Hollywood, seperti Jennifer Lawrence, Jenny McCarthy, Rihanna, Kate Upton, Mary Elizabeth Winstead, Kristen Dunst, Ariana Grande, dan Victoria Justice.[65]

Jumlah pengguna iCloud yang relatif banyak berpotensi berkembang pesat melihat tren penggunaan Apple dewasa ini di seluruh dunia termasuk di Indonesia. Sehingga potensi pelanggaran privasi saat ini di bidang komputasi awan sangat besar. Meningkatnya jumlah data yang tersimpan di 'awan' dalam jaringan (*cloud*), termasuk perkembangan yang relatif baru.

---

[64] Wahyudi Djafar dan Asep Komarudin, *Op. Cit.,* hlm. 12.

[65] MerdekaFM, iCloud Dibobol Ratusan Foto Pribadi Celebs Di Expos, edisi 5 September 2014, diakses melalui: http://www.merdekafm.com /posting/read/17/iCloud_Dibobol_Ratusan_Foto_Pribadi_Celebs_Di_Expos, pada tanggal 11 September 2014 Pukul 09.30 WIB.

Ketika data pribadi ditransmisikan ke internet, muncul ancaman risiko karena individu kehilangan kontrol atas data tersebut. Setelah data tersimpan di *cloud*, risiko lain muncul dari penyedia layanan *cloud* karena penyedia layanan *cloud* memungkinkan untuk memindahkan informasi atau data dari satu yurisdiksi ke yurisdiksi lainnya atau dari operator ke operator lainnya, atau dari satu mesin ke mesin lainnya, tanpa pemberitahuan kepada pemilik data.[66]

Dengan mempertimbangkan semua ancaman dan potensi pelanggaran yang telah dijelaskan di atas, pengaturan pelindungan data pribadi dimaksudkan untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. Pengaturan ini akan melindungi data pribadi individu terhadap penyalahgunaan pada saat data tersebut memiliki nilai tinggi untuk kepentingan bisnis, yang pengumpulan serta pengolahannya menjadi kian mudah dengan perkembangan teknologi informasi komunikasi. Perkembangan pengaturan terhadap pelindungan data pribadi secara umum akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai pelindungan data pribadi. Hal ini akan memperkuat dan memperkokoh posisi Indonesia sebagai pusat bisnis dan investasi tepercaya, yang merupakan suatu strategi kunci dalam perkembangan ekonomi Indonesia.

Bagi kepentingan konsumen, kebutuhan akan pelindungan data pribadi konsumen terutama di era di mana data pribadi menjadi sangat berharga untuk kepentingan bisnis, menimbulkan kekhawatiran bahwa data pribadi konsumen dijual atau digunakan tanpa persetujuan konsumen sebagaimana

[66] Wahyudi Djafar dan Asep Komarudin, *Loc. Cit.*

contoh pelanggaran yang telah diuraikan sebelumnya. Oleh karena itu pelindungan data pribadi yang bersifat khusus dalam suatu undang-undang sangat diperlukan guna memastikan bahwa data pribadi konsumen dilindungi dengan baik.

Bagi perkembangan ekonomi, pelindungan data pribadi yang bersifat khusus akan memperkuat posisi Indonesia sebagai pusat bisnis dan investasi tepercaya dan menciptakan lingkungan yang kondusif untuk pertumbuhan manajemen data global dan industri pengolahan data seperti komputasi awan untuk berkembang di Indonesia.

Ketiadaan hukum mengenai pelindungan data pribadi yang bersifat umum di Indonesia dapat dilihat sebagai suatu kelemahan yang menyebabkan beberapa perusahaan tidak memilih Indonesia sebagai lokasi untuk pusat penyimpanan datanya. Padahal, perkembangan pengaturan pelindungan data pribadi akan mendukung pembangunan masa depan Indonesia sebagai pusat data global.

Pengaturan tentang data pribadi sangat diperlukan karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman dan keamanan data pribadi dan secara umum pengaturan data pribadi adalah untuk mencari keseimbangan antara kebutuhan akan pelindungan data pribadi individu dengan kebutuhan pemerintah dan pelaku bisnis untuk memperoleh dan memproses data pribadi untuk keperluan yang wajar dan sah.

Saat ini, Indonesia belum memiliki undang-undang mengenai pelindungan data pribadi secara khusus. Untuk itu, dengan berbagai macam permasalahan di atas pemerintah Indonesia dituntut untuk melindungi masyarakat dan mengatur masalah privasi atas data pribadi dan menyiapkan berbagai

bentuk perlindungan hukum. Selain itu, dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional 2005-2025 juga telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus meningkatkan pemanfaatan ilmu pengetahuan dan teknologi. Salah satunya melalui peraturan yang terkait dengan privasi.[67]

2. Praktik Penyelenggaraan di Negara Lain

a. Pelindungan Privasi atas Data Pribadi dalam Perjanjian Internasional

Beberapa instrumen hukum multilateral yang mengatur prinsip-prinsip privasi data yang diakui secara internasional telah menjadikan fondasi bagi hukum pelindungan data nasional yang modern. Beberapa di antara instrumen tersebut berkembang dengan pengaturan data privasi yang spesifik, dan beberapa instrumen lain mengatur mengenai aturan umum yang mencakup beberapa masalah termasuk di antaranya privasi. Berikut berbagai perjanjian internasional yang melindungi privasi:

1) *Organization for Economic Co-operation and Development* (OECD) *Privacy Guidelines*

Kebanyakan dari rezim pelindungan data terinspirasi dari OECD's 1980 tentang Pedoman Privasi ("*Privacy Guidelines*"). Pedoman tersebut berlaku bagi semua data pribadi yang didefinisikan sebagai "semua informasi yang berkaitan kepada individu yang teridentifikasi dan yang dapat diidentifikasi ("*identifiable*")." Pedoman-pedoman tersebut tidak

[67] Rencana Pembangunan Jangka Panjang 2005-2025, hlm. 108.

mengikat secara hukum namun telah diakui sejak lama sebagai pernyataan dari norma-norma yang membangun data privasi pribadi dan mengarahkan anggota-anggota OECD dan organisasi-organisasi privat dalam membentuk kebijakan mereka.

Pedoman ini mendukung pengumpulan data-data pribadi yang didapatkan secara sah dan sesuai hukum dan data tersebut akurat, mutakhir dan relevan serta diperlukan sesuai dengan tujuan pengumpulan data tersebut (Bagian II Prinsip-Prinsip Dasar). Informasi pribadi harus dilindungi dengan pengamanan yang sesuai dan tidak boleh dibuka atau tersedia bagi publik untuk tujuan selain dari alasan awal mengapa data tersebut dikumpulkan, kecuali dengan persetujuan dari pemilik data tersebut atau dari otoritas hukum.

Pedoman-pedoman ini menjelaskan bahwa prinsip-prinsip di bawah ini harus dilaksanakan ketika melakukan pemrosesan data pribadi:

a) Pembatasan pengumpulan: harus terdapat suatu batasan dalam hal pengumpulan data pribadi. Data pribadi harus didapatkan dengan menggunakan cara-cara yang sah secara hukum, adil, dan dengan pengetahuan serta persetujuan pemilik data.
b) Kualitas data: data pribadi harus sesuai dengan tujuan awal pengumpulan data, akurat, lengkap serta mutakhir.
c) Spesifikasi tujuan: tujuan pengumpulan data harus spesifik dan setiap penggunaan selanjutnya dari data tersebut harus terbatas hanya sesuai dengan tujuan tersebut.

d) Pembatasan pengungkapan: data tidak boleh dibuka, diungkapkan, tersedia untuk umum atau digunakan untuk tujuan di luar tujuan yang spesifik kecuali atas persetujuan pemilik data atau persetujuan otoritas hukum.
e) Langkah-langkah pengamanan: data yang disimpan harus mendapatkan pengamanan yang memadai agar dapat terlindungi dari kehilangan, kerusakan, penggunaan, perubahan atau pengungkapan yang tidak sah.
f) Keterbukaan: harus ada terdapat suatu kebijakan umum pemrosesan data yang dibuka kepada masyarakat terkait prosedur pemrosesan data pribadi oleh pengendali data pribadi.
g) Partisipasi individu: individu harus memiliki hak untuk mendapatkan informasi tentang data pribadinya, termasuk hak untuk menghapus dan mengoreksi data yang dimiliki tidak akurat.
h) Pertanggungjawaban: pengendali data bertanggung jawab untuk mengelola data pribadi sesuai dengan prinsip-prinsip pemrosesan data pribadi.

Banyak perusahaan multinasional mematuhi prinsip-prinsip pelindungan data sebagai bentuk penjaminan kepatuhan minimum dalam suatu yurisdiksi di mana pelindungan data tidak diatur secara ketat atau bahkan tidak diatur sama sekali. Walaupun dianggap sebagai sebuah fondasi, namun sayangnya prinsip-prinsip tersebut tidak cukup kuat karena hanya bersifat *self regulation* dan tidak menyediakan solusi praktis untuk penegakan hukum bagi negara-negara yang

melanggarnya. Tanpa sistem *check and balances* yang menjamin kepatuhan terhadap prinsip tersebut, sering kali pelindungan data seseorang hanya dicantumkan dalam hukum kontrak yang merupakan sebuah area di mana orang-orang pada umumnya jarang untuk memperkarakannya.

2) Perbaikan OECD *Privacy Guidelines*

Negara-negara anggota *European Union* (EU) dan *European Commission* (EC) telah memberikan tekanan untuk segera dilakukannya perbaikan terhadap OECD *Privacy Guidelines*. Perbaikan tersebut akan membawa pedoman tersebut mendekati standar dari EU *Data Protection* dan mengisi kekosongan dalam area-area mengenai transfer informasi pribadi. Peninjauan *Privacy Guidelines* sedang dilakukan OECD *Working Party on Information Security and Privacy* (WPISP).

Sebagai langkah pertama dari review tersebut, anggota OECD telah setuju mengenai Kerangka Acuan/*Term of Reference* (ToR) sebagai kerangka kerja (*roadmap*) untuk melakukan peninjauan. Seperti tercantum dalam ToR tersebut, WPISP telah memanggil para pemangku kepentingan, kelompok ahli dari pemerintahan, otoritas penegakan privasi, akademisi, pengusaha, organisasi kemasyarakatan dan komunitas pengguna internet. Kelompok ahli diketuai oleh Jennifer Stoddart, yang merupakan *Privacy Commissioner* dari Canada dan telah mendiskusikan beberapa tema di antaranya:

i). peran dan tanggung jawab dari aktor-aktor kunci;

ii). pembatasan geografis dalam hal arus informasi yang melewati batas negara;

iii). langkah implementasi dan penegakan yang proaktif.

Kelompok para ahli membuat rekomendasi sebagai pertimbangan bagi anggota OECD pada bulan November 2012, dimana rekomendasi tersebut sekarang ini sedang dipertimbangkan. Rekomendasi tersebut mencakup di antaranya:

i). pengantar konsep dari program manajemen privasi yang harus dipelihara oleh semua pengatur data dikarenakan semua data pribadi berada di bawah kendali mereka. Pengantar tersebut tidak hanya ditujukan bagi pengoperasian pengaturan data saja namun juga semua bentuk pengoperasian yang memungkinkan para pengatur data tersebut bertanggung jawab;

ii). syarat-syarat bahwa pengatur data harus memberitahukan kepada otoritas yang berwenang ketika terjadi pelanggaran keamanan yang menyangkut data pribadi, dan harus memberitahukan kepada orang yang bersangkutan ketika pelanggaran keamanan tersebut dapat membahayakan mereka;

iii). definisi dan syarat yang jelas mengenai otoritas penegakan privasi; dan

iv). pemutakhiran konsep dan pengaturan mengenai arus informasi yang melewati batas negara.

3) Dewan Eropa/ *Council of Europe* (CoE)

CoE atau Dewan Eropa telah mengadopsi *European Convention for the Protection of Human Rights* tahun 1950 Pasal 8 menyatakan bahwa: "*everyone has the right to respect for his private and family life, his home and his correspondence*".[68]

Hak tersebut diartikan secara luas dan dengan istilah teknologi yang netral sehingga berlaku bagi pasar elektronik dan lingkungan online. Kasus-kasus dalam *European Court of Human Rights* (ECHR) menegaskan bahwa Pasal 8 mengatur mengenai pelindungan penting bagi informasi pribadi. Sebagai contoh, dalam kasus M.S.v. Sweden ECHR menyatakan bahwa "pelindungan data pribadi khususnya data medis adalah penting bagi orang-orang untuk dapat menikmati hak-hak mereka khususnya mengenai penghormatan terhadap kehidupan privasi dan keluarga seperti yang dijamin dalam Pasal 8.[69] Dalam kasus Malone v. United Kingdom, ECHR menjelaskan bahwa Pasal 8 mencakup tidak hanya percakapan telepon namun juga perjalanan informasi seperti nomor telepon.[70]

Seiring dengan perkembangan teknologi yang sangat cepat dan perkembangan fasilitas tempat penyimpanan elektronik, CoE merasa bahwa ECHR perlu didukung oleh hukum yang lebih modern dan lebih rinci untuk mengatasi pengumpulan dan pengolahan data pribadi yang dipandangnya tidak adil.[71] Sebagai hasilnya, di tahun

---

[68] European Convention for the Protection of Human Rights, Nov. 4, 1950, E.T.S. 5, dapat diakses pada http://conventions.coe.int/treaty/en/Treaties /Html/005.htm, diakses pada tanggal 4 November 2014 Pukul 10.00 WIB.
[69] M.S. v. Sweden, 27 August 1997, reports 1997-IV
[70] Malone v. United Kingdom, 20 August 1984, 82 Eur. Ct. H. R. (ser A).
[71] Mark F. Kightlinger, E. Jason Albert, and Daniel P. Cooper, *Op.Cit.*

1981, CoE mengadopsi *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (*DP Convention*).[72] Konvensi ini berlaku bagi pengolahan otomatis data pribadi baik dalam sektor privat maupun publik. "Data Pribadi" berarti informasi-informasi yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi (pemilik data).

Selain keberlakuan yang luas dari *DP Convention*, yang mencakup semua jenis dari pengaturan data atau pengguna termasuk orang perorangan atau perusahaan, otoritas publik, lembaga atau badan yang berwenang untuk menentukan tujuan dari data pribadi, ada banyak cara untuk membedakan dari aturan-aturan untuk data yang tidak diolah secara otomatis dan data yang berhubungan dengan suatu badan misalnya organisasi. (Pasal 3.2-3.6). Lebih lanjut, negara-negara boleh mengurangi kewajibannya yang berhubungan dengan pengolahan data yang adil dan sah secara hukum dengan melarang pengolahan otomatis terhadap data dengan kategori khusus yang menampakan ras, opini politis, kepercayaan dan agama, kesehatan dan kehidupan seksual dan adanya pengamanan tambahan (Pasal 5, Pasal 6, dan Pasal 8). Hal ini diperbolehkan ketika pengurangan kewajiban tersebut didasarkan pada hukum nasional dan dianggap sebagai langkah yang perlu dalam negara demokrasi untuk melindungi keamanan negara, keamanan publik, kepentingan keuangan dari negara atau

[72] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981 (selanjutnya disebut DP Convention).

mencegah terjadinya tindak pidana, pelindungan pemilik data atau hak dan kebebasan orang lain.

> *provided for by national law and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others. (Pasal 9)*

Dalam menanggapi kritikan terhadap adanya kekosongan hukum, DP *Convention* dilengkapi dengan Protokol Tambahan tahun 2001.[73] mengenai otoritas pengawasan dan arus data yang melewati wilayah negara. Pada bulan Maret 2010, CoE selanjutnya mulai melakukan modernisasi terhadap DP Convention, untuk menghadapi tantangan-tantangan terhadap privasi sebagai akibat dari penggunaan informasi baru dan teknologi komunikasi dan juga memperkuat mekanisme kelanjutan dari Konvensi.[74] Konsultasi publik telah diluncurkan pada tahun 2011.[75]

DP Convention sejauh ini telah digantikan dengan EU *Data Protection Directive*. Bagi kebanyakan anggota EU, *Directive* ini merupakan instrumen terbaru walaupun DP *Convention* masih menjadi konvensi yang penting bagi banyak negara yang tidak terikat dengan peraturan nasional untuk melindungi privasi. Sekarang ini terdapat

---

[73] Lihat: http://conventions.coe.int/Treaty /EN/Treaties /Html/181.htm, diakses pada 15 Oktober 2014 Pukul 11.00 WIB.

[74] http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/CoE_response_to_privacy_challenges_Modernisation_of_Convention_108_EN_May_2011.pdf, diakses pada tanggal 15 Oktober 2014 Pukul 13.40 WIB.

[75] *Compilation of replies to CoE's public consultation on the DP Convention modernization:* http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD- BUR_2011_01_%20prov_MOS_12_05_11_PUBLIC.pdf, diakses pada tanggal 15 Oktober 2014 Pukul 13.30 WIB.

gerakan untuk mengajak non negara Eropa untuk melakukan aksesi terhadap *DP Convention*.

4) EU Data Protection Directive

The European Union DP Directive (*Directive*) diperkenalkan tahun 1995 dengan tujuan untuk mengharmonisasi peraturan nasional di antara negara-negara anggota EU. *Directive* dianggap sebagai satu di antara rezim yang paling kuat, namun demikian bukan berarti tanpa kekurangan karena sekarang ini *Directive* tersebut telah digantikan oleh General Data Protection Regulation yang efektif berlaku pada Mei 2018.

Tujuan dari *Directive* adalah untuk melindungi privasi individu khususnya mengenai pengolahan data pribadi. *Directive* ini mencakup semua data pribadi yakni informasi mengenai individu yang teridentifikasi dan yang dapat diidentifikasi, atau "pemilik data". *Directive* ini memberikan kewajiban langsung kepada orang atau organisasi yang menentukan tujuan dan langkah-langkah pengolahan data pribadi atau yang biasa dikenal dengan "pengatur data".

Data *Protection Directive* berlaku bagi organisasi publik dan privat, namun untuk badan publik berlaku beberapa pembebasan kewajiban (*exemption*) yang membatasi akibat dari Directive tersebut terhadap mereka. Directive juga memberikan pembatasan terhadap pengiriman informasi pribadi ke luar negara non-EU yang tidak memenuhi tingkat perlindungan yang pantas (Pasal 25). Tingkat kepantasan perlindungan dinilai berdasarkan semua keadaan di sekitar pengoperasian pengiriman data. Keadaan tersebut di antaranya adalah sifat dari data

tersebut, tujuan, dan durasi dari pengolahan yang diajukan, negara tujuan akhir dan hukum yang berlaku di negara tersebut serta aturan-aturan profesional dan langkah-langkah pengamanan yang dipatuhi negara tersebut. Pasal 26 memungkinkan syarat-syarat tersebut dituangkan dalam peraturan-peraturan kontraktual. Beberapa kelompok perusahaan multinasional juga mengambil manfaat dari proses *Binding Corporate Rules* (BCR) bagi pengiriman antar kelompok. Sistem BCR dikembangkan oleh regulator EU dalam usaha untuk membuat proses pematuhan menjadi semakin efisien, sebagai alternatif model kontrak dan/atau EU-US *Safe Harbor Agreement*. Kompleksitas, harga yang mahal dan panjangnya prosedur persetujuan telah mempengaruhi penggunaan praktis dari BCR dan hanya sedikit perusahaan yang telah sukses melalui itu.

5) GDPR

General Data Protection Regulation (GDPR) merupakan peraturan Uni Eropa (UE) tentang pelindungan data individu yang tinggal di wilayah UE dan *European Economic Area* (EEA). GDPR merupakan peraturan yang mengganti keberadaan peraturan *Data Protection Directive* 95/46/EC.[38] GDPR mulai berlaku di UE pada 25 Mei 2018 lalu dan resmi menggantikan *General Data Protection Directive* (GDPD) di UE tahun 1995. Peraturan ini bertujuan terutama agar masyarakat memiliki kontrol lebih atas data pribadi mereka dan dapat

melindungi kerahasiaan data masyarakat Uni Eropa, misal dari permasalahan kebocoran data.[76]

Dalam Article 3 GDPR, disebutkan bahwa GDPR memiliki jangkauan keberlakuan ekstrateritorial, yang mencakup sebagai berikut:

1. kegiatan pemrosesan data pribadi yang dilakukan oleh pengendali atau prosesor yang didirikan di Uni Eropa, terlepas dari apakah pemrosesan data pribadi tersebut dilakukan di wilayah Uni Eropa;
2. kegiatan pemrosesan data pribadi pemilik data pribadi yang berada di Uni Eropa oleh pengendali atau prosesor yang tidak didirikan di Uni Eropa, dimana kegiatan pemrosesan tersebut terkait dengan:
    a. penawaran barang atau jasa, terlepas dari ada tidaknya pembayaran kepada pemilik data di Uni Eropa;
    b. pemantauan perilaku yang dilakukan di dalam wilayah Uni Eropa;
3. kegiatan pemrosesan data pribadi yang dilakukan oleh pengendali yang tidak didirikan di Uni Eropa, namun di tempat dimana hukum negara anggota Uni Eropa berlaku berdasarkan hukum internasional.

Dalam Article 6 GDPR, diatur bahwa pemrosesan data pribadi harus dilakukan secara sah, dengan memenuhi satu atau lebih persyaratan berikut:

1. terdapat persetujuan pemrosesan data pribadi dari

76

pemilik data untuk satu atau lebih tujuan;

2. pemenuhan kewajiban perjanjian dalam hal pemilik data merupakan salah satu pihak atau untuk memenuhi permintaan pemilik data pada saat akan melakukan perjanjian;
3. pemenuhan kewajiban hukum, dimana pengendali merupakan subyeknya;
4. pemenuhan pelindungan kepentingan yang sah (vital interest) pemilik data atau individu lain;
5. pelaksanaan pelayanan publik untuk kepentingan umum atau pelaksanaan kewenangan pengendali data; atau
6. pemenuhan kepentingan yang sah yang dimiliki oleh pengendali atau pihak ketiga, kecuali apabila kepentingan tersebut dikesampingkan oleh kepentikan atau hak dasar dan kebebasan pemilik data yang memerlukan pelindungan data pribadi, utamanya apabila pemilik data adalah anak.

Lebih lanjut, GDPR mengatur hak-hak pemilik data yang komprehensif. Dalam Chapter 6, Article 12 sampai Article 22 GDPR, sebagai berikut:

1. hak atas informasi yang jelas (*right to be informed*);
2. hak akses (*right to access*);
3. hak atas portabilitas data (*right to data portability*);
4. hak atas perbaikan data (*right to rectification)*;
5. hak atas penghapusan data (hak untuk dilupakan) (*right to erasure (right to be forgotten*);
6. hak atas pembatasan pemrosesan data pribadi (*right to restriction of processing*);

7. hak untuk mengajukan keberatan (*right to object*); dan
8. hak terkait tindakan pengambilan keputusan individual yang dibuat secara otomatis (*automated individual decision-making),* termasuk pemrofilan.

Dalam Article 23 GDPR, hak-hak pemilik data tersebut dapat dikecualikan untuk kepentingan berikut:

1. kepentingan nasional;
2. pertahanan;
3. kepentingan publik;
4. pencegahan, penyelidikan, deteksi, atau penuntutan tindak pidana, atau pelaksanaan hukuman pidana;
5. tujuan penting lain dari kepentingan umum Uni Eropa ataupun negara anggota;
6. pelindungan kebebasan peradilan dan proses peradilan;
7. pencegahan, penyelidikan, deteksi, dan penuntutan pelanggaran etik profesi yang diatur;
8. pelaksanaan fungsi pengawasan, inspeksi atau regulasi;
9. pelindungan pemilik data atau hak dan kebebasan orang lain; dan
10. pelaksanaan gugatan perdata.

Berdasarkan Chapter 5, Article 45-50 GDPR, transfer data ke luar wilayah Uni Eropa harus memenuhi satu atau lebih persyaratan berikut:

1. adanya keputusan dari komisi bahwa negara tempat kedudukan pengendali data atau organisasi

internasional yang menerima transfer memiliki tingkat pelindungan data pribadi yang setara atau lebih tinggi;

2. adanya *appropriate safeguard,* antara lain dalam bentuk:
    a. instrument hukum yang mengikat dan dapat dilaksanakan antar otoritas atau badan publik;
    b. peraturan perusahaan yang mengikat (*binding corporate rules*);
    c. klausula standar pelindungan data pribadi;
    d. kode etik dan mekanisme sertifikasi yang telah disetujui; atau
    e. perjanjian internasional.

6) Amerika Serikat

Amerika Serikat tidak memiliki suatu hukum pelindungan data yang terunifikasi, dan hukum pelindungan datanya terpisah dalam ratusan hukum tingkat federal dan negara bagian. Pada tingkat federal, Federal Trade Commission Act (15 U.S. Code §41 *et. seq.*) yang memberikan kewenangan secara luas kepada US Federal Trade Commission (FTC) untuk melakukan penegakan hukum untuk melindungi konsumen dari praktik-praktik yang tidak adil maupun penipuan, serta untuk menegakkan hukum federal terkait privasi dan pelindungan data. FTC telah mengambil posisi bahwa "tindakan penipuan ("*deceptive practices*") juga termasuk kegagalan perusahaan untuk patuh pada komitmen privasinya yang telah dipublikasikan, dan kegagalan untuk menyediakan pengamanan atas informasi personal

yang layak, selain juga penggunaan iklan ataupun metode pemasaran yang menipu.[77]

Hukum pelindungan data di Amerika Serikat kebanyakan bersifat sektoral maupun berfokus pada tipe data tertentu. *Driver's Privacy Protection Act 1994 (18 U.S. Code § 2721 et. seq.)* mengatur mengenai privasi dan pembukaan informasi pribadi yang dikumpulkan oleh Departemen Kendaraan Bermotor negara-negara bagian Amerika Serikat. Pelindungan data pribadi anak diatur dalam *Children's Online Privacy Protection Act (15 U.S. Code §2720 et.seq*), yang melarang pemrosesan daring data terkait anak di bawah 13 tahun, dan mensyaratkan publikasi pemberitahuan privasi dan pengumpulan persetujuan orang tua yang telah diverifikasi ketika terdapat pengumpulan data mengenai anak. Lebih lanjut, pemerintah federal dan sebagian besar negara bagian telah mengundangkan legislasi yang mempidanakan perekaman komunikasi tanpa persetujuan salah satu atau seluruh pihak yang terkait.[78]

Beberapa hukum negara bagian juga dapat menerapkan pembatasan-pembatasan maupun kewajiban-kewajiban bagi pelaku usaha terkait dengan pengumpulan, penggunaan, pembukaan, pengamanan, ataupun retensi data yang berkategori khusus, seperti data biometrik, riwayat medis, nomor SIM, nomor jaminan sosial, riwayat finansial, riwayat pidana, dan sebagainya. Lebih lanjut, seluruh negara bagian di AS telah

[77] Steven Chabinsky and F. Paul Pittman, "USA: Data Protection 2019", http:// https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa/, diakses 14 Januari 2020.
[78] *Ibid.*

mengadopsi kebijakan kewajiban pemberitahuan kegagalan pelindungan data yang perlaku bagi data pribadi kategori tertentu warganya.[79]

Pada 1 Januari 2020 yang lalu, California Consumer Privacy Act (California Civil Code §1798.100-§1798.199) (CCPA) yang diundangkan oleh negara bagian California pada 2018 yang lalu. Menurut American Bar Association, CCPA merupakan hukum terkait privasi terlengkap di Amerika Serikat hingga saat ini.[80]

CCPA berlaku bagi pelaku usaha yang memenuhi ketentuan sebagai berikut:

1. memiliki keuntungan tahunan kotor sebesar $25 juta;
2. membeli, menjual, menerima, atau membagi untuk kepentingan komersial data pribadi dari 50.000 atau lebih konsumen, rumah tangga, atau perangkat; atau
3. memperoleh 50% atau lebih keuntungan tahunannya dari penjualan data pribadi konsumen.

Perusahaan induk ataupun anak perusahaan dari perusahaan yang memenuhi kualifikasi di atas juga harus tunduk pada CCPA.

Dalam CCPA, subyek pelindungan data adalah "consumers", yang melingkupi penduduk negara California. Melalui CCPA ini, pemilik data memiliki hak untuk mendapatkan salinan data yang diproses perusahaan, dan perusahaan wajib memenuhi permintaan tersebut dalam waktu 45 hari. Pemilik data

[79] *Ibid.*
[80] Elaine F. Harwell, "What Business Need to Know About the California Consumer Privacy Act", https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/, diakses 14 Januari 2020

hanya dapat melakukan permintaan informasi tersebut maksimal dua kali setahun, dan untuk jangka waktu 12 bulan kebelakang. Kegagalan perusahaan pemroses data untuk memenuhi permintaan pelaksanaan hak tersebut diancam dengan denda sejumlah $2.500 hingga $7.500.[81]

b. Perbandingan Pengaturan Data Pribadi di Hongkong, Singapura, Malaysia, dan Korea Selatan

1). Prinsip Pelindungan Data Pribadi

Personal Data Privacy Ordinance of 1995 (PDPO) Hong Kong merupakan peraturan perundang-undangan yang pertama kali mengatur masalah privasi data secara komprehensif, di Asia. Selama 18 (delapan belas) tahun diimplementasikan oleh *Privacy Commisioner for Personal Data* (PCPD) yaitu otoritas di Hongkong yang menangani masalah privasi data. Prinsip perlindungan privasi data yang terkandung dalam PDPO tidak dapat sepenuhnya dilaksanakan. Oleh karena itu, dilakukan perubahan besar terhadap PDPO pada tahun 2012.[82]

i). Prinsip Pelindungan data Pribadi di Hongkong[83]

(a) Batasan Pengumpulan Data Pribadi

Pengumpulan data pribadi terbatas pada pengumpulan data pribadi secara sah untuk tujuan yang secara langsung berhubungan dengan fungsi dari pengumpul. Data yang dikumpulkan harus

[81] Kari Paul, "California's groundbreaking privacy law takes effect in January. What does it do?", https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do, diakses pada 14 Januari 2020.

[82] Greeneaf, Graham, *Asian Data Privacy Laws - Trade and Human Rights Perspectives*, Oxford University Press, New York, 2014, hlm. 80.

[83] *Ibid,* hlm. 92-100.

cukup, namun pengumpulan data pribadi tidak boleh melebihi tujuan pengumpulan data tersebut di atas.[84]

(b) Penggunaan dan Pengungkapan Data Pribadi

Prinsip ini membatasi pengungkapan data pribadi hanya untuk atau secara langsung berhubungan dengan tujuan awal pengumpulan data pribadi tersebut, atau apabila subjek data menyatakan persetujuan.

(c) Kewajiban Kualitas Data dan Pemberian Saran kepada Pihak Ketiga

Prinsip ini mewajibkan seluruh langkah yang mungkin diambil untuk menjamin akurasi data pribadi (dengan mempertimbangkan tujuan penggunaan dan setiap tujuan yang langsung berhubungan), dan untuk menghapus atau tidak menggunakan data yang tidak akurat. Data yang tidak akurat didefinisikan sebagai data yang tidak benar, menyesatkan, tidak lengkap, atau tidak mutakhir.[85] Penggunaan data yang tidak akurat tidak dengan sendirinya menjadi suatu pelanggaran apabila seluruh langkah yang mungkin untuk menghindari tidak akuratnya data tersebut telah diambil. Komisioner dapat mengeluarkan "*enforcement notice*" (surat teguran), yang meminta perbaikan-perbaikan secara sistematis apabila langkah-langkah penjaminan akurasi data tidak dilakukan. Subjek data dapat

[84] Shchedule 1, Data Protection Principle 1 (1).
[85] Seksi 2 (1) Personal Data Protection Ordonance (PDPO) Hongkong.

meminta untuk mengoreksi informasi yang tidak akurat.[86] Ketika pihak ketiga menerima data yang tidak akurat, "*data user*" harus, apabila memungkinkan menginformasikan pihak ketiga tersebut agar subjek data dapat memperbaiki data.

(d) Penghapusan dan Pemusnahan Data Pribadi

Berdasarkan prinsip ini, data pribadi tidak boleh disimpan lebih lama dari jangka waktu yang diperlukan untuk pemenuhan tujuan (termasuk setiap tujuan yang langsung berhubungan) untuk tujuan tersebut data digunakan atau akan digunakan di masa depan.

(e) Kewajiban Keamanan Data

Berdasarkan prinsip ini, pengendali data pribadi wajib melakukan setiap langkah yang memungkinkan untuk melindungi data pribadi dari akses yang tidak disengaja, atau pemrosesan, penghapusan, penghilangan, dan penggunaan tidak sah (tanpa hak). Tindakan-tindakan pengamanan data ini memperhatikan berbagai faktor, misalnya jenis data, lokasi penyimpanan fisik data, dan potensi-potensi bahaya terhadap data. PDPO tidak memberikan pengaturan khusus terhadap data sensitif, tidak seperti hukum di Eropa.

(f) Keterbukaan mengenai praktik-praktik

"*Data User*" harus mengambil langkah-langkah untuk menjamin bahwa setiap orang (tidak hanya subjek data) dapat menentukan kebijakan dan

[86] Seksi 22 Personal Data Protection Ordonance (PDPO) Hongkong.

praktik mengenai data pribadi, jenis data pribadi yang disimpan "Data User", dan tujuan utama penggunaannya. Prinsip ini diambil dari *OECD "openess" principle*. Prinsip ini digunakan oleh Komisioner untuk mewajibkan organisasi-organisasi dan badan hukum di Hong Kong memublikasikan Kebijakan Privasi (*Privacy Policy Statement*) mereka ke publik. Ketiadaan Publikasi kebijakan privasi di perusahaan-perusahaan ataupun organisasi merupakan pelanggaran dari prinsip ini dan Komisioner di Hong Kong dapat melayangkan surat teguran (*enforcement notice*).

ii). Prinsip Pelindungan data Pribadi di Malaysia[87]

Data Pribadi di Malaysia dilindungi oleh *the Personal Data Protection Act* No. 709 of 2010 (PDPA Malaysia). Seksi 5 sampai dengan Seksi 12 PDPA Malaysia memuat tujuh prinsip pelindungan data pribadi yaitu: prinsip umum pengolahan berdasarkan persetujuan, pemberitahuan dan pilihan, pengungkapan, keamanan, integritas data (retensi dan akses). Prinsip-prinsip tersebut lebih dipengaruhi oleh *EU Data Protection Directive* daripada *OECD Guidelines* atau *APEC Framework*.[88]

(a) Prinsip Umum pengolahan berdasarkan persetujuan (*the General Principle-Processing with Consent*)

[87] Sivarasa Rasiah, Badan Peguam Malaysia dalam Greenleaf, Graham, *Asian Data Privacy Laws, Oxford University Press*, UK, 2014., hlm. 320-328.
[88] Ibid. hlm. 324.

Prinsip umum yang diatur dalam seksi 6 PDPA mengatur bahwa pengguna data tidak dapat mengolah data pribadi kecuali subjek data telah memberikan persetujuan. "Pengolahan" / "*Processing*" memiliki definisi yang saat luas, mencakup segala sesuatu dari mula pengumpulan, penyimpanan, penggunaan, dan pengungkapan, sampai dengan penghancuran data pribadi.[89] Pengolahan data pribadi tanpa persetujuan dimungkinkan misalnya apabila menyangkut, kepentingan vital subjek data dan pemrosesan data pribadi berdasarkan perintah peraturan perundang-undangan atau untuk kepentingan peradilan. Pengecualian ini tidak berlaku terhadap data pribadi sensitif, yang hanya dapat diproses sesuai dengan pasal 40 PDPA 2011.

Seksi 3 *Personal Data Protection Regulation* 2013 mengatur relatif detail mengenai persetujuan (*Consent*).[90] Persetujuan harus dibuat dalam bentuk yang dapat direkam dan dipelihara dengan baik. Bagi anak yang berusia di bawah 18 tahun, persetujuan dapat diberikan dari orang tua atau wali mereka.

(b) Keabsahan, Kebutuhan, dan Tidak berlebihan (*Lawfulness, necessary and not excessive*)

Seksi 6 ayat (3) PDPA menambahkan 3 (tiga) batas umum lainnya pada pengolahan data

[89] Seksi 3 *Personal Data protection Act* (PDPA) 2011, definisi "*Processing*".
[90] Seksi 3 *Personal Data Protection Regulation* 2013.

pribadi, berdasarkan tujuannya, yaitu: (a) pengolahan harus dilakukan untuk tujuan yang sah, dan berkaitan langsung dengan kegiatan pengguna data; (b) pelaksanaan pengolahan data harus secara langsung dibutuhkan atau berkaitan dengan tujuan pengolahan data; dan (c) data pribadi yang diolah harus cukup untuk mencapai tujuan pengolahan data, namun tidak boleh berlebihan.

(c) Prinsip Pengumpulan dan Pemberitahuan (*Collection and Notice Principle*)

Pengguna data yang akan melakukan pengolahan data terlebih dahulu harus mendapatkan persetujuan subjek data.[91] Pengguna data wajib memberikan 'pemberitahuan tertulis' mengenai tujuan pengumpulan data pribadi.[92] Pemberitahuan harus diberikan 'sesegera mungkin', dan ketika data yang dikumpulkan dari subjek data yang tersirat pemberitahuan.

(d) Prinsip Penggunaan dan Pengungkapan (*Use and Disclosure Principles*)

Penggunaan data pribadi Seksi 6 ayat (3) PDPA yang mensyaratkan bahwa data pribadi tidak dapat diproses kecuali:

(i) data pribadi diolah untuk tujuan yang sah secara langsung berkaitan dengan aktivitas pengguna data , dan

[91] Seksi 6 *Personal Data protection Act* (PDPA) Malaysia.
[92] Seksi 7 *Personal Data protection Act* (PDPA) Malaysia.

(ii) pengolahan data pribadi diperlukan atau langsung berhubungan dengan tujuan pengumpulan data pribadi.

Penggunaan sekunder didasarkan pada persetujuan, bukan didasarkan pada adanya hubungan langsung dengan tujuan pengumpulan.

Di sisi lain, data pribadi hanya dapat diungkapkan untuk tujuan awal pengumpulan data pribadi atau tujuan yang 'berhubungan langsung' untuk itu,[93] dan juga harus termasuk ke dalam 'kelas pihak ketiga" yang telah diberitahukan oleh pengguna data bahwa mereka dapat mengungkapkan data.[94] Pengguna Data masih harus menetapkan bahwa pemberitahuan tersebut merupakan persetujuan subjek data yang tersirat untuk memproses data. Karena pemberitahuan tersebut bukan merupakan 'cek kosong' bagi pengguna data untuk mengungkapkan data pribadi kepada siapa pun yang mereka pilih. Selain itu, pengungkapan juga dimungkinkan karena pengecualian yang diatur dalam Seksi 6 PDPA.

Seksi 5 *Personal Data Protection Regulations* 2013 mengharuskan pengguna data harus membuat daftar pengungkapan data pribadi yang berhubungan langsung dengan tujuan

[93] Seksi 8 (a*) Personal Data protection Act* (PDPA) Malaysia.
[94] *Personal Data protection Act* (PDPA) Malaysia. Seksi 7 ayat (1) (e) dan 8 (b).

pengungkapan. Akan tetapi, daftar pengungkapan tersebut tidak diperlukan apabila pengungkapan yang dilakukan atas pengecualian dalam Seksi 6 PDPA.

(e) Data pribadi sensitif (*Sensitive Personal Data*)

Data pribadi sensitif adalah data pribadi mengenai kesehatan atau kondisi fisik, mental, pilihan politik, agama, keyakinan lainnya, tuduhan melakukan pelanggaran, dan data pribadi lainnya yang oleh menteri berwenang ditentukan sebagai data pribadi sensitif. Data sensitif juga harus berupa "data pribadi"[95] dan karena "data pribadi" terbatas pada "informasi mengenai transaksi komersial", maka hal ini membatasi lingkup pelindungan data pribadi sensitif.[96] Malaysia hanya menggunakan sebagian dari kategori data sensitif di Uni Eropa, menghilangkan pengategorian asal ras atau etnis, keanggotaan serikat buruh, dan kehidupan seks dari data pribadi sensitif, meskipun hal-hal tersebut adalah topik sensitif dalam kehidupan masyarakat Malaysia.[97]

Untuk dapat melakukan pengolahan data pribadi yang sensitif dibutuhkan "persetujuan eksplisit". Pengolahan data pribadi sensitif juga dimungkinkan apabila tanpa persetujuan apabila pengolahan tersebut masuk ke dalam

[95] Seksi 4 Personal Data protection Act (PDPA) Malaysia.
[96] *Ibid.* hlm.327.
[97] *Ibid.*

kategori pengecualian.[98] Diantara daftar pengecualian yang sangat luas tentang persetujuan yaitu pengecualian bahwa data sensitif diproses untuk menjalankan fungsi-fungsi yang diberikan pada setiap orang dengan atau berdasarkan undang-undang atau untuk tujuan lain yang ditetapkan oleh menteri yang berwenang. Terdapat juga pengecualian apabila seseorang telah memublikasi data pribadi sensitif mereka sendiri.[99] Namun, terdapat kekhawatiran bahwa ketentuan pengecualian pemrosesan data pribadi sensitif akan disalahgunakan oleh negara Malaysia (yang tidak terikat oleh PDPA).

(f) Prinsip keamanan (*Security Principle*)

Prinsip keamanan mengharuskan pengguna data 'mengambil langkah-langkah yang dapat diterapkan' untuk memenuhi enam faktor keamanan.[100] Seksi 6 *Personal Data Protection Regulations* mewajibkan pengguna data untuk memiliki kebijakan keamanan yang sesuai dengan 'standar keamanan' yang ditetapkan secara berkala oleh Komisioner dalam pelindungan data pribadi di Malaysia.[101] Mereka juga harus memastikan bahwa setiap pengolah data yang bertindak atas nama mereka mematuhi kebijakan tersebut.

[98] Seksi 40 Personal Data protection Act (PDPA) Malaysia.
[99] Seksi 40 Ayat (2) Personal Data protection Act (PDPA) Malaysia.
[100] Seksi 9 Personal Data protection Act (PDPA) Malaysia.
[101] Seksi 6 Personal Data protection Act (PDPA) Malaysia.

(g) Prinsip retensi data dan hak untuk memblokir pemrosesan (*Data Retention Principle and Rights to Block Processing*)

Data pribadi tidak dapat disimpan lebih lama lagi apabila pemenuhan tujuan yang sah telah tercapai. Pengguna data memiliki tanggung jawab untuk memastikan bahwa data pribadi tersebut kemudian dihancurkan atau secara permanen dimusnahkan.[102] Pengguna data harus tunduk pada "retensi standar" yang ditetapkan Komisioner pelindungan data pribadi.[103]

Subjek data berdasarkan Seksi 38 PDPA dapat menarik persetujuan pengolahan data mereka setiap waktu dan untuk hal itu pengguna data harus mematuhinya. Hal ini terkait dengan pengecualian yang tertuang dalam Seksi 6 PDPA, di mana persetujuan untuk pengolahan data pribadi tidak diperlukan.

Subjek data juga dapat melakukan pemberitahuan untuk meminta penghentian pengolahan, atau larangan memulai melakukan pengolahan, untuk jangka waktu tertentu atau untuk tujuan tertentu, apabila (untuk alasan lain) pengolahan mungkin menyebabkan kerugian substansial atau tekanan terhadap subjek data atau orang lain.[104]

[102] Seksi 10 Personal Data protection Act (PDPA) Malaysia.
[103] Seksi 7 Personal Data Protection Regulations Malaysia 2013.
[104] Seksi 42 PDPA Malaysia.

Hak untuk menarik izin pengolahan berdasarkan seksi 38 PDPA sangat penting terutama dalam praktik pemasaran langsung. Penggunaan data pribadi untuk praktik pemasaran langsung bukan salah satu pengecualian terhadap persyaratan adanya persetujuan pengolahan data, dengan demikian subjek data dapat menarik kembali persetujuan pemrosesan data pribadi dalam praktik pemasaran langsung. Dengan kata lain subjek data memiliki hak untuk keluar dari penggunaan pemasaran langsung d setiap saat, dan terlepas dari persetujuan yang ia berikan sebelumnya.[105]

(h) Prinsip integritas data (*Data Integrity Principle*)

Seorang pengguna data harus mengambil langkah yang wajar untuk memastikan bahwa data pribadi akurat, lengkap, tidak menyesatkan dan terus *up-to-date* dengan memperhatikan tujuan, termasuk tujuan langsung terkait.[106] Data pribadi juga harus sesuai dengan 'integritas data standar' dapat ditetapkan oleh Komisioner pelindungan data pribadi.[107]

(i) Prinsip Akses dan Koreksi (*Access and Correction* Principle)

Subjek data yang memiliki hak standar untuk mengakses data pribadi mereka dan untuk

[105] Abu Bakar Munir dalam Greenleaf, Graham, Op Cit., hlm. 328.
[106] Seksi 11 Personal Data protection Act (PDPA) Malaysia.
[107] Seksi 8 Personal Data Protection Regulations 2013.

memperbaikinya apabila data pribadi tersebut tidak akurat, tidak lengkap, menyesatkan atau tidak up-to-date. Hal ini dikecualikan apabila permintaan subjek data ditolak berdasarkan undang-undang.[108] Alasan, prosedur penolakan permintaan akses dan koreksi diatur dalam seksi 30-37 PDPA. Kemudian *Personal Data Protection Regulations* 2013 menetapkan persyaratan subjek data berhak mendapatkan hak akses dan koreksi, misalnya subjek data harus mencantumkan nama, alamat, dan nomor kartu tanda penduduk, kecuali Komisioner Pelindungan Data Pribadi menentukan lain.

iii). Prinsip Pelindungan Data Pribadi di Singapura

Data Pribadi di Singapura dilindungi oleh *The Personal Data Protection Act No. 26 of 2012 Singapore* (PDPA 2012 Singapura). PDPA 2012 Singapura, memuat beberapa prinsip pelindungan data pribadi, di antaranya:

(a) Prinsip *Consent*

Suatu organisasi, dapat memperoleh, menggunakan atau membuka data pribadi seseorang apabila mendapat kesepakatan dari subyek data.

(b) *Purpose*

Suatu organisasi dapat memperoleh atau mengumpulkan, menggunakan dan membuka

[108] Seksi 12 PDPA Malaysia.

data pribadi seseorang dalam keadaan apapun, dan apabila mereka menginformasikan kepada subyek data tujuan dari diminta atau dikumpulkannya, digunakan dan diumumkannya data pribadi seseorang kepada yang bersangkutan.

(c) *Reasonableness*

Suatu organisasi dapat mengumpulkan, menggunakan atau mengumumkan data pribadi seseorang apabila ia melakukannya dengan tujuan yang pantas dan beralasan.

iv). Prinsip Pelindungan Data Pribadi di Korea Selatan

Prinsip Pelindungan Data Pribadi termuat dalam *Pasal 3 Personal Information Protection Act (Pipa) 2011.* Prosesor data pribadi harus:

(a) memiliki tujuan jelas dan spesifik;
(b) memproses data pribadi hanya untuk pencapaian tujuan pengumpulan data pribadi.
(c) memastikan data pribadi akurat dan lengkap serta mutakhir;
(d) memperhatikan keamanan data pribadi;
(e) mengumumkan kebijakan privasi dan menjamin hak akses;
(f) mengelola dengan cara yang tidak melanggar hak subyek data;
(g) berusaha mengelola data pribadi tanpa menyertakan nama subyek data, apabila mungkin; dan

(h) berusaha meningkatkan kepercayaan subjek data dengan menaati ketentuan hukum.

2). Komisi Pelindungan Data Pribadi

i) Komisi Pelindungan Data Pribadi Hongkong

Personal Data Privacy Ordinance of 1995 memberikan mandat untuk mendirikan Komisioner Privasi Data Pribadi (*Privacy Commissioner for Personal Data*) sebagai badan independen yang bertugas mengawasi dan menyosialisasikan kepatuhan terhadap PDPO. Fungsi dari Komisioner Privasi Data Pribadi sangat luas, termasuk di antaranya mengawasi dan memasyarakatkan kepatuhan terhadap PDPO, menyosialisasikan kesadaran dan pengertian masyarakat terhadap PDPO, memeriksa legislasi yang diajukan agar pemberlakuan legislasi tersebut tidak akan mempengaruhi privasi individual, melaksanakan pemeriksaan sistem pemrosesan data pribadi, dan melakukan penelitian dalam hal privasi.

ii) Komisi Pelindungan Data Pribadi Singapura

Di Singapura dikenal dengan istilah *Personal Data Protection Commission and Administration*. Lembaga dibentuk oleh menteri terkait yang terdiri atas tidak kurang dari 3 (tiga) dan tidak lebih dari 17 (tujuh belas) anggota. Fungsi dari pada komisi ini adalah:

(a) untuk mendorong kesadaran mengenai pelindungan data di Singapura;

(b) untuk menerima konsultasi, advokasi, teknis, manajemen, atau jasa lainnya terkait dengan pelindungan data;
(c) untuk memberikan masukan kepada pemerintah terhadap semua permasalahan yang terkait dengan pelindungan data;
(d) untuk mewakili Pemerintah di dunia internasional terkait dengan pelindungan data pribadi;
(e) untuk melaksanakan penelitian dan pendidikan dan mendorong kegiatan edukasi terkait dengan pelindungan data pribadi, termasuk di dalamnya mengatur, melaksanakan seminar, *workshop* dan simposium terkait dengan perlindungan data pribadi dan mendorong lembaga lainnya untuk melaksanakan kegiatan-kegiatan lain;
(f) untuk mengatur kerja sama teknis dan pertukaran di pelindungan data pribadi, dengan lembaga atau organisasi lainnya, termasuk pelindungan data pribadi asing dan internasional, LSM, atas nama pemerintah;
(g) untuk menegakkan dan melaksanakan undang-undang ini;
(h) untuk menegaskan fungsi atau tugas terhadap komisi ini dalam undang-undang tertulis lainnya; dan
(i) untuk terlibat dalam kegiatan lainnya dan melaksanakan tugasnya atas izin menteri

atau untuk menunjuk komisi atas perintah dari *gazette.*

Selain *Personal Data Protection Commission and Administration,* dikenal juga *Advisory committees. Advisory committees* merupakan komisi penasihat yang berjumlah dua atau lebih dan ditunjuk oleh menteri untuk memberikan masukan kepada komisi terkait dengan tugasnya dalam Undang-Undang. Komisi dapat berkonsultasi kepada *Advisory committees* terkait dengan pelaksanaan dari fungsinya dan tugasnya dan untuk melaksanakan kewenangannya berdasarkan undang-undang namun tidak mengikat seperti layaknya konsultasi.

Komisi dapat menunjuk seseorang atau kantor, sejumlah inspektur dan pegawai lainnya, untuk menjadi pegawai publik atau karyawan. Komisi dapat mendelegasikan fungsi, tugas dan kewenangannya kepada orang yang telah ditunjuk sesuai dengan persyaratan yang berlaku atau batasan-batasan yang ada yang diberikan oleh komisi.

Selain Komisi Informasi, dalam undang-undangnya juga diatur mengenai Komisi Banding pelindungan data dalam *Section 33*. Komisi banding pelindungan data ini terdiri dari 3 atau lebih anggota dari panel banding.

Setiap organisasi atau orang dapat mengajukan banding terhadap segala putusan

komisi dalam jangka waktu 28 hari terhadap arahan atau putusan dari Komisi. Banding juga dapat diajukan kepada pengadilan atau pengadilan banding.

iii) Komisi Pelindungan Data Pribadi Malaysia

Komisi pelindungan data pribadi di Malaysia disebut dengan *Personal Data Protection Commissioner.* Berdasarkan Seksi 47 PDPA Malaysia, Komisioner mempunyai hak untuk menarik pendaftaran dari pengguna data ketika komisi menemukan bahwa: [109]

(a) pengguna data (*data user*) telah gagal dalam memenuhi semua ketentuan yang ada dalam PDPA Malaysia;
(b) pengguna data telah gagal untuk patuh dan mengikuti persyaratan dan batasan yang ada terkait dengan diterbitkannya sertifikat pendaftaran;
(c) penerbitan sertifikat pendaftaran dikeluarkan berdasarkan fakta yang salah dari pengguna data; dan
(d) pengguna data berhenti untuk memproses data pribadi.

iv) Komisi Pelindungan Data Pribadi Korea Selatan

Personal Information Protection Act 2011 (PIPA Korea Selatan) mengatur tentang pembentukan komisi pelindungan data pribadi yang disebut

[109] Seksi 18 Personal Data protection Act (PDPA) Malaysia.

Personal Information Protection Commission (PIPC). Menurut *Article 7* PIPA Korea Selatan, PIPC dibentuk untuk mempertimbangkan dan menyelesaikan permasalahan terkait perlindungan data. Anggota PIPC terdiri dari lima belas orang komisioner yang dipilih oleh Presiden. Fungsi dari PIPC di antaranya adalah mendiskusikan atau mempertimbangkan dan menyelesaikan:[110]

(a) pelaksanaan *basic plan* dan *implementation plan* yang terdapat dalam PIPA Korea Selatan;
(b) masalah perbaikan kebijakan, sistem dan peraturan yang berhubungan dengan pelindungan data;
(c) masalah koordinasi posisi yang ditempati institusi publik dalam hal pemrosesan data pribadi; dan
(d) hal-hal lain yang berkenaan dengan pelaksanaan pasal-pasal di dalam PIPA 2011 Korea Selatan.

3). Sanksi pidana pelanggaran hak atas data pribadi di Hongkong, Singapura, Malaysia, dan Korea Selatan

i) Sanksi pidana di Hongkong[111]

Pengguna data (*data user*) yang melanggar surat teguran (*enforcement notice*) dari *Privacy Commissioner for Personal Data* diancam dengan

[110] Seksi 8 Personal Information Protection Act (PIPA) Korea Selatan.
[111] Seksi 50 A PDPO Hong Kong.

denda dan penjara maksimum 2 (dua) tahun. Apabila pelanggaran masih dilanjutkan *data user* setelah adanya hukuman maka pemerintah dapat menjatuhkan denda tambahan sebesar 1000 dollar per hari. Kemudian apabila masih saja melanggar maka denda harian dapat ditingkatkan menjadi 2000 dollar per hari.

ii) Sanksi pidana di negara Singapura[112]

PDPA 2012 di Singapura mengatur penalti bagi pelanggaran beberapa ketentuan di dalamnya termasuk denda sampai USD 790.000 dan atau pidana penjara sampai dengan 3 tahun.

iii) Sanksi pidana di negara Malaysia[113]

Pelanggaran terhadap ketentuan PDPA 2010 di Malaysia juga dapat mengakibatkan seseorang mendapatkan denda atau sanksi penjara.

iv) Sanksi pidana di negara Korea Selatan[114]

PIPA Korea Selatan yang memulai berlaku pada Maret 2012 memiliki pasal mengenai sanksi pidana penjara dan denda maksimal 100 *million won* (USD 92,000).

4). Komisi Pengawas

Hampir di setiap negara yang mengatur Data Pribadi memiliki suatu komisi pengawas untuk menjamin undang-undangnya dapat diterapkan secara efektif.

---

[112] Data Privacy and Security Team, "South East Asia: Data Protection Update", Bryan Cave Bulletin, diunduh pada 16 Oktober 2015, Pukul 16.22, https://www.bryancave.com/images/content/2/0/v2/2020/Bryan-Cave-Client-Bulletin-South-East-Asia-Data-Protection-Updat.pdf diakses Januari 2015

[113] *ibid*

[114] *ibid*

Terdapat 3 (tiga) pola pendirian komisi yang bertugas menjamin pelaksanaan pelindungan data pribadi berdasarkan Undang-Undang (lihat gambar 1.1 di bawah). Pola yang pertama, adalah pendirian komisi yang berdiri secara tersendiri (independen), dan memiliki tugas dan fungsi pokok berdasarkan undang-undang pelindungan data pribadi. Pola yang kedua, adalah pemberian tugas dan fungsi yang berhubungan dengan pelindungan data pribadi ke dalam suatu komisi yang telah ada sebelumnya, dalam hal ini misalnya disatukan dengan Komisi Informasi Publik. Pola yang ketiga, adalah memberikan kewenangan kepada pemerintah untuk membentuk komisi di bawah koordinasi kementrian dengan didasari oleh undang-undang.

Gambar 1.1

Pola Pendirian Komisi

Negara yang menerapkan pola pertama adalah Singapura dan Hong Kong. Tujuan utama pembentukan komisi pelindungan data pribadi adalah untuk menjamin

pelindungan data pribadi melalui sosialisasi, monitoring, dan supervisi atas kepatuhan dan penegakan undang-undang pelindungan data.

Pola kedua, misalnya diterapkan di Kerajaan Inggris. The Information Commissioner's Office, sebuah lembaga independen yang didirikan untuk menegakan hak-hak informasi. Lembaga ini berperan untuk menjamin pelindungan hak informasi dalam kepentingan publik. The Information Commissioner's Office di Kerajaan Inggris tidak hanya menjamin hak-hak dalam undang-undang pelindungan data saja (Data Protection Act 1998), tetapi juga menjamin hak-hak informasi yang terkandung dalam Privacy and Electronic Communications (EC Directive) Regulations 2003, Freedom of Information Act 2000, the Environmental Information Regulations 2004, INSPIRE Regulations, dan Re-use of Public Sector Information Regulations.[115]

Negara yang menerapkan pola ketiga adalah Malaysia. Menteri yang berwenang berdasarkan perintah Undang-Undang menunjuk seseorang untuk menjadi *Personal Data Protection Commissioner.*[116] Tujuan utama *Personal Data Protection Commisioner* tersebut adalah melaksanakan fungsi dan kewenangan yang diberikan undang-undang pelindungan data di Malaysia. Karena komisioner ditunjuk oleh menteri, maka komisioner bertanggung jawab terhadap menteri.[117] Dalam hal ini adalah Menteri Komunikasi dan Multimedia.

---

[115] Lihat website resmi *Information Commission Office* (ICO), "About ICO" diakses di https://ico.org.uk/about-the-ic, pada Minggu 20 September 2015, Pukul 5.00 WIB.

[116] *Section* 47 (1) *Personal Data Protection Act* (PDPA) Malaysia 2010.

[117] Lihat Section 48-49 *Personal Data Protection Act* (PDPA) 2010.

Dengan mempertimbangkan hal-hal yang telah dijelaskan di atas, maka dalam Rancangan Undang-Undang Pelindungan Data Pribadi juga memiliki 3 (tiga) pilihan. Pertama, yaitu membentuk komisi independen yang khusus menangani masalah pelindungan data pribadi. Kedua, melekatkan tugas dan fungsi tambahan dari komisi yang telah ada sebelumnya, dalam hal ini adalah Komisi Informasi Pusat (KIP). KIP sebagai sebuah lembaga mandiri yang lahir berdasarkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik mulai menjalankan fungsi dan wewenangnya pada 1 Mei 2010. Komisi Informasi terdiri atas Komisi Informasi Pusat yang berkedudukan di ibu kota Negara, Komisi Informasi Provinsi yang berkedudukan di ibu kota provinsi, dan dalam hal dibutuhkan Komisi Informasi kabupaten/kota yang masing-masing berkedudukan di ibu kota kabupaten/kota.[118] Susunan keanggotaan Komisi Informasi Pusat berjumlah 7 (tujuh) orang Komisioner yang harus mencerminkan unsur dari pemerintah dan unsur masyarakat. Untuk keanggotaan Komisi Informasi pada tingkat daerah, Komisi Informasi provinsi/ kabupaten/kota, Komisionernya berjumlah 5 (lima) orang yang juga harus mencerminkan unsur dari pemerintah dan unsur masyarakat.[119] Pilihan ketiga, memberikan kewenangan kepada pemerintah untuk membentuk komisi di bawah koordinasi kementerian.

[118] Website resmi Komisi Informasi Pusat Indonesia, "Tentang KIP", diakses di http://www.komisiinformasi.go.id /category/profil/tentang-kip pada Minggu 20 September 2015, Pukul 5.00 WIB.
[119] *Ibid.*

Pada umumnya hukum pelindungan data menghendaki dibentuknya otoritas pengawas atau Data Protection Authorities (DPAs). Struktur pertanggungjawaban yang jelas adalah kunci bagi dimungkinkannya warga negara atau pelanggan untuk mendapatkan keadilan (pemulihan).

Otoritas pengawas dalam bentuk komisi ini tidak hanya diperlukan keberadaannya, namun juga harus memiliki kewenangan, ketidakberpihakan, dan menjadi Badan yang akan mengawasi implementasi hukum pelindungan data. Peraturan yang kuat tetap tidak akan efektif jika tidak didukung oleh kewenangan penegakan yang kuat dan prosedur ganti rugi yang pantas walaupun kemampuan regulator untuk memberikan hukuman masih terbatas. Misalnya, UK Information Commissioner (ICO) hanya diperbolehkan untuk memberikan denda maksimal £500,000 untuk pelanggaran serius di tahun 2011.[120] Namun demikian, efek jera dari pemberian denda ini tetap perlu ditelaah kembali mengingat harga untuk pematuhan terhadap aturan tersebut sering kali lebih tinggi dari denda itu sendiri. Hukuman pidana dapat menjadi pelengkap yang berguna sebagai akibat dari skandal *phone-hacking* di Inggris[121], ICO telah diperbaharui[122] dengan memperkenalkan aturan

[120] http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties guidance_120110.pdf, diakses pada tanggal 10 September 2014 Pukul 13.20 WIB.

[121] Artikel berita BBC, *"Phone-hacking scandal: Timeline"*, 28 Februari 2012, diakses di http://www.bbc.co.uk/news/uk-14124020, diakses pada tanggal 10 September 2014 Pukul 13.30 WIB.

[122] http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY.ashx, diakses pada tanggal 11 September 2014 Pukul 10.00 WIB.

penghukuman 2 tahun penjara bagi pengguna data pribadi yang dicuri.

Walaupun komisi pengawas memiliki kewenangan, mereka terkadang tidak mampu untuk melaksanakan peran mereka karena keterbatasan dana. Misalnya dalam kasus yang terjadi di Romania dimana regulator disana mulai bekerja tahun 2006 namun pekerjaan mereka terganggu secara serius dikarenakan kurangnya sumber dana yang mereka miliki.[123] Keuangan mereka di tahun 2009 sangat rendah sehingga ketika seharusnya mereka harus mempekerjakan 50 pegawai, mereka hanya sanggup 35 pegawai yang dipekerjakan.[124] Akibatnya, mereka harus membatasi tindakan investigasi mereka ke ibu kota yaitu Bucharest.[125]

Ketidakberpihakan dari Komisi Pengawas adalah faktor penting, mengingat hanya badan tersebut yang benar-benar berada di tengah-tengah industri dan pemerintah. Di Jerman misalnya, Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, or BfDI) secara sukses memonitor pematuhan terhadap pelindungan data baik oleh badan publik juga penyedia jasa pos dan telekomunikasi.[126]

[123] https://www.privacyinternational.org/article/romania-privacy-profile#_ftn26, diakses pada tanggal 12 September 2014 Pukul 20.00 WIB.
[124] Bogdan Manolea, Romania National Report – EDRi , December 2009, dapat diakses di http://www.ldh-france.org/IMG/pdf/ETUDE-ROUMANIE-EN. pdf, diakses pada tanggal 13 September 2014 Pukul 22.00 WIB.
[125] ANSPDCP 2009 *Annual Rapport Romania*n, dapat diakses di http://www.dataprotection.ro/servlet/View Document?id=623., diakses pada tanggal 11 September 2014 Pukul 21.00 WIB.
[126] https://www.privacyinternational.org/article/germany-privacy-profile, \diakses pada tanggal 14 November 2014 Pukul 13.00 WIB.

BfDI, yang memiliki pegawai sejumlah 70 orang[127], mengurusi sekitar 5516 keluhan tertulis dan menjalankan setidaknya 75 investigasi setiap tahun.[128] Di Kanada, baik Undang-Undang Privasi dan Personal Information Protection and Electronic Documents Act (PIPEDA) diawasi oleh Komisi Privasi Federal Kanada yakni seorang aparat dari Parlemen yang ditunjuk oleh dan harus melaporkan kepada Parlemen Kanada.[129] Komisioner memiliki kewenangan investigasi yang luas di antaranya untuk memanggil paksa saksi dan memberikan kesaksian, memasuki kediaman dalam rangka mendapatkan dokumen dan melaksanakan wawancara, dan untuk membuat rekomendasi, namun tidak dapat mengeluarkan perintah atau memberikan sanksi hukum.[130] PIPEDA mensyaratkan bahwa semua organisasi menunjuk satu orang pegawai yang bertanggung jawab terhadap kebijakan dan praktek organisasi dan kepada siapa keluhan serta penyelidikan dapat diteruskan. Penunjukan pegawai/pejabat pelindungan data pribadi yang profesional dan mempunyai pengetahuan di bidang pelindungan data pribadi diperlukan untuk memberikan panduan atas

[127] http://www.bfdi.bund.de/cln_030/nn_531068/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2007/PM-15-07-Uebergabe21TB.html__nnn=true, diakses pada tanggal 14 November 2014 Pukul 13.20 WIB.

[128] *Federal Commissioner for Data Protection and Freedom of Information* (Bundesbeauftragterfür den Datenschutz und die Informationsfreiheit, BfDI), Tätigkeitsbericht (Bi-Annual Report) 2005-2006, 24 April 2007 at 160, dapat diakses di: http://www.bfdi.bund.de/cln_030/nn_531940/___Shared Docs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006, templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf

[129] Privacy Commissioner of Canada: http://www.priv.gc.ca/, diakses pada tanggal 14 November 2014 Pukul 13.30 WIB.

[130] Https://www.privacyinternational.org/article/phr2006-canada, diakses pada tanggal 14 November 2014 Pukul 13.35 WIB.

penerapan kepatuhan undang-undang pelindungan data pribadi oleh pengendali data pribadi ataupun prosesor data pribadi. Hal ini juga diperlukan untuk memitigasi pelanggaran yang terkait dengan pemrosesan data pribadi.

Pada akhirnya, peran Badan Pengawas akan sangat tergantung dari kemandirian dan ketidakberpihakan dan keefektifannya dalam bekerja. Terdapat dua model utama yang berlaku dalam yurisdiksi di seluruh negara yakni kombinasi antara regulator privasi dan kebebasan informasi atau FOI dan regulator independen.

Tabel 1.2

MODEL KOMISI PENGAWAS

Model Komisi Independen	Model Satu Komisi	Model Komisi di Bawah Koordinasi Pemerintah
• Model ini dianut oleh negara-negara Uni Eropa dan beberapa negara di Asia seperti Singapura, Hong Kong, dan Korea Selatan. • Keuntungan dari model ini memang bisa meminimalisir konflik dalam satu komisi, khususnya dalam menentukan suatu informasi terbuka atau tertutup.	• Model ini seperti dianut di Estonia, Hungary, Malta, Mexico, Serbia, Thailand, dan the United Kingdom. • Pada model ini dalam satu komisi akan ada dua kamar komisi, satu kamar sebagai komisi informasi dan kamar lainnya sebagai komisi data proteksi. • Biasanya terjadi di negara-negara dengan penyusunan legislasi yang berbeda antara keterbukaan informasi dan pelindungan data pribadi, sehingga komisi kedua disisipkan dalam komisi yang pertama.	• Model ini dianut oleh Malaysia. • Model ini lebih efisien pembentukannya, sehingga dapat dijadikan alternatif bagi negara yang baru memiliki undang-undang pelindungan data pribadi.

5). Transfer Data Lintas Negara

Perkembangan terakhir pengaturan hukum pelindungan data pribadi mengatur tentang pembatasan pengiriman data pribadi yang ketat ke negara yang dituju. Apabila negara yang dituju dianggap belum memiliki

perlindungan yang memadai/*adequate* maka harus diterapkan beberapa syarat tambahan misalnya melalui kontrak atau perjanjian bilateral. Contohnya di Negara Malaysia, pengendali data dan pribadi dilarang untuk melakukan transfer data ke luar wilayah Malaysia, kecuali ke wilayah yurisdiksi yang ditentukan oleh Menteri Malaysia yang bertanggung jawab melindungi data pribadi atas rekomendasi Komisioner.[131] Setiap pelanggaran terhadap ketentuan tersebut diancam denda paling banyak tiga ratus ribu ringgit atau penjara untuk jangka waktu tidak lebih dari 2 (dua) tahun atau keduanya.

Wilayah yurisdiksi yang diterima oleh Malaysia adalah wilayah negara yang dianggap mampu menyediakan pelindungan data dan informasi pribadi seperti halnya yang diberikan Malaysia. Terdapat 2 (dua) kondisi agar dapat melakukan transfer data pribadi. Pertama, negara tersebut harus memiliki undang-undang pelindungan data pribadi yang secara substansi menyerupai undang-undang yang melindungi data dan informasi pribadi di Negara Malaysia. Kedua, negara yang diterima Menteri Malaysia harus menyediakan perlindungan terhadap data dan informasi pribadi yang setidaknya setingkat dengan *The Personal Data Protection Act No.* 709 *of* 2010.[132]

---

[131] Seksi 129 (1) Personal Data Protection Act (PDPA) 2010 Malaysia menyatakan: *"A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette."*

[132] Seksi 129 (2) The Personal Data Protection Act (PDPA) 2010 Malaysia menyatakan:*"For the purposes of subsection (1), the Minister may specify any place outside Malaysia if—*

(a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or

Selain keadaan yang telah disebutkan di atas, transfer data dan informasi pribadi ke luar Malaysia juga dapat terjadi apabila:[133]

Subyek data menyetujui transfer data ke luar Malaysia,

1). Transfer data diperlukan untuk melaksanakan perjanjian antara pengendali data dan subyek data,
2). Transfer diperlukan untuk menyetujui atau melaksanakan perjanjian antara pengendali data dan pihak ketiga atas permintaan subyek data atau untuk kepentingan subyek data.
3). Transfer dilakukan untuk tujuan persidangan atau untuk mendapatkan bantuan hukum atau untuk

(b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act."

[133] Seksi 129 The Personal Data Protection Act (PDPA) 2010 Malaysia menyatakan*: "Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if—*
(a) the data subject has given his consent to the transfer
(b) The transfer is necessary for the performance of a contract between the data subject and the data user;
(c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which—
(i) is entered into at the request of the data subject;or
(ii) is in the interests of the data subject;
(d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or forestablishing, exercising or defending legal rights;
(e) the data user has reasonable grounds for believing thatin all circumstances of the case—
(i) the transfer is for the avoidance or mitigation ofadverse action against the data subject;
(ii) it is not practicable to obtain the consent in writingof the data subject to that transfer; and
(iii)if it was practicable to obtain such consent, thedata subject would have given his consent;
(f) the data user has taken all reasonable precautions andexercised all due diligence to ensure that the personaldata will not in that place be processed in any mannerwhich, if that place is Malaysia, would be a contraventionof this Act;
(g) the transfer is necessary in order to protect the vitalinterests of the data subject; or
(h) the transfer is necessary as being in the public interestin circumstances as determined by the Minister."

mengadakan, melaksanakan atau mempertahankan hak berdasarkan hukum.

4). Pengguna data memiliki dasar beralasan untuk mempercayai bahwa dalam segala macam kondisi:
   a). Transfer dilakukan untuk menghindari atau pencegahan tindakan merugikan hak, keuntungan, keistimewaan, dan kewajiban atau kepentingan pemilik data.
   b). Tidak memungkinkan untuk memperoleh persetujuan tertulis dari subyek data yang ditransfer.
   c). Jika memungkinkan untuk mendapatkan persetujuan, subyek data diyakini akan memberikan persetujuan.
5). Pengguna data telah mengambil semua tindakan pencegahan yang wajar dan melakukan semua *due diligence* untuk memastikan bahwa, data pribadi tidak akan diproses di tempat tersebut dengan dengan cara apapun yang, jika tempat itu adalah Malaysia, akan menjadi suatu pelanggaran terhadap *The Personal Data Protection Act No.* 709 *of* 2010 Malaysia.
6). Transfer dibutuhkan untuk melindungi kepentingan vital dari subyek data.
7). Transfer dibutuhkan untuk kepentingan publik dalam keadaan yang ditentukan oleh Menteri.

Persyaratan-persyaratan tersebut hampir senada dengan apa yang diatur oleh hukum negara-negara Eropa. Pada dasarnya Malaysia melarang transfer data pribadi keluar wilayah negara Malaysia dengan pengecualian-

pengecualian. Keseluruhan pengaturan mengenai transfer data pribadi tersebut dibutuhkan untuk melindungi subyek data pribadi.

3. Konsep Pelindungan Data Pribadi

Pengaturan yang akan disusun diharapkan dapat melindungi data pribadi individu terhadap penyalahgunaan pengumpulan serta pengolahannya dipermudah dengan teknologi informasi dan komunikasi saat ini. Perkembangan pengaturan data pribadi secara umum akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai pelindungan data pribadi. Hal ini akan lebih mendorong dan memperkuat posisi Indonesia sebagai pusat bisnis terpercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia.

Bagi kepentingan konsumen, kebutuhan akan pelindungan data pribadi konsumen terutama di era di mana data pribadi menjadi lebih sangat berharga bagi kepentingan bisnis, menimbulkan kekhawatiran bahwa data pribadi konsumen dijual atau digunakan tanpa persetujuan mereka, sebagaimana contoh pelanggaran yang telah diuraikan sebelumnya. Untuk itu, terlihat kebutuhan akan suatu perundang-undangan mengenai pelindungan data pribadi yang bersifat khusus untuk memastikan bahwa data pribadi konsumen dilindungi dengan baik.

Bagi perkembangan ekonomi, pelindungan data pribadi yang bersifat khusus akan memperkuat posisi Indonesia sebagai pusat bisnis dan investasi tepercaya dan menciptakan lingkungan yang kondusif untuk pertumbuhan manajemen data

global dan industri pengolahan data seperti komputasi awan untuk berkembang di Indonesia.

Ketiadaan hukum mengenai pelindungan data pribadi yang bersifat umum di Indonesia dapat dilihat sebagai suatu kelemahan yang menyebabkan beberapa perusahaan tidak memilih Indonesia sebagai lokasi untuk pusat penyimpanan datanya. Padahal, perkembangan pengaturan pelindungan data pribadi akan mendukung pembangunan masa depan Indonesia sebagai pusat data global.

Pengaturan tentang data pribadi sangat diperlukan karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman dan keamanan data pribadi dan secara umum pengaturan data pribadi adalah untuk mencari keseimbangan antara kebutuhan akan pelindungan data pribadi individu dengan kebutuhan Pemerintah dan pelaku bisnis untuk memperoleh dan memproses data pribadi untuk keperluan yang wajar dan sah.

Sebagai salah satu anggota masyarakat internasional, Indonesia harus menyesuaikan dengan perkembangan masyarakat internasional yang telah mengatur masalah mengenai hak privasi atas data pribadi. Dengan demikian perlu dilakukan harmonisasi pengaturan mengenai hak privasi atas data pribadi yang diatur dalam hukum nasional dengan pengaturan di negara lain, agar tercipta suatu kepastian hukum bagi pengguna yang akan mendorong perkembangan dan kemajuan berbagai bidang Indonesia.

D. Kajian terhadap Implikasi Penerapan Sistem Baru yang Akan Diatur dalam Undang-Undang terhadap Aspek Kehidupan Masyarakat dan Dampaknya terhadap Aspek Beban Keuangan Negara

1. Dampak pada Pemerintah

Data dan informasi memiliki peran yang sangat signifikan terhadap kehidupan masyarakat di abad ke-21 ini. Penyelenggaraan pemerintahan, kegiatan bisnis maupun perdagangan berkenaan dengan data pribadi, mulai dari level nasional, regional hingga internasional. Penyusunan RUU Pelindungan Data Pribadi akan menciptakan suatu sistem administrasi pemerintahan yang efisien dan efektif dalam memberikan pelayanan bagi masyarakat. RUU Pelindungan Data Pribadi akan membentuk tata kelola perlindungan data pribadi penduduk dan sekaligus melindungi hak-hak dasar warga negara. Lebih jauh lagi, pemerintah saat ini telah mengesahkan Undang-Undang No 24 Tahun 2014 tentang Administrasi Kependudukan sebagai contoh adalah merupakan kebijakan pemerintah untuk menghimpun seluruh data dan informasi setiap penduduk dengan memberikan nomor induk kependudukan sekaligus diberikan perlindungan atas data dan informasi pribadi, namun tidak ada penjabaran lebih lanjut. Demikian pula berbagai peraturan perundang-undangan yang memberikan hak kepada pengendali data pribadi untuk melakukan penghimpunan data dan informasi penduduk, tidak diberikan pengaturan yang mewajibkan pengendali data pribadi untuk melindungi data dan informasi pelanggan yang telah diserahkannya.

Kondisi peraturan perundang-undangan tersebut di atas telah menjadikan adanya kebutuhan suatu Undang-Undang yang

mampu menjamin perlindungan bagi seseorang atas data dan informasinya. Kebutuhan akan regulasi terhadap berbagai aktivitas yang melibatkan pemanfaatan teknologi informasi dan komunikasi dirasakan semakin penting. Hal disebabkan karena aktivitas-aktivitas tersebut telah mempengaruhi dan bahkan merubah paradigma di berbagai bidang, terutama bidang yang terkait dengan informasi dan teknologi.

Bagi pemerintah, RUU Pelindungan Data Pribadi akan menciptakan iklim investasi yang lebih baik, karena pelindungan data pribadi yang diberikan oleh RUU Pelindungan Data Pribadi akan mendorong perkembangan di sektor bisnis. Hal tersebut disebabkan karena meningkatnya tingkat kepercayaan masyarakat terhadap sektor bisnis bahwa data pribadi mereka terlindungi.

RUU Pelindungan Data Pribadi tidak secara signifikan akan menimbulkan beban terhadap keuangan negara, antara lain terkait dengan rencana pembentukan Komisi Pelindungan Data Pribadi. Namun potensi beban ini dapat dihilangkan dengan mengintegrasikan Komisi PDP pada komisi yang telah ada dalam hal ini Komisi Informasi atau dengan menempatkan komisi di bawah koordinasi pemerintah, dalam hal ini Menteri yang diberi kewenangan oleh undang-undang. Selain itu beban keuangan negara muncul dalam hal penyesuaian sistem informasi yang ada di instansi atau lembaga pemerintah.

2. Dampak pada Pelaku Usaha

RUU ini juga dimaksudkan untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. RUU Pelindungan Data Pribadi akan melindungi data pribadi individu terhadap penyalahgunaan pada saat data tersebut

memiliki nilai tinggi untuk kepentingan bisnis, yang pengumpulan serta pengolahannya menjadi kian mudah dengan teknologi informasi dan komunikasi. Perkembangan pengaturan atas pelindungan data pribadi secara umum akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai pelindungan data pribadi. Hal ini akan memperkuat dan memperkokoh posisi Indonesia sebagai pusat bisnis tepercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia seperti dalam sektor telekomunikasi, sektor penyedia jasa keuangan, sektor kesehatan dan sektor pendidikan.

Hukum mengenai pelindungan data pribadi juga akan memperkuat posisi Indonesia sebagai pusat bisnis tepercaya dan menciptakan lingkungan yang kondusif untuk pertumbuhan manajemen data global dan industri pengolahan data seperti *cloud computing*, untuk berkembang di Indonesia. Indonesia, memiliki banyak keunggulan kompetitif sebagai lokasi untuk *data hosting*, seperti infrastruktur telekomunikasi, lokasi geografis, keamanan dari bencana alam dan kehandalan sumber daya listrik. Namun, ketiadaan hukum mengenai perlindungan data di Indonesia dapat menjadi suatu kelemahan yang menyebabkan beberapa perusahaan global tidak memilih Indonesia sebagai lokasi untuk pusat penyimpanan datanya atau bisnis. Perkembangan pengaturan pelindungan data pribadi akan mendukung pembangunan masa depan Indonesia sebagai pusat data global. Kekurangan dalam hal legislasi untuk pelindungan data berpotensi untuk menjadi hambatan terhadap aliran informasi antara Indonesia dengan negara-negara lain terutama akan menghambat arus keluar masuk data pribadi pada tingkat

negara-negara MEA karena pengaturan data pribadi telah menjadi komitmen MEA dalam melancarkan *e-commerce* dan membawa kerugian terhadap kegiatan perdagangan Indonesia dalam ekonomi global. Tampak bahwa legislasi pelindungan data pribadi makin dilihat sebagai fitur dasar dalam kerangka hukum untuk kegiatan perekonomian.

3. Dampak pada Masyarakat

Pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi. Perlindungan data pribadi secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa pemilik data tetap mengendalikan informasinya. Data pribadi, yang bisa digunakan sebagai alat untuk mengidentifikasi seseorang, melekat kepada pemiliknya, dan hanya bisa digunakan sesuai peruntukannya sebagaimana disepakati sesuai alas haknya.

Selain itu, kebutuhan akan urgensi pengaturan data pribadi juga dilatarbelakangi oleh munculnya berbagai keluhan dari masyarakat baik yang disampaikan oleh perseorangan, kelompok dan organisasi. Pelindungan data pribadi kerap kali terganggu melalui media cetak ataupun elektronik. Penyalahgunaan penggunaan data pribadi di Indonesia kian marak terjadi dalam beberapa tahun terakhir. Pesatnya perkembangan teknologi dalam berbagai layanan jasa yang menginginkan akses terhadap data pribadi dan menggunakan data pribadi pengguna sebagai basis pelayanan. Di era digital,

hampir setiap aktifitas dalam kehidupan manusia yg dilakukan di ruang digital, membutuhkan/meminta data pribadi yang berpotensi menerobos ranah privasi. Sejalan dengan penggunaan media sosial seperti Facebook, Twiter, Line, di Indonesia yang meningkat secara tajam, data statistik menunjukkan bahwa pengguna internet pada tahun 2018 mencapai jumlah 171,17 juta pengguna aktif internet dan sekaligus pengguna aktif media sosial. Sebanyak 19,1% dari pengguna internet tersebut menggunakan internet untuk mengakses sosial media.[134]

Menurut Softpedia, data paling banyak diserang oleh penjahat siber adalah data pribadi (30%) dan data kredensial (22%) dari berbagai situs web.[135]

Keberadaan Undang-Undang Pelindungan Data Pribadi diharapkan dapat menumbuhkan kesadaran masyarakat akan pentingnya melindungi data pribadi, hak-hak masyarakat sebagai pemilik data pribadi yang memilik kontrol terhadap data pribadinya, serta penggunaan data pribadi sesuai dengan peruntukan yang sudah disepakati dan memenuhi prinsip pelindungan data pribadi. Selain itu, dengan adanya Undang-Undang Pelindungan Data Pribadi diharapkan dapat mencegah penyalahgunaan data pribadi dan mengurangi tingkat pelanggaran terkait data pribadi sehingga dapat memberikan kepastian hukum dan rasa aman bagi Warga Negara Indonesia.

[134] APJII, "Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2018", http://apjii.or.id/survei, diakses pada 10 Januari 2020.
[135] Agustin Setyo Wardani, "765 Juta Korban Terjerat Kejahatan Siber pada kuartal II 2018", https://www.liputan6.com/tekno/read/3658996/765-juta-korban-terjerat-kejahatan-siber-pada-kuartal-ii-2018, diakses pada 10 Januari 2020.

BAB III
EVALUASI DAN ANALISIS
PERATURAN PERUNDANG-UNDANGAN TERKAIT

Terdapat tiga jenis sistem hukum yang berlaku di Indonesia, yaitu sistem hukum adat, hukum perdata, dan hukum islam. Ketiganya memiliki sistem tersendiri serta peraturan terpisah yang diatur oleh pejabat pemerintah yang berbeda dan diberlakukan di pengadilan yang terpisah. Perbedaan sistem hukum ini telah berkembang dan hidup berdampingan di Indonesia selama berabad-abad. Dalam sistem hukum Indonesia, tidak terdapat hak untuk mendapatkan privasi dan pelindungan data pribadi. Inisiatif untuk memberikan pelindungan terhadap privasi dan data pribadi berasal dari permintaan mitra internasional Indonesia dalam kerja sama ekonomi. Indonesia memiliki posisi strategis pada perdagangan internasional, termasuk perdagangan elektronik.

Indonesia telah menandatangani pedoman OECD pada tahun 2004, dan mengikuti pedoman untuk menegakkan penerapan privasi dan regulasi pelindungan data. Indonesia sebagai anggota APEC, juga telah mengikuti Kerangka Privasi APEC 2004 *(APEC Privacy Framework*), yang dengan jelas menyebutkan dalam kata pengantar:

> *Potensi perdagangan elektronik tidak dapat diwujudkan tanpa kerja sama pemerintah dan pelaku bisnis untuk mengembangkan dan menerapkan teknologi dan kebijakan yang membahas isu-isu termasuk privasi.*

Keanggotaan dalam APEC diharapkan dapat merangsang legislasi nasional untuk penyeimbang antara melindungi serta mempromosikan kerja sama ekonomi khususnya dalam perdagangan elektronik antar anggota.

Di Indonesia, ada kekhawatiran mengenai pelindungan privasi dan pelindungan data karena belum ada undang-undang yang jelas. Oleh karena itu, masalah pelindungan privasi dan data pribadi telah menjadi agenda mendesak. Banyak Negara membuat ketentuan tentang privasi dan pelindungan data pribadi, namun tidak dengan Indonesia. Peningkatan dan pengembangan ilmu pengetahuan dan teknologi, globalisasi, dan kekuatan media telah mendesak kebutuhan akan privasi dan pelindungan data pribadi. Hambatan terhadap peraturan pelindungan privasi dan data pribadi sesungguhnya berasal dari sejarah Indonesia sendiri. Sebagai negara Asia, Indonesia sangat sulit untuk mendefinisikan dan mengatur privasi. Sebagian besar negara di Asia tidak tahu tentang privasi. Privasi belum dipandang sebagai masalah "serius" di Asia, termasuk Indonesia. Kebanyakan orang Asia secara tradisional hidup dalam masyarakat komunal, yang tidak memberi perhatian untuk privasi. Istilah Privasi sebagai hak asasi manusia berasal dari bangsa Barat dan menjadi penting dalam era teknologi informasi dan komunikasi (ICT). Oleh karena itu, dasar hukum untuk membentuk hukum tentang perlindungan privasi dan data di Indonesia dapat diambil dari berbagai sumber.

Privasi dan pelindungan data pribadi merupakan isu yang sudah berkembang dan menjadi perhatian di Indonesia**.** Pemerintah membuat beberapa peraturan perundang-undangan terkait privasi dan pelindungan data pribadi di berbagai bidang. Sebagai contoh, pelindungan data merupakan sesuatu yang didiskusikan ketika perusahaan multinasional mengumpulkan dan memproses pegawai atau data konsumen diseluruh dunia dalam satu data di suatu

negara. Masalah privasi data merupakan sesuatu yang muncul ketika data pribadi diberikan.[136]

Privasi merupakan hak asasi manusia yang fundamental. Sebagai suatu konsep privasi merupakan hal yang sulit untuk didefinisikan. Privasi sulit untuk didefinisikan dalam pengertian yang universal. Walaupun privasi sulit untuk didefinisikan namun istilah privasi digunakan dalam pengertian yang luas terkait dengan pelindungan data pribadi.[137]

Pengaturan privasi dan pelindungan data pribadi di Indonesia tidak dapat ditemukan dalam satu peraturan. Para sarjana di Indonesia selalu merujuk pada Pasal 28 G dari Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagai pedoman untuk membuat peraturan yang lebih khusus tentang pelindungan data pribadi. Pasal 28 G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan:

> *setiap orang berhak atas perlindungan 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*

Berdasarkan ketentuan tersebut, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 tidak secara eksplisit menyebut mengenai privasi dan pelindungan data pribadi. Ketentuan ini hanya menjelaskan perlindungan hak asasi manusia.

Indonesia telah membuat beberapa peraturan perundang-undangan yang di dalamnya mengatur mengenai privasi dalam berbagai bidang. Untuk memahami lebih lanjut mengenai

---

[136] Richard D Emmerson, SoewitoSuhardiman, Eddy MurhtyKardono, *Indonesia Report in Annual review of Data Protection and Privacy Laws*, Financier Wolrd Wide, December, 2012, hlm. 62.

[137] Heppy Endah Palupy, *Thesis: Privacy and Data Protection: Indonesia Legal Framework*, *Master Program in Law and TerchnologyUniversiteit Van Tilburg*, 2011, hlm. 4.

bagaimana Indonesia mengatur tentang privasi dan pelindungan data pribadi, maka bagian selanjutnya akan membahas peraturan seperti Undang-Undang Perbankan, Undang-undang Telekomunikasi, Undang-Undang Perlindungan Konsumen, Undang-Undang Kependudukan, Undang-Undang Hak Asasi Manusia, Undang-Undang Administrasi Kependudukan, Undang-Undang Informasi Transaksi Elektronik (ITE), Undang-Undang Keterbukaan Informasi Publik, Undang-Undang Kesehatan dan peraturan perundang-undangan lainnya. Berikut peraturan di Indonesia terkait privasi dan pelindungan data pribadi:

A. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (UU Perbankan).

Undang-Undang Perbankan merupakan upaya pemerintah untuk memberikan kepastian hukum dalam kegiatan perbankan. Undang-Undang Perbankan dalam pengaturannya meliputi masalah-masalah perbankan sebagai lembaga serta aspek kegiatannya; asas, fungsi, dan tujuan bank; rambu-rambu yang harus dipenuhi oleh bank; perilaku petugasnya; hak, kewajiban, tugas, dan tanggung jawab bank; para pelaku serta pihak yang terkait dalam bisnis perbankan; serta hal lain yang berkenaan dengan dunia perbankan tersebut.

Nasabah dalam melakukan penyimpanan atau menggunakan produk bank lainnya harus memberikan data pribadi yang dianggap perlu kepada bank. Berdasarkan asas kepercayaan dan kerahasiaan, bank harus dapat menjaga kepercayaan nasabah serta melindungi privasi dari nasabah yang telah memberikan serta memercayakan data pribadinya

kepada pihak bank. Dalam Undang-Undang Perbankan, hak privasi nasabah dilindungi dengan diaturnya perihal rahasia bank. Pasal 1 ayat (28) Undang-Undang Perbankan menyebutkan rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.

Pasal 40 Undang-Undang Perbankan menyebutkan bahwa masalah rahasia bank, bank diwajibkan untuk merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali dalam hal-hal tertentu yang diperbolehkan. Pengaturan tersebut mengisyaratkan perlindungan privasi nasabah tidak hanya berkenaan dengan data keuangan (simpanan atau produk bank lain) miliknya tetapi juga data pribadi nasabah yang bersifat informasi ataupun keterangan yang menyangkut identitas atau data pribadi lain di luar data keuangan.

Menurut Pasal 47 ayat (2) Undang-Undang Perbankan, yang berkewajiban memegang teguh rahasia bank adalah:

1. Anggota Dewan Komisaris Bank;
2. Anggota Direksi Bank;
3. Pegawai Bank; dan,
4. Pihak terafiliasi lainnya dari Bank

Undang-Undang Perbankan memberikan beberapa pengecualian terhadap kewajiban dijaganya rahasia bank. Pengecualian-pengecualian tersebut adalah:[138]

1. Untuk kepentingan perpajakan dapat diberikan pengecualian kepada pejabat pajak berdasarkan perintah

[138] BAB VII tentang Rahasia Bank, Pasal 41 sampai dengan Pasal 44 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Pimpinan Bank Indonesia atas permintaan Menteri Keuangan (Pasal 41);

2. Untuk penyelesaian piutang bank yang sudah diserahkan kepada Badan Urusan Piutang dan Lelang Negara/Panitia Urusan Piutang Negara, dapat diberikan pengecualian kepada Pejabat Badan Urusan Piutang dan Lelang Negara/PUPN atas izin Pimpinan Bank Indonesia (Pasal 41A);
3. Untuk kepentingan peradilan dalam perkara pidana dapat diberikan pengecualian kepada polisi, jaksa atau hakim atas izin Pimpinan Bank Indonesia (Pasal 42);
4. Dalam perkara perdata antara bank dengan nasabahnya dapat diberikan pengecualian tanpa harus memperoleh izin Pimpinan Bank Indonesia (Pasal 43);
5. Dalam rangka tukar menukar informasi di antara bank kepada bank lain dapat diberikan pengecualian tanpa harus memperoleh izin dari Pimpinan Bank Indonesia (Pasal 44);
6. Atas persetujuan, permintaan atau kuasa dari nasabah penyimpan secara tertulis dapat diberikan pengecualian tanpa harus memperoleh izin Pimpinan Bank Indonesia [Pasal 44A ayat (1)]; dan
7. Atas permintaan ahli waris yang sah dari nasabah penyimpan dana yang telah meninggal dunia [Pasal 44A ayat (2)].

Untuk mendukung pengaturan perlindungan dari data pribadi nasabah tersebut, pengaturan pidana dari pelanggaran rahasia bank juga diatur dalam Pasal 47 ayat (1) dan ayat (2).

B. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Industri telekomunikasi merupakan industri yang memiliki perkembangan sangat pesat dengan nilai ekonomi yang tinggi. Indonesia telah aktif dalam membuka arus investasi bagi industri telekomunikasi sejak tahun 1980an. Tahun 1989, Indonesia mulai mengembangkan kebijakan dan peraturan perundang-undangan mengenai telekomunikasi dengan mengesahkan Undang-Undang Nomor 3 Tahun 1989 tentang Telekomunikasi. Undang-undang tersebut menjadi pijakan utama bagi pengembangan industri telekomunikasi di Indonesia. Pada tahun 1999 undang-undang tersebut disempurnakan serta disesuaikan dengan perkembangan telekomunikasi yang telah semakin maju dan dipandang tidak relevan untuk dikuasai oleh Badan Usaha Milik Negara saja. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Undang-Undang Telekomunikasi) kemudian disahkan untuk menggantikan undang-undang telekomunikasi sebelumnya.

Penyelenggaraan telekomunikasi berhubungan erat dengan transmisi, interkoneksi, serta perpindahan data dan informasi dengan cepat. Perpindahan informasi serta data pribadi ini dapat terjadi dengan sangat mudah dan cepat. Oleh karena itu untuk menjaga lalu lintas informasi dari penyelenggaraan telekomunikasi, dalam Pasal 18 ayat (1) diatur kewajiban penyelenggara telekomunikasi untuk mencatat atau merekam secara rinci pemakaian dari jasa telekomunikasi. Pasal 22 Undang-Undang Telekomunikasi melarang dilakukannya akses ke jaringan dan/atau jasa telekomunikasi atau telekomunikasi khusus secara tanpa hak, tidak sah, atau dengan manipulasi.

Selain pengaturan tersebut, perolehan atas informasi yang disalurkan melalui jaringan telekomunikasi dilarang dalam bentuk apapun sebagaimana diatur dalam Pasal 40. Hal ini menunjukan perlindungan privasi dari pengguna jasa telekomunikasi atas data pribadi miliknya yang ditransmisikan melalui penyelenggaraan telekomunikasi.[139]

Kerahasiaan dari data pribadi maupun informasi pribadi lain milik pengguna jasa telekomunikasi dilindungi dan wajib dijaga kerahasiaannya oleh penyelenggara telekomunikasi. Pasal 42 ayat (1) Undang-Undang Telekomunikasi mewajibkan penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan dan/atau jasa telekomunikasi yang diselenggarakannya. pengecualian terhadap kerahasiaan ini antara lain untuk kepentingan proses peradilan pidana atas permintaan tertulis jaksa agung atau kepala kepolisian serta penyidik.[140]

Pengaturan sanksi pidana dari pelanggaran pasal-pasal perlindungan privasi atas data pribadi pengguna jasa telekomunikasi di atas di antaranya terdapat dalam Pasal 56 dan Pasal 57 Undang-Undang Telekomunikasi. Pelanggaran atas pasal-pasal tersebut diancam dengan sanksi pidana baik berupa denda maupun pidana penjara.

C. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Undang-Undang Perlindungan Konsumen).

[139] Penjelasan Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

[140] Pasal 42 Ayat (2) dan Penjelasan Pasal 42 Ayat (2) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Data dan informasi yang dijamin oleh Undang-Undang Perlindungan Konsumen adalah informasi mengenai barang dan jasa, bukan informasi mengenai data pribadi konsumen. Akan tetapi, perlindungan konsumen menurut Pasal 2 Undang-Undang Perlindungan Konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan dan keselamatan konsumen, serta kepastian hukum tidak dijabarkan menjadi ketentuan pelindungan data pribadi konsumen. Seharusnya, perlindungan konsumen mencakup juga pelindungan data dan informasi.

Data pribadi mengenai konsumen sering kali didapatkan ketika konsumen menggunakan jasa atau membeli suatu barang. Sebagai contoh ketika konsumen menggunakan jasa kesehatan atau jasa perbankan, data-data yang didapatkan pelaku usaha kemudian disalahgunakan untuk kepentingan promosi, baik produk dari pelaku usaha yang sama atau bahkan data tersebut berpindah tangan kepada pihak di luar pelaku usaha yang berhubungan langsung dengan konsumen.

Promosi sendiri diatur dalam Undang-Undang Perlindungan Konsumen. Pengertian mengenai Promosi dijelaskan dalam Ketentuan Umum yang termuat dalam Pasal 1 ayat (6) yaitu: *Kegiatan pengenalan atau penyebarluasan informasi suatu barang dan/atau jasa untuk menarik minat beli konsumen terhadap barang dan/atau jasa yang akan dan sedang diperdagangkan.*

Kegiatan promosi yang banyak dipraktikkan oleh penyedia jasa dan penjual barang menjadi suatu masalah tersendiri apabila menggunakan data pribadi yang didapatkan dari pihak lain, tanpa persetujuan konsumen. Lebih jauh lagi promosi yang biasanya melalui media telepon, pesan pendek,

surat ataupun surat elektronik tersebut dapat menjadi promosi yang tidak diinginkan konsumen, bahkan mengganggu bagi sebagian orang. Hal tersebut salah satunya karena nomor telepon, alamat tempat tinggal, dan lain sebagainya merupakan privasi seseorang. Dari hal tersebut terlihat bahwa konsumen secara tidak langsung dirugikan oleh kegiatan promosi yang menggunakan data pribadi konsumen.

Namun dalam Undang-Undang Perlindungan Konsumen tidak ada ketentuan yang melarang promosi yang menggunakan data-data pribadi masyarakat yang didapatkan tanpa persetujuan masyarakat tersebut. Pasal 9 ayat (1) Undang-Undang Perlindungan Konsumen, hanya melarang menawarkan, memproduksikan, mengiklankan suatu barang dan/atau jasa secara tidak benar, dan/atau seolah-olah:

1. barang tersebut telah memenuhi dan/atau memiliki potongan harga, harga khusus, standar mutu tertentu, gaya atau mode tertentu, karakteristik tertentu, sejarah atau guna tertentu;
2. barang tersebut dalam keadaan baik dan/atau baru;
3. barang dan/atau jasa tersebut telah mendapatkan dan/atau memiliki sponsor, persetujuan, perlengkapan tertentu, keuntungan tertentu, ciri-ciri kerja atau aksesori tertentu;
4. barang dan/atau jasa tersebut dibuat oleh perusahaan yang mempunyai sponsor, persetujuan atau afiliasi;
5. barang dan/atau jasa tersebut tersedia;
6. barang tersebut tidak mengandung cacat tersembunyi;
7. barang tersebut merupakan kelengkapan dari barang tertentu;
8. barang tersebut berasal dari daerah tertentu;

9. secara langsung atau tidak langsung merendahkan barang dan/atau jasa lain;
10. menggunakan kata-kata yang berlebihan, seperti aman, tidak berbahaya, tidak mengandung risiko atau efek samping tampak keterangan yang lengkap;
11. menawarkan sesuatu yang mengandung janji yang belum pasti.

Selanjutnya berdasarkan Pasal 9 ayat (3) Undang-Undang Perlindungan Konsumen, pelaku usaha yang melakukan pelanggaran hal-hal di atas dilarang melanjutkan penawaran, promosi, dan pengiklanan barang dan/atau jasa tersebut. Terhadap ketentuan tersebut sanksi pidana dapat dijatuhkan kepada pelanggar berdasarkan Pasal 62 Undang-Undang Perlindungan Konsumen, yaitu pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp 2.000.000.000,00 (dua miliar rupiah).

Ketentuan di atas tidak mencakup mengenai pelindungan data pribadi milik konsumen. Oleh karena itu, konsumen di Indonesia tidak memiliki dasar hukum yang menjamin hak privasi sebagai konsumen. Dalam hal ini masih terjadi kekosongan hukum sehingga prilaku pelaku usaha tidak menghormati hak privasi atas data pribadi konsumen. Pada akhirnya konsumen lah yang kembali dirugikan oleh prilaku pelaku usaha tersebut.

D. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Undang-Undang HAM).

Dalam Pasal 29 ayat (1) Undang-Undang HAM diakui hak setiap orang atas perlindungan diri pribadi, keluarga,

kehormatan, martabat, dan hak miliknya. Hak privasi perlu mendapat pengakuan sebagai bagian dari HAM yang dilindungi. Hak privasi menjadi sangat penting dengan perkembangan masyarakat modern di mana pertukaran serta perpindahan informasi dapat terjadi dengan cepat dan mudah. Tidak menutup kemungkinan terjadi perpindahan data ataupun informasi pribadi seseorang secara tidak sah dan dipergunakan tanpa seizin pemiliknya.

Pasal 14 ayat (2) Undang-Undang HAM mengatur bahwa salah satu hak mengembangkan diri adalah hak untuk mencari, memperoleh, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia. Pasal 32 Undang-Undang HAM mengatur bahwa kemerdekaan dan rahasia dalam hubungan komunikasi melalui sarana elektronik dijamin, kecuali atas perintah hakim atau kekuasaan yang lain yang sah sesuai dengan ketentuan perundangan.

Pengaturan yang terdapat dalam Pasal 14 ayat (2) serta Pasal 32 Undang-Undang HAM di atas menunjukkan terdapatnya keseimbangan antara adanya hak untuk memperoleh (mencari, memperoleh, menyimpan) serta menyampaikan informasi, dengan hak atas diakuinya kerahasiaan dalam komunikasi termasuk di dalamnya data pribadi untuk menyimpan informasi terutama yang berhubungan dengan informasi pribadi seseorang. Dapat disimpulkan bahwa jaminan terhadap diakuinya hak privasi seseorang dalam Pasal 32 Undang-Undang HAM terutama adalah dalam perlindungan terhadap informasi serta data pribadi yang seseorang.

E. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan).

Dalam ketentuan umum pada Pasal 1 angka 9 disebutkan bahwa data kependudukan, adalah data perseorangan dan/atau data agregat yang terstruktur sebagai hasil dari kegiatan Pendaftaran Penduduk dan Pencatatan Sipil. Pasal 1 angka 22 disebutkan data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Dalam pengertian dari data pribadi yang terdapat dalam Undang-Undang Administrasi Kependudukan telah terdapat amanat perlindungan kerahasiaan dari data pribadi.

Pasal 2 menjamin hak setiap penduduk untuk memperoleh perlindungan atas data pribadi, kepastian hukum atas kepemilikan dokumen, serta informasi mengenai data hasil pendaftaran penduduk dan pencatatan sipil atas dirinya dan/atau keluarganya. Dalam Pasal 2 huruf f disebutkan bahwa penduduk berhak untuk memperoleh ganti rugi dan pemulihan nama baik sebagai akibat kesalahan dalam pendaftaran penduduk dan pencatatan sipil serta penyalahgunaan data pribadi oleh instansi pelaksana.

Pasal 8 ayat (1) huruf e Undang-Undang Administrasi Kependudukan menyebutkan kewajiban instansi pelaksana melaksanakan urusan administrasi kependudukan yang diantaranya meliputi menjamin kerahasiaan dan keamanan data atas peristiwa kependudukan dan peristiwa penting.

Kerahasiaan serta keamanan data atas peristiwa kependudukan dan peristiwa penting telah menjadi tanggung jawab dari instansi pelaksana administrasi kependudukan.

Perlindungan dari data dan dokumen kependudukan dipertegas dalam Pasal 79 ayat (1) yang menyebutkan bahwa data dan dokumen kependudukan wajib disimpan dan dilindungi oleh negara. Kewajiban perlindungan atas kerahasiaan Data Pribadi Penduduk juga kembali dipertegas dalam Pasal 85 ayat (3) yang menyebutkan bahwa harus dijaga kebenarannya dan dilindungi kerahasiaannya oleh penyelenggara dan instansi pelaksana.

Pasal 84 ayat (1) menyebutkan data pribadi penduduk yang harus dilindungi. Data pribadi tersebut antara lain memuat nomor Kartu Keluarga (KK); Nomor Induk Kependudukan (NIK); tanggal/bulan/tahun lahir; keterangan tentang kecacatan fisik dan/atau mental; NIK ibu kandung; NIK ayah; dan beberapa isi catatan peristiwa penting. Amanat perlindungan atas kerahasiaan data pribadi penduduk terdapat dalam Pasal 85 ayat (1) yang menyebutkan bahwa data pribadi penduduk wajib disimpan dan dilindungi oleh negara.

Data penduduk yang dihasilkan oleh sistem informasi dan tersimpan di dalam *data base* kependudukan dapat dimanfaatkan untuk berbagai kepentingan, seperti dalam menganalisa dan merumuskan kebijakan kependudukan, menganalisa dan merumuskan perencanaan pembangunan, pengkajian ilmu pengetahuan.[141] Dengan demikian baik pemerintah maupun non-pemerintah untuk kepentingannya

[141] Penjelasan Pasal 83 Ayat (1) Undang Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

dapat diberikan izin terbatas dalam arti terbatas waktu dan peruntukannya.

Pasal 87 ayat (1) mengatur bahwa pengguna data pribadi penduduk yang merupakan instansi pemerintah atau swasta dapat memperoleh dan menggunakan data pribadi dari petugas pada penyelenggara dan instansi pelaksana yang memiliki hak akses. Yang dimaksud dengan pengguna data pribadi penduduk adalah instansi pemerintah dan swasta yang membutuhkan informasi data sesuai dengan bidangnya.[142]

Hak akses atas data pribadi serta dokumen kependudukan diberikan oleh menteri sebagai penanggung jawab atas hak akses kepada petugas pada penyelenggara dan instansi pelaksana penyelenggaraan administrasi kependudukan sebagaimana disebutkan dalam Pasal 79 ayat (2). Hak akses yang diberikan di antaranya adalah hak untuk memasukkan, menyimpan, membaca, mengubah, meralat dan menghapus, serta mencetak data, menyalin data dan dokumen kependudukan.

Selain hak akses di atas, dalam Pasal 86 ayat (1) juga disebutkan bahwa Menteri sebagai penanggung jawab memberikan hak akses kepada petugas pada penyelenggara dan instansi pelaksana untuk memasukkan, menyimpan, membaca, mengubah, meralat dan menghapus, menyalin data serta mencetak data pribadi.

Larangan atas ilegal akses serta penyalahgunaan data pribadi ataupun dokumen kependudukan yang terdapat dalam sistem administrasi kependudukan terdapat dalam Pasal 77 yang melarang setiap orang untuk mengubah, menambah atau

[142] *Ibid.*

mengurangi tanpa hak, isi elemen data pada dokumen kependudukan.

Ancaman pidana atas pelanggaran privasi serta penyalahgunaan data pribadi dalam administrasi kependudukan selanjutnya diatur dalam Pasal 93 yang mengancam pidana penjara serta denda bagi setiap penduduk yang dengan sengaja memalsukan surat dan/atau dokumen kepada Instansi Pelaksana dalam melaporkan Peristiwa Kependudukan dan Peristiwa Penting. Selanjutnya Pasal 94 mengancam dengan pidana setiap orang yang tanpa hak dengan sengaja mengubah, menambah, atau mengurangi isi elemen data pada dokumen kependudukan.

Setiap orang yang tanpa hak mengakses *data base* kependudukan dalam Pasal 86 ayat (1) dipidana dengan pidana penjara serta denda dalam Pasal 95. Demikian pula bagi setiap orang atau badan hukum yang tanpa hak mencetak, menerbitkan, dan/atau mendistribusikan blangko dokumen kependudukan dalam Pasal 96. Dalam hal pejabat dan petugas pada Penyelenggara dan Instansi Pelaksana membantu melakukan tindak pidana pejabat yang bersangkutan juga diancam akan dipidana sebagaimana disebutkan dalam Pasal 98 ayat (2).

F. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE)

Pengertian sistem elektronik menurut Pasal 1 angka 5 Undang-Undang ITE adalah serangkaian perangkat dan

prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Berdasarkan pengertian sistem elektronik tersebut, dapat diketahui bahwa yang termasuk ke dalam sistem elektronik adalah jaringan internet, layanan *e-banking*, *e-government*, jejaring sosial, media elektronik, *website*, dan lain sebagainya.

Dalam pemanfaatan teknologi informasi, pelindungan data pribadi merupakan salah satu bagian dari hak privasi. Untuk memberikan rasa aman bagi pengguna sistem elektronik, dalam Undang-Undang ITE diatur mengenai perlindungan atas data pribadi dan hak privasi yang tertuang dalam Pasal 26 ayat (1) Undang-Undang ITE, yang berbunyi:

> *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.*

Untuk memperjelas makna dari perlindungan hak privasi yang dilindungi oleh Undang-Undang ITE, dalam penjelasan Pasal 26 dijelaskan bahwa hak pribadi dalam pasal tersebut mengandung pengertian sebagai berikut:[143]

1. hak merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
2. hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
3. hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

[143] Penjelasan Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Sebagaimana ditentukan dalam Pasal 26 Undang-Undang ITE, penggunaan setiap informasi dan data pribadi melalui media elektronik yang dilakukan tanpa persetujuan pemilik data tersebut adalah sebuah pelanggaran hak privasi.

Meskipun terdapat pengakuan atas perlindungan hak privasi serta data pribadi dalam informasi dan transaksi elektronik dalam Undang-Undang ITE sebagaimana terdapat dalam Pasal 26 beserta penjelasannya, kewajiban perlindungan serta upaya perlindungan yang seharusnya dilakukan oleh pihak-pihak terkait seperti penyelenggara sistem elektronik ataupun pemerintah belum terdapat dalam Undang-Undang ITE.

Landasan pemikian yang mendasari lahirnya Undang-Undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) yang diundangkan pada tanggal 21 April 2008 yakni hakikat keberadaan dunia maya atau dunia siber (*cyberspace*) bahwa sebuah konstruksi maya yang diciptakan oleh komputer yang di dalamnya berisi data-data abstrak yang berfungsi sebagai berikut: (1) aktualisasi diri; (2) wadah bertukar gagasan; dan (3) sarana penguatan prinsip demokrasi. Manusia dapat masuk ke dalam sistem data dan jaringan komputer tersebut kemudian mendapatkan suatu perasaan bahwa mereka benar-benar telah memasuki suatu ruang yang tidak memiliki keterikatan sama sekali dengan realitas-realitas fisik. Oleh karena itu, aktivitas-aktivitas di dunia siber mempunyai karakter, yaitu: (1) mudah, (2) penyebarannya sangat cepat dan meluas yangd apat diakses oleh siapapun dan dimanapun, dan (3) dapat bersifat destruktif dari pemuatan materi penghinaan dan/atau pencemaran nama baik dengan menggunakan media elektronik sangat luar biasa

karena memiliki corak viktimisasi yang tidak terbatas. Dengan memahami hakekat dunia siber beserta karakternya,maka diperlukan pengaturan tersendiri untuk mengakomodasi perkembangan dan konvergensi Teknologi Informasi, yang dapat digunakan sebagai sarana dalam melakukan kejahatan. Akan tetapi, dalam kenyataannya, perjalanan implementasi dari UU ITE mengalami persoalan-persoalan sebagai berikut:

Pertama, dibatalkannya pengaturan tatacara intersepsi yang akan diatur menggunakan peraturan pemerintah, keputusan Mahkamah konstitusi (MK) Nomor 5/PUU-VIII/2010 yang bacakan dalam Sidang Pleno pada hari Kamis 24 Februari 2011, yang Menyatakan Pasal 31 ayat (4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bertentangan dengan Undang-Undang Dasar NRI Tahun 1945 sehingga tidak mempunyai kekuatan hukum mengikat. Isi Pasal 31 ayat (4) adalah "Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah". Menurut MK, pengaturan mengenai intersepsi harusnya diatur dengan undang-undang.

Kedua, munculnya keberatan sebagian masyarakat terhadap Pasal 27 ayat (3) tentang pencemaran nama baik dan/atau penghinaan melalui internet yang berujung pada constitutional review Pasal 27 ayat (3) ke Mahkamah Konstitusi oleh dua pihak, masing-masing permohonan pertama oleh Narliswandi Piliang pada tanggal 25 November 2008 dan permohonan kedua oleh Eddy Cahyono dan kawan-kawan pada tanggal 5 Januari 2009. dalam sidang constitutional review di Mahkamah Konstitusi terungkap yang menjadi keberatan para pihak penggugat tersebut adalah terhadap ketentuan pidana

yang termaktub dalam UU ITE, terutama ancaman sanksi pidana pada Pasal 45 ayat (1) yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Ketentuan ini dinilai terlalu berat dibandingkan dengan ancaman sanksi dalam Pasal 310 ayat (1) KUHP yaitu pidana penjara paling lama 9 (Sembilan) bulan atau pidana denda paling banyak empat ribu lima ratus rupiah. Dampak pengaturan ancaman pidana penjara 5 (lima) tahun atau lebih, membawa konsekuensi sesuai dengan ketentuan KUHAP bahwa tersangka pelaku tindak pidana Pasal dimaksud dapat dikenakan penahanan.

G. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Undang-Undang Keterbukaan Informasi Publik).

Pasal 1 ayat (1) Undang-Undang Keterbukaan Informasi Publik mengatur bahwa informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.[144] Sedangkan pengertian informasi publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu Badan Publik yang berkaitan dengan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan Badan Publik lainnya yang berkaitan dengan

[144] Pasal 1 ayat 1 Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

kepentingan publik.[145] Dari pengertian informasi publik tersebut, terlihat bahwa badan publik sebagaimana yang diatur dalam undang-undang melakukan pengumpulan data dan informasi yang berkaitan dengan penyelenggaraannya. Pengumpulan data dan informasi tersebut juga termasuk pengumpulan data dan informasi milik masyarakat yang dihimpun sedemikian rupa sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Pelindungan data dan informasi publik yang dihimpun oleh badan publik diatur dalam Pasal 6 ayat (3) Undang-Undang Keterbukaan Informasi Publik. Berdasarkan aturan tersebut, terdapat informasi publik yang tidak dapat diberikan oleh badan publik, yaitu:[146]

1. informasi yang dapat membahayakan negara;
2. informasi yang berkaitan dengan kepentingan perlindungan usaha dari persaingan usaha tidak sehat;
3. informasi yang berkaitan dengan hak-hak pribadi;
4. informasi yang berkaitan dengan rahasia jabatan; dan/atau
5. informasi publik yang diminta belum dikuasai atau didokumentasikan.

Dari ketentuan tersebut, telah jelas bahwa badan publik tidak dapat memberikan informasi publik yang salah satumya berkaitan dengan hak-hak pribadi. Lebih jauh, dalam Pasal 52 Undang-Undang Keterbukaan Informasi Publik ditentukan bahwa badan publik yang dengan sengaja tidak menyediakan, tidak memberikan, dan/atau tidak menerbitkan informasi

[145] Pasal 1 ayat 2 Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.
[146] Pasal 6 ayat 3 Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

publik berupa informasi publik secara berkala, informasi publik yang wajib diumumkan secara serta-merta, informasi publik yang harus diberikan atas dasar permintaan sesuai dengan undang-undang ini, dan mengakibatkan kerugian bagi orang lain dikenakan pidana kurungan paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp. 5.000.000,00 (lima juta rupiah).[147]

H. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (Undang-Undang Kesehatan).

Perlindungan terhadap riwayat kesehatan pasien terdapat dalam Pasal 57 ayat (1) Undang-Undang Kesehatan yang mengakui hak setiap orang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan. Selanjutnya dalam Pasal 57 ayat (2) diatur mengenai ketentuan pengecualian atas rahasia kondisi kesehatan pribadi yang tidak berlaku dalam hal:

1. perintah undang-undang;
2. perintah pengadilan;
3. izin yang bersangkutan;
4. kepentingan masyarakat; atau
5. kepentingan orang tersebut.

Meskipun terdapat pengakuan hak pasien untuk mendapatkan perlindungan atas data pribadinya yang berupa riwayat kesehatan, namun pelindungan data pribadi pasien tidak secara penuh diatur dalam Undang-Undang Kesehatan. Di dalam Undang-Undang Kesehatan tidak terdapat pengaturan sanksi ataupun hukuman bagi pelanggaran privasi yang

[147] Pasal 52 Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

dilakukan atas riwayat kesehatan pasien. Tidak terdapat pengaturan sanksi baik administratif atau pidana baik atas akses secara tidak sah maupun penyalahgunaan dari data pribadi pasien oleh pihak yang tidak berhak.

I. Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian (Undang-Undang Perasuransian).

Pasal 67 Undang-Undang Perasuransian mengatur masalah perlindungan informasi oleh pihak lain yang ditunjuk atau ditugasi oleh Otoritas Jasa Keuangan dalam menjalankan fungsi pengawasan dan sebagian dari fugsi pengaturan. Pihak tersebut dilarang menggunakan atau mengungkapkan informasi apa pun yang bersifat rahasia kepada pihak lain, kecuali dalam rangka pelaksanaan fungsi, tugas, dan wewenangnya berdasarkan keputusan Otoritas Jasa Keuangan atau diwajibkan oleh undang-undang.

J. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Undang-Undang Otoritas Jasa Keuangan)

Pasal 33 ayat (1) Undang-Undang tentang Otoritas Jasa Keuangan mengatur mengenai kerahasiaan informasi. Setiap orang perseorangan yang menjabat atau pernah menjabat sebagai anggota Dewan Komisioner, pejabat atau pegawai Otoritas Jasa Keuangan (selanjutnya disebut OJK) dilarang menggunakan atau mengungkapkan informasi apa pun yang bersifat rahasia kepada pihak lain, kecuali dalam rangka pelaksanaan fungsi, tugas, dan wewenangnya berdasarkan keputusan OJK atau diwajibkan oleh Undang-Undang.

Selanjutnya dalam Pasal 33 ayat (2) ditentukan bahwa setiap Orang yang bertindak untuk dan atas nama OJK, yang dipekerjakan di OJK, atau sebagai staf ahli di OJK, dilarang

menggunakan atau mengungkapkan informasi apa pun yang bersifat rahasia kepada pihak lain, kecuali dalam rangka pelaksanaan fungsi, tugas, dan wewenangnya berdasarkan keputusan OJK atau diwajibkan oleh Undang-Undang.

Otoritas Jasa Keuangan juga telah mengatur kerahasiaan data pribadi konsumen dalam Peraturan OJK No.1/POJK.7/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan juga mengatur bahwa Pelaku Usaha Jasa Keuangan dilarang dengan cara apapun, memberikan data dan/atau informasi mengenai konsumennya kepada pihak ketiga. Apabila Pelaku Usaha Jasa Keuangan telah mendapatkan data konsumen dari dan/atau hendak diberikan kepada pihak lain maka harus berdasarkan kewajiban peraturan perundang-undangan, atau harus disertai pernyataan tertulis bahwa konsumen tersebut telah menyetujui untuk memberikan data atau informasi pribadi kepada pihak manapun termasuk pelaku jasa keuangan. Konsumen boleh merubah kesepakatan pengungkapan data atau informasi pribadi yang telah diberikan sebelumnya secara tertulis.

K. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).

Di dalam pengaturan yang terdapat dalam PP PSTE, salah satu hal yang menjadi sorotan serta mendapat perhatian besar adalah berkenaan dengan pelindungan data dan informasi, terutama yang bersifat pribadi dalam transaksi elektronik. Perlindungan terhadap data pribadi yang bersifat elektronik ini terutama melihat kepada kemudahan yang diberikan oleh

perkembangan sistem elektronik yang memudahkan transmisi serta kases akan data dan informasi.

Dalam ketentuan umum PP PSTE pada Pasal 1 ayat (29) disebutkan bahwa data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.

Salah satu bentuk data yang dilindungi adalah yang berbentuk informasi elektronik. Pasal 1 ayat (8) PP PSTE menjelaskan informasi elektronik sebagai satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi. Informasi elektronik ini dapat terdapat dalam sistem elektronik atau berupa sebuah dokumen elektronik.

Dalam PP PSTE, perlindungan privasi terutama dalam kerahasiaan data pribadi diatur dalam beberapa pasal, yaitu:

1. Pasal 14, yang mengatur mengenai prinsip, ruang lingkup, dan alas hak pemrosesan data pribadi, serta kewajiban pemberitahuan dalam hal terjadinya kegagalan pelindungan data pribadi; dan
2. Pasal 15 hingga Pasal 17, yang mengatur mengenai penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan.

Pelanggaran terhadap upaya pelindungan data pribadi tersebut, penyelenggara sistem elektronik akan diberikan sanksi administratif sebagaimana terdapat dalam Pasal 100. Sanksi

administratif tersebut dapat berupa teguran tertulis, denda administratif, penghentian sementara, serta dikeluarkan dari daftar penyelenggara sistem elektronik, agen elektronik, penyelenggara sertifikasi elektronik, atau lembaga sertifikasi keandalan.

L. Peraturan Presiden Nomor 26 Tahun 2009 sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Presiden Nomor 112 Tahun 2013 tentang Perubahan Keempat atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (Perpres KTP).

Perpres KTP merupakan perubahan keempat dari Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional yang sebelumnya telah diubah dengan Peraturan Presiden Nomor 35 Tahun 2010 tentang Perubahan atas Peraturan Presiden Nomor 26 Tahun 2009 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, dan diubah kedua kalinya dengan Peraturan Presiden Nomor 67 Tahun 2011 tentang Perubahan Kedua atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, dan Peraturan Presiden Nomor 126 Tahun 2012 tentang Perubahan Ketiga atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.

Di dalam KTP termuat kode keamanan dan rekaman elektronik sebagai alat verifikasi dan validasi data jati diri

penduduk.[148] Kode keamanan adalah alat identifikasi jati diri yang menunjukan identitas diri penduduk secara tepat dan akurat sebagai autentikasi diri yang memastikan dokumen kependudukan sebagai milik orang tersebut, sedangkan rekaman elektronik berisi biodata, tanda tangan, pas foto, dan sidik jari tangan penduduk yang bersangkutan.[149]

Rekaman serta data-data pribadi penduduk disimpan dalam *data base* kependudukan dan dapat diakses oleh pihak-pihak yang berkepentingan sesuai dengan Undang-Undang Administrasi Kependudukan. Instansi pemerintah dan swasta yang membutuhkan informasi data sesuai dengan bidangnya, dapat memperoleh dan menggunakan data pribadi dari petugas pada penyelenggara dan instansi pelaksana yang memiliki hak akses.

Di dalam Perpres tentang KTP tersebut tidak terdapat pengaturan yang menyebutkan kewajiban perlindungan terhadap data pribadi milik penduduk yang terdapat dalam KTP dan database kependudukan. Meskipun demikian, semangat Perpres KTP sejalan dengan Undang-Undang Administrasi Kependudukan memiliki amanat perlindungan terhadap data pribadi. Selain itu, di dalam Perpres KTP diatur bahwa KTP Elektronik merupakan KTP yang dilengkapi dengan *chip* serta sistem pengamanan khusus.[150]

---

[148] Pasal 6 ayat (1) Peraturan Presiden Nomor 35 Tahun 2010 tentang Perubahan atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.

[149] Pasal 1 angka 8 Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.

[150] Pasal 10 A Ayat (1) Peraturan Presiden Republik Indonesia Nomor 67 Tahun 2011 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.

M. Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah (PBI No. 7/6/PBI/2005).

PBI No. 7/6/PBI/2005 merupakan bentuk nyata dari peraturan pelaksana yang dikeluarkan Bank Indonesia demi melindungi privasi nasabah bank atas data pribadinya. PBI No. 7/6/PBI/2005 ditetapkan berdasarkan pertimbangan bahwa transparansi terhadap penggunaan data pribadi yang disampaikan nasabah kepada bank diperlukan untuk meningkatkan perlindungan terhadap hak-hak pribadi nasabah dalam berhubungan dengan bank.

Dalam Pasal 9 ayat (1) PBI No 7/6/PBI/2005, disebutkan sebagai berikut:

> *Bank wajib meminta persetujuan tertulis dari nasabah dalam hal bank akan memberikan dan atau menyebarluaskan data pribadi nasabah kepada pihak lain untuk tujuan komersial, kecuali ditetapkan lain oleh peraturan perundang-undangan lain yang berlaku.*

Dalam meminta persetujuan nasabah atas penggunaan ataupun penyebarluasan data pribadi milik nasabah, bank harus menjelaskan tujuan serta konsekuensi dari penggunaan data tersebut. Hal ini terutama bagi penggunaan data pribadi nasabah untuk tujuan komersial, digunakan pihak lain untuk memperoleh keuntungan.[151]

Pasal 10 ayat (2) selanjutnya mengatur bahwa dalam meminta persetujuan nasabah yang bersangkutan, harus dilakukan dengan penandatanganan sebuah formulir persetujuan yang telah dibuat khusus untuk persetujuan penggunaan data pribadi nasabah tersebut. Klausul permintaan

[151] Penjelasan Pasal 9 ayat 1 Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah.

persetujuan tersebut bersifat *opt-in*. Berarti bank dilarang melakukan hal-hal yang menjadi tujuan pencantuman klausul tersebut, sebelum nasabah memberikan persetujuan atas klausul.[152]

Selain dari pada penggunaan data pribadi nasabah bank, penggunaan data pribadi oleh bank yang sebelumnya diperoleh pihak lain untuk tujuan komersial juga diatur dalam PBI No. 7/6/PBI/2005. Dalam Pasal 11 PBI No. 7/6/PBI/2005 disebutkan apabila bank akan menggunakan data pribadi seseorang dan atau sekelompok orang yang diperoleh dari pihak lain untuk tujuan komersial, maka bank wajib untuk memiliki jaminan tertulis dari pihak yang bersangkutan yang berisi persetujuan tertulis dari orang-orang yang bersangkutan untuk disebarluaskan data pribadinya oleh bank.

Pelanggaran oleh bank atas transparansi penggunaan data pribadi oleh bank yang telah diatur dalam PBI No. 7/6/PBI/2005 dikenakan sanksi administratif serta dijadikan bahan perhitungan dalam komponen penilaian tingkat kesehatan bank pada aspek manajemen bank.[153]

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

Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDPSE) diatur sebagai pelaksanaan amanat dari Ketentuan Pasal 15 ayat (3) Peraturan Pemerintah

[152] Penjelasan Pasal 10 ayat 2 Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah.
[153] Penjelasan Pasal 12 ayat 2 Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah.

(PP) Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Sehubungan dengan telah dicabutnya PP Nomor 82 Tahun 2012 tersebut, Permen PDPSE ini perlu disesuaikan dengan PP Nomor 71 Tahun 2019 tentang PSTE.

Dalam Permen PDPSE, istilah data pribadi didefinisikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Frasa data perseorangan tertentu merupakan 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. Dari definisi tersebut, terdapat batasan kualifikasi data pribadi yang dilindungi yaitu hanya terbatas pada data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya dalam perspektif Peraturan Menteri tentang PDPSE.

Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi. Untuk setiap kegiatan tersebut harus berdasarkan pada asas perlindungan Data Pribadi yang baik meliputi: (1) penghormatan terhadap Data Pribadi sebagai privasi; (2) Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan; (3) berdasarkan Persetujuan; (4) relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan; (5) kelaikan Sistem Elektronik yang

digunakan; (6) iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi; (7) ketersediaan aturan internal pemrosesan perlindungan Data Pribadi; (8) tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna; (9) kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi; dan (10) keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.

Dalam pelaksanaanya, Peraturan Menteri tentang PDPSE memberikan hak kepada pemilik data pribadi meliuti: (1) atas kerahasiaan Data Pribadinya; (2) mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri; (3) mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pemrosesan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; (4) mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan (5)meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan. Disamping memberikan hak kepada pemilik data pribadi, Peraturan Menteri tentang PDPSE juga menegaskan kewajiban Penyelenggara Sistem Elekronik yakni: (1) melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan; (2) menjaga

kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi; (3) memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut: (a) harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi; (b) dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya; (c) harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan (d) pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut; (4) memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan; (5) menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya; (6) memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi; (7) memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pemrosesan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-

undangan; (8) 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 (9) menyediakan narahubung (contact person) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pemrosesan Data Pribadinya.

Disamping mengatur hak pemilik data pribadi dan kewajiban Penyelenggara Sistem Elektroni, Peraturan Menteri tentan PDPSE juga mengatur kewajiban pengguna meliputi: (1) menjaga kerahasiaan Data Pribadi yang diperoleh, dikumpulkan, diolah, dan dianalisisnya; (2) menggunakan Data Pribadi sesuai dengan kebutuhan Pengguna saja; (3) melindungi Data Pribadi beserta dokumen yang memuat Data Pribadi tersebut dari tindakan penyalahgunaan; dan (4) bertanggung jawab atas Data Pribadi yang terdapat dalam penguasaannya, baik penguasaan secara organisasi yang menjadi kewenangannya maupun perorangan, jika terjadi tindakan penyalahgunaan.

Media penyelesaian sengketa juga dibuka dengan memberikan hak kepada setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan pengaduan kepada Menteri atas kegagalan perlindungan kerahasiaan Data Pribadi dengan upaya penyelesaian sengketa secara musyawarah atau melalui upaya penyelesaian alternatif lainnya. Sedangkan pengawasan dilaksanakan oleh Menteri dan/atau pimpinan Intansi Pengawas dan Pengatur Sektor dengan melibatkan peran serta masyarakat.

BAB IV
LANDASAN FILOSOFIS, SOSIOLOGIS, DAN YURIDIS

Secara teoritis undang-undang yang baik adalah undang-undang yang dapat memenuhi atau dapat dipertanggungjawabkan baik secara filosofis, sosiologis, maupun yuridis.

A. Landasan Filosofis

Secara filosofis upaya pengaturan menyangkut hak privasi atas data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak-hak dasar manusia. Oleh karena itu, penyusunan Rancangan Undang-Undang Pelindungan Data pribadi memiliki landasan filosofis yang kuat dan dapat dipertanggungjawabkan.

Landasan filosofis perlindungan data pribadi adalah Pancasila yaitu *rechtsidee* (cita hukum) yang merupakan konstruksi pikir (ide) yang mengarahkan hukum kepada apa yang dicita-citakan. Rudolf Stamler, mengatakan bahwa *rechtsidee* berfungsi sebagai *leitsern* (bintang pemandu) bagi terwujudnya cita-cita sebuah masyarakat. Dari *rechtsidee* itulah disusun konsep dan politik hukum dalam sebuah negara. Cita hukum tersebut merupakan suatu yang bersifat normatif, dan juga konstitutif. Normatif artinya berfungsi sebagai prasyarat *transcendental* yang mendasari tiap hukum positif yang bermartabat, dan merupakan landasan moral hukum dan sekaligus tolak ukur sistem hukum positif. Cita hukum yang konstitutif berarti *rechtsidee* berfungsi mengarahkan hukum pada tujuan yang ingin dicapai. Gustaf Radbruch menyatakan bahwa "*rechtsidee*" berfungsi sebagai dasar yang bersifat konstitutif bagi hukum positif, memberi makna bagi hukum. *Rechtsidee* menjadi tolok ukur yang bersifat regulatif, yaitu

menguji apakah hukum positif adil atau tidak. Cita hukum akan mempengaruhi dan berfungsi sebagai asas umum yang memberikan pedoman (*guiding principle*), norma kritik (kaidah evaluasi), dan faktor yang memotivasi dalam penyelenggaraan hukum (pembentukan, penemuan, penerapan hukum dan perilaku hukum).

Sila kedua Pancasila yaitu, ”Kemanusiaan yang adil dan beradab” merupakan landasan filosofis perlindungan data pribadi, hal ini mengingat bahwa perlindungan dimaksud akan menciptakan keadilan dan membentuk peradaban manusia yang menghormati dan menghargai data pribadi.

Sebagai konsekuensi dari kedudukan Pancasila yang terkandung dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagai *staatsfundamentalnorm*, maka secara yuridis nilai-nilai Pancasila harus diderivasikan ke dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan selanjutnya pada seluruh peraturan perundang-undangan lain. Dalam kerangka ini, maka negara hukum Indonesia dapat pula dinamakan negara hukum Pancasila.[154]

Kelima sila Pancasila menjadi satu kesatuan merupakan satu kesatuan sistem filsafat bangsa Indonesia. Sila pertama, Ketuhanan Yang Maha Esa mengandung filosofi bahwa bangsa Indonesia meyakini keberadaan Tuhan Yang Maha Esa dan menyadari keterbatasan mahluk Tuhan. Sila kedua,

---

[154] Muhammad Tahir Azhary, *Negara Hukum: Suatu Studi tentang Prinsip-Prinsipnya Dilihat dari Segi Hukum Islam, Implementasinya pada Periode Negara Madinah dan Masa Kini,* Kencana, Bogor, 2003, hlm. 102. Negara Hukum Pancasila memiliki ciri-ciri: hubungan yang erat antara agama dan negara; bertumpu pada Ketuhanan Yang Maha Esa; kebebasan agama dalam arti positif, ateis metidak dibenarkan dan komunisme dilarang; serta asas kekeluargaan dan kerukunan. Unsur-unsur utamanya: Pancasila, MPR, sistem konstitusi, persamaan dan peradilan bebas.

kemanusiaan yang adil dan beradab, memiliki filosofi bahwa negara Indonesia berusaha mewujudkan suatu kemaslahatan umat manusia. Sila ketiga, persatuan Indonesia, memiliki filosofi bahwa dengan persatuan, bangsa Indonesia akan kuat dan secara bersama-sama berupaya untuk mewujudkan tujuan bernegara. Sila keempat, kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam permusyawaratan/ perwakilan, mengandung filosofi bahwa negara Republik Indonesia berbentuk demokrasi dalam setiap bidang kehidupan bernegara. Sila kelima, keadilan sosial bagi seluruh rakyat Indonesia, memiliki filosofi bahwa bangsa Indonesia berkeinginan untuk memberikan keadilan dan kesejahteraan secara formal dan substansial kepada rakyat Indonesia.[155]

Pancasila terkandung dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sebagai konstitusi negara Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang merupakan hukum dasar bagi pembentukan hukum positif mengandung empat ide pokok, yang oleh para ahli disepakati sebagai cita hukum Indonesia, yaitu: pertama, cita perlindungan yang terkandung dalam frasa "Negara melindungi segenap bangsa Indonesia, dan seluruh tumpah darah Indonesia dengan berdasarkan atas persatuan"; kedua, cita keadilan sosial, yang terkandung dalam frasa "Negara berhak mewujudkan keadilan sosial bagi seluruh rakyat Indonesia"; ketiga, cita kemanfaatan yang terkandung dalam frasa "Negara yang berkedaulatan rakyat, berdasar kerakyatan dan permusyawaratan perwakilan"; dan keempat, cita keadilan umum, yang terkandung dalam frasa "Negara

[155] Candra Irawan, *Politik Hukum Hak Kekayaan Intelektual Indonesia,* Mandar Maju, Bandung, 2011, hlm. 22

berdasar atas Ketuhanan Yang Maha Esa". Cita perlindungan mengandung makna cita hukum yang menjamin perlindungan segenap bangsa Indonesia, sesuai dengan prinsip keadilan kumulatif yang dikemukakan oleh Jeremy Bentham, bahwa fungsi hukum yang utama adalah memberi penghidupan, mendorong persamaan, dan memelihara keamanan bagi semua orang. Cita keadilan sosial mencerminkan hukum yang menjamin keadilan dalam hidup bermasyarakat, yakni mewujudkan keadilan sosial bagi seluruh masyarakat, yang mengutamakan perlakuan adil bagi seluruh rakyat Indonesia tanpa memandang ras, golongan, dan agama. Keadilan semacam ini oleh Aristoteles dan Thomas Aquinas sebagai keadilan distributif, yaitu pembagian barang dan kehormatan pada masing-masing anggota masyarakat sesuai dengan kedudukannya dalam masyarakat. Cita kemanfataan yang merupakan cita hukum dalam bernegara yakni cita tentang kegunaan hukum dalam bernegara.

Menurut Sunaryati Hartono, falsafah hukum yang dianut oleh para pendiri bangsa Indonesia adalah bahwa rakyat Indonesia menganut paham Hak Dasar Manusia, baik sebagai kelompok maupun sebagai perorangan.[156] Terkait dengan perlindungan data pribadi, hal ini dapat dipahami bahwa perlindungan terhadap data pribadi merupakan perwujudan perlindungan hak asasi manusia yang sesuai dengan paham yang dianut oleh Bangsa Indonesia.

Negara hukum yang demokratis adalah cita-cita para pendiri negara (*the founding fathers*) Republik Indonesia, karena

[156] Sunaryati Hartono, "Mencari Filsafat Hukum Indonesia yang Melatar belakangi Pembukaan Undang-Undang Dasar 1945", dalam Sri Rahayu Oktorina dan Niken Savitri, *Butir-Butir Pemikiran dalam Hukum, Memperingati 70 Tahun Prof. Dr. B. Arief Sidharta, S.H.,* PT. Refika Aditama, Bandung, 2008, hlm. 150.

dengan negara hukum yang demokratis, selain keadilan sebagai tujuan negara hukum (*rechtsstaat*), juga diupayakan tercapainya peningkatan kesejahteraan umum dan kecerdasan bangsa sebagaimana menjadi tujuan negara kesejahteraan (*welvaarrtstaat*).[157] Dengan lain perkataan, yang diharapkan oleh penyusun Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 bukanlah semata negara hukum dalam arti yang sangat sempit atau negara berdasar undang-undang; bukan pula kehidupan bernegara berdasarkan supremasi hukum semata, tetapi kehidupan berbangsa dan bernegara yang membawa keadilan sosial bagi seluruh rakyat Indonesia; baik bagi seluruh bangsa Indonesia sebagai satu kesatuan politik, tetapi juga bagi tiap-tiap warga negaranya; tua-muda, tinggi-rendah, kaya-miskin, tanpa perbedaan asal-usul ethnologis atau rasial, atau tinggi rendahnya status sosial seseorang, atau apa agama yang dianutnya.[158]

B. Landasan Sosiologis

Secara sosiologis perumusan aturan tentang pelindungan data pribadi juga dapat dipahami karena adanya kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, pengelolaan, penyebarluasan data pribadi. Perlindungan yang memadai atas privasi menyangkut data dan pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data pribadi untuk berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya. Dengan demikian pengaturan ini akan menciptakan keseimbangan antara hak-hak individu dan masyarakat yang diwakili

[157] *Ibid.*hlm.151.
[158] *Ibid,* hlm. 152.

kepentingannya oleh negara. Pengaturan tentang pelindungan data pribadi ini akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi.

Secara sosiologis terkesan bahwa masyarakat Indonesia belum atau kurang menghargai privasi karena nilai-nilai tersebut bukan berasal dari bangsa Indonesia, padahal secara sosiologis masyarakat juga menghargai privasi dengan keberadaan nilai penghargaan terhadap sikap tindak yang ajeg di tengah masyarakat dengan tidak mengganggu atau mengusik kehidupan setiap individu sebagai anggota masyarakat. Tindakan-tindakan seperti itu bahkan disadari sebagai tindakan yang kurang pantas atau berpotensi bertentangan dengan nilai-nilai luhur berbangsa dan bernegara. Hal ini juga dapat dilihat berdasarkan hasil survei yang menunjukan bahwa ada kesadaran dan pengharapan masyarakat terhadap perlindungan privasi dan data pribadi.

Pengabaian terhadap perlindungan privasi dan kurangnya kesadaran masyarakat terhadap perlindungan privasinya, memberikan ruang atas terjadinya sejumlah pelanggaran dan penyalahgunaan data pribadi seseorang. Kasus yang banyak terjadi di Indonesia diantaranya jual beli data warga yang kemudian menjadi sasaran praktik pemasaran suatu produk. Produk yang ditawarkan pun bervariasi, mulai dari racun tikus, telepon seluler, kartu kredit, produk asuransi dan produk perbankan atau jasa keuangan lainnya. Hal ini menunjukan bahwa pemanfaat data yang diperjualbelikan telah terfragmentasi di banyak sektor.

Data yang diperjualbelikan bisa pula berwujud akun atau pengikut di media sosial. Artinya, berkembangnya aplikasi

teknologi memberikan andil terhadap semakin beragamnya bentuk pelanggaran terhadap data pribadi seseorang, seperti munculnya sebuah pesan berisi iklan jika seseorang berada di tempat tertentu yang biasa disebut *Location-Based Messaging*. Biasanya praktik tersebut terjadi tanpa didahului dengan suatu perjanjian antara *provider* dan pemilik data.

C. Landasan Yuridis

Landasan yuridis tentang Perlindungan Data Pribadi, bersumber kepada Pasal 28G dan Pasal 28H Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Dengan demikian Perlindungan Data Pribadi merupakan salah satu bentuk perwujudan amanat konstitusi dan harus diatur dalam bentuk Undang-Undang. Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa, ”setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu merupakan hak asasi”. Lebih lanjut, Pasal 28H ayat (4) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa, “setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapa pun.” Pasal-pasal ini menjadi pertimbangan perlunya dibentuk peraturan perundang-undangan yang melindungi data pribadi.

Putusan Mahkamah Konstitusi Nomor 006/PUU-I/2003 semakin mempertegas bahwa pengaturan pelindungan data pribadi harus dalam bentuk undang-undang. Dalam Putusan Mahkamah Konstitusi tersebut antara lain disebutkan bahwa

ketentuan yang menyangkut HAM, harus dalam bentuk undang-undang.

Selain itu, dalam Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional 2005-2025 juga telah ditentukan bahwa untuk mewujudkan bangsa yang berdaya saing harus meningkatkan pemanfaatan ilmu pengetahuan dan teknologi. Salah satunya melalui peraturan yang terkait dengan privasi, dan hal tersebut terkait dengan HAM.

Amanah perlindungan hak asasi manusia terkait data pribadi tersebut kemudian diimplementasikan dalam Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, dalam Pasal 3 disebutkan bahwa:

(1) Setiap orang dilahirkan bebas dengan harkat dan martabat manusia yang sama dan sederajat serta dikaruniai akal dan hati nurani untuk hidup bermasyarakat, berbangsa, dan bernegara dalam semangat persaudaraan.
(2) Setiap orang berhak atas pengakuan, jaminan, perlindungan dan perlakuan hukum yang adil serta mendapat kepastian hukum dan perlakuan yang sama di depan hukum.
(3) Setiap orang berhak atas perlindungan hak asasi manusia dan kebebasan dasar manusia, tanpa diskriminasi.

Pelaksanaan hak asasi manusia khususnya yang terkait dengan data pribadi, harus pula memperhatikan hak-hak orang lain dan pembatasan yang dilakukan untuk menjamin kepentingan atau ketertiban umum sebagai wujud asas fungsi sosial. Hal ini diatur dalam Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa:

(1) Setiap orang wajib menghormati hak asasi manusia orang lain dalam tertib kehidupan bermasyarakat, berbangsa, dan bernegara.

(2) Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

Selain konstitusi dan Undang-Undang HAM, juga terdapat ketentuan mengenai data pribadi di antaranya, dalam Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Di samping itu terdapat pula ketentuan-ketentuan yang terkait dengan keberadaan data pribadi, namun belum secara tegas dan efektif melindungi data pribadi di antaranya, Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, dan Undang-Undang Nomor 28 Tahun 2007 tentang Perubahan Ketiga atas Undang-Undang Nomor 6 Tahun 1983 tentang Ketentuan Umum dan Tata Cara Perpajakan.

BAB V
JANGKAUAN, ARAH PENGATURAN, DAN RUANG LINGKUP MATERI MUATAN RANCANGAN UNDANG-UNDANG

Naskah Akademik ini pada akhirnya berfungsi mengarahkan ruang lingkup materi muatan Rancangan Undang-Undang tentang Pelindungan Data Pribadi yang akan dibentuk. Substansi Rancangan Undang-Undang Pelindungan Data Pribadi harus bisa melindungi kepentingan masyarakat Indonesia dengan melihat berbagai permasalahan hukum yang muncul dan akan muncul. Dari segi jangkauan harus dapat menjangkau berbagai aktifitas masyarakat yang berkaitan dengan perlindungan data pribadi di samping itu substansi pengaturan harus memperhatikan "*common elements*"[159] (unsur-unsur yang mengandung persamaan) dari berbagai regulasi perlindungan data pribadi yang berkembang baik dalam lingkup internasional, regional maupun praktik-praktik negara lain maka materi muatan dalam RUU tentang Pelindungan Data Pribadi idealnya mengatur hal-hal sebagai berikut:

A. Sasaran

Keadaan yang ingin diwujudkan melalui pengaturan pelindungan data pribadi adalah sebagai berikut:

1. terlindungi dan terjaminnya hak dasar warga negara melalui regulasi perlindungan atas data pribadi.
2. meningkatnya budaya kesadaran masyarakat dalam pelindungan data pribadi.
3. terjaminnya masyarakat untuk mendapatkan pelayanan dari pemerintah, pelaku bisnis dan organisasi lainnya.

[159] Lihat Konsep RUU Perlindungan Data Pribadi Kementerian Pendayagunaan Aparatur Negara, 2005.

4. terhindarnya negara Indonesia dari segala macam eksploitasi dan penyalahgunaan data berkaitan dengan data pribadi warga Indonesia.
5. meningkatkan pertumbuhan ekonomi digital dan industri teknologi, informasi dan komunikasi melalui upaya kesetaraan regulasi pelindungan data pribadi untuk mendukung mekanisme "*trans-border flow of data*" dalam transaksi perdagangan internasional.

Sasaran tersebut di atas, menjadi konsiderans terbentuknya Rancangan Undang-Undang Pelindungan Data Pribadi. Pada dasarnya sasaran tersebut dapat dilihat dalam bagian "menimbang" yang memuat uraian pokok-pokok pikiran filosofis, sosiologis dan yuridis yang menjadi latar belakang pembentukan Undang-Undang Pelindungan Data Pribadi, yaitu:

1. pelindungan atas data pribadi adalah pengakuan dan perlindungan atas hak-hak dasar manusia yang telah dilindungi berdasarkan Hukum Internasional, Regional dan Nasional;
2. pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi, perlu diberikan landasan hukum yang kuat untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;perlindungan atas data pribadi merupakan kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, pengelolaan, penyebarluasan data pribadi;
3. pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan

menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi;

4. pelindungan yang memadai menyangkut data pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya; dan
5. bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi diperlukan pengaturan mengenai pelindungan data pribadi dalam suatu undang-undang.

B. Arah dan Jangkauan Pengaturan

Arah pengaturan dari Rancangan Undang-Undang ini adalah

- memberikan pengaturan nasional yang memuat prinsip-prinsip umum perlindungan, syarat sah pemrosesan dan istilah yang seragam dalam pemrosesan data pribadi.
- untuk memberikan tata kelola terhadap setiap tindakan pemrosesan semua jenis data pribadi baik yang berada di Indonesia maupun data pribadi warga negara Indonesia yang berada di luar negeri.

Jangkauan pengaturan rancangan undang-undang ini adalah pemerintah, perorangan maupun korporasi baik yang badan hukum maupun tidak badan hukum.

C. Ruang Lingkup dan Materi Muatan

1. Ketentuan Umum

Memuat rumusan akademik mengenai pengertian istilah dan frasa. Batasan pengertian atau definisi dan hal-hal lain yang bersifat umum yang mencerminkan asas, maksud, dan tujuan dimuat dalam ketentuan Undang-Undang. Definisi dan batasan pengertian yang digunakan, sebagai berikut:

a. Data Pribadi

Pengertian Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau digabungkan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik. Adapun contoh data pribadi antara lain seperti nama, tanggal lahir, ID Nomor kartu, nomor paspor, karakteristik, sidik jari, status perkawinan, keluarga, pendidikan, pekerjaan, rekam medis, perawatan medis, informasi genetik, kehidupan seksual, pemeriksaan kesehatan, catatan kriminal, informasi kontak, kondisi keuangan, kegiatan sosial dan informasi lainnya yang mungkin langsung atau tidak langsung digunakan untuk mengidentifikasi orang pribadi yang hidup.

b. Informasi

Yang dimaksud dengan informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan

format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.

c. Pengendali Data Pribadi

Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

d. Prosesor Data Pribadi

Prosesor Data Pribadi adalah pihak yang melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.

e. Setiap Orang

Setiap Orang adalah orang perseorangan atau Korporasi.

f. Pemilik Data Pribadi

Pemilik Data Pribadi adalah orang perseorangan selaku subyek data yang memiliki Data Pribadi yang melekat pada dirinya

g. Badan Publik

Badan Publik adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat dan/atau luar negeri.

h. Korporasi

Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi baik merupakan badan hukum maupun bukan badan hukum sesuai peraturan perundang-undangan.

i. Menteri

Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

2. Materi yang Akan Diatur

a. Jenis Data Pribadi

1) Data Pribadi Yang Bersifat Umum

Dalam hal ini, yang dimaksud dengan Data Pribadi yang bersifat umum antara lain berupa nama lengkap, jenis kelamin, kewarganegaraan, maupun agama, atau Data Pribadi yang harus dikombinasikan sehingga memungkinkan untuk mengidentifikasi seseorang.

2) Data Pribadi Yang Bersifat Spesifik

Data Pribadi yang bersifat spesifik adalah data dan informasi yang berkaitan dengan data dan informasi kesehatan, data biometrik, data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, serta data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

b. Hak Pemilik Data Pribadi

Salah satu tujuan pokok dari Undang-Undang tentang Perlindungan Data Pribadi adalah

perlindungan yang layak terhadap hak pemilik data pribadi. Adapun hak-hak pemilik data pribadi yang perlu diperhatikan mencakup, antara lain:

i. hak untuk meminta Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi;
ii. hak untuk melengkapi data pribadi miliknya sebelum diproses oleh pengendali data pribadi;
iii. hak untuk mengakses data pribadi miliknya miliknya sesuai dengan ketentuan peraturan perundang-undangan;
iv. hak untuk memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi miliknya sesuai dengan ketentuan perundang-undangan;
v. hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi miliknya;
vi. hak untuk menarik kembali persetujuan pemrosesan data pribadi miliknya yang telah diberikan kepada pengendali data pribadi;
vii. Hak untuk menarik kembali persetujuan pemrosesan data yang telah diberikan pada pengendali data pribadi;
viii. hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*);

ix. hak untuk memilih atau tidak memilih pemrosesan data pribadi melalui mekanisme pseudonim untuk tujuan tertentu;
x. hak untuk menunda atau membatasi pemrosesan data pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi;
xi. hak untuk menuntut dan menerima ganti rugi atas pelanggaran data pribadi miliknya sesuai ketentuan peraturan perundang-undangan;
xii. hak untuk mendapatkan dan/atau menggunakan data pribadi miliknya dari pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik atau perangkat keras yang digunakan dalam interoperabilitas antar sistem elektronik; dan
xiii. hak untuk menggunakan dan mengirimkan data pribadi miliknya ke pengendali data pribadi lainnya.

c. Pemrosesan Data Pribadi

Pemrosesan data pribadi meliputi perolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, dan/atau penghapusan atau pemusnahan.

Pemrosesan data pribadi dilakukan sesuai dengan prinsip pelindungan data pribadi meliputi:

i. pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, patut, dan transparan;
ii. pemrosesan data pribadi dilakukan sesuai dengan tujuannya;
iii. pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi;
iv. pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
v. pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan data pribadi;
vi. pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan pelindungan data pribadi;
vii. data pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan pemilik data pribadi kecuali ditentukan lain oleh peraturan perundang-undangan; dan
viii. pemrosesan Data Pribadi dilakukan secara bertanggung jawab dengan memenuhi pelaksanaan prinsip pelindungan Data Pribadi dan dapat dibuktikan secara jelas .

d. Pengecualian Terhadap Perlindungan Data Pribadi

Dalam keadaan-keadaan tertentu, dengan alasan-alasan yang sah dan diatur oleh undang-undang, maka hak pemilik data pribadi serta kewajiban pengendali dan prosesor data pribadi dapat dikecualikan dengan alasan-alasan yang sah meliputi, namun tidak terbatas pada:

i. untuk kepentingan pertahanan dan keamanan nasional;
ii. untuk kepentingan proses penegakan hukum;
iii. untuk kepentingan umum dalam rangka penyelenggaraan negara;
iv. untuk kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan; atau
v. untuk agregat data yang pemrosesannya ditujukan guna kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara.

Pengecualian tersebut dilaksanakan hanya dalam rangka pelaksanaan ketentuan Undang-Undang.

Dalam melakukan pemrosesan data pribadi, pengendali data pribadi wajib menjaga kerahasiaan data pribadi. Namun ketentuan tersebut dikecualikan untuk hal-hal sebagaimana berikut:

i. pemilik data pribadi telah memberikan persetujuan sesuai dengan syarat persetujuan;
ii. diperlukan untuk tujuan melaksanakan kewajiban dan/atau hak tertentu dari pengendali data pribadi atau dari pemilik data pribadi di bidang

ketenagakerjaan, jaminan sosial, perpajakan, pengawasan sektor termasuk sektor keuangan, penyelenggaraan administrasi kependudukan, dan/atau kesejahteraan sosial yang memberikan pelindungan terhadap hak dasar dan kepentingan pemilik data pribadi;

iii. diperlukan untuk melindungi kepentingan pemilik data pribadi yang tidak cakap baik secara fisik maupun hukum; dan/atau

iv. diperlukan untuk kepentingan proses penegakan hukum.

e. Kewajiban Pengendali Dan Prosesor Data Pribadi Dalam Pemrosesan Data Pribadi

Mengingat pengendali data pribadi dalam kenyataannya dapat merupakan badan hukum, maka perlu ditetapkan secara jelas hak-hak dan kewajibannya dalam undang-undang tentang pelindungan data pribadi. beberapa kewajiban pengendali data pribadi mencakup :

i. kewajiban untuk menjaga kerahasiaan data pribadi;

ii. kewajiban pengendali data pribadi wajib untuk memberikan informasi kepada pemilik data pribadi mengenai: legalitas dari pemrosesan data pribadi, tujuan pemrosesan data pribadi, jenis dan relevansi data pribadi yang akan diproses, periode retensi dokumen yang memuat data pribadi, rincian mengenai informasi yang dikumpulkan,

jangka waktu pemrosesan data pribadi, dan hak pemilik data pribadi;

iii. kewajiban untuk melakukan penundaan dan pembatasan serta menghentikan pemrosesan data pribadi dalam hal pemilik data pribadi menarik kembali persetujuan pemrosesan data pribadi;

iv. kewajiban untuk melindungi dan memastikan keamanan serta melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi, termasuk memastikan pelindungan dan mencegah pemrosesan Data Pribadi secara tidak sah;

v. Kewajiban untuk melakukan perekaman terhadap seluruh kegiatan pemrosesan Data Pribadi

vi. Kewajiban untuk memberikan akses kepada Pemilik Data Pribadi terhadap Data Pribadi yang diproses beserta rekam jejak pemrosesan Data Pribadi;

vii. Kewajiban untuk menolak memberikan akses perubahan terhadap Data Pribadi kepada Pemilik Data Pribadi dalam hal tertentu;

viii. Kewajiban untuk memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi dan wajib memberitahukan hasil pembaruan dan/atau perbaikan Data Pribadi kepada Pemilik Data Pribadi;

ix. Kewajiban untuk menjamin akurasi, kelengkapan, dan konsistensi data pribadi;

x. Kewajiban untuk melakukan pemrosesan data pribadi sesuai dengan tujuan pemrosesan data pribadi yang disetujui oleh pemilik data pribadi;
xi. Kewajiban untuk mengakhiri, menghapus, dan memusnahkan data pribadi;
xii. Kewajiban untuk menghentikan pemrosesan data pribadi dalam hal pemilik data pribadi menarik kembali persetujuan pemrosesan data pribadi;
xiii. Kewajiban untuk menyampaikan pemberitahuan secara tertulis dalam hal terjadi kegagalan pelindungan data pribadi; dan
xiv. Kewajiban untuk bertanggung jawab atas seluruh pemrosesan data pribadi.

Dalam hal pengendali data pribadi menunjuk prosesor data pribadi, prosesor data pribadi wajib melakukan pemrosesan data pribadi berdasarkan instruksi atau perintah pengendali data pribadi. oleh karena itu, beberapa kewajiban pengendali data pribadi berlaku juga terhadap prosesor data pribadi mencakup:

i. Kewajiban untuk menjaga kerahasiaan data pribadi;
ii. Kewajiban untuk melindungi dan memastikan keamanan serta melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi, termasuk memastikan pelindungan dan mencegah pemrosesan data pribadi secara tidak sah;
iii. Kewajiban untuk melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi; dan

v. Kewajiban untuk menjamin akurasi, kelengkapan, dan konsistensi data pribadi.

f. Transfer Data Pribadi

Dalam perkembangan globalisasi, satu hal yang harus diperhatikan adalah bahwa meskipun tujuan utama dari perumusan undang-undang ini adalah untuk mengakomodasikan secara maksimal kepentingan nasional, namun tetap memperhatikan kepentingan-kepentingan negara lain dan/atau masyarakat internasional. Konsekuensinya, perumusan undang-undang ini harus memperhatikan arah kecenderungan pengaturan internasional yang berlaku, atau setidak-tidaknya memenuhi standar internasional. Pemenuhan standar internasional yang berlaku akan mempermudah pergaulan dan tata hubungan internasional, termasuk dalam kegiatan perdagangan, investasi dan keuangan internasional. Dalam dunia global pasti akan terjadi transfer data pribadi yang bersifat transnasional. Dengan menerapkan standar internasional yang berlaku, maka akan mengurangi hambatan-hambatan yang mungkin timbul.

Menyangkut transfer data pribadi yang bersifat lintas batas nasional, telah terdapat beberapa dokumen internasional seperti OECD *Guidelines*, *EU General Data Protection Regulation, ASEAN Framework on Personal Data Protection* maupun *APEC Privacy Framework* yang dapat digunakan sebagai acuan dalam merumuskan

norma-norma hukum nasional yang akan diformulasikan dalam Undang-undang tentang Pelindungan Data Pribadi.

g. Pembentukan Pedoman Perilaku Pengendali Data Pribadi

Pengendali Data Pribadi melalui asosiasinya dapat membentuk kode etik dalam pengelolaan data pribadi. Hal ini ditujukan untuk memberikan ruang pengaturan secara sendiri di dalam melaksanakan pengelolaan data pribadi. Namun, pembentukan kode etik tersebut tidak boleh bertentangan dengan ketentuan dan pedoman perilaku yang diatur dalam rancangan undang-undang ini.

h. Kerja Sama Internasional

Kerjasama internasional dalam perumusan dan penerapan Undang-Undang tentang Perlindungan Data Pribadi merupakan keharusan yang dilaksanakan berdasarkan prinsip-prinsip kerja sama internasional, baik yang bersumber kepada peraturan nasional maupun internasional yang berlaku.

Kerja sama internasional dilakukan oleh Pemerintah dengan pemerintah negara lain atau organisasi internasional terkait dengan pelindungan Data Pribadi.

Kerja sama internasional sebagaimana dimaksud dilaksanakan dalam bentuk kerja sama formal atau berdasarkan prinsip timbal balik.

i. Peran Pemerintah dan Peran Masyarakat

a. Peran Pemerintah

Dalam penyelenggaraan pelindungan data pribadi, Pemerintah menjamin pelaksanaan Pelindungan Data Pribadi berdasarkan Undang-Undang ini.

b. Peran Masyarakat

Masyarakat dapat berperan serta, baik secara langsung maupun tidak langsung dalam mendukung terselenggaranya pelindungan Data Pribadi sesuai dengan ketentuan undang-undang ini.

Pelaksanaan peran serta masyarakat dalam meningkatkan kesadaran pentingnya Pelindungan Data Pribadi sebagaimana dimaksud dapat dilakukan melalui pendidikan, pelatihan, advokasi, bimbingan teknis, dan/atau sosialisasi.

j. Penyelesaian Sengketa

Penyelesaian sengketa yang diatur dalam undang-undang perlindungan data pribadi ini dilakukan baik melalui penyelesaian di luar pengadilan dan melalui pengadilan.

Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses pengadilan dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan.

k. Larangan Dalam Penggunaan Data Pribadi (Perbuatan yang Dilarang)

Perbuatan yang perlu dilarang dalam penggunaan data pribadi karena berpotensi merugikan antara lain:

1. memperoleh, mengungkapkan dan/atau menggunakan Data Pribadi yang bukan miliknya secara melawan hukum;
2. memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam dan/atau melanggar pelindungan Data Pribadi secara melawan hukum;
3. menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang secara melawan hukum;
4. memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain;
5. menjual atau membeli data pribadi.

l. Ketentuan Sanksi

Atas berbagai bentuk pelanggaran yang dilakukan terhadap ketentuan undang-undang ini perlu ditetapkan sanksi yang proporsional dengan perbuatan/pelanggaran yang dilakukan. Penerapan sanksi selain untuk memberikan efek jera juga diterapkan untuk memberikan edukasi untuk merubah perilaku publik untuk lebih memahami perlunya

menghargai hak pemilikdata pribadi. Sanksi dapat berupa sanksi administratif, sanksi pidana dan sanksi perdata.

Pelanggaran terhadap kewajiban pemrosesan data pribadi dikenakan sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, ganti kerugian, dan/atau denda administratif.

Dalam setiap undang-undang pelindungan data, beberapa negara menerapkan sanksi pidana mengingat banyaknya kasus pencurian data pribadi yang mengarah kepada tindak kriminal. Penetapan besaran sanksi dapat dirumuskan dengan disesuaikan kepada peraturan perundang-undangan yang berlaku. Penetapan sanksi perlu dilengkapi dengan mekanisme penegakan hukumnya yang disesuaikan dengan ketentuan peraturan perundang-undangan yang berlaku. Dalam rancangan undang-undang ini termuat beberapa ancaman dengan sanksi berupa pidana denda. Jika perbuatan dilakukan korporasi maka sanksi yang dikenakan berupa denda yang lebih besar dari sanksi yang dikenakan terhadap perorangan.

m. Ketentuan Peralihan

Dalam rancangan undang-undang ini perlu dirumuskan aturan peralihan yang akan berfungsi mengatur masa peralihan dan tahap pemberlakuan Undang-Undang tentang Pelindungan Data Pribadi nantinya dikaitkan dengan peraturan perundangan

yang berlaku. Ketentuan peralihan diperlukan dalam upaya harmonisasi undang-undang pelindungan data pribadi dengan peraturan perundang-undangan lainnya.

n. Ketentuan Penutup

Semua ketentuan peraturan perundang-undangan yang mengatur mengenai pelindungan Data Pribadi dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang ini.

BAB VI
PENUTUP

A. Simpulan

Berdasarkan uraian pada bab sebelumnya, maka dapat dirangkum, sebagai berikut:

1. Permasalahan data pribadi dalam kehidupan bermasyarakat, berbangsa dan bernegara akan terlindungi dengan adanya Undang-Undang Pelindungan Data Pribadi.
2. Pengaturan mengenai perlindungan data yang ada belum cukup efektif karena masih tersebar dalam beberapa pengaturan yang bersifat sektoral sehingga belum memberikan perlindungan yang optimal.
3. Secara filosofis upaya pengaturan menyangkut hak privasi atas data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak-hak dasar manusia. Oleh karena itu, penyusunan Rancangan Undang-Undang Pelindungan Data Pribadi memiliki landasan filosofis yang kuat dan dapat dipertanggungjawabkan. Landasan filosofis perlindungan data pribadi adalah Pancasila yaitu *rechtsidee* (cita hukum) yang merupakan konstruksi pikir (ide) yang mengarahkan hukum kepada apa yang dicita-citakan. Secara sosiologis rumusan Rancangan Undang-Undang Pelindungan Data Pribadi dikarenakan adanya kebutuhan untuk memberikan perlindungan terhadap individu sehubungan dengan pengumpulan, pemrosesan, dan pengelolaan data pribadi. Secara yuridis Rancangan Undang-Undang Pelindungan Data Pribadi merupakan

kewajiban konstitusi negara yang diatur dalam Pasal 28G, Pasal 28H, dan Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

4. Konsep pengaturan perlindungan data pribadi yang tepat adalah melalui pengaturan yang bersifat komprehensif yang akan mengatur baik perorangan maupun badan hukum dan organisasi kemasyarakatan.

B. Saran

Untuk tindak lanjut dari pengkajian ini dapat direkomendasikan hal-hal, sebagai berikut:

1. Mengingat urgensi keberadaan Rancangan Undang-Undang tentang Pelindungan Data Pribadi, maka kajian ini perlu ditindaklanjuti dengan aktivitas-aktivitas seperti: studi komparasi beberapa negara-negara yang telah mengatur perlindungan data pribadi secara lebih mendalam untuk mematangkan "*common elements*" dari substansi pengaturan Rancangan Undang-Undang yang dianggap sebagai acuan, melakukan *advanced review* terhadap perkembangan internasional terutama yang terjadi di *European Union* dan OECD yang dalam proses mengamandemen ketentuan-ketentuan yang telah berlaku. Melakukan koordinasi, diskusi mendalam dan sosialisasi dengan berbagai kepentingan terkait;
2. Untuk segera disusun Rancangan Undang-Undang Perlindungan Data Pribadi, dan dimasukkan dalam Program Legislasi Nasional Prioritas 2020 sebagai usulan Kementerian Komunikasi dan Informatika.

DAFTAR PUSTAKA

Literatur:

Abu Bakar Munir, Siti Hajar Mohd Yasin, *Privacy and Data Protection,* Sweet &Mawell Asia, Malaysia, 2002,

_____, *Personal data Protection in Malaysia,* Sweet & Maxwell Asia, 2010

Adnan Buyung Nasution & A. Patra M. Zen, *Instrumen Internasional Pokok Hak Asasi Manusia*, ed.III., Yayasan Obor Indonesia, Yayasan Lembaga Bantuan Hukum Indonesia dan Kelompok Kerja Ake Arif, Jakarta, 2006.

Asplund, Knut D, Suparman Marzuki dan Eko Riyadi, (ed.), *Hukum Hak Asasi Manusia,* Pusat Studi Hak Asasi Manusia Universitas Islam Indonesia, PUSHAM UII, Yogyakarta, 2008.

Banisar, *Privacy & Human Rights,An International Survey of Privacy Laws and Developments,* Electronic *Privacy* Information Centre, Washington. D.C, 2000.

Bendit, Theodore M., *Law as Rule and Principle, Problems of Legal Philosphy*, Stanford University Press, Stanford-California, 1978.

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, PT. Refika Aditama, Bandung, 2010.

Edmon Makarim, *Kompilasi Hukum Telematika,* PT Raja Grafindo Perkasa,Jakarta 2003.

Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Rajawali Pers, Jakarta, 2010.

Emmerson, Richard D., et.al, *Indonesia Report in Annual review of Data Protection and Privacy Laws*, Financier Wolrd Wide, December, 2012.

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

Greeneaf, Graham, *Asian Data PrivacyLaws - Trade and Human Rights Perspectives*, Oxford University Press, New York, 2014.

Hofstadter and Horowitz, *The Right of Privacy*, Central Book Company, New York, 1964.

Jayawickrama, Nihal, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence*, Cambridge University Press, United Kingdom, 2002.

M. Arsyad Sanusi, *Teknologi Informasi & Hukum E-commerce,* PT. Dian Ariesta, Jakarta, 2004.

Michael, James, *Privacy and Human Rights, an International and Comparative Study, with Special Reference to developments in Information Technology,* UNESCO, France, 1994.

Moh. Mahfud MD, dkk, *Pendidikan Kewarganegaraan dan HAM,* UII Press, Yogyakarta, 2003.

Muhammad Tahir Azhary, *Negara Hukum: SuatuStuditentangPrinsip-Prinsipnya Dilihat dari Segi Hukum Islam, Implementasinya pada Periode Negara Madinah dan Masa Kini,* Kencana, Bogor, 2003.

Muhammad Tholchah Hasan, *Perlindungan Terhadap Korban Kekerasan Seksual (Advokasi atas Hak Asasi Perempuan)*, Refika, Bandung, 2001.

Murray Andrew, *Information Technology Law, The Law and Society,* Oxford University Press, New York, 2010.

Paton, GW, *Textbook of Jurisprudence*, Oxford University Press, London, 1964.

Satjipto Rahardjo, *IlmuHukum*, Penerbit Citra Aditya Bhakti, Bandung, Cetakan V, 2000.

Sinta Dewi Rosadi, *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, Widya Padjadjaran, Bandung, 2009.

_____, *Praktik Negara-Negara dalam Mengatur Privasi dalam E-Commerce*, Widya Padjadjaran, Bandung, 2009.

Solove, Daniel J., *The Digital Person, Technology and Privacy in the Information Age,* West Group Publication, New York University Press, New York, 2004, hlm 13-17.

Sunaryati Hartono, *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20*, Penerbit Alumni, Bandung, 1994.

_____, "Mencari Fisafah Hukum Indonesia yang Melatar belakangi Pembukaan Undang-Undang Dasar 1945", dalam Sri Rahayu Oktorina dan Niken Savitri, *Butir-Butir Pemikiran dalam Hukum, Memperingati 70 Tahun Prof. Dr. B. Arief Sidharta, S.H.,*PT. Refika Aditama, Bandung, 2008.

Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci,* Elsam, Jakarta, 2014

Westin, Allan, Westin, Alan F, *Privacy and Freedom,* London, 1967.

Jurnal:

B. Arief Sidharta, "Kajian Kefilsafatan tentang Negara Hukum", *Jentera (Jurnal Hukum),* "Rule of Law", Pusat Studi Hukum dan Kebijakan (PSHK), Jakarta, edisi 3 Tahun II, November 2004.

Berzanson, Randall P., "The Right to Privacy Revisited : Privacy, News and Social Change", *California Law Review*, Vol 80, 1992.

Branscomb, Anne W., Global Governance of Global Networks: "A survey of Transborder Data Flows in Transition", *Vanderbilt Law Review,* Vol. 36, 1983.

Edmon Makarim, Analisis Terhadap Kontroversi Rancangan Peraturan Pemerintah Tentang Tata Cara Intersepsi Yang Sesuai Hukum (Lawful Interception), *Jurnal Hukum & Pembangunan* Tahun Ke-40 No. 2 April 2010.

Gormley, Ken, *One Hundred Years of Privacy*,*Wisconsin Law Review,* Volume 52.

Marcy E.Peek, "Information Privacy and Corporate Power : Toward a Re-Imagination of Information Privacy Law", *Seton Hall Law Review,* Vol 37, 2006.

Warren, Samuel & Brandeis, Louis D., "The Right To Privacy", *Harvard Law Review*, Volume 4, 1890.

Zarsky, Tal Z.,*Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall solutions to the Problems of Information Privacy in the Internet Society*, University Miami Law Review, Vol 58, 2004.

Makalah/Tesis:

Heppy EndahPalupy, *Thesis: Privacy and Data Protection: Indonesia Legal Framework*, Master Program in Law and TerchnologyUniversiteit Van Tilburg, 2011.

Artikel Internet:

Artikel berita BBC, "Phone-hacking scandal: Timeline", 28 Fwbruari 2012, diakses di http://www.bbc.co.uk/news/uk-

14124020, diakses pada tanggal 10 September 2014 Pukul 13.30 WIB.

Artikel Berita, “Researchers reverse Netflix anonymization”, 14 Desember 2007, http://www.securityfocus.com/news/11497, diakses pada Januari 2015 Pukul 17.00 WIB. Lihat Juga Artikel Berita Forbes Tech, “Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study”, 25 April 2013, http://www.forbes.com/sites/adamtanner /2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/, diakses pada Januari 2015 Pukul 17.00 WIB.

Artikel Berita, Tech in Asia,“Berapa jumlah pengguna website, mobile, dan media sosial di Indonesia?” 21 Januari 2015, https://id.techinasia.com/laporan-pengguna-website-mobile-media-sosial-indonesia”, diakses pada 20 Desember 2014 Pukul 18.00 WIB.

Artikel Berita, Waspada Online, “e-ktp ternyata bermasalah”, diakses melalui http://www.waspada.co.id/index.php?option=com_content &view=article&id=341427:e-ktp-ternyata-bermasalah&catid=77:fokuredaksi&Itemid=131, pada 15 Nove-mber 2014 Pukul 13.00 WIB.

Data Privacy and Security Team, “South East Asia: Data Protection Update”, Bryan Cave Bulletin, diunduh pada 16 Oktober 2015, Pukul 16.22, https://www.bryancave.com/images/content/2/0/v2/2020/ Bryan-Cave-Client-Bulletin-South-East-Asia-Data-Protection-pdat.pdf

Hasil Survei Statista sampai dengan Oktober 2019, diakses di https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ pada 13 Januari 2020.

APJII, "Hasil Survei Penetrasi dan Perilaku Pengguna Internet Indonesia 2018", http://apjii.or.id/survei, diakses pada 10 Januari 2020.

Agustin Setyo Wardani, "765 Juta Korban Terjerat Kejahatan Siber pada kuartal II 2018", https://www.liputan6.com/tekno/read/3658996/765-juta-korban-terjerat-kejahatan-siber-pada-kuartal-ii-2018, diakses pada 10 Januari 2020.

http://www.privacyinternational.org.Countries.index.html, diakses tanggal 10 Januari, 2007.

http://conventions.coe.int/Treaty/EN/Treaties/Html/181.htm, diakses pada 15 Oktober 2014 Pukul 11.00 WIB.

http://rahard.worldpress.com/2009, diakses pada tanggal 30 maret 2009.

http://watch.com/internetsehat, diakses tanggal 1 Maret, 2009.

http://www.bfdi.bund.de/cln_030/nn_531068/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2007/PM-15-07-Uebergabe21TB.html__nnn=true, diakses pada tanggal 14 November 2014 Pukul 13.20 WIB.

http://www.businessweek.com/technology/content/apr2007/tc20070414_675511.htm

http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/CoE_response_to_privacy_challenges_Modernisation_of_Convention_108_EN_May_2011.pdf,diakses pada tanggal 15 Oktober 2014 Pukul 13.40 WIB.

http://www.dataprotection.ro/servlet/ViewDocument?id=623., Diakses pada tanggal 11 September 2014 Pukul 21.00 WIB.

http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY.ashx, diakses pada tanggal 11 September 2014 Pukul 10.00 WIB.

http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties guidance_120110.pdf, diakses pada tanggal 10 September 2014 Pukul 13.20 WIB.

https://www.privacyinternational.org/article/germany-privacy-profile, \diakses pada tanggal 14 November 2014 Pukul 13.00 WIB.

Https://www.privacyinternational.org/article/phr2006-canada, diakses pada tanggal 14 November 2014 Pukul 13.35 WIB.

MerdekaFM, iCloud Dibobol Ratusan Foto Pribadi Celebs Di Expos, edisi 5 September 2014, diakses melalui: http://www.merdekafm.com/posting/read/17/iCloud_Dibobol_Ratusan_Foto_Pribadi_Celebs_Di_Expos, pada tanggal 11 September 2014 Pukul 09.30 WIB.

Privacy Commissioner of Canada: http://www.priv.gc.ca/, diakses pada tanggal 14 November 2014 Pukul 13.30 WIB.

Website resmi Information Commission Office (ICO), "About ICO" diakses di https://ico.org.uk/about-the-ic, pada Minggu 20 September 2015, Pukul 5.00 WIB.

Website resmiKomisiInformasiPusat Indonesia, "Tentang KIP", diakses di http://www.komisiinformasi.go.id/category/profil/tentang-kippadaMinggu 20 September 2015, Pukul 5.00 WIB.

Sumber Lain:

ANSPDCP 2009 Annual Rapport Romanian

Bogdan Manolea, Romania National Report – EDRi , December 2009

Canadian Internet Policy and Public Interest Clinic (CIPPIC) v. Facebook, 2008 diakses dalam http://www.cippic.ca/uploads/newrelease, diakses 1 April, 2009.

Candra Irawan, *PolitikHukum Hak Kekayaan Intelektual Indonesia,* Mandar Maju, Bandung, 2011.

Compilation of replies to CoE's public consultation on the DP Convention modernisation:http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD-BUR_2011_01_%20prov_MOS_12_05_11_ PUBLIC.pdf, diakses pada tanggal 15 Oktober 2014 Pukul 13.30 WIB.

Constitution of Portugal

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981

EC Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 16 May 2011.

European Convention for the Protection of Human Rights, Nov. 4, 1950, E.T.S. 5.

Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragterfür den Datenschutz und die Informationsfreiheit, BfDI), Tätigkeitsbericht (Bi-Annual Report) 2005-2006, 24 April 2007.

Graham Greenleaf, *76 Global Data Protection Laws,* Privacy Laws & Business Special Report, September 2011.

ICCPR

Kightlinger, Mark F.et. al., Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981

M.S. v. Sweden, 27 August 1997, reports 1997-IV.

Malone v. United Kingdom, 20 August 1984, 82 Eur. Ct. H. R. (ser A)

Personal Data protection Act (PDPA) Malaysia 2010

Personal Data Protection Ordonance (PDPO) Hong Kong.

Personal Data Protection Regulation 2013.

Personal Information Protection Act (PIPA) Korea Selatan.

Personal Information Protection and Electronic Documents Act Canada (S.C. 2000, c. 5).

Press Release No 117/15 Court of Justice of the European Union, 6 October 2015.

Privacy International Report, 2013

Rencana Pembangunan Jangka Panjang 2005-2025

Shchedule 1, Data Protection Principle 1 (1).

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981.

The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

The Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980).

Kamus:

Black, Henry Campbell, *Black's Law Dictionary*, Fifth Edition, West Publishing, USA, 1979

Kamus Besar Bahasa Indonesia, Edisi 3, Departemen Pendidikan Nasional dan P.T Balai Pustaka, Jakarta 2001.

Peraturan perundang-undangan:

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Undang-Undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik

Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan

Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian.

Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Republik Indonesia Nomor 67 Tahun 2011 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional

Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah

Kitab Undang-Undang Hukum Perdata

RUU Perlindungan Data Pribadi Kementerian Pendayagunaan Aparatur Negara, 2005.