Jurnal SuaraHukum
Volume 3 Nomor 1, March 2021
P-ISSN:2656-534X, E-ISSN:2656-5358

Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara

Nadiah Tsamara

Fakultas Hukum, Universitas Indonesia, Depok, Indonesia
nadiah.tsamara@ui.ac.id

Article history:
Received: 7 December 2020 | Last Revision: 10 February 2021 | Accepted: 20 February 2021

Abstract

The development of information and communication technology shows a significant increase. In the development of information technology and technology, personal information consisting of names, e-mails and cell phone numbers is very valuable data because there is economic value obtained in the business world, but technology can also be very dangerous if its use is not restricted, such as in the case of not protecting personal data, while privacy of personal data is important because it involves a person's dignity and freedom of expression, but data is not protected because in Indonesia there is no obligation in positive law which specifically regulates and provides sanctions for violations. This study aims to discuss the regulation in the perspective of comparative law in Europe, America, Hongkong, Malaysia, Singapore, South Korea, and Japan. This study uses normative legal research using asttutory approach and comparative approach that examines and analyses legal sources. This study discovers that the regulation of personal data protection in Indonesia has not been fully and thoroughly regulated compared to the regulations in several other countries, that there is a need for legal harmonization of personal data protection that is mature and deep.
Keywords: *Personal Data Protection, Privacy Rights, Personal Data, Comparative Law*

Abstrak

Perkembangan teknologi informasi dan komunikasi menunjukkan peningkatan yang signifikan. Dalam perkembangan teknologi informasi dan teknologi, informasi data pribadi yang terdiri dari nama, surel, dan nomor telepon genggam merupakan data yang sangat berharga karena terdapat nilai ekonomi yang didapatkan dalam dunia bisnis, namun penggunaan teknologi juga berbahaya apabila tidak diberikan batasan, seperti tidak dilindunginya data pribadi dari seseorang, sedangkan privasi dan data pribadi merupakan hal yang penting karena menyangkut harkat dan

martabat seseorang serta kebebasan berekspresi. Tidak dilindunginya data pribadi di Indonesia diakibatkan oleh tidak ada suatu kewajiban dalam hukum positif yang secara khusus mengatur dan memberikan sanksi atas pelanggaran terhadap perlindungan data peribadi. Penelitian ini bertujuan untuk membahas regulasi dalam perspektif hukum komparatif di Eropa, Amerika, Hongkong, Malaysia, Singapura, Korea Selatan, dan Jepang, Penelitian ini menggunakan jenis penelitian normatif dengan menggunakan pendekatan perundangan-undangan dan pendekatan komparatif untuk meneliti dan menganalisis sumber-sumber hukum. Studi ini bertujuan untuk menemukan bahwa regulasi perlindungan data pribadi di Indonesia belum mengatur secara matang dan mendalam dibandingkan dengan aturan di beberapa negara lain, sehingga diperlukan adanya harmonisasi hukum dari perlindungan data pribadi yang matang dan mendalam.
Kata Kunci: Perlindungan data pribadi, Hak Privasi, Data Pribadi, Hukum Perbandingan.

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi menunjukkan peningkatan cukup signifikan. Peningkatan kualitas masyarakat Indonesia secara berkelanjutan yang memanfaatkan teknologi informasi serta ilmu pengetahuan merupakan salah satu tujuan pembangunan nasional sekaligus menjadi suatu tantangan global (Sudaryanti 2013). Akan tetapi, perlu diperhatikan pula bahwa penggunaan teknologi informasi bagai pisau bermata dua. Teknologi jika dimanfaatkan dengan baik dapat membantu kehidupan manusia, namun teknologi juga dapat menjadi sangat berbahaya apabila tidak dibatasi penggunaannya, seperti dalam hal tidak dilindunginya data pribadi (Aprilianti 2020).

Penggunaan internet (*interconnection networking*) yang menjadi media informasi dan komunikasi elektronik yang menyediakan beragam aktivitas baik berupa jasa maupun produk seperti *e-commerce* (perdagangan/bisnis melalui media elektronik), *e-education* (pendidikan), *e-health* (kesehatan), *e-government* (pemerintahan), *e-payment* (keuangan), transportasi, pariwisata serta perkembangan *cloud computing* atau komputasi awan yaitu aplikasi yang menyediakan ruang penyimpan data pengguna

seperti *google drive, iCloud, Dropbox, Youtube* dan sebagainya. Ruang lingkup dari salah satu pembaharuan dalam bidang teknologi informasi dan komunikasi yaitu melakukan pengumpulan, penyimpanan, pembagian, dan penganalisaan data secara efektif dan efisien antar industri/perusahaan atau masyarakat (Dewi 2016).

Dalam perkembangan teknologi informasi dan teknologi, informasi data pribadi yang terdiri dari nama, *e-mail*, nomor telepon genggam merupakan data yang sangat berharga karena dapat nilai ekonomi yang didapatkan dalam dunia bisnis. Hal tersebut dinamakan *digital dossier* atau berkas digital yang merupakan kumpulan informasi data pribadi yang dimiliki oleh sebagian besar bahkan hampir seluruh orang dengan memanfaatkan teknologi internet yang dikembangkan oleh pihak swasta yang sangat beresiko terjadinya pelanggaran hak privasi atas data pribadi seseorang (Tejomurti 2018).

Peningkatan kebutuhan teknologi informasi dan komunikasi menyebabkan berbagai tindakan kriminal muncul yang dapat mengakibatkan kerugian baik materiil maupun immaterial bagi seseorang (Widyaningrat, I. A. W., & Dharmawan 2014). Meningkatnya aktivitas jumlah pengguna internet menyebabkan isu mengenai perlindungan data pribadi menjadi hal yang serius karena penyebarannya dapat dilakukan dengan mudah dan cepat melalui teknologi sehingga menimbulkan risiko "bocor"nya data pribadi seseorang. Pada tahun 2011, terjadi pembobolan data pribadi sebanyak 25 juta pelanggan Telkomsel, kemudian hal serupa terjadi lagi pada September 2019 kemarin masyarakat dikejutkan dengan adanya kebocoran data penumpang oleh maskapai penerbangan Lion Air dan Batik Air yang mencapai puluhan juta data. Kebocoran data penumpang termasuk informasi Kartu Tanda Penduduk (KTP) dan paspor penumpang yang diakses dalam ruang penyimpanan (*cloud*

computing) Amazon Web Services (AWS) yang diakses melalui web yang tersimpan dalam *filebackup* bulan Mei 2019 untuk maskapai Malindo Air dan Thai Air. Kebocoran data tersebut sangat rentan disalahgunakan yang dapat menyebabkan timbulnya beberapa kasus tindakan kriminal misalnya pencurian identitas maupun penipuan apalagi mengingat perkembangan ekonomi modern saat ini ke arah *digital economy* berbasis *economy creative*, data pribadi termasuk sebagai informasi yang sangat penting bagi para pebisnis. Data Norton Report 2013 mencatat bahwa tingkat potensi dan risiko terhadap tindakan kriminal dalam dunia maya di Indonesia memasuki status darurat dan terus menunjukkan peningkatan yaitu yang dilansir dari laman Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) (Latumahina 2014).

Saat ini Indonesia belum memiliki undang-undang yang komprehensif mengenai perlindungan data pribadi. Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD 1945) sebagai konstitusi Indonesia tidak secara eksplisit mengatur mengenai perlindungan data sebagai salah satu bentuk penghormatan atau pengakuan, perlindungan dan pemenuhan HAM dalam bentuk perlindungan privasi. Meskipun UUD 1945 menyatakan dengan tegas adanya perlindungan terhadap hak asasi manusia. Dalam UUD 1945 ketentuan mengenai perlindungan data, secara implisit bisa ditemukan dalam pasal 28F dan 28G (1), mengenai kebebasan untuk menyimpan informasi dan perlindungan atas data dan informasi yang melekat kepadanya. Hal ini juga yang mendasari semua peraturan perundang-undangan selaku aturan yang mengatur tentang privasi sebagai HAM, selain untuk kepastian hukum (sebagai salah satu syarat suatu negara hukum), termasuk Undang-Undang Perlindungan Data Pribadi yang nantinya akan terbentuk (Yuking 2018).

RUU Perlindungan Data Pribadi (RUU PDP) belum menemukan kejelasan atas jadwal pembahasan lanjutannya. Menurut Wakil Ketua Baleg DPR RI Willy Aditya, kelanjutan RUU PDP bergantung kesiapan Kementerian Komunikasi dan Informatika (Kemenkominfo) seperti dilansir dari CNNIndonesia.com. Saat ini, isu perlindungan data pribadi diatur oleh 32 Undang-Undang dan beberapa regulasi turunannya. Akibatnya, pelaksanaan dan pengawasan terkait isu ini tersebar di berbagai kementerian/lembaga. Sebagai contoh, penyalahgunaan data pribadi di *e-commerce* setidaknya diatur oleh UU Telekomunikasi, UU Informasi dan Transaksi Elektronik (ITE), UU Perlindungan Konsumen, dan UU Perdagangan. Sehingga secara tidak langsung, urusan perlindungan data pribadi merupakan kewenangan Kementerian Perdagangan serta Kementerian Komunikasi dan Informatika. Tanpa koordinasi yang kuat dari kementerian tersebut, implementasi dan pengawasan perlindungan konsumen akan sulit dipastikan. Hal ini tak jarang menimbulkan tumpang tindih peraturan tentang PDP. Sehingga, salah satu yang didorong dalam pembahasan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) adalah harmonisasi dan sinkronisasi dari Undang-Undang yang sudah ada.

Pada Sidang Umum PBB 2013, negara-negara anggota menyepakati adanya hak untuk privasi. Negara-negara anggota diminta untuk transparan dan bertanggung jawab ketika mengumpulkan data pribadi. Uni Eropa memiliki General Data Protection (GDPR) yang menjalankan aturan perlindungan data pribadi pada Mei 2018. Prinsip-prinsip yang berlaku dalam EU GDPR juga diungkapkan oleh ahli teknologi dan hukum perlindungan data pribadi, Berend van der Eijk, beliau menjelaskan mengenai prinsip transparansi bahwa warga memiliki hak untuk mengakses, mengubah, dan menghapus data pribadi mereka pada waktu tertentu dari data pelanggan perusahaan. Perusahaan

juga diminta untuk transparan mengenai mengapa mereka mengumpulkan data dan bagaimana mereka akan menggunakannya. Perlindungan data personal yang ada dalam GDPR terkait masalah ras, etnis, politik, kesehatan, gender, dan seksualitas yang berlaku.

Penelitian ini jika dibandingkan dengan penelitian-penelitian sebelumnya memiliki kesamaan dari segi topik, yaitu perlindungan privasi atas data pribadi, tetapi berbeda pada pokok analisisnya maka menjadi penting untuk mengkaji secara mendalam isu hukum yang berkaitan dengan bagaimana pengaturan perlindungan privasi atas data pribadi di beberapa negara. Penelitian ini bertujuan untuk mendiskusikan pengaturan dalam perspektif perbandingan hukum di beberapa negara.

Berdasarkan latar belakang di atas maka permasalahan yang diangkat, yaitu: Bagaimana perbandingan aturan mengenai perlindungan privasi atas data pribadi antara Indonesia dengan negara lain?

B. METODE PENELITIAN

Jenis penelitian ini adalah penelitian yuridis normatif, yakni penelitian hukum yang berbasis atau mengacu kepada kaidah-kaidah atau norma-norma hukum yang terdapat dalam peraturan perundang-undangan (Mertokusumo 2001). Bahan hukum yang digunakan dalam penelitian ini antara lain: bahan hukum primer, sekunder, dan tersier. Bahan hukum primer, yaitu bahan-bahan yang bersifat mengikat (Seokanto 2003), yang dalam penelitian ini berupa peraturan perundang-undangan, antara lain sebagai berikut: Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, *General*

Data Protection Regulation European Union, Data Protection Act 1998, US Privacy Act 1974, Personal Data Privacy Ordinance of 1995, The Personal Data Protection Act No. 709 of 2010, Personal Data Protection Act 2012, Personal Information Protection (Pipa) 2011, Data Protection Art, Peraturan Menteri Komunikasi dan Informasi Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, serta peraturan-peraturan lainnya. Bahan ini akan menjadi acuan untuk memberikan pemahaman mengenai pengaturan perlindungan dan pertanggungjawaban data pribadi. Sedangkan bahan hukum sekunder, yaitu bahan hukum yang isinya memberikan penjelasan mengenai bahan hukum primer (Soekanto 1989). Bahan hukum sekunder yang digunakan dalam penelitian ini adalah buku, jurnal, media elektronik, hasil penelitian, hasil karya dari kalangan hukum, dan seterusnya. Dan bahan hukum tersier, yaitu bahan hukum yang memberikan petunjuk dan penjelasan mengenai bahan hukum primer dan sekunder, misalnya kamus. Pendekatan yang digunakan adalah pendekatan perundang-undangan (*the statute approach*) yaitu mengkaji aturan hukum terkait isu perlindungan data pribadi dan pendekatan komparatif (*comparative approach*) yaitu perbandingan pengaturan perlindungan data pribadi dalam perspektif perbandingan hukum. Teknik pengumpulan bahan hukum dilakukan dengan cara *library research*, yaitu teknik dengan melakukan penelitian terhadap sejumlah literatur perpustakaan. Teknik analisis data yang digunakan yaitu penggambaran atau uraian konteks dari postulat hukum yang dianalisis secara deskriptif analitis.

C. HASIL DAN PEMBAHASAN

1. Ketentuan Hukum mengenai Perlindungan Privasi Data Pribadi di Beberapa Negara

Sejarah mencatat bahwa negara yang mengundangkan untuk pertama kalinya undang-undang perlindungan data adalah negara bagian Hesse di Jerman, yaitu pada tahun 1970. Kemudian diikuti oleh Swedia pada tahun 1973 dan Amerika Serikat pada tahun 1974 dan Inggris pada tahun 1984. Dalam penelitian ini akan digambarkan ketentuan hukum mengenai perlindungan privasi data dan/atau informasi pribadi, yaitu *Directive on the Protection of Personal Data* (95/46/EC) yang merupakan pedoman pembentukan undang-undang mengenai perlindungan data bagi negara-negara Uni Eropa, *Data Protection Act* 1998 di Inggris, ketentuan hukum perlindungan data di Amerika Serikat yaitu *Privacy Act* 1974 (Makarim 2005), dan ketentuan hukum terbaru mengenai perlindungan data di Uni Eropa yaitu EU 679/2016 *Regulation The Protection of Natural Persons with Regard to The Processing of Personal Data and on The Free Movement of Such Data (General Data Protection Regulation).*

1) European Union – General Data Protection Regulation

Pada tanggal 20 Februari 1995 Dewan Menteri Uni Eropa menyetujui rancangan petunjuk/instruksi (*Directive*) yang disebut sebagai "*Directive 95/46/EC of the Parliament and The Council on the Free Movement of such Data*". *Directive* ini secara formal disetujui pada tanggal 24 Oktober 1995 dan baru akan berlaku efektif tiga tahun kemudian yaitu pada tahun 1998. *Directive* ini mengharuskan kelima belas negara Uni Eropa untuk mengundangkan peraturan yang berkenaan dengan pengolahan data pribadi (processing of personal data).

Dalam Pasal 1 dinyatakan bahwa tujuan dari *directive* ini adalah untuk melindungi hak-hak dasar dan kebebasan dari setiap orang khususnya hak atas privasi dalam kaitannya dengan pemrosesan data pribadi. Dalam *directive* ini pengolahan (*processing*) didefinisikan sebagai: "setiap tindakan atau kumpulan tindakan, baik secara otomatis maupun tidak, termasuk, tetapi tidak terbatas pada pengumpulan, perekaman, pengorganisasian, penyimpanan, penyesuaian, atau perubahan, pencairan, konsultasi, penggunaan, penyingkapan, dengan pengiriman, penyebaran, atau cara lainnya yang bijak, penjajaran atau kombinasi pembatasan, penghapusan atau pengrusakan" (Makarim 2005). Data pribadi didefinisikan sebagai setiap informasi yang berhubungan untuk mengidentifikasikan atau dapat mengidentifikasikan seseorang. Hal ini tidak hanya berupa informasi tertulis termasuk juga foto-foto, kesan audiovisual dan rekaman suara dari seseorang atau yang dapat mengidentifikasikan seseorang (Makarim 2005).

Sehubungan dengan itu, perlu diketahui bahwa pihak-pihak yang diatur dalam *directive* ini adalah antara lain sebagai berikut (Makarim 2005):

1. Subjek data, yaitu orang yang data pribadinya diproses.
2. *Controller*, yaitu pribadi hukum, otoritas publik, agen atau Lembaga lain yang baik sendiri maupun bersama-sama menentukan tujuan dan cara pemrosesan data pribadi; jika tujuan dan cara pemrosesan data ditentukan oleh negara atau undang-undang *controller* ditentukan oleh negara atau undang-undang.
3. *Process*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang memproses data pribadi atas nama *controller*.

4. *Third party*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain kecuali subjek data, *controller*, *processor*, atau orang lain di bawah wewenang *controller* atau *processor*, berwenang untuk mengolah data.
5. *Recipient*, yaitu seseorang atau badan hukum, otoritas publik, agen atau badan lain yang kepadanya data disingkapkan.
6. *Supervisory Authorities*, yaitu badan/lembaga publik yang independen pribadi, yang mempunyai wewenang untuk menyelidiki kegiatan pengolahan data, termasuk hak untuk mengakses data tersebut dan wewenang untuk menghalangi pengiriman data ke pihak ketiga. Badan ini harus juga mendengarkan keluhan dari subjek data dan harus mengeluarkan laporan paling tidak laporan tahunan sesuai dengan undang-undang perlindungan data yang bertugas mengawasi perlindungan data.

Rumusan lingkup *directive* ini ditetapkan pada pemrosesan data pribadi, baik secara keseluruhan ataupun sebagian dengan alat otomatis, dan *directive* ini tidak dapat diterapkan pada dua hal, yaitu terhadap masalah keamanan nasional dan Undang-Undang Tindak Pidana dan mengenai pengolahan data pribadi yang dilakukan oleh orang (pribadi kodrati) dalam kegiatan murni untuk kepentingan pribadi. Undang-undang nasional yang dibuat dalam rangka pemenuhan *directive* ini harus menjamin agar pemrosesan data pribadi akurat, *up to date*, relevan dan tidak berlebih-lebihan. Data pribadi hanya dapat digunakan untuk tujuan-tujuan yang sah untuk alasan data-data tersebut dikumpulkan dan disimpan dalam suatu

bentuk serta tidak boleh disimpan lebih lama dari waktu yang diperlukan untuk tujuan tersebut.

Data pribadi dapat diproses hanya dengan persetujuan dari subjek data jika secara hukum dipersyaratkan, atau untuk melindungi kepentingan umum atau kepentingan yang sah dari pihak swasta (*private party*), kecuali jika kepentingan-kepentingan tersebut melanggar kepentingan-kepentingan subjek data. Pemrosesan data mengenai ras atau suku bangsa, pendapat-pendapat politik, agama, bujukan-bujukan filosofis atau mengenai Kesehatan atau kehidupan seksual dilarang sama sekali dan dalam kebanyakan kasus dilarang tanpa persetujuan tertulis dari subjek data.

Pengolahan data (*data processor*) harus menginformasikan subjek data yang datanya diproses minimal hal-hal, yaitu identitas dari controller atau perwakilannya jika ada; tujuan pemrosesan data; informasi lain, seperti siapa saja *recipients* atau kategori *recipients*, apakah tanggapan terhadap masalahnya adalah keharusan atau sukarela, keberadaan hak untuk mengakses dan hak untuk meralat data mengenai dirinya. *Controller* juga harus menginformasikan hal yang sama bagi mereka yang datanya dikumpulkan tanpa persetujuan mereka. *Controller* diwajibkan untuk melakukan kegiatan pengolahan data secara sah sesuai dengan undang-undang, jika tidak dapat dikenakan hukuman dan setiap orang yang haknya dilanggar dapat diberikan ganti rugi.

Dalam perkembangannya, European Union mengesahkan General Data Protection Regulation 679/2016 yang mengatur lebih lanjut mengenai perlindungan terhadap data pribadi. EU 679/2016 mengatur tentang

perlindungan data secara umum. Terkait dengan pemanfaatan terhadap data pribadi, dalam Artikel 5 Regulasi ini terdapat prinsip-prinsip yang harus digunakan dalam mengolah data pribadi. Prinsip-prinsip yang berkaitan dengan pengolahan data pribadi tersebut adalah:

1. Diolah secara sah, adil, dan transparan sehubungan dengan subjek data (sesuai prinsip hukum, keadilan, dan transparan);
2. Dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah, dan tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut: pemrosesan lebih lanjut untuk tujuan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistic harus dianggap sesuai dengan tujuan awal (Batasan tujuan);
3. Memadai, relevan, dan terbatas pada apa yang diperlukan sehubungan dengan tujuan pemrosesannya (minimisasi data);
4. Akurat dan jika perlu terus diperbaharui: setiap langkah yang wajar harus diambil untuk memastikan bahwa data pribadi yang tidak akurat, dengan memperhatikan tujuan pemrosesannya, dihapus atau diperbaiki tanpa penundaan (akurasi);
5. Disimpan dalam bentuk yang memungkinkan identifikasi subjek data tidak lebih dari yang diperlukan untuk tujuan data pribadi diproses: data pribadi dapat disimpan dalam jangka waktu yang lebih lama sepanjang data pribadi akan diproses semata-mata untuk tujuan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis, atau tujuan statistic tunduk pada penerapan teknis dan

organisasi yang sesuai. Tindakan tersebut dipersyaratkan oleh Regulasi ini untuk melindungi hak dan kebebasan subjek data (pembatasan penyimpanan);

6. Diproses dengan cara yang menjamin keamanan data pribadi yang sesuai, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan terhadap kerugian, kerusakan, atau kerusakan yang tidak disengaja dengan menggunakan tindakan teknis atau organisasi yang tepat (integritas dan kerahasiaan).

Dalam peraturan ini, *controller* bertanggung jawab untuk dan dapat menunjukkan kesesuaian dalam mengolah data sesuai dengan prinsip "diolah secara sah, adil, dan transparan sehubungan dengan subjek data (sesuai dengan prinsip hukum, keadilan, dan transparansi)." Pengolahan terhadap data akan dianggap legal hanya jika dan sejauh salah satu dari hal berikut berlaku:

1. Subjek data telah memberikan persetujuan untuk memproses data pribadinya untuk satu atau lebih tujuan tertentu;
2. Pemrosesan diperlukan untuk kinerja suatu kontrak dimana subjek data adalah pihak atau untuk mengambil langkah-langkah atas permintaan subjek data sebelum menandatangani kontrak;
3. Pengolahan diperlukan untuk memenuhi kewajiban hukum yang menjadi subjek pengendali;
4. Pengolahan diperlukan untuk melindungi kepentingan vital subjek data atau orang alami lainnya;

5. Pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan kewenangan resmi yang diberikan kepada pengontrol;
6. Pemrosesan diperlukan untuk kepentingan sah yang diperlukan oleh *controller* atau pihak ketiga, kecuali jika kepentingan tersebut ditolak oleh kepentingan atau hak dan kebebasan mendasar dari subjek data yang memerlukan perlindungan data pribadi, khususnya dimana subjek data adalah anak kecil.

2) Inggris – Data Protection Act 1998

Undang-Undang Perlindungan Data (*Data Protection Act* 1998) yang menggantikan *Data Protection Act* 1984 telah berlaku efektif sejak tanggal 1 Maret 2000. Undang-Undang ini lahir akibat perkembangan penggunaan komputer yang semakin pesat yang menimbulkan kekhawatiran terhadap informasi tentang seseorang yang diproses tanpa sepengetahuan mereka serta tanpa adanya kemampuan untuk mengakses informasi tersebut atau memperbaikinya jika salah. Undang-Undang ini berusaha menjaga keseimbangan antara hak dari setiap individu dan kemampuan pihak lain untuk memproses data mengenai mereka. Hal yang berubah dari Undang-Undang sebelumnya adalah bahwa Undang-Undang yang baru ini dapat diterapkan pada data yang diproses secara manual, tidak hanya pada data yang diproses komputer saja, adanya kategori data sensitif, dan larangan pengiriman data ke negara lain yang tidak mempunyai perlindungan data yang cukup (Makarim 2005).

Para pihak yang diatur dalam ketentuan *Data Protection Act* 1998, adalah meliputi (Makarim 2005):

1. *The Data Protection Commissioner*

   Semua pengguna data yang menguasai data pribadi harus mendaftar pada badan ini.

2. *Data Subject*/subjek data

   Artinya setiap individu yang menjadi subjek dari data pribadi tersebut.

3. *Data Controller* (pengguna data)

   Artinya setiap orang yang menentukan tujuan dan cara mengolah data pribadi.

4. *Data Processor*

   Artinya yang dipersamakan dengan *computer bureau* (biro komputer), yaitu orang (di luar pegawai *data controller*) yang memproses data atas nama data controller.

Data Protection Act 1998 juga mengatur mengenai hak-hak subjek data, yaitu bahwa setiap individu yang menjadi subjek data sehubungan dengan data pribadi mengenai mereka yang dimiliki oleh orang/pihak lain mempunyai hak untuk mengakses informasi, mencegah pemrosesan yang dapat menyebabkan kerusakan atau keadaan yang membahayakan, hak untuk meminta kompensasi, hak untuk mengambil tindakan untuk membatasi, menghalang-halangi, menghapus atau menghancurkan data yang tidak akurat serta mempunyai hak untuk meminta *commissioner* untuk membuat penyelesaian terhadap tindakan-tindakan yang melanggar ketentuan-ketentuan dalam Undang-Undang ini. Ketentuan dalam *Data Protection Act* 1998 juga memberikan pengecualian-pengecualian terhadap masalah-masalah yang terkait dengan keamanan nasional, kejahatan, perpajakan, kesehatan, Pendidikan, dan kerja sosial.

3) Amerika – US Privacy Act 1974

Departemen Kesehatan Amerika Serikat pada tahun 1973 mengemukakan prinsip-prinsip umum perlindungan data pribadi yang termuat dalam *Fair Information Practices* yang terdiri atas 5 prinsip dasar, yaitu (Rosadi 2009):

1. *Notices / Awareness*

   Konsumen harus diberitahu terlebih dahulu data pribadi mereka akan diakses oleh pihak kedua dan harus melalui beberapa proses seperti:

   a. Pemilik data harus diberitahu tentang identifikasi para pihak yang akan mengoleksi informasi pribadinya (*identification of the entity collecting the data*);
   b. Pemilik data harus mendapat informasi mengenai tujuan penggunaan informasi pribadinya (*identification of the users to which data will be put*);
   c. Pemilik data harus diberitahu pihak-pihak mana saja yang akan mengolah informasi pribadinya (*identification of any potential recipients of the data*);
   d. Peruntukan data tersebut (*the nature of the data collected and the means but which it is collected if not obvious*);
   e. Pemilik data harus diberikan kesempatan untuk membiarkan atau menolak penyebaran informasi pribadinya (*whether the provisions of the requested data is voluntary or requires and the consequences of a refusal to provide the requested information*);
   f. Langkah-langkah yang harus diambil oleh pihak yang akan mengoleksi data untuk menjaga kerahasiaan, integritas serta

keamanan informasi pribadinya (*steps taken by the data collector to ensure the confidentiality, integrity and quality of the data*).

2. *Choice / Consent*

   Konsumen mempunyai hak untuk memilih apakah akan menyetujui atau tidak apabila informasi pribadinya akan diakses oleh pihak lain di dalam transaksi *online*. Proses cukup mudah dengan menge-klik pilihan ini dan biasanya muncul pada setiap *website*.

3. *Access / Participation*

   Prinsip ini memberi peran aktif kepada konsumen yaitu berhak untuk dapat mengakses informasi tentang dirinya kepada pihak manapun dan berhak untuk selalu mengoreksi informasi pribadinya.

4. *Integrity / Security*

   Data yang diakses harus tepat dan aman untuk menjaga ketepatan dan keamanan suatu data maka pihak kedua harus menempuh beberapa langkah seperti harus selalu melakukan pemeriksaan ulang tentang ketepatan datanya termasuk selalu menghubungi pihak pertama kemudian dari segi keamanan pihak kedua harus memiliki penguasaan secara teknik bagaimana untuk mengamankan data tersebut termasuk proses filterisasi sehingga data yang telah terkumpul tidak dapat ditembus oleh pihak yang tidak bertanggung jawab.

5. *Enforcement / Redress*

   Suatu prinsip tidak dapat secara efektif diberlakukan apabila tidak ada mekanisme untuk penegakan hukum.

> Berbeda dengan di Eropa, Amerika Serikat tidak mempunyai suatu undang-undang yang mengatur mengenai perlindungan data dan/atau informasi secara keseluruhan, mengenai pengumpulan, pengkomunikasian dan penggunaan semua informasi mengenai individu-individu. Selain itu, pengaturannya hanya dibatasi hanya suatu pihak tertentu, misalnya pemerintah atau industri-industri tertentu, misalnya perbankan, asuransi, dan lain-lain (Makarim 2005).

Privacy Act 1974 ini menekankan pembatasan pengumpulan dan informasi pribadi oleh agen-agen pemerintah federal. Undang-Undang ini tidak berlaku bagi pengumpulan data pribadi oleh lembaga-lembaga swasta (Makarim 2005). Undang-undang ini menekankan agar agen-agen pemerintah bertanggung jawab dalam mengumpulkan, memelihara, menggunakan, atau menghapuskan catatan-catatan informasi yang dapat mengidentifikasikan seseorang dalam cara yang dapat menjamin bahwa perbuatan tersebut untuk tujuan yang sah dan berguna serta merupakan informasi yang baru dan akurat untuk tujuan penggunaannya, dan perlindungan yang cukup disediakan untuk penyalahgunaan informasi tersebut (Makarim 2005). Intinya Undang-Undang ini mencoba memberikan suatu kontrol pada setiap orang pada tingkatan tertentu terhadap penggunaan informasi mengenai mereka yang diproses oleh pemerintah federal. Jadi meskipun terdapat beberapa pengecualian, Undang-Undang ini pada umumnya melarang setiap agen pemerintah dari membuka catatan yang berhubungan dengan seseorang tanpa persetujuan orang tersebut.

4) Hongkong – Personal Data Privacy Ordinance of 1995

Hongkong menjadi negara yang pertama kali mengatur secara komprehensif mengenai masalah privasi atas data pribadi di Asia, yaitu *Personal Data Privacy Ordinance of 1995* (PDPO) yang telah dilakukan perubahan besar pada tahun 2012. Implementasi peraturan perundang-undangan tersebut dilakukan oleh lembaga khusus penanganan isu privasi data pribadi yang bernama *Privacy Commisioner for Personal Data* (PCPD).

Prinsip perlindungan hak privasi data pribadi di Hongkong mencakup Batasan pengumpulan data yang dilakukan berdasarkan tujuan pengumpulannya secara sah, penggunaan dan pengungkapan data pribadi harus sesuai dengan tujuannya dan persetujuan dari pemiliknya, kualitas data pribadi yang benar, penyimpanan data pribadi oleh pihak ketiga memiliki batas waktu, pengelola data pribadi diwajibkan untuk melindungi dari akses yang tidak dapat dipertanggungjawabkan, dan keterbukaan "*data user*" yang digunakan oleh Hongkong yang mewajibkan pihak ketiga pengelola data (organisasi atau perusahaan) untuk mempublikasikan kebijakan privasi kepada publik, jika dilanggar maka pemerintah Hongkong memberikan surat somasi kepada pihak ketiga yang bersangkutan (Greeneaf 2014).

5) Malaysia – The Personal Data Protection Act No. 709 of 2010

Malaysia memiliki *The Personal Data Protection Act No. 709 of 2010* (PDPA Malaysia). Terdapat tujuh prinsip dalam PDPA Malaysia yang diadopsi dari *EU Data Protection Directive* dari *OECD Guidelines* atau *APEC Framework*. Adanya PDPA 2012 di Malaysia maka jaminan keamanan data pribadi dari pengguna internet menjadi meningkat. Karena PDPA Malaysia banyak mengacu

pada aturan dalam *EU Data Protection Directive* dari *OECD Guidelines* atau *APEC Framework* maka Malaysia juga mengatur dalam PDPA bahwa tidak diizinkannya melakukan transfer data pribadi ke luar Malaysia, kecuali telah mendapatkan izin dari Menteri Informasi, Kebudayaan dan Komunikasi serta negara atau tempat yang menjadi tempat mentransfer data pribadi dapat memberikan jaminan perlindungan data pribadi yang setara dengan PDPA berikan (Greeneaf 2014).

6) Singapura – Personal Data Protection Act 2012

Singapura memiliki Personal Data Protection Act (PDPA) 2012. Pengaturan mengenai data pribadi di Singapura berlaku penuh sejak tahun 2014. Aturan mengenai data pribadi antara Malaysia dan Singapura memiliki banyak kesamaan karena keduanya mengadopsi aturan yang terdapat dalam *European Data Protective Directive* (EUDP). Tetapi terdapat perbedaan dalam aturan milik Malaysia dan Singapura, yaitu PDPA 2012 milik Singapura dilengkapi dengan sebuah badan khusus pendaftaran nomor telepon bernama *Do Not Call* (DNC) *Registry*, dimana masyarakat memiliki hak untuk menerima maupun menolak pesan singkat (SMS atau MMS) dari pihak ataupun organisasi *marketing* yang tidak diinginkan (Latumahina 2014).

7) **Korea Selatan – Personal Information Protection (Pipa) 2011**

Perlindungan privasi atas data pribadi di Korea Selatan dalam *Personal Information Protection (Pipa)* 2011. Prinsip perlindungan privasi atas data pribadi yang dimiliki Korea Selatan tidak berbeda jauh dengan aturan yang dimiliki oleh Hongkong, yaitu tujuan yang jelas dalam proses pengumpulan data pribadi (dipastikan akurat, lengkap, dan benar) yang digunakan sesuai dengan tujuannya,

menjaga keamanan data pribadi dan pengelolaan data pribadi yang tidak boleh melanggar hak yang bersangkutan sesuai dengan ketentuan hukum (Latumahina 2014).

8) Jepang – Data Protection Art

Jepang telah memiliki regulasi perlindungan privasi data pribadi sejak tahun 2000. *Data Protection Art* merupakan aturan hukum yang diadopsi oleh Pemerintah Federal Jepang. Perumusan aturan hukum terkait dengan perlindungan privasi atas hak pribadi dicetuskan oleh Keidanren, yaitu *representative body* yang secara khusus mengatur mengenai permasalahan industry dan perdagangan di Jepang. Pengaturan data pribadi sebagai bentuk perlindungan pemerintah Jepang dalam era persaingan dagang di Uni Eropa maka lahirlah *Data Protection Art* (Indriyani 2017). Prinsip-prinsip perlindungan data pribadi dalam *Data Protection Art* yaitu data pribadi bersifat rahasia, pemilik data pribadi yang tercatat mengetahui dengan pasti tujuan penggunaan data pribadinya oleh pihak manapun, terdapat persetujuan berupa *privacy policy* sebagai bentuk penggunaan data yang tidak sesuai dengan persetujuan, pemilik data pribadi berhak untuk melakukan perubahan maupun perbaikan data pribadinya, dan apabila terjadi pelanggaran penggunaan data pribadi maka diharuskan adanya pemulihan kembali atau ganti rugi yang diakibatkan oleh pelanggaran yang ditimbulkan di kemudian hari.

2. Ketentuan Hukum mengenai Perlindungan Privasi Data Pribadi di Indonesia

Di Indonesia, Undang-Undang yang secara khusus mengatur mengenai perlindungan data pribadi memang belum ada, namun aspek perlindungannya sudah tercermin dalam peraturan perundang-undangan lainnya. Aspek perlindungan *privacy* di

Indonesia yang paling mendasar tercantum di dalam Konstitusi Indonesia, yaitu Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD 1945), diatur pada Bab XA mengenai Hak Asasi Manusia dalam Pasal 28C sampai dengan 28I, yang di antaranya:

1. Pasal 28C (1) menyatakan bahwa "Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia". Pasal tersebut secara implisit dapat memayungi hak untuk merasa aman dan nyaman, *to be let alone* yang merupakan kebutuhan dasar manusia. Hak untuk memperoleh manfaat dari ilmu pengetahuan dan teknologi dapat juga menjadi landasan hukum untuk perlindungan data privasi pada sistem elektronik.
2. Pasal 28D (1) menyatakan bahwa "Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum". Pasal tersebut memberikan landasan hukum perlindungan terhadap privasi secara eksplisit.

Konstitusi Indonesia tidak secara eksplisit mengatur mengenai perlindungan data pribadi di dalam UUD 1945. Begitu juga dengan privasi, meskipun UUD 1945 menyatakan dengan tegas adanya perlindungan terhadap hak asasi manusia. Namun UUD 1945 menunjukkan adanya landasan hukum yang kuat dan mendasar untuk adanya pengaturan lebih lanjut bagi pelaksanaan privasi dan perlindungan privasi yang termasuk juga data privasi. Dalam UUD 1945 ketentuan mengenai data privasi secara implisit bisa ditemukan dalam Pasal 28F dan perlindungan terkait data privasi di dalam Pasal 28C dan 28G (1) UUD 1945 mengenai kebebasan untuk menyimpan informasi

dan perlindungan atas data dan informasi yang melekat kepadanya. Selanjutnya, akan dibahas mengenai undang-undang dan peraturan lainnya di Indonesia yang mengandung perlindungan terhadap data pribadi.

1. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Dalam Undang-Undang ini terdapat ketentuan mengenai kebebasan untuk berkomunikasi dan mendapatkan informasi secara pribadi sekaligus pula jaminan terhadap privasinya. Dalam Pasal 14 ayat (2) dinyatakan bahwa salah satu hak mengembangkan diri adalah hak untuk mencari, memperoleh, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis sarana yang tersedia. Ini berarti adanya keseimbangan antara hak untuk memperoleh informasi dengan hak atas privasi, yaitu hak untuk menyimpan informasi terutama yang berhubungan dengan informasi pribadi seseorang (Makarim 2005).

Pasal 32 Undang-Undang ini juga 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. Pasal tersebut menunjukkan terdapat hak atas diakuinya kerahasiaan dalam komunikasi termasuk di dalamnya privasi untuk menyimpan informasi terutama yang berhubungan dengan data privasi seseorang (Rosadi 2009).

2. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

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

ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data privasi seseorang harus dilakukan atas persetujuan orang yang bersangkutan, ayat (2) kemudian menyatakan setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Sebagaimana tercantum dalam Pasal 26 Undang-Undang ITE, penggunaan setiap informasi dan data privasi melalui media elektronik yang dilakukan tanpa persetujuan pemilik data tersebut adalah sebuah pelanggaran hak privasi. Undang-Undang ITE juga mengatur lebih lanjut bahwa mengakses sistem elektronik untuk memperoleh informasi atau dokumen elektronik, dan memindahkan serta mentransfer informasi elektronik adalah perbuatan yang dilarang dan diancam dengan pidana.

Perlindungan data pribadi dalam sebuah sistem elektronik berdasarkan UU ITE meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh Penyelenggara Sistem Elektronik (PSE), dan perlindungan dari akses dan intervensi yang dilakukan secara ilegal. Terkait perlindungan terhadap data pribadi dari penggunaan tanpa izin, Pasal 26 UU ITE mensyaratkan bahwa pemanfaatan data pribadi dalam sebuah media elektronik harus mendapat persetujuan dari pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan.

Persetujuan sebagaimana dimaksud dalam UU ITE bukan hanya mengenai pernyataan "*yes*" atau "*no*" dalam perintah (*command*) "*single click*" maupun "*double click*", melainkan harus juga didasari atas kesadaran seseorang dalam memberikan persetujuan terhadap penggunaan atau pemanfaatan data pribadi sesuai dengan tujuan atau kepentingan yang disampaikan pada saat perolehan data.

3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa hal yang berkenaan dengan kerahasiaan informasi. Antara lain dalam Pasal 22 dinyatakan bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau manipulatif: (a) akses ke jaringan telekomunikasi; dan/atau (b) akses ke jasa telekomunikasi; dan/atau (c) akses ke jaringan telekomunikasi khusus. Bagi pelanggar, ketentuan tersebut diancam pidana penjara maksimal enam tahun dan/atau denda maksimal Rp.600.000.000,- (enam ratus juta rupiah).

Menurut Peraturan Pemerintah Tahun 2000 tentang Penyelenggaraan Telekomunikasi yang merupakan peraturan pelaksana dari Undang-Undang Nomor 36 Tahun 1999, internet dimasukan ke dalam jenis jasa multimedia, yang diidentifikasikan sebagai penyelenggara jasa telekomunikasi yang menawarkan layanan berbasis teknologi informasi. Hal tersebut menunjukkan bahwa pengaturan internet termasuk ke dalam hukum telekomunikasi.

4. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Di dalam pengaturan yang terdapat dalam PP PSTE 2012, salah satu hal yang menjadi sorotan serta mendapat perhatian besar adalah berkenaan dengan privasi serta perlindungan data dan informasi, terutama yang bersifat elektronik ini terutama melihat kepada kemudahan yang diberikan oleh perkembangan sistem elektronik yang memudahkan transmisi serta akses akan data dan informasi (Rosadi 2009).

Dalam PP ini, perlindungan privasi terutama dalam kerahasiaan data privasi diatur dalam beberapa pasal. Pasal 12 ayat (1) huruf c menyatakan bahwa penyelenggara sistem elektronik wajib untuk menjaga rahasia, keutuhan, dan

ketersediaan Data Pribadi yang dikelolanya serta menjamin bahwa pemanfaatan terhadap Data Pribadi berdasarkan persetujuan dari pemilik Data Pribadi. Pasal 22 ayat (1), Pasal 38 ayat (2), Pasal 39 ayat (1), Pasal 55 ayat (3), serta Pasal 68 ayat (1) juga mewajibkan adanya perlindungan terhadap informasi elektronik. Dalam pasal-pasal tersebut ditekankan pentingnya bagi penyelenggara sistem elektronik untuk menjaga kerahasiaan data pribadi serta pentingnya persetujuan dari pemilik data pribadi untuk dapat melakukan pemanfaatan terhadap data pribadi tersebut. Lebih lanjut mengenai perlindungan data pribadi oleh PSE, Pasal 15 ayat (2) PP PSTE mengatur bahwa dalam hal terjadi kegagalan dalam perlindungan rahasia data pribadi yang dikelolanya, PSE wajib memberitahukan secara tertulis kepada pemilik pribadi.

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

Peraturan Menteri ini yang dimaksud dengan data pribadi sebagaimana tercantum dalam Pasal 1 ayat (1) adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Kemudian pada Pasal 2 ayat (1) dinyatakan bahwa perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisaan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Lebih lanjut ditentukan bahwa dalam melaksanakan ketentuan sebagaimana dimaksud dalam Pasal 2 ayat (1) tersebut harus berdasarkan asas-asas perlindungan data pribadi yang baik, yang salah satunya meliputi penghormatan terhadap data pribadi sebagai privasi. Ruang lingkup privasi dalam Peraturan Menteri ini tercantum di dalam Pasal 2 ayat (3) yaitu kebebasan

Pemilik Data Pribadi untuk menyatakan rahasia atau tidak menyatakan rahasia data pribadinya, kecuali ditentukan lain sesuai dengan ketentuan peraturan perundang-undangan.

Menurut Peraturan Menteri ini, perlindungan data pribadi dalam sistem elektronik dilakukan pada proses perolehan dan pengumpulan; pengolahan dan penganalisaan; penyimpanan; penampilan, pengumuman, pengiriman, penyebarluasan, dan/atau pembukaan akses; pemusnahan. Selain mengatur mengenai ruang lingkup data privasi dan perlindungan data privasi, peraturan ini juga menekankan pentingnya persetujuan dari pemilik data pribadi untuk dapat mengolah dan menganalisis data serta pentingnya penghormatan terhadap kerahasiaan data pribadi. Hal tersebut ditekankan kembali di dalam Pasal 21 yang menyatakan bahwa untuk dapat menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan/atau membuka akses data pribadi dalam sistem elektronik hanya dapat dilakukan atas persetujuan kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan dan setelah diverifikasi keakuratan dan kesesuaian dengan tujuan perolehan dan pengumpulan data pribadi tersebut. Oleh sebab itu, dapat disimpulkan yang menjadi titik berat dalam memperoleh akses terhadap pemanfaatan data pribadi adalah persetujuan dari pemilik data pribadi.

6. Naskah Akademis Rancangan Undang-Undang Perlindungan Data Pribadi

Perlindungan Data dan Informasi merupakan kajian yang baru dalam bidang hukum (Rianarizkiwati 2014), menyebabkan jaminan atas hak perlindungan data dan informasi pribadi belum terdapat suatu peraturan perundang-undangan khusus yang secara ideal menjadi payung hukum untuk mengatur seluruh aktivitas pada seluruh

bidang kehidupan di Indonesia (Rianarizkiwati 2014). Hal ini didukung dengan kondisi masyarakat yang semakin rumit dan kompleks dilatarbelakangi dengan pesatnya perkembangan ilmu pengetahuan dan teknologi sehingga membutuhkan perubahan yang cepat untuk menjamin kebutuhan perlindungan hukum masyarakat di berbagai bidang. Kebutuhan tersebut mengakibatkan kecenderungan timbulnya gejala *hiper*-regulasi, yaitu pengaturan berlebih terhadap suatu hal (Husein 2005).

Sejalan dengan perihal *hiper*-regulasi tersebut, perlindungan Data dan Informasi Pribadi tersebar dalam beberapa peraturan perundang-undangan sesuai dengan bidang masing-masing yang mengatur perlindungan Data dan Informasi Pribadi dalam sektor yang berbeda. Pengaturan hukum terkait perlindungan Data dan Informasi Pribadi masih bersifat parsial dan sektoral sehingga belum bisa memberikan perlindungan yang optimal dan efektif terhadap suatu data sebagai bagian dari hak atas privasi. Komitmen Negara untuk melakukan perlindungan atas Data dan Informasi Pribadi tergambar melalui berbagai peraturan perundang-undangan yang tersebar di berbagai bidang yang mengakui perlindungan atas hak seseorang terhadap Data dan Informasi Pribadi miliknya. Adapun idealnya, pengaturan oleh negara mengenai perlindungan Data dan informasi pribadi cukup dituangkan dalam satu peraturan khusus yang dapat menjangkau seluruh aktivitas masyarakat pada bidang dan sektor yang berbeda, tidak hanya dalam kegiatan *online* tetapi juga termasuk kegiatan *offline* (Rianarizkiwati 2014).

Berbagai faktor pendukung tersebut kemudian mendorong pemerintah untuk merealisasikan perlindungan Data dan Informasi Pribadi dengan membuat suatu Peraturan Perundang-Undangan mengenai Perlindungan Data Pribadi. Hingga saat ini, gagasan tersebut masih berbentuk Rancangan Undang-Undang Perlindungan

Data Pribadi (Rianarizkiwati 2014). Dalam Rancangan Undang-Undang tersebut diatur mengenai hak dan kewajiban para pihak sebagai subjek hukum yang berkaitan dengan konsep Perlindungan Data dan Informasi Pribadi. Berdasarkan aturan tersebut, pihak Pemilik memiliki hak-hak terhadap Data dan Informasi pribadinya yang ditegaskan dalam prinsip perlindungan Data dan Informasi Pribadi.

D. PENUTUP

Berdasarkan uraian di atas maka dapat disimpulkan bahwa regulasi Perlindungan Data Pribadi di Indonesia belum mengatur secara matang dan mendalam dibandingkan dengan aturan di beberapa negara lain, terdapat beberapa peraturan di Indonesia yang mengatur mengenai perlindungan data pribadi, yaitu UUD 1945, UU HAM, UU Adminduk, UU ITE, PP PSTE dan Permen Kominfo tentang perlindungan data pribadi serta beberapa peraturan sektoral lainnya, namun beberapa dari peraturan tersebut terlihat ketidakharmonisan maka diperlukan adanya unifikasi hukum. Terlebih RUU Perlindungan Data Pribadi masuk prolegnas sejak 2019 sehingga perlu perhatian dan analisa yang tinggi untuk merancang RUU ini menjadi Undang-Undang yang kuat dan adil. Saran yang dapat diberikan, yaitu diperlukan adanya harmonisasi hukum dari perlindungan data pribadi yang matang dan mendalam. Pemerintah perlu membuat dan menjalankan layaknya *Data Protection Agency* di Uni Eropa (sudah dicanangkan dengan adanya Komisi di RUU Perlindungan Data Pribadi) dengan baik dan tegas untuk melakukan kontrol terhadap hubungan hukum antara pemilik data pribadi dan pengendali data.

Berdasarkan uraian di atas maka dapat penulis sarankan agar pemerintah perlu segera mengesahkan pemberlakuan RUU Perlindungan Data Pribadi sebagai peraturan

perundang-undangan yang harmonis dan sinergis mengenai Perlindungan Data dan Informasi Pribadi. Dimana hal ini merupakan peran dan tanggung jawab Negara dalam menjamin hak asasi manusia yaitu hak atas privasi juga untuk melindungi terutama dalam kegiatan teknologi informasi dan komunikasi. Hal ini tentu bertujuan untuk mengurangi berbagai pelanggaran dalam praktik Perlindungan Data dan Informasi Pribadi.

DAFTAR PUSTAKA

Artikel Jurnal

Dewi, S. 2016. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Jurnal Yustisia* 5(1):22–40.

Indriyani, M. 2017. "Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System." *Justitia Jurnal Hukum* 1(2):191–208.

Latumahina, R. E. 2014. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya." *Jurnal Gema Aktualita* 3(2):14–25.

Sudaryanti, K. D. 2013. "Perlindungan Hukum Terhadap Investor Dalam Perdagangan Obligasi Secara Elektronik." *Kertha Wicara* 2(1):1–5.

Tejomurti, K. 2018. "Legal Protection for Urban Online-Transportation-User's Personal Data Disclosure in the Age of Digital Technology." *Padjajaran Journal of Law* 5(3):487–88.

Widyaningrat, I. A. W., & Dharmawan, N. K. S. 2014. "Tanggung Jawab Hukum Operator Telepon Selular Bagi Pengguna Layanan Jasa Telekomunikasi Dalam Hal Pemotongan Pulsa Secara Sepihak Di Denpasar." *Jurnal Ilmu Hukum* 2(5):1–5.

Yuking, Ana Sofa. 2018. "Urgensi Peraturan Perlindungan Data Pribadi Dalam Era Bisnis Fintech." *Jurnal Hukum Dan Pasarmodal* VIII(16):1.

Buku

Greeneaf, Graham. 2014. *Asian Data Privacy Laws-Trade and Human Rights Perspective.* New York: Oxford University Press.

Husein, Jimmly Asshidiqie &. Zainal A. M. 2005. *Hukum Tata Negara Dan Pilar-Pilar Demokrasi: Serpihan Pemikiran Hukum, Media, Dan HAM*. Jakarta: Sinar Grafika.

Makarim, Edmon. 2005. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian.* Jakarta: Raja Grafindo Persada.

Mertokusumo, Sudikno. 2001. *Penelitian Hukum Suatu Pengantar*. Yogyakarta: Liberty.

Rosadi, Sinta Dewi. 2009. *CyberLaw I (Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional)*. Bandung: Widya Padjajaran.

Seokanto, Sri Mamudji dan Soerjono. 2003. *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*. Jakarta: PT. Raja Grafindo Persada.

Soekanto, Soerjono. 1989. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia.

Tesis atau Disertasi

Rianarizkiwati, Nenny. 2014. "Kebebasan Informasi versus Hak Atas Privasi: Tanggungjawab Negara Dalam Perlindungan Data Pribadi." Universitas Indonesia.

Website

Aprilianti, Ira. 2020. "Hari Konsumen Nasional Perlindungan Data Pribadi Di Tengah Pandemi Covid 19." *Referensi.Eslam.or.Id* 1. Retrieved November 14, 2020 (https://referensi.elsam.or.id/2020/04/hari-konsumen-nasional-perlindungan-data-pribadi-di-tengah-pandemi-covid-19/).