KERANGKA HUKUM PERLINDUNGAN DATA PRIBADI DALAM PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI INDONESIA

Faiz Rahman
Fakultas Hukum Universitas Gadjah Mada
Email: faiz.rahman@ugm.ac.id
Naskah diterima: 2/9/2020, direvisi: 4/3/2021, disetujui: 16/3/2021

Abstract

Personal data protection becomes one of the important aspects that need to be applied in implementing e-Government (SPBE). One of the reasons is the Government's plans to use and manage citizens' data, including their personal data, through the utilization of new technologies, including big data, Internet of Things, Artificial Intelligence, etc.; and also several cases regarding breach of personal data that occurred in the recent years. This research is intended to examine the intersection of individual and the State's interests and to understand the dynamics of personal data protection regulations, especially related to SPBE. This research indicates that: First, it is essential to incorporate individual interests in the privacy protection and information security and the State's interests in developing public services through the utilization of citizen's personal data in the personal data protection legal framework; and Second, Laws regarding personal data are sporadically regulated with varying levels of arrangements. To overcome potential regulatory inconsistencies, there are several means need to be done, such as immediately ratify the Personal Data Bill, which include the discussion on the definition of personal data, classification of data, and accomodating the personal data protection principles; restricting access to certain types of personal data; and improving information security standards.

Keywords: personal data protection, legal framework, e-Government.

Abstrak

Perlindungan data pribadi menjadi salah satu aspek penting yang perlu diterapkan dalam penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE). Hal ini salah satunya dilihat dari rencana pemerintah dalam menggunakan dan mengelola data masyarakat, termasuk data pribadi, melalui pemanfaatan berbagai teknologi baru seperti *big data*, *Internet of Things*, *Artificial Intelligence*, dan lain sebagainya; serta beberapa kasus pelanggaran atau penyalahgunaan data pribadi yang terjadi beberapa waktu silam. Oleh karena itu, penelitian ini dimaksudkan untuk mengkaji persinggungan kepentingan antara individu dengan negara dalam penggunaan data pribadi, serta memahami dinamika pengaturan perlindungan data pribadi, khususnya yang terkait dengan SPBE. Hasil penelitian ini menunjukkan bahwa: Pertama, kepentingan individu atas perlindungan privasi dan keamanan informasi, serta kepentingan Negara dalam mengembankan pelayanan kepada masyarakat melalui pemanfaatan data pribadi masyarakat menjadi penting untuk diakomodasi dalam kerangka hukum perlindungan data pribadi; dan Kedua, pengaturan mengenai data pribadi pada level UU masih diatur secara sporadis dengan tingkat pengaturan yang berbeda-beda. Untuk mengatasi potensi inkonsistensi pengaturan, setidaknya terdapat beberapa hal yang perlu dilakukan seperti segera mengesahkan RUU Data Pribadi, termasuk di dalamnya membahas terkait dengan definisi dan klasifikasi data, mengakomodasi prinsip-prinsip perlindungan data pribadi, pembatasan akses terhadap data pribadi jenis tertentu, serta meningkatkan standar keamanan informasi yang dipegang.

Kata kunci: perlindungan data pribadi, kerangka hukum, Sistem Pemerintahan Berbasis Elektronik.

A. Pendahuluan

Pesatnya perkembangan teknologi telah masuk ke berbagai aspek kehidupan manusia, baik dalam aspek kehidupan sosial, budaya, ekonomi, politik, maupun hukum. Penggunaan teknologi juga telah secara signifikan mengubah pola komunikasi, interaksi, bahkan sampai dalam rangka pelayanan pemerintah kepada masyarakatnya.[1] Dalam konteks pemerintahan, pemanfaatan teknologi untuk penyelenggaraan pemerintahan dan pelayanan kepada masyarakat tersebut sering disebut sebagai *e-Government*. Apabila ditelusuri ke belakang, gelombang pertama penerapan *e-Government* sendiri telah terjadi di berbagai negara sejak awal tahun 2000an, baik di negara maju maupun negara berkembang,[2] termasuk di Indonesia.

Penerapan *e-Government* di Indonesia sendiri dapat ditelusuri kembali sejak tahun 2001, melalui dikeluarkannya Instruksi Presiden Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia (Inpres Telematika 2001). Selanjutnya, pada tahun 2003, dikeluarkan Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government* (Inpres *E-Government*) yang secara spesifik berisi mengenai kebijakan pemerintah dalam penerapan *e-Government* di Indonesia. Dalam pertimbangannya, dinyatakan bahwa keluarnya Instruksi Presiden *a quo* adalah untuk mendorong pemanfaatan teknologi dalam proses pemerintahan guna meningkatkan efisiensi, efektifitas, transparansi, dan akuntabilitas dalam penyelenggaraan pemerintahan.[3]

Melalui Inpres *E-Government*, pimpinan kementerian, lembaga, dan daerah didorong untuk mengambil langkah-langkah yang diperlukan serta merumuskan rencana tindak lanjut penerapan *e-Government* dengan berpedoman pada Lampiran Instruksi Presiden tersebut.Pada intinya, Lampiran Instruksi Presiden *E-Government* berisi kebijakan-kebijakan utama dalam pengembangan *e-Government* di Indonesia.[4] Berbagai inisiatif yang dilakukan oleh pemerintah pada waktu itu rupanya dapat membawa Indonesia menduduki peringkat 70 dalam *E-GovernmentDevelopment Index* (EGDI) pada tahun 2003.[5] Meskipun demikian, posisi Indonesia dalam EGDI cukup fluktiatif dan cenderung menurun, hingga pada tahun 2018 menduduki peringkat 107,[6] dan akhirnya bisa kembali naik di posisi 88 pada Laporan EGDI Tahun 2020.[7]

Lebih lanjut, guna menguatkan landasan penerapan *e-Government* di Indonesia, pada tahun 2018, diundangkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Perpres SPBE). Pada prinsipnya, SPBE sendiri merupakan *e-Government* apabila dilihat dari definisi dalam Perpres *a quo*, yakni "penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE".[8] Definisi tersebut setidaknya sejalan dengan pemaknaan *e-Government* oleh *Organisation for Economic Co-opration and Development* (OECD)[9] dan *European Parliament*[10].

1. Lihat Rachel Silcock. 2001. What Is *e-Government. Parliamentary Government* 54, hlm. 88.
2. Lihat dalam Svenja Falk, Andrea Rommele, dan Michael Silverman. "The Promise of Digital Government". Dalam Svenja Falk, et al (eds). 2017. *Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens*. Switzerland: Springer Internasional Publishing, hlm. 6.
3. Lihat Konsiderans huruf b Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*.
4. Lihat Lampiran Instruksi Presiden Nomor 3 Tahun 2003 berisi dokumen mengenai kebijakan dan strategi-strategi nasional yang utama dalam pengembangan *e-Government* di Indonesia.
5. Lihat United Nations. 2003. *UN Global E-Government Survei 2003.* New York: United Nations, hlm. 61.
6. Lihat United Nations. 2018. *United Nations E-Government Survei* 2018. New York: United Nations, hlm. 229.
7. Lihat United Nations. 2020. *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* New York: United Nations, hlm. 278.
8. Pasal 1 angka 1 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
9. Menurut OECD, *e-Government* adalah penggunaan teknologi informasi, khususnya internet, sebagai alat untuk mencapai pemerintah yang lebih baik. Lihat dalam Organisation for Economic Co-operation and Development. 2003. *The E-Government Imperative*. Paris: Organisation for Economic Co-operation and Development, hlm. 23.
10. European Parliament mendefinisikan E-Government sebagai "istilah yang digunakan untuk menjelaskan penerapan teknologi informasi dan komunikasi untuk meningkatkan pelayanan publik dan partisipasi masyarakat dalam negara yang demokratis". Lihat dalam European Parliament. 2015. *eGovernment: Using technology to improve public services and democratic participations*. European Union, hlm. 3.

Melalui penerapan SPBE, pemerintah juga berupaya untuk memanfaatkan berbagai teknologi baru seperti *big data*, *Internet of Things*, *Artificial Intelligence*, dan lain sebagainya.[11] Hal tersebut tertuang dalam Rencana Induk SPBE sebagaimana terlampir dalam Perpres SPBE. Pemanfaatan berbagai teknologi tersebut tentu memiliki tantangan tersendiri, terutama dalam kaitannya dengan isu privasi dan perlindungan data pribadi. Hal ini mengingat melalui penggunaan berbagai teknologi di atas, data masyarakat dapat dikumpulkan dan diolah secara masif oleh pemegang data, yang dalam hal ini adalah pemerintah.

Isu privasi dan perlindungan data pribadi perlu menjadi perhatian dalam penyelenggaraan SPBE. Era digital saat ini justru memberikan tantangan tersendiri terhadap integritas privasi atas data pribadi.[12] Salah satu hal yang menjadikan era digital sebagai tantangan terhadap privasi atas data pribadi adalah sifat dari informasi yang terdigitasi (*digitised information*) yang mendorong terbentuknya lingkungan yang tidak menghormati privasi atas data pribadi, mengingat data pribadi menjadi mudah dikumpulkan dan disebarkan.[13] Selain itu, isu mengenai portabilitas data (*data portability*) juga menjadi tantangan tersendiri,[14] yang mana saat ini teknologi *cloud computing* semakin banyak digunakan, termasuk oleh instansi pemerintahan, untuk menyimpan berbagai data, termasuk data pribadi.

Hal ini salah satunya dapat dilihat dari sejumlah kasus yang melibatkan data pribadi masyarakat yang dipegang oleh instansi pemerintah. Misalnya, kasus "kebocoran data" NIK dan KK dalam proses registrasi kartu SIM pada tahun 2018,[15] kasus pembobolan rekening yang menimpa wartawan senior Ilham Bintang karena datanya yang terdaftar di sistem daring Otoritas Jasa Keuangan (OJK) disalahgunakan,[16] dan kebocoran data 2,3 juta data kependudukan dalam daftar pemilih tetap Pemilu 2014 yang dipegang oleh KPU.[17] Kemudian, beberapa waktu lalu juga sempat ramai di media mengenai kebocoran data pasien Covid-19.[18] Beberapa kasus di atas setidaknya dapat menunjukkan pentingnya kerangka hukum perlindungan data pribadi yang baik dalam penerapan SPBE.

Selain itu, perlindungan data pribadi dalam konteks penerapan SPBE juga menjadi hal yang penting karena data dan informasi sendiri merupakan salah satu unsur esensial dari SPBE.[19] Adapun data dan informasi dalam Perpres SPBE memiliki cakupan yang sangat luas, yakni mencakup semua jenis data dan informasi yang dimiliki oleh instansi pusat dan pemerintah daerah, dan/atau yang diperoleh dari masyarakat, pelaku usaha, dan/atau pihak lain.[20] Lebih lanjut, dalam penggunaan data dan informasi,

11. Berbagai inisiatif ini dapat dilihat dalam Rencana Induk Sistem Pemerintahan Berbasis Elektronik Nasional (Lampiran Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik).
12. Lihat Warren B. Chik. 2013. The Singapore Personal Data Protection Act and an assessment of future trends in data privacy. *Computer Law and Security Review* Volume 5, hlm. 555.
13. Lihat *Ibid*.
14. *Ibid*, 556.
15. Lihat Kustin Ayuwuragil. "Kominfo Akui 'Pencurian' NIK dan KK Saat Registrasi Kartu SIM". *CNN Indonesia*. 6 April 2018. Diakses tanggal 21 Agustus 2020. https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim.
16. CNN Indonesia. "Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank". *CNN Indonesia*. 6 Februari 2020. Diakses tanggal 21 Agustus 2020. https://www.cnnindonesia.com/nasional/20200205211241-12-472073/pembobolan-rekening-ilham-bintang-data-dijual-orang-bank.
17. Riyan Setiawan. "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014". *Tirto*. 22 Mei 2020. Diakses tanggal 21 Agustus 2020. https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B. Lihat juga Kompas.com. "Penjelasan KPU soal Dugaan Kebocoran Data Kependudukan di DPT Pemilu. *Kompas*. 22 Mei 2020. Diakses tanggal 21 Agustus 2020. https://nasional.kompas.com/read/2020/05/22/09063931/penjelasan-kpu-soal-dugaan-kebocoran-data-kependudukan-di-dpt-pemilu.
18. Kompas.com. "Hacker Klaim Miliki Data Hasil Tes Pasien Covid-19 di Indonesia". *Kompas*. 20 Juni 2020. Diakses tanggal 21 Agustus 2020. https://tekno.kompas.com/read/2020/06/20/07592607/hacker-klaim-miliki-data-hasil-tes-pasien-covid-19-di-indonesia.
19. Pasal 7 ayat (2) huruf f Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
20. Lihat Pasal 26 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

dinyatakan bahwa penggunaannya diutamakan secara bagi pakai (*sharing*).[21] Artinya, data yang dipegang oleh suatu instansi dapat digunakan pula oleh instansi lain dengan didasarkan pada hal-hal tertentu sebagaimana ditentukan dalam Perpres SPBE. Ditambah lagi, diundangkannya Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres Satu Data) semakin menguatkan penerapan penggunaan data secara bagi pakai (*sharing*).

Selanjutnya, dengan memperhatikan kerangka regulasi perlindungan data pribadi yang ada, hingga saat ini Indonesia belum memiliki undang-undang yang spesifik dan komprehensif mengatur perlindungan data pribadi seperti misalnya *Personal Data Protection Act 2010* di Malaysia, *Personal Data Protection Act 2012* di Singapura, dan *General Data Protection Regulation* (GDPR) di EU yang berlaku sejak tahun 2018. Pengaturan mengenai data pribadi justru ditemukan dalam Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk). UU *a quo* juga merupakan UU pertama yang memberikan definisi yuridis mengenai data pribadi, yakni data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.[22] Lebih lanjut, wacana untuk membentuk UU Perlindungan Data Pribadi (UU PDP) pun sejatinya sudah mengemuka sejak tahun 2014.[23] Saat ini, draft RUU PDP yang terbaru telah masuk dalam Prolegnas 2020-2024 dan sekarang sudah memasuki tahap pembahasan.[24]

Dengan berbagai inisiatif pemerintah dalam penggunaan teknologi baru dalam pengelolaan data dan pemanfaatan data secara bagi pakai sebagaimana telah dijelaskan di atas, serta berbagai kasus yang melibatkan data pribadi masyarakat yang dipegang oleh beberapa instansi Negara beberapa waktu ke belakang, menjadi penting untuk menelaah kerangka hukum perlindungan data pribadi dalam konteks penerapan SPBE.Berdasarkan pemaparan di atas, penelitian ini berfokus membahas mengenai dinamika pengaturan perlindungan data pribadi, secara spesifik dilihat dari perspektif penerapan *e-Government* (SPBE). Dengan demikian, diharapkan penelitian ini dapat melengkapi dan menambah perspektif dalam kajian hukum perlindungan data pribadi yang telah ada. Berdasarkan latar belakang di atas, terdapat dua permasalahan yang diangkat dalam penelitian ini: Pertama, telaah terhadap persinggungan kepentingan antara individu dengan negara dalam penggunaan dan pemanfaatan data pribadi dalam penerapan SPBE; dan Kedua, telaah terhadap dinamika pengaturan perlindungan data pribadi yang terkait dengan penyelenggaraan SPBE di Indonesia.

Dalam penelitian ini, metode yang digunakan adalah metode penelitian hukum normatif yang menekankan pada penelitian kepustakaan terhadap data sekunder,[25] dengan sifat penelitian deskriptif,[26] serta berbentuk evaluatif dan preskriptif.[27] Terdapat tiga pendekatan yang digunakan dalam menjawab permasalahan yang diangkat, yakni pendekatan undang-undang, konseptual, dan komparatif.[28] Pendekatan konseptual digunakan utamanya untuk menjawab permasalahan pertama mengenai titik singgung kepentingan individu dan Negara. Sedangkan, untuk menjawab permasalahan kedua mengenai dinamika pengaturan perlindungan data pribadi terkait dengan penyelenggaraan SPBE, digunakan ketiga pendekatan tersebut.

21. Penggunaan data secara bagi pakai pada prinsipnya adalah penggunaan suatu data secara bersama-sama (*sharing*) oleh lebih dari satu instansi. Istilah "bagi pakai" diperkenalkan dalam Perpres SPBE. Lihat misalnya Pasal 26 ayat (3) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
22. Pasal 1 angka 22 Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.
23. Lihat dalam Devy Kurnia. "Kemkominfo Siapkan RUU Perlindungan Data Pribadi". *Kementerian Komunikasi dan* Informatika. 7 Oktober 2015. Diakses tanggal 21 Agustus 2020. https://kominfo.go.id/index.php/content/detail/6142/Kemkominfo+Siapkan+RUU+Perlindungan+Data+Pribadi/0/sorotan_media.
24. Lihat dalam Dewan Perwakilan Rakyat. "Program Legislasi Nasional Prioritas". *Dewan Perwakilan Rakyat*. Diakses tanggal 21 Agustus 2020. http://www.dpr.go.id/uu/prolegnas.
25. Soerjono Soekanto. 2007. *Pengantar Penelitian Hukum.* Jakarta: UI Press, hlm. 9.
26. Soerjono Soekanto dan Sri Mamudji. 2015. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Press, hlm. 14.
27. *Ibid*, 10.
28. Peter Mahmud Marzuki, 2005. *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana.

B. Pembahasan

B.1. Data Pribadi dan Persinggungan Kepentingan antara Individu dengan Negara

Perbincangan mengenai perlindungan data pribadi kerap dikaitkan dengan perlindungan terhadap hak privasi. Bahkan, dalam Penjelasan UU ITE 2016, hak atas data pribadi dijelaskan sebagai salah satu bagian dari *privacy rights*, yang mana mengandung pengertian sebagai berikut:[29]

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

Dari ketiga hal tersebut, dapat dilihat bahwa salah satu pengertian dari *privacy rights* berdasarkan Penjelasan UU ITE mencakup hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Pengertian tersebut secara implisit menunjukkan bahwa subyek data (individu) pada dasarnya memiliki kontrol penuh atas informasi tentang dirinya.[30]

Kemudian, apabila dikaitkan dengan penyelenggaraan *e-Government*, yang pada prinsipnya merujuk pada penggunaan teknologi informasi dan komunikasi dalam penyelenggaraan pemerintahan,[31] maka pengumpulan, penggunaan, dan pengelolaan data masyarakat oleh Negara menjadi suatu keniscayaan. Ditambah lagi, dalam Rencana Induk SPBE sebagaimana terlampir dalam Perpres SPBE, terdapat upaya untuk memanfaatkan berbagai teknologi baru seperti *big data*, IoT, dan AI,[32] yang mana beberapa contoh teknologi tersebut menggunakan data dan informasi yang dimiliki oleh instansi pemerintah atau Negara sebagai 'bahan bakar' agar berbagai teknologi tersebut dapat bekerja. Dalam diskursus yang berkembang, terdapat pandangan yang mengatakan bahwa saat ini, data memiliki nilai tersendiri layaknya aset.[33] Sebagai contoh, perkembangan pesat beberapa perusahaan internet terbesar seperti Google, Facebook, dan Twitter sendiri tidak terlepas dari peran mereka dalam mengumpulkan, mengelola, dan menganalisis data pribadi.[34]

Hal yang menjadi permasalahan adalah pengumpulan dan pengolahan data individu masyarakat secara masif, terutama oleh instansi pemerintah, dianggap tidak sejalan dengan konsep tradisional hak atas privasi yang ditujukan untuk memberikan perlindungan terhadap individu dengan memberikan hak kepada individu untuk mengontrol informasi pribadi mereka.[35] Bart van der Sloot[36] menyatakan dua alasan mengapa pengumpulan dan pengolahan data secara masif oleh pemerintah menjadi permasalahan:

---

29. Penjelasan Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
30. Hal ini sejalan apabila dikaitkan dengan doktrin privasi pada tahun 1970-an yang menekankan pada peran penuh subyek data untuk menentukan sifat dan sejauh apa pengungkapan dirinya. Lihat dalam Bart van der Sloot. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?". Dalam Ronald Leenes, *et al* (Eds). 2017. *Data Protection and Privacy: (In)visibilities and Infrastructures*. Switzerland: Springer Internasional Publishing, hlm. 5.
31. Lihat misalnya definisi yang diberikan oleh OECD dalam Organisation for Economi Cooperation and Development. 2014. *Recomendation of the Council on Digital Government Strategies*. Paris: OECD Publishing, hlm. 6; dan EU dalam European Parliament. 2015. *eGovernment: Using technology to improve public services and democratic participations*. European Union, hlm. 3.
32. Lihat dalam Lampiran Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
33. Lihat dalam Wahyudi Djafar. "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan". *SeminarHukum dalam Era Analisis Big Data,* Program Pasca Sarjana Fakultas Hukum UGM. 26 Agustus 2019. Lihat juga World Economic Forum. 2011. *Personal Data: The Emergence of a New Aset Class – Opportunities for the Telecomunications Industry*. World Economic Forum, hlm. 4.
34. World Economic Forum, *Ibid*, 9.
35. Lihat dalam Bart van der Sloot, *Loc.cit.*
36. *Ibid.*

Pertama, pemrosesan data sering kali tidak hanya dilakukan terhadap data privat atau sensitif, tetapi data yang bersifat publik dan non-sensitif seperti kepemilikan kendaraan, kode pos, jumlah anak, dan lain sebagainya.[37]

Kedua, doktrin privasi pada waktu itu menekankan pada hak dari subjek data untuk memiliki peran sepihak dalam menentukan sifat dan sejauh apa pengungkapan dirinya. Namun demikian, karena pemrosesan data sering kali tidak hanya berkaitan dengan data privat dan sensitif, hak atas kontrol oleh subjek data dirasa tidak dimungkinkan dan tidak beralasan, karena berbanding terbalik dengan data privat dan sensitif, subjek data tidak memiliki kepentingan personal dalam mengontrol (sebagian) data publik dan umum.

Selanjutnya, dengan mendasarkan pada dua argumen tersebut, van der Sloot juga menyatakan bahwa terminologi data pribadi (*personal data*) tidak hanya mencakup data yang sifatnya sensitif atau privat, tetapi mencakup data publik dan non-sensitif.[38] Alih-alih memberikan hak untuk mengontrol (data), fokus dari prinsip-prinsip perlindungan data adalah pada keadilan dan kewajaran dalam pemrosesan data.[39]

Penjelasan di atas menunjukkan bahwa sebenarnya terdapat pula karakteristik yang berbeda namun berkaitan antara data pribadi dan privasi. Di satu sisi, dapat dikatakan bahwa setiap data privat atau sensitif itu merupakan data pribadi, tetapi tidak semua data pribadi merupakan privasi seseorang. Lebih lanjut, dalam konteks EU saja, hak atas perlindungan data pribadi sebagai salah satu *fundamental rights* ditempatkan dalam pasal yang berbeda dengan hak atas privasi dalam *the Charter of Fundamental Rights of the European Union*.[40] Hal ini memperlihatkan bahwa dalam konteks EU, perlindungan data pribadi sudah terlepas dari hak atas privasi, baik pada level *fundamental rights* maupun level regulasi dibawahnya, dan saat ini dianggap sebagai doktrin yang bersifat independen.[41] Apabila mendasarkan pada penjelasan di atas, maka sejatinya dapat terlihat bagaimana dua kepentingan dalam upaya pemanfaatan data pribadi ini saling bersinggungan. Di satu sisi, individu memiliki kepentingan terhadap kontrol atas data pribadinya, sehingga tidak terjadi pengungkapan yang tidak diinginkan atau pun disalahgunakan.[42] Meskipun kebanyakan doktrin privasi menekankan pada subyektifitas individu untuk menilai apakah suatu informasi merupakan privasinya (sehingga dapat diungkapkan atau tidak), namun salah satu poin penting dalam konteks perlindungan data pribadi adalah bagaimana upaya perlindungan data pribadi juga dapat menjadi sarana untuk melindungi privasi seseorang.[43] Kendati demikian, tidak dapat dipungkiri bahwa privasi sendiri sejatinya merupakan salah satu hak asasi manusia yang telah diakui dan dijamin perlindungannya secara internasional[44] dan nasional[45].

37. Bart van der Sloot. 2014. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law* Volume 4 Issue 3, hlm. 308.
38. *Ibid*. Lihat juga Allan F. Westin dan Michael A. Baker, 1972. *Databanks in a Free Society: Computers, Record-keeping and Privacy*. New York: The New York Times Book.
39. Hak atas privasi diatur dalam *Article 7 the Charter of Fundamental Rights of the European Union*, sedangkan hak atas perlindungan data pribadi diatur dalam *Article 8*. Selengkapnya lihat dalam *Charter of Fundamental Rights of the European Union* (2012/C 326/02).
40. Bart van der Sloot. "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?". *Op.cit.*, 6.
41. Meskipun di atas ditunjukkan salah satunya bahwa perlindungan data pribadi dalam konteks EU telah "lepas" dari perlindungan dalam privasi baik pada level hak fundamental dan peraturan-peraturan di bawahnya, namun doktrin-doktrin yang digunakan dalam perlindungan data pribadi sendiri masih memiliki keterkaitan yang cukup erat dengan doktrin-doktrin dalam privasi. Sebagai contoh, doktrin "Privacy by Design" yang kemudian ditransformasikan dalam GDPR menjadi "Data Protection by Design".
42. Sebagai contoh, lihat Robert Walters, Leon Trakman, dan Bruno Zeller. 2019. *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches*. Singapura: Springer, hlm. 13-15.
43. Sebagai contoh, lihat Article 17 *International Covenant on Civil and Political Rights, entry into force 23 March 1976*.
44. Dalam beberapa literatur dinyatakan bahwa Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 merupakan landasan dari hak atas privasi.
45. Priyank Jain, Manasi Gyanchandani, dan Nilay Khare. 2016. Big data privacy: a technological perspective and review. *Journal of Big Data* Volume 3 Nomor 25, hlm. 4.

Di sisi lain, Negara juga membutuhkan data pribadi masyarakat untuk digunakan dalam meningkatkan pelayanan pemerintah kepada masyarakatnya. Hal ini tidak terlepas dari fakta yang terjadi saat ini yang setidaknya dapat menunjukkan bahwa instansi pemerintah secara berkelanjutan melakukan pengumpulan dan pemrosesan terhadap data dengan jumlah yang besar.[46] Ditambah lagi, pandemi Covid-19 yang terjadi saat ini semakin mengakselerasi transformasi digital, yang salah satunya adalah melalui digitalisasi pelayanan publik.[47] Melalui pelayanan publik menggunakan teknologi digital, secara tidak langsung terjadi pula pengumpulan data masyarakat luas melalui berbagai layanan yang disediakan secara digital, tidak terkecuali data pribadi.

Sebagaimana telah dipaparkan sebelumnya, meskipun tidak semua data pribadi merupakan data yang bersifat sensitif atau privat, bukan berarti kemudian Negara mengesampingkan hak subyek data atas data pribadinya.[48] Ditambah lagi, dengan pemanfaatan berbagai teknologi baru seperti *big data, AI, machine learning*, dan lain sebagainya, terdapat pula faktor keamanan yang perlu diperhatikan oleh Negara dalam rangka pemrosesan data pribadi masyarakatnya menggunakan berbagai teknologi tersebut. Hal ini disebabkan adanya potensi ancaman terhadap privasi dan data pribadi seperti peretasan atau penyalahgunaan data pribadi yang dikumpulkan menggunakan berbagai teknologi baru sebagaimana disebutkan di atas.[49]

Isu lain yang kemudian mengemuka dalam kaitannya dengan kepentingan individu dan negara adalah terkait dengan menyeimbangkan hak atas privasi dengan menjamin keterbukaan informasi dan data.[50] Di era digital seperti sekarang ini, Negara juga dituntut untuk terbuka kepada masyarakatnya, termasuk dalam kaitannya dengan data yang dipegang oleh instansi pemerintah atau Negara. Namun demikian, sebagaimana dipaparkan sebelumnya, tidak semua data yang dipegang oleh instansi Negara bisa dibuka kepada publik. Hal ini bisa dikarenakan sifat data tersebut yang rahasia, atau karena data tersebut merupakan data pribadi yang sifatnya privat atau sensitif.

Lebih lanjut, hal lain yang juga berkaitan erat dengan perlindungan data pribadi adalah mengenai keamanan siber. Hukum perlindungan data pribadi pada prinsipnya berfokus pada upaya perlindungan dan fasilitasi terhadap pengumpulan dan penggunaan data pribadi, sedangkan hukum keamanan siber membahas tindak kriminal yang terjadi melalui sistem dan infrastruktur komputer.[51] Dengan demikian, adanya potensi pelanggaran terhadap privasi yang terjadi dari suatu tindak pidana siber pun merupakan suatu hal yang tidak dapat dikesampingkan. Aspek hukum dan teknologi memiliki andil yang penting dalam rangka memastikan upaya perlindungan data pribadi masyarakat yang dipegang oleh instansi pemerintah atau Negara terjamin keamanannya.

Berbagai kasus dugaan kebocoran dan penyalahgunaan data yang dipegang oleh beberapa instansi pemerintahan dan Negara sebagaimana disebutkan pada bagian Pendahuluan sejatinya dapat menunjukkan bagaimana aspek keamanan ini menjadi satu hal yang penting dalam upaya perlindungan data pribadi masyarakat. Hal ini juga sekaligus menunjukkan bahwa Negara memiliki

46. Deborah Agostino, Michela Arnaboldi, dan Melisa Diaz Lema. 2021. New development: COVID-19 as an accelerator of digital transformation in public service delivery. *Public Money & Management* Volume 51 Nomor 1, hlm. 69.

47. Hak subyek data atas data pribadinya sebagai contoh adalah hak atas transparansi terhadap pemrosesan data pribadi, hak untuk mengakses data pribadi terkait dirinya, hak untuk perbaikan data, hak untuk membatasi pemrosesan data dalam keadaan tertentu, hak atas portabilitas data, dan lain sebagainya. Sebagai contoh, lihat dalam *Chapter 3 – Rights of the data subject Regulation (EU) 2016/679 (General Data Protection Regulation).*

48. Lihat misalnya, Gagan Deep Sharma, Anshita Yadav, dan Ritika Chopra. 2020. Artificial intelligence and effective governance: A review, critique and research agenda. *Sustainable* Futures Volume 2, hlm. 4. Lihat juga Priyank Jain, Manasi Gyanchandani, dan Nilay Khare. *Loc.cit.*

49. Lebih lengkap lihat dalam penelitian yang dilakukan oleh Institute for Criminal Justice Reform (Anggara, Supriyadi Widodo Eddyono, dan Wahyudi Djafar. 2015. *Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia.* Jakarta: Institute for Criminal Justice Reform).

50. Robert Walters, Leon Trakman, dan Bruno Zeller. *Op.cit.*, 375.

51. Lihat Konsiderans huruf b Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government.*

peranan yang krusial dalam menjamin pemenuhan kepentingan individu dan Negara dalam pemanfaatan data pribadi, serta memastikan keamanan data pribadi yang dipegang oleh instansi pemerintah atau Negara. Sehingga, hal tersebut dapat meminimalisir terjadinya pelanggaran terhadap privasi yang disebabkan oleh kejahatan siber, yang salah satunya dapat terjadi melalui penyalahgunaan data pribadi.

Dengan melihat pentingnya dua kepentingan di atas untuk diakomodasi, perlu dipahami bagaimana konstruksi peraturan perundang-undangan mengatur keduanya dalam konstruksi hukum perlindungan data pribadi. Untuk itu, bagian selanjutnya akan mengelaborasi kerangka hukum perlindungan data pribadi dalam konteks penyelenggaraan SPBE di Indonesia.

B.2. Kerangka Hukum Perlindungan Data Pribadi dalam Kaitannya dengan Penerapan SPBE di Indonesia

1. Dinamika Pengaturan Perlindungan data Pribadi dalam Kaitannya dengan SPBE

Perkembangan *e-Government* pada dasarnya tidak terlepas dari berbagai upaya yang dilakukan oleh pemerintah di berbagai negara dalam rangka meningkatkan kualitas layanannya, salah satunya melalui pemanfaatan teknologi informasi. Di Indonesia sendiri, inisiasi penerapan e-Government dapat dilihat melalui dikeluarkannya beberapa kebijakan seperti Inpres *E-Government* pada tahun 2003 dan beberapa regulasi yang merupakan tindak lanjut dari Inpres *a quo* seperti Keputusan Menteri Kominfo tentang Penyusunan Rencana Induk Pengembangan e-Government Lembaga dan Peraturan Menteri Kominfo tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional.

Apabila merujuk pada beberapa kebijakan yang ada pada waktu itu, terutama dalam Inpres *E-Government*, dapat dilihat bahwa *e-Government* ini dimaknai sebagai pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan (*e-Government*), yang tujuannya adalah untuk meningkatkan efisiensi, efektivitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan.[52] Dalam perkembangannya, pengaturan mengenai *e-Government* "dibadankan" dalam Perpres SPBE. Dalam Perpres *a quo*, SPBE didefinisikan sebagai penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.[53] Pengaturan dalam Perpres SPBE setidaknya menunjukkan adanya upaya untuk mengubah paradigma penerapan *e-Government* dari yang sebelumnya terkesan lebih menekankan pada aspek teknologi (dibandingkan pemerintahannya), menjadi pada aspek penyelenggaraan pemerintahannya. Sehingga, teknologi di sini ditempatkan sebagai sarana untuk mendukung penyelenggaraan pemerintahan.

Apabila kembali ditarik ke belakang, penggunaan teknologi informasi dalam penyelenggaraan pemerintahan banyak dilakukan melalui pembentukan "sistem informasi" pada sektor-sektor yang spesifik. Sebagai contoh, Sistem Informasi Lingkungan Hidup dalam Undang-Undang Nomor 32 Tahun 2009 tentang Perlindungan dan Pengelolaan Lingkungan Hidup, Sistem Informasi Kearsipan dalam Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, Sistem Informasi Desa dan Sistem Informasi Pembangunan Wilayah Pedesaan dalam Undang-Undang Nomor 6 Tahun 2014 tentang Desa, dan Sistem Informasi Pemerintahan Daerah dan Sistem Informasi Pembangunan Daerah dalam Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah. Dengan berbagai macam sistem informasi yang muncul secara sporadis dalam berbagai undang-undang tersebut, integrasi layanan menjadi salah satu pekerjaan rumah tersendiri bagi pemerintah, khususnya dalam rangka meningkatkan layanan kepada masyarakat.

Hal yang menjadi benang merah antara perlindungan data pribadi dengan penyelenggaraan SPBE adalah berkaitan dengan bagaimana Negara atau pemerintah menggunakan data mengenai masyarakat yang dimilikinya, mengingat data dan informasi merupakan salah satu unsur penting dalam SPBE.[54] Dalam Perpres SPBE, data dan informasi ini

52. Pasal 1 angka 1 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
53. Lihat Pasal 4 ayat (2) huruf f Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
54. Lihat Pasal 26 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

memiliki cakupan yang luas, meliputi semua jenis data dan informasi yang dimiliki oleh instansi pusat dan pemerintah daerah, dan/atau yang diperoleh dari masyarakat, pelaku usaha, dan/atau pihak lain.[55] Ditambah lagi, penekanan pada penggunaan data dan informasi secara bagi pakai, memungkinkan suatu data digunakan secara bersama-sama oleh beberapa instansi pemerintahan.Dengan perkembangan teknologi yang semakin pesat, tidak dapat dipungkiri potensi kompleksitas permasalahan yang muncul semakin tinggi pula, termasuk salah satunya berkaitan dengan privasi dan data pribadi.

Dalam pembahasan sebelumnya, dapat dilihat bahwa di satu sisi individu (warga negara) memiliki kepentingan atas kontrol data pribadi yang dikumpulkan dan digunakan oleh instansi pemerintah atau Negara, serta perlunya jaminan atas keamanan data pribadinya, utamanya terkait dengan keamanan privasi sebagai salah satu hak asasi manusia yang dilindungi secara internasional dan nasional. Di sisi lain, Negara memerlukan data (pribadi) warga negaranya untuk dapat meningkatkan pelayanan yang diberikan dalam rangka memenuhi kebutuhan warga negaranya melalui pemanfaatan berbagai teknologi informasi. Selain itu, dengan melihat peran penting Negara dalam kerangka perlindungan terhadap data pribadi sebagaimana pula telah dijelaskan sebelumnya, kehadiran kerangka hukum perlindungan data pribadi dalam penyelenggaraan SPBE menjadi suatu keniscayaan untuk memberikan kepastian dan jaminan hukum dalam penerapan upaya perlindungan data pribadi dalam penyelenggaraan SPBE.

Untuk melihat dinamika pengaturan data pribadi yang terkait dengan penerapan SPBE, penting untuk kemudian melakukan pemetaan terhadap berbagai peraturan perundang-undangan, utamanya pada level undang-undang. Hal ini mengingat undang-undang sebagai sebuah peraturan perundang-undangan yang berlaku umum dan memiliki legitimasi kuat, serta menjadi landasan hukum dalam pengenaan sanksi – utamanya sanksi pidana. Lebih lanjut, apabila dikaitkan dengan upaya perlindungan HAM, maka undang-undang menjadi satu-satunya peraturan perundang-undangan di bawah UUD NRI Tahun 1945 yang dapat mengatur dan melakukan pembatasan terhadap HAM.[56] Maka dari itu, elaborasi pengaturan terhadap upaya perlindungan HAM sudah seharusnya diatur pada level undang-undang, termasuk berkaitan dengan privasi dan data pribadi.

Selanjutnya, untuk memetakan berbagai undang-undang yang terkait dengan penyelenggaraan SPBE, jenis Layanan SPBE sebagaimana diatur dalam Perpres SPBE digunakan sebagai dasar dalam melakukan pemetaan. Nomenklatur Layanan SPBE dalam Perpres *a quo* didefinisikan sebagai keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE yang memiliki nilai manfaat.[57] Layanan SPBE sendiri dimanfaatkan oleh Pengguna SPBE yang meliputi instansi pusat, pemerintah daerah, pegawai ASN, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkannya.[58] Dengan melihat konstruksi pengaturan dalam Perpres SPBE, Layanan SPBE sebagai suatu luaran dari penggunaan aplikasi SPBE yang dimanfaatkan oleh berbagai pihak memegang peranan sentral agar layanan pemerintahan dan publik dapat tersampaikan kepada seluruh Pengguna SPBE. Hal ini juga dikaitkan dengan salah satu unsur penting dalam SPBE yakni data dan informasi, yang salah satunya merupakan data pribadi yang didapatkan dari masyarakat luas. Dengan demikian, data pribadi masyarakat yang dipegang oleh instansi pemerintah atau Negara, salah satunya didapatkan melalui Layanan SPBE.

Lebih lanjut, Layanan SPBE sendiri terdiri atas (a) layanan administrasi pemerintahan berbasis elektronik; dan (b) layanan publik berbasis elektronik. Layanan administrasi berbasis elektronik pada

55. Hal ini salah satunya dapat dilihat dalam rumusan Pasal 28J ayat (2) yang menyatakan "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".
56. Lihat Pasal 1 angka 4 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
57. Lihat Pasal 1 angka 26 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
58. Lihat Pasal 42 ayat (2) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

dasarnya merupakan Layanan SPBE yang mendukung tata laksana internal birokrasi pemerintahan untuk meningkatkan kinerja dan akuntabilitas instansi pemerintahan.[59] Adapun jenis layanan ini antara lain meliputi layanan yang mendukung kegiatan perencanaan, penganggaran, keuangan, pengadaan barang dan jasa, kepegawaian, kearsipan, pengelolaan barang milik negara, pengawasan, dan akuntabilitas kinerja.[60] Kemudian, layanan publik berbasis elektronik merupakan Layanan SPBE yang mendukung pelaksanaan pelayanan publik pada instansi pemerintahan.[61] Jenis layanan publik berbasis elektronik sendiri antara lain meliputi layanan pada bidang pendidikan, pengajaran, pekerjaan dan usaha, tempat tinggal, komunikasi dan informasi, lingkungan hidup, kesehatan, jaminan sosial, energi, perbankan, perhubungan, dan sumber daya alam, pariwisata.[62]

Mendasarkan pada jenis Layanan SPBE di atas, dilakukan pemetaan terhadap berbagai undang-undang yang memiliki pengaturan terkait dengan data pribadi. Selengkapnya dapat dilihat pada Tabel 1.

Tabel 1. Ketentuan Terkait Data Pribadi yang Terkait dengan Layanan SPBE
Sumber: Diolah dari berbagai undang-undang, 2020.

59. Lihat Pasal 43 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
60. Lihat Pasal 42 ayat (3) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
61. Lihat Pasal 33 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
62. Robert Walters, Leon Trakman, Bruno Zeller. *Op.cit.*, 402.

Sebelum masuk ke dalam analisis pengaturan terkait dengan data pribadi dalam berbagai UU di atas, setidaknya terdapat hal yang perlu dipahami bersama untuk melihat apakah berbagai peraturan tersebut sudah cukup sebagai landasan perlindungan data pribadi – baik secara umum maupun spesifik pada masing-masing sektor. Perlu diketahui bersama, meskipun data pribadi merupakan sebuah isu yang sering diperbincangkan di dunia internasional, hingga saat ini belum terdapat *Model Law* yang benar-benar dapat diacu atau menjadi pedoman.[63] Hal ini kembali lagi dikarenakan banyaknya variasi data yang digunakan baik di sektor publik maupun privat.[64]

Lebih lanjut, dengan memperhatikan perkembangan yang terjadi saat ini, produk hukum yang paling dekat dikatakan sebagai *Model Law* adalah GDPR yang telah berlaku sejak tahun 2018. Mengacu pada GDPR, setidaknya terdapat poin-poin utama sebagai prasyarat dalam perlindungan privasi dan data pribadi, diantaranya:[65]

a. *requiring the consent of subjects for data processing* (persetujuan dari subyek data dalam pemrosesan data)
b. *anonumizing collected data to protect privacy* (anonimisasi data yang dikumpulkan)
c. *providing data breach notifications* (memberikan notifikasi apabila terdapat pelanggaran data)
d. *safely handling the transfer of data across borders* (memastikan keamanan transfer data lintas negara)
e. *requireing certain companies to appoint a data protection officer to oversee GDPR compliance* (menunjuk *data protection officer* untuk mengawasi kepatuhan terhadap aturan yang berlaku)

Untuk itu, perlu dianalisis apakah berbagai UU yang ada, setidaknya memuat pengaturan yang terkait dengan beberapa persyaratan utama di atas.

Lebih lanjut, berdasarkan penelusuran yang telah dilakukan, setidaknya terdapat 15 (lima belas) UU yang berkaitan dengan Layanan SPBE di atas dan memiliki pengaturan mengenai data pribadi atau setidak-tidaknya berkaitan dengan perlindungan terhadap data pribadi. Dapat dicermati dalam berbagai UU di atas, pengaturan mengenai data pribadi cukup bervariasi sesuai dengan jenisnya, ada yang pengaturannya sangat umum, implisit, bahkan sampai yang sifatnya spesifik.

Ketentuan yang secara umum atau implisit mengatur mengenai data pribadi dalam kaitannya dengan penyelenggaraan SPBE dapat dilihat pada UU ITE, UU Keterbukaan Informasi Publik (KIP), UU Pelayanan Publik, dan UU OJK. Dalam UU ITE misalnya, diatur ketentuan mengenai penggunaan data pribadi yang harus dilakukan atas persetujuan orang yang bersangkutan.[66] Namun dalam UU *a quo* tidak diatur mengenai apa yang dimaksud dengan data pribadi itu. Sehingga, apabila melihat secara historis pengaturan, definisi data pribadi dalam UU ITE merujuk pada definisi data pribadi dalam UU Adminduk, sebelum akhirnya definisi tersebut "diperbaiki" dalam PP PSTE 2019 sebagaimana telah dibahas pada bagian sebelumnya. Selain itu, dalam UU ITE juga tidak diatur mengenai sanksi terhadap pelanggaran pasal terkait dengan penggunaan data pribadi.

Kemudian, dalam UU KIP dapat ditemukan pengaturan mengenai pengecualian pembukaan akses informasi publik yang terkait dengan rahasia pribadi. Namun demikian, data tersebut tetap dapat dibuka apabila pihak yang rahasianya diungkap memberikan persetujuan tertulis dan/atau

63. *Ibid*.
64. Lihat dalam Juliana De Groot. 2018. What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019. *Digital Guardian*. 5 Agustus 2020. Diakses tanggal 30 Agustus 2020. https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection. Poin-poin tersebut sejalan dengan beberapa poin *legal measures* dalam *Global Cybersecurity Indeks*, yang antara lain meliputi kebijakan keamanan siber terkait dengan perlindungan data, pemberitahuan kegagalan data, dan perlindungan privasi. Lihat dalam International Telecommunication Union. 2018. *Global Cybersecurity Index 2018*. Switzerland: ITU Publication, hlm. 69.
65. Lihat Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
66. Lihat Pasal 18 ayat (2) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

pengungkapan berkaitan dengan posisi seseorang dalam jabatan-jabatan publik.[67] Pelanggaran terhadap ketentuan mengenai informasi yang dikecualikan dapat dikenakan sanksi pidana sesuai ketentuan dalam UU KIP. Sama dengan UU ITE, dalam UU KIP diatur mengenai adanya persetujuan dalam konteks pembukaan data. Dalam konteks pemrosesan data, tidak ditemukan ketentuan yang eksplisit mengatur dalam kedua UU di atas.

Selanjutnya, dalam UU Pelayanan Publik diatur mengenai larangan membocorkan informasi yang wajib dirahasiakan sesuai dengan peraturan perundang-undangan.[68] Meskipun tidak dijelaskan apa informasi yang wajib dirahasiakan dalam UU Pelayanan Publik, namun apabila mengacu pada definisi dalam UU Adminduk, maka dapat ditafsirkan bahwa informasi tersebut termasuk data pribadi, mengingat definisi data pribadi mencakup data perseorangan yang dilindungi kerahasiaannya. Selain ketentuan tersebut, tidak terdapat ketentuan lain yang berkaitan dengan perlindungan terhadap data pribadi. Padahal, UU Pelayanan Publik juga memegang peranan yang sentral sebagai payung hukum pelayanan publik di Indonesia.

Selain ketiga UU di atas, UU OJK juga memiliki pengaturan yang berkaitan dengan data pribadi, yakni mengenai larangan menggunakan atau mengungkapkan informasi apa pun yang bersifat rahasia kepada pihak lain.[69] Sama halnya dengan penjelasan mengenai informasi yang bersifat rahasia dalam UU Pelayanan Publik, maka dapat ditafsirkan bahwa informasi tersebut termasuk data pribadi. Ketentuan lebih lanjut mengenai kerahasiaan, penggunaan dan pengungkapan informasi justru baru diatur pada level Peraturan Dewan Komisioner.[70] Dalam UU OJK diatur mengenai sanksi pidana terhadap pelanggaran terhadap ketentuan terkait dengan data pribadi di atas.

Selain UU sebagaimana dipaparkan di atas, setidaknya terdapat 11 (sebelas) UU yang mengatur data pribadi pada sektor-sektor yang lebih spesifik. Dalam kategori layanan administrasi pemerintahan misalnya, dapat dilihat pengaturan dalam UU Kearsipan, UU ASN, dan UU Pengampunan Pajak. Dalam UU Kearsipan, diatur mengenai kewajiban pencipta arsip untuk menjaga kerahasiaan arsip yang bersifat tertutup, yang salah satunya adalah mengenai rahasia atau data pribadi.[71] Namun demikian, sama halnya dengan UU ITE, dalam UU Kearsipan tidak dijelaskan apa yang dimaksud dengan data pribadi, sehingga acuannya merujuk pada UU Adminduk. Adapun sanksi terhadap pelanggaran ketentuan di atas dapat dikenakan sanksi pidana sebagaimana diatur dalam UU Kearsipan.

Contoh lain dalam UU ASN, diatur mengenai pengumpulan dan pengelolaan data pegawai ASN melalui Sistem Informasi ASN yang dikelola oleh BKN. Namun demikian, tidak dapat ditemukan ketentuan mengenai tindakan yang dilakukan apabila terjadi pelanggaran terhadap data pribadi. Ketentuan yang dapat ditemukan adalah mengenai keharusan Sistem Informasi ASN harus memiliki sistem keamanan yang dipercaya.[72] Selanjutnya, dalam konteks UU Pengampunan Pajak, diatur mengenai manajemen data dan informasi oleh Menteri Keuangan yang dikumpulkan dari Wajib Pajak dalam rangka pengampunan pajak. Data dan informasi tersebut tidak dapat diminta oleh siapa pun atau diberikan kepada pihak mana pun kecuali atas persetujuan Wajib Pajak yang bersangkutan.[73] Berbeda dengan UU ASN, setidaknya dalam UU Pengampunan Pajak diatur mengenai perlunya persetujuan dalam pengungkapan data pribadi.

67. Lihat Pasal 34 huruf i Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.
68. Lihat Pasal 33 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.
69. Lihat Pasal 33 ayat (5) Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan. Lihat juga Peraturan Dewan Komisioner Otoritas Jasa Keuangan Nomor 01/17/PDK/XII/2012 tentang Kode Etik Otoritas Jasa Keuangan.
70. Lihat Pasal 44 dan Pasal 66 Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan.
71. Lihat Pasal 127 ayat (3) Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara.
72. Lihat Pasal 21 ayat (3) Undang-Undang Nomor 11 Tahun 2016 tentang Pengampunan Pajak.
73. Lihat Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lihat juga Pasal 41 Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah.

Selain layanan administrasi pemerintahan, dalam konteks layanan publik sebagaimana kategorisasi dalam Perpres SPBE, dari hasil penelusuran yang dilakukan, setidaknya terdapat tiga sektor utama yang mengatur mengenai data pribadi. **Pertama**, sektor perbankan. Pada sektor ini, terdapat setidaknya dua UU yang mengatur mengenai data pribadi, yakni UU Perbankan dan UU Perbankan Syariah. Kedua UU tersebut pada dasarnya mengatur hal yang serupa yakni mengenai kewajiban pengelola data – Bank dan pihak terafiliasi – untuk melindungi dan menjaga kerahasiaan informasi nasabah dan simpanannya.[74] Namun demikian, terdapat beberapa pengecualian dalam pengelolaan data nasabah tersebut, termasuk dalam konteks penggunaan dan pengungkapan data. Dalam kedua UU di atas, data nasabah dapat diungkapkan untuk kepentingan penegakan hukum,[75] maupun untuk kepentingan lain atas persetujuan dari nasabah.[76]

Kedua, sektor kesehatan. Dalam sektor ini terdapat cukup banyak UU yang mengatur mengenai data kesehatan pasien, yakni dalam UU Praktik Kedokteran,[77] UU Kesehatan,[78] UU Rumah Sakit,[79] UU Tenaga Kesehatan,[80] dan UU Keperawatan.[81] Semua UU tersebut pada prinsipnya mengatur mengenai kewajiban untuk melindungi data pribadi pasien. Namun demikian, hampir semua UU di atas tidak mengatur mengenai sanksi apabila terjadi pelanggaran data. Ketentuan mengenai sanksi yang secara eksplisit diatur dapat ditemukan pada UU Tenaga Kesehatan yang mengatur pemberian sanksi administratif apabila terjadi pelanggaran terhadap pasal terkait kewajiban menyimpan rahasia kesehatan. Padahal, apabila merujuk pada beberapa klasifikasi data pribadi sebagaimana dijelaskan pada bagian sebelumnya, data pada sektor kesehatan dapat dikategorikan sebagai data pribadi yang bersifat sensitif atau khusus. Lebih lanjut, penggunaan teknologi informasi di sektor digital tentu mau tidak mau akan sangat bergantung pada data sensitif tersebut, utamanya berkaitan dengan data kesehatan pasien. Selain itu, berbagai tindakan yang menyebabkan pelanggaran, termasuk pelanggaran data dalam sektor kesehatan masuk dalam ranah organisasi profesi. Dengan adanya isu mengenai kebocoran data pasien Covid-19 beberapa waktu lalu,[82] maka kerangka hukum yang kuat mengenai data pribadi, termasuk di sektor kesehatan, menjadi sesuatu yang penting dan urgen.

Ketiga, sektor administrasi kependudukan. Pada sektor ini, UU yang menjadi payung pengaturan adalah UU Adminduk. Dapat dikatakan bahwa sektor ini merupakan sektor yang datanya cukup sering disasar oleh oknum tidak bertanggung jawab, seperti contohnya pada kasus penyalahgunaan data NIK dan KK pada registrasi kartu SIM pada 2018 silam, kasus kebocoran data kependudukan di DPT Pemilu 2014, dan kasus dugaan kebocoran data pasien Covid-19, salah satu data yang diduga bocor adalah NIK.[83]

Lebih lanjut, UU *a quo* juga merupakan satu-satunya UU yang memberikan definisi data pribadi. Dalam UU *a quo*, data pribadi didefinisikan sebagai data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi

74. Lihat Pasal 41, Pasal 41A, dan Pasal 42 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lihat Pasal 42 dan Pasal 43 Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah.
75. Lihat Pasal 44A Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Lihat juga Pasal 47 Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah.
76. Lihat Pasal 46 sampai dengan Pasal 48 Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.
77. Lihat Pasal 57 Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
78. Lihat Pasal 32 dan Pasal 38 Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit.
79. Lihat Pasal 73 Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan.
80. Lihat Pasal 38 dan Pasal 39 Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan.
81. Lihat misalnya. Binti Mufarida. Data Pasien Covid-19 Bocor, Bukti Lemahnya Perlindungan Data Pribadi. *Sindo News*. 21 Juni 2020. Diakses tanggal 30 Agustus 2020. https://nasional.sindonews.com/read/76844/15/data-pasien-covid-19-bocor-bukti-lemahnya-perlindungan-data-pribadi-1592741202.
82. Lihat dalam CNN Indonesia. Data Covid-19 Warga RI Bocor, NIK hingga Hasil Rapid Test. *CNN Indonesia*. 19 Juni 2020. Diakses tanggal 30 Agustus 2020. https://www.cnnindonesia.com/teknologi/20200619212544-185-515376/data-covid-19-warga-ri-bocor-nik-hingga-hasil-rapid-test.
83. Pasal 1 angka 22 Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

kerahasiaannya.[84] Apabila dicermati, definisi tersebut merupakan definisi yang bersifat umum dan tidak secara spesifik ditujukan pada sektor administrasi kependudukan. Sehingga, menjadi konsekuensi logis apabila berbagai UU yang muncul setelahnya merujuk pada definisi data pribadi sebagaimana diatur dalam UU Adminduk meskipun UU ini bersifat sektoral.

Namun demikian, definisi data pribadi dalam UU Adminduk memiliki permasalahan tersendiri. Apabila melihat definisi data pribadi dalam *EU Directive 1995*[85] dan GDPR[86] misalnya, definisi tersebut hanya mencakup ruang lingkup data pribadi, yakni "data perseorangan tertentu", sedangkan sifat dari data pribadi yang dapat mengidentifikasikan secara langsung maupun tidak langsung, tidak dicantumkan dalam definisi tersebut. Unsur dalam definisi data pribadi dalam UU Adminduk lebih fokus pada upaya yang dilakukan terhadap data tersebut, yakni terkait dengan penyimpanan, perawatan, dan menjaga kebenaran data, serta merupakan data yang dilindungi kerahasiaannya.

Pertanyaannya, apakah data yang diinterpretasikan sebagai data pribadi menurut berbagai definisi yang ada, tetapi tidak dilindungi kerahasiaannya, tetap masuk dalam klasifikasi data pribadi? Bahkan, dalam UU Adminduk sendiri, diatur mengenai jenis-jenis data pribadi yang harus dilindungi. Jika ditafsirkan secara *a contrario*, maka pertanyaan selanjutnya adalah apakah terdapat data pribadi yang tidak harus dilindungi? Apabila iya, maka tentu hal tersebut justru inkonsisten dengan definisi data pribadi dalam UU Adminduk yang salah satu unsurnya adalah perlindungan terhadap kerahasiaannya.

Dalam perkembangannya, terdapat peraturan lain yang mendefinisikan data pribadi secara berbeda, yakni Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang mencabut Peraturan Pemerintah No. 82 Tahun 2012. Dalam PP tersebut, data pribadi didefinisikan sebagai 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 non elektronik.[87] Apabila membandingkan dengan beberapa negara seperti Korea Selatan, Singapura, Malaysia, dan Jepang yang masing-masing sudah memiliki UU PDP sendiri, definisi data pribadi dalam PP *a quo* memiliki kemiripan dengan berbagai UU PDP di beberapa negara di atas, yakni berkaitan dengan ruang lingkup data (mencakup semua informasi tentang individu) dan sifat data pribadi (dapat mengidentifikasi secara langsung maupun tidak langsung individu tersebut).[88]

---

84. Dalam *EU Directive 1995*, data pribadi (personal data) didefinisikan sebagai *"[...] 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*". Lihat dalam Article 2(a) *Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995.

85. GDPR mendefinisikan personal data sebagai "[...] *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*". Lihat Article 4(1) *Regulation (EU) 2016/679 (General Data Protection Principles)*.

86. Pasal 1 angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Definisi data pribadi dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang sebelumnya menggunakan definisi yang sama dengan yang diatur dalam UU Administrasi Kependudukan.

87. Sebagai pembanding, lihat definisi data pribadi dalam Pasal 2 ayat (1) *Act on the Protection of Personal Information (Act No. 57 of May 30, 2003)* (Jepang); Pasal 4 *Personal Data Protection Act 2010 (Act 709)* (Malaysia); Pasal 2 angka 1 *Personal Information Protection Act (2011)* (Korea Selatan); dan Pasal 2 dan Pasal 23 *Personal Data Protection Act 2012 (No. 26 of 2012)* (Singapura).

88. Lihat Pasal 54 ayat (1) Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan 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.

Berbeda dengan beberapa negara di atas yang sudah memiliki undang-undang khusus mengenai data pribadi, hal yang perlu menjadi perhatian adalah definisi baru data pribadi ini diatur dalam level Peraturan Pemerintah. Sehingga, terdapat potensi bahwa penggunaan definisi tersebut tidak diikuti karena terdapat ketentuan pada level yang lebih tinggi, yakni di level undang-undang yang juga memberikan definisi data pribadi secara umum, meskipun dalam aturan yang sifatnya spesifik. Meskipun tidak dapat dipungkiri bahwa PP PSTE 2019 telah "memperbaiki" definisi data pribadi, namun apabila dilihat dari perspektif perundang-undangan, ketentuan dalam PP PSTE 2019 justru inkonsisten dengan UU Adminduk yang memiliki kedudukan lebih tinggi dalam hierarki peraturan perundang-undangan di Indonesia.

Lebih lanjut, apabila mencermati Tabel 1 di atas, terdapat perubahan jenis data pribadi yang dilindungi oleh UU Adminduk. Apabila menggunakan kategorisasi dalam GDPR atau *Personal Data Protection Act 2010* di Malaysia, maka data pribadi yang dilindungi dalam perubahan UU Adminduk 2013 merupakan data yang masuk klasifikasi data pribadi spesifik/sensitif. Meskipun demikian, apabila melihat definisi data pribadi dalam UU Adminduk, maka pengaturan data pribadi justru menunjukkan ketidaksesuaian dengan definisi data pribadi dalam UU *a quo*.

Adapun mekanisme perlindungan data pribadi penduduk secara lebih detail diatur dalam PP No. 40 Tahun 2019 tentang Pelaksanaan UU No. 23 Tahun 2006 tentang Administrasi Kependudukan Sebagaimana Telah Diubah dengan UU No. 24 Tahun 2013 tentang Perubahan atas UU No. 23 Tahun 2006 tentang Administrasi Kependudukan. Namun demikian, pengaturan perlindungan data pribadi penduduk hanya ditujukan pada data pribadi yang harus dilindungi sebagaimana diatur dalam Pasal 84 UU Adminduk.[89] Bentuk perlindungan yang diatur dalam PP *a quo* meliputi perlindungan pada hak akses dan kerahasiaan data.[90] Ketentuan perlindungan data pribadi dalam PP ini dapat dikatakan tidak tuntas karena Pasal 57 PP *a quo* masih memberikan delegasi pengaturan pada level Peraturan Menteri.

Dengan mencermati ketentuan dalam berbagai UU di atas, terlihat bahwa secara umum pengaturan terkait data pribadi cukup bervariasi dan sporadis. Apabila dilihat dari beberapa prasyarat dalam perlindungan privasi dan data pribadi di atas, maka poin yang diatur dalam sebagian besar UU di atas hanya berkaitan dengan persetujuan subyek data (khususnya dalam kaitan dengan pengungkapan data). Poin lain seperti anonimisasi data dan notifikasi pelanggaran data justru tidak diatur.

Dalam konteks kerangka pengaturan yang ada saat ini, ketentuan detail mengenai perlindungan data pribadi baru dapat ditemukan pada level peraturan pelaksanaan dari UU, antara lain PP PSTE 2019 dan Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo PDPSE). Dalam PP PSTE 2019 misalnya, diatur kewajiban Penyelenggara Sistem Elektronik[91] untuk melaksanakan prinsip perlindungan data pribadi dalam pemrosesan data pribadi yang dipegang.[92] Adapun pemrosesan tersebut meliputi tahap perolehan pengumpulan sampai dengan tahap penghapusan atau pemusnahan.[93] Ketentuan mengenai persetujuan dari subyek data dalam pemrosesan data dan pemberitahuan apabila terjadi kegagalan dalam perlindungan data pribadi

89. Lihat Pasal 54 ayat (2) Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan 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.

90. Setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. Lihat Pasal 1 angka 4 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

91. Lihat Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

92. Lihat Pasal 14 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

93. Lihat Pasal 14 ayat (3) sampai dengan ayat (5) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

dapat ditemukan pula dalam PP *a quo*.[94] Sedangkan, untuk anonimisasi data dan pengiriman data dari wilayah Indonesia ke luar wilayah Indonesia dapat ditemukan pada Permenkominfo PDPSE.[95]

Dari pembahasan di atas, dapat terlihat bagaimana gambaran mengenai kerangka hukum perlindungan data pribadi, terutama dalam konteks penyelenggaraan SPBE. Pada level UU, dapat dilihat bahwa ketentuan mengenai data pribadi diatur secara sporadis dan bervariasi dengan tingkat pengaturan yang beragam. Secara garis besar, pengaturan masih cukup umum, bahkan ada yang cukup minim. Namun demikian, dalam konteks ketentuan teknis, dapat dikatakan Indonesia sudah memiliki aturan yang bisa dijadikan sebagai pedoman perlindungan data pribadi dalam penyelenggaraan SPBE, yakni PP PSTE 2019 dan Permenkominfo PDPSE. Meskipun, definisi data pribadi dalam PP dan Permenkominfo *a quo* menunjukkan inkonsistensi dengan definisi dalam UU Adminduk sebagaimana dipaparkan sebelumnya.

Berdasarkan penjelasan di atas, bagian selanjutnya memaparkan mengenai hal-hal yang perlu diperhatikan dan dipertimbangkan untuk dapat memperkuat upaya perlindungan data pribadi, utamanya dalam penyelenggaraan SPBE. Sehingga, kepentingan Negara dan kepentingan warga negara (individu) dapat diakomodasi dengan baik.

2. Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan SPBE: Mau dibawa ke mana?

Berdasarkan penjelasan pada bagian sebelumnya, dapat dilihat sejatinya bahwa pengaturan mengenai data pribadi pada level UU masih sporadis dengan substansi pengaturan yang beragam. Hadirnya banyak UU yang mengatur mengenai data pribadi sejatinya juga memiliki potensi yang besar menimbulkan inkonsistensi pengaturan. Lebih lanjut, dengan adanya dua definisi data pribadi yang berlaku – yakni dalam UU Adminduk dan PP PSTE 2019, ada potensi juga menimbulkan kebingungan dalam penerapannya. Meskipun apabila dilihat dari hierarki peraturan perundang-undangan, maka seharusnya definisi UU Adminduk-lah yang digunakan. Namun demikian, PP PSTE 2019 sebagai pengaturan yang bersifat teknis memiliki definisinya sendiri yang digunakan sebagai dasar dalam pengaturan perlindungan data pribadi, terutama dalam Sistem Elektronik. Selain itu, Permenkominfo PDPSE yang seharusnya menjadi pelaksana dari PP PSTE menggunakan definisi data pribadi sesuai dengan ketentuan dalam UU Adminduk. Hal tersebut sejatinya merupakan konsekuensi logis mengingat Permenkominfo PDPSE merupakan pelaksana dari PP PSTE 2012 yang pada waktu itu juga menggunakan definisi data pribadi seperti yang diatur dalam UU Adminduk. Meskipun masalah definisi kerap dianggap sepele, namun pendefinisian suatu nomenklatur dalam peraturan memegang peranan yang vital karena menentukan maksud dari berbagai materi muatan yang diatur dalam peraturan tersebut. Adanya perbedaan definisi berpotensi besar untuk membuat perbedaan arah pengaturan dan pelaksanaan dari suatu peraturan.

Dengan mendasarkan berbagai pemaparan sebelumnya, setidaknya terdapat langkah-langkah hukum yang dapat dilakukan untuk dapat meningkatkan upaya perlindungan data pribadi dalam penyelenggaraan SPBE di Indonesia. Pertama, RUU Perlindungan Data Pribadi harus didorong untuk segera disahkan. Sebagaimana diketahui, saat ini RUU Perlindungan Data Pribadi merupakan salah satu RUU yang sudah masuk tahap pembahasan. Kehadiran suatu UU yang khusus mengatur perlindungan data pribadi dapat meminimalisir dan menghilangkan gap pengaturan yang ada pada berbagai UU yang ada saat ini. Selain itu, tidak dapat dipungkiri bahwa pada akhirnya suatu sistem atau teknologi yang dibangun harus tunduk pada

94. Lihat Pasal 15 dan Pasal 22 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Khusus terkait dengan anonimisasi data, dalam Permenkominfo *a quo* menyatakan bahwa data pribadi yang disimpan dalam Sistem Elektronik harus merupakan data yang terenkripsi.
95. Lihat misalnya Nik Thompson, Antony Mullins, dan Thanavit Chongsutakawewong. 2020. Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly* Volume 37, hlm. 6.

ketentuan hukum yang berlaku di suatu negara.[96] Dengan demikian, kehadiran UU yang mengatur perlindungan data pribadi dapat menjadi satu payung hukum yang jelas dan kuat, terutama dalam kerangka perlindungan hak atas privasi dan data pribadi. Hal ini tentunya akan mendukung upaya perlindungan data pribadi dalam konteks penyelenggaraan SPBE. Jika dibandingkan dengan beberapa Negara yang tidak punya pengaturan spesifik mengenai *e-Government*, kehadiran UU spesifik mengenai perlindungan data pribadi menjadi salah satu kebutuhan penting dalam penyelenggaraan *e-Government*.[97]

Kedua, redefinisi data pribadi. Masih terkait dengan RUU Perlindungan Data Pribadi, definisi data pribadi memegang peranan penting untuk menentukan arah pengaturan dan penerapan upaya perlindungan data pribadi, apalagi dalam penyelenggaraan SPBE. Dengan melihat berbagai definisi data pribadi yang telah dianalisis sebelumnya, maka definisi data pribadi dapat dirumuskan dengan mengacu pada PP PSTE 2019 yang mendefinisikan data pribadi sebagai "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."[98] Definisi tersebut setidaknya sudah dapat menunjukkan ruang lingkup data (semua data) dan sifat data (bisa digunakan untuk mengidentifikasi secara langsung maupun tidak langsung.

Ketiga, perlunya klasifikasi data pribadi. Sebagaimana halnya Korea Selatan, Malaysia, Singapura, dan EU yang mengatur data pribadi yang bersifat khusus atau sensitif,[99] adanya klasifikasi data menjadi hal yang dapat dipertimbangkan dalam penyelenggaraan upaya perlindungan data pribadi. Meskipun pada prinsipnya semua data pribadi perlu dilindungi, namun klasifikasi data pribadi sekiranya diperlukan dalam konteks pemrosesan terhadap data pribadi, apalagi yang dipegang oleh instansi pemerintah atau Negara. Sebagai contoh, data kesehatan tentu harus diproses secara berbeda dengan data kependudukan atau data perbankan. Bahkan, dalam konteks Indonesia saja, terdapat jenis data kependudukan yang sifatnya khusus seperti data genetik atau biometrik, yang apabila dikomparasikan dengan pengaturan dalam GDPR masuk dalam kategori khusus. Dalam konteks data kesehatan juga, pengaturan dalam GDPR, *Personal Data Protection Act2010* Malaysia dan *Personal Data Protection Act 2012* Singapura mengklasifikasikan data terkait kesehatan sebagai data pribadi yang bersifat khusus.

Keempat, pembatasan akses data pribadi tertentu. Sebagaimana tertuang dalam Rencana Induk SPBE, salah satu upaya percepatan implementasi SPBE dilakukan dengan mengutamakan prinsip keamanan dan interoperabilitas, yang antara lain melalui penerapan prinsip penggunaan fasilitas bersama untuk pusat data, jaringan komunikasi pemerintah dan aplikasi umum, serta memastikan keamanan, kerahasiaan, keterkinian, akurasi, serta keutuhan data dan informasi dalam pelaksanaan SPBE.[100] Interoprabilitas sendiri secara umum merupakan kemampuan sistem elektronik dengan karakteristik yang berbeda untuk berbagi pakai data secara terintegrasi.[101] Dengan melihat arah penerapan SPBE yang salah satunya dilakukan melalui bagi pakai data, maka pembatasan akses bagi pakai terhadap data pribadi tertentu menjadi penting.

96. Sebagai contoh, dapat dilihat dari beberapa negara yang menempati urutan tertinggi dalam EGDI 2020, misalnya UK (peringkat 7) yang memiliki *Data Protection Act 2018*, Singapura (peringkat 12) dengan *Personal Data Protection Act 2012*, Jepang (peringkat 14) dengan *Act on the Protection of Personal Information*. Bahkan Swedia (peringkat 6) sudah memiliki *Personal Data Act* sejak tahun 1998.

97. Pasal 1 angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

98. Lihat Pasal 4 *Personal Data Protection Act 2010 (Act 709)* (Malaysia); Pasal 23 *Personal Information Protection Act (2011)* (Korea Selatan); Pasal 23 *Personal Data Protection Act 2012 (No. 26 of 2012)*(Singapura); Pasal 9 Regulation (EU) 2016/679 (General Data Protection Regulation) (European Union).

99. Lihat Rencana Induk Sistem Pemerintahan Berbasis Elektronik Nasional, 19. Dalam Lampiran Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

100. Lihat Andi Nugroho. Draf Aturan Interoperabilitas Data Dirilis, Kominfo Minta Masukan Publik hingga 30 Juni. *Cyberthreat*. 12 Juni 2020. Diakses tanggal 30 Agustus 2020. https://cyberthreat.id/read/7079/Draf-Aturan-Interoperabilitas-Data-Dirilis-Kominfo-Minta-Masukan-Publik-hingga-30-Juni.

101. Lihat Article 25(1) *Regulation (EU) 2016/679 (General Data Protection Principles)*.

Kelima, penerapan prinsip-prinsip *Data Protection by Design* dan *by Default*. Prinsip ini sejatinya mengadopsi prinsip-prinsip *Privacy by Design* yang ada sebelumnya. Dalam GDPR, *Data Protection by Design* dimaksudkan bahwa organisasi atau instansi sejak tahap paling awal mendesain pemrosesan data dan pada saat pemrosesan tersebut dilakukan, harus menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk dapat mengintegrasikan pengamanan yang diperlukan dalam pemrosesan data untuk memenuhi persyaratan yang diatur dan melindungi hak dari subyek data.[102] Sedangkan *Data Protection by Default* dimaksudkan bahwa organisasi atau instansi harus memastikan data pribadi diproses dengan perlindungan privasi yang tertinggi, sehingga secara *default* data pribadi hanya dapat diakses dengan tujuan tertentu dan tidak dapat diakses oleh sembarang orang.[103] Dengan demikian, poin penting yang juga perlu diakomodasi adalah pengaturan mengenai hak-hak subyek data juga harus diperjelas.

Keenam, meningkatkan standar keamanan data dan implementasi keamanan informasi. Apabila merujuk pada ketentuan yang berlaku, maka aturan teknis mengenai keamanan informasi dapat ditemukan dalam Permenkominfo No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Keamanan informasi sendiri didefinisikan sebagai terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.[104] Dalam aspek ini, hal yang tentu perlu diperhatikan adalah memastikan bahwa instansi pemerintahan dan Negara benar-benar menerapkan standar keamanan informasi dalam pemrosesan data pribadi masyarakat.

C. Penutup

C.1. Kesimpulan

Terdapat dua kesimpulan yang diambil berdasarkan seluruh pembahasan di atas. **Pertama**, dalam kaitannya dengan persinggungan antara kepentingan individu dan Negara dalam pemanfaatan data pribadi dalam penyelenggaraan SPBE. Individu, di satu sisi memiliki kepentingan terhadap privasi dan keamanan atas data pribadi yang dipegang oleh instansi pemerintahan atau Negara, sehingga tidak disalahgunakan. Negara, di sisi lain perlu menggunakan data pribadi masyarakat untuk dapat meningkatkan pelayanan administrasi dan publik yang diberikan, sehingga dapat memenuhi kebutuhan masyarakat. Selain itu, adanya kebutuhan atas keterbukaan informasi perlu dibarengi dengan perlindungan terhadap privasi masyarakatnya. Maka dari itu, kedua kepentingan tersebut penting untuk diakomodasi dalam kerangka hukum perlindungan data pribadi dalam penyelenggaraan SPBE.

Kedua, terkait dengan dinamika kerangka hukum perlindungan data pribadi dalam kaitannya dengan penyelenggaraan SPBE, dari hasil penelusuran dan analisis yang dilakukan terhadap berbagai UU yang mengatur mengenai data pribadi, dapat dilihat bahwa ketentuan dalam berbagai UU masih cukup umum dengan tingkat pengaturan yang bervariasi. Berbagai UU yang dianalisis secara umum hanya mengatur mengenai perlunya persetujuan subyek data dalam pengungkapan data dan sanksi apabila terjadi pelanggaran data. Adanya persetujuan ini merupakan hal yang signifikan dalam konteks perlindungan data pribadi, mengingat pemroses atau pengontrol data pada prinsipnya hanya dapat menggunakan data pribadi dari subyek data atas persetujuannya. Lebih lanjut, ketentuan teknis lain seperti anonimisasi data, notifikasi pelanggaran data, dan pengiriman data antar negara baru diatur pada level peraturan pelaksanaan seperti dalam PP dan Peraturan Menteri.

102. Lihat Article 25(2) *Regulation (EU) 2016/679 (General Data Protection Principles)*.
103. Pasal 1 angka 6 Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.
104. Leon Trakman, Robert Walters, dan Bruno Zeller. 2020. Digital consent and data protection law – Europe and Asia-Pacific experience. *Information & Communications Technology Law* Volume 29 Nomor 2, hlm. 248.

Dalam kaitannya dengan definisi data pribadi sendiri, terdapat adanya inkonsistensi pengaturan antara UU dengan peraturan yang lebih teknis. Hal tersebut menimbulkan potensi permasalahan, terutama dalam konteks implementasi peraturan perundang-undangan. Adanya kemungkinan untuk "memilih" definisi yang menguntungkan pihak tertentu menjadi hal yang perlu dihindari untuk menjamin adanya kepastian hukum. Dengan mempertimbangkan kondisi pengaturan yang ada saat ini, penting rasanya kehadiran suatu UU tersendiri sebagai dasar yang kuat dalam upaya perlindungan data pribadi, apalagi dalam konteks penyelenggaraan SPBE di Indonesia.

C.2. Saran

Untuk dapat meningkatkan upaya perlindungan data pribadi dalam penyelenggaraan SPBE, sebagaimana telah disebutkan sebelumnya, maka RUU PDP yang saat ini sudah masuk tahap pembahasan perlu didorong untuk segera disahkan sebagai payung hukum pelaksanaan perlindungan data pribadi, terutama dalam penyelenggaraan SPBE. Termasuk di dalamnya perlu diberikan kejelasan mengenai definisi data pribadi, klasifikasi data pribadi, serta akomodasi terhadap prinsip-prinsip perlindungan data pribadi sebagai landasan pelaksanaan perlindungan data pribadi yang menjunjung tinggi hak privasi masyarakat. Selain itu, pembatasan akses terhadap data pribadi yang bersifat spesifik atau sensitif juga perlu untuk dirumuskan dengan matang agar bisa mendukung penerapan interoperabilitas data dan informasi yang tidak melanggar privasi. Hal terakhir yang tidak kalah penting adalah perlunya memastikan bahwa semua instansi pemerintahan dan Negara menerapkan dan meningkatkan standar keamanan atas data dan informasi yang dipegang, sehingga dapat meminimalisir dampak yang timbul atas ancaman atau serangan siber terhadap data dan informasi.

Daftar Pustaka

Buku

European Parliament. 2015. *eGovernment: Using technology to improve public services and democratic participations.* European Union.

Institute for Criminal Justice Reform. Anggara, Supriyadi Widodo Eddyono, dan Wahyudi Djafar, *Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia* (Jakarta: Institute for Criminal Justice Reform, 2015).

International Telecommunication Union, *Global Cybersecurity Index 2018* (Switzerland: ITU Publication, 2018).

Marzuki, Peter Mahmud, *Penelitian Hukum: Edisi Revisi* (Jakarta: Kencana, 2005).

Organisation for Economic Co-operation and Development, *The E-Government Imperative* (Paris: Organisation for Economic Co-operation and Development, 2003).

Organisation for Economi Cooperation and Development, *Recomendation of the Council on Digital Government Strategies* (Paris: OECD Publishing, 2014).

Soekanto, Soerjono, *Pengantar Penelitian Hukum* (Jakarta: UI Press, 2007).

Soekanto, Soerjono, dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Rajawali Press, 2015).

United Nations, *UN Global E-Government Survei 2003* (New York: United Nations, 2003).

United Nations, *United Nations E-Government Survei* 2018, (New York: United Nations, 2018).

United Nations, *E-Government Survei 2020: Digital Government in the Decade of Action for Sustainable Development* (New York: United Nations, 2020).

Walters, Robert, Leon Trakman, dan Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (Sinapura: Springer, 2019).

Westin, Allan F., dan Michael A. Baker, *Databanks in a Free Society: Computers, Record-keeping and Privacy* (New York: The New York Times Book, 1972).

World Economic Forum, *Personal Data: The Emergence of a New Aset Class – Opportunities for the Telecomunications Industry* (World Economic Forum, 2011).

Falk, Svenja; Andrea Rommele, dan Michael Silverman, "The Promise of Digital Government" dalam Svenja Falk, et al (eds), *Digital Government: Leveraging Innovation to Improve Public Sector Performance and Outcomes for Citizens* (Switzerland: Springer Internasional Publishing, 2017).

Sloot, Bart van der, "Legal Fundamentalism: Is Data Protection Really a Fundamental Right?" dalam Ronald Leenes, *et al* (Editor), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Switzerland: Springer Internasional Publishing, 2017).

Jurnal

Agostino, Deborah; Michela Arnaboldi, dan Melisa Diaz Lema, "New development: COVID-19 as an accelerator of digital transformation in public service delivery", *Public Money & Management* 51(1) (2021).

Chik, Warren B., "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy", *Computer Law and Security Review* 5 (2013).

Jain, Priyank; Manasi Gyanchandani; dan Nilay Khare, "Big data privacy: a technological perspective and review", *Journal of Big Data* 3(25) (2016).

Sharma, Gagan Deep; Anshita Yadav, dan Ritika Chopra, "Artificial intelligence and effective governance: A review, critique and research agenda", Sustainable Futures 2 (2020).

Silcock, Rachel, "What Is *e-Government*." *Parliamentary Government* 54 (2001).

Sloot, Bart van der, "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation", *Internasional Data Privacy Law* 4 Issue 3 (November 2014).

Thompson, Nik; Antony Mullins; dan Thanavit Chongsutakawewong, "Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand", *Government Information Quarterly* 37 (2020).

Trakman, Leon; Robert Walters; dan Bruno Zeller, "Digital consent and data protection law – Europe and Asia-Pacific experience", *Information & Communications Technology Law* 29(2) (2020).

Internet

Ayuwuragil, Kustin, "Kominfo Akui 'Pencurian' NIK dan KK Saat Registrasi Kartu SIM", *CNN Indonesia*, 6 April 2018, https://www.cnnindonesia.com/teknologi/20180305204703-213-280691/kominfo-akui-pencurian-nik-dan-kk-saat-registrasi-kartu-sim.

CNN Indonesia, "Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank", *CNN Indonesia*, 6 Februari 2020, https://www.cnnindonesia.com/nasional/20200205211241-12-472073/pembobolan-rekening-ilham-bintang-data-dijual-orang-bank.

CNN Indonesia, "Data Covid-19 Warga RI Bocor, NIK hingga Hasil Rapid Test", *CNN Indonesia*, 19 Juni 2020, https://www.cnnindonesia.com/teknologi/20200619212544-185-515376/data-covid-19-warga-ri-bocor-nik-hingga-hasil-rapid-test.

Dewan Perwakilan Rakyat, "Program Legislasi Nasional Prioritas", *Dewan Perwakilan Rakyat*, http://www.dpr.go.id/uu/prolegnas.

Groot, Juliana De, "What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019, *Digital Guardian*, 5 Agustus 2020, https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

Kompas.com, "Hacker Klaim Miliki Data Hasil Tes Pasien Covid-19 di Indonesia", *Kompas*, https://tekno.kompas.com/read/2020/06/20/07592607/hacker-klaim-miliki-data-hasil-tes-pasien-covid-19-di-indonesia, 20 Juni 2020.

Kompas.com, "Penjelasan KPU soal Dugaan Kebocoran Data Kependudukan di DPT Pemilu", *Kompas*, 22 Mei 2020, https://nasional.kompas.com/read/2020/05/22/09063931/penjelasan-kpu-soal-dugaan-kebocoran-data-kependudukan-di-dpt-pemilu.

Mufarida, Binti, "Data Pasien Covid-19 Bocor, Bukti Lemahnya Perlindungan Data Pribadi", *Sindo News*, 21 Juni 2020, https://nasional.sindonews.com/read/76844/15/data-pasien-covid-19-bocor-bukti-lemahnya-perlindungan-data-pribadi-1592741202.

Nugroho, Andi. "Draf Aturan Interoperabilitas Data Dirilis, Kominfo Minta Masukan Publik hingga 30 Juni", *Cyberthreat.id*, 12 Juni 2020, https://cyberthreat.id/read/7079/Draf-Aturan-Interoperabilitas-Data-Dirilis-Kominfo-Minta-Masukan-Publik-hingga-30-Juni.

Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens (July, 1973)", https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

Setiawan, Riyan, "KPU Membenarkan 2,3 Juta Data yang Bocor Merupakan DPT Tahun 2014", *Tirto*, 22 Mei 2020, https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B.

Makalah

Djafar, Wahyudi, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan", *Seminar Hukum dalam Era Analisis Big Data,* Program Pasca Sarjana Fakultas Hukum UGM, 26 Agustus 2019.

Peraturan Perundang-undangan

Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*.

Peraturan Dewan Komisioner Otoritas Jasa Keuangan Nomor 01/17/PDK/XII/2012 tentang Kode Etik Otoritas Jasa Keuangan.

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

Peraturan Pemerintah Nomor 40 Tahun 2019 tentang Pelaksanaan 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.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran.

Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

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

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah.

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan..

Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan.

Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit..

Undang-Undang No. 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan..

Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara.

Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan.

Undang-Undang Nomor 38 Tahun 2014 tentang Keperawatan.

Undang-Undang Nomor 11 Tahun 2016 tentang Pengampunan Pajak.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Ketentuan Hukum Internasional

Act on the Protection of Personal Information (Act No. 57 of May 30, 2003) (Jepang, 2003).

Charter of Fundamental Rights of the European Union (2012/C 326/02).

Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

International Covenant on Civil and Political Rights, entry into force 23 March 1976.

Personal Data Protection Act 2010 (Act 709) (Malaysia, 2010).

Personal Data Protection Act 2012 (No. 26 of 2012) (Singapura, 2012).

Personal Information Protection Act (2011) (Korea Selatan, 2011).

Regulation (EU) 2016/679 (General Data Protection Principles).