BAB III

IMPLIKASI PEMROSESAN DATA PRIBADI TERHADAP KORPORASI PENYELENGGARA SISTEM ELEKTRONIK (PSE) BERDASARKAN UU PDP

Pada bab sebelumnya, pembahasan difokuskan terkait dengan perbandingan regulasi perlindungan data pribadi sebelum dan sesudah berlakunya UU PDP dalam hal pemrosesan data pribadi. Sementara itu, bab ini membahas secara spesifik dan mendalam terkait dengan ketentuan pemrosesan data pribadi dengan lingkup pembahasan atau analisisnya hanya terfokus pada seluruh ketentuan yang ada dalam UU PDP.

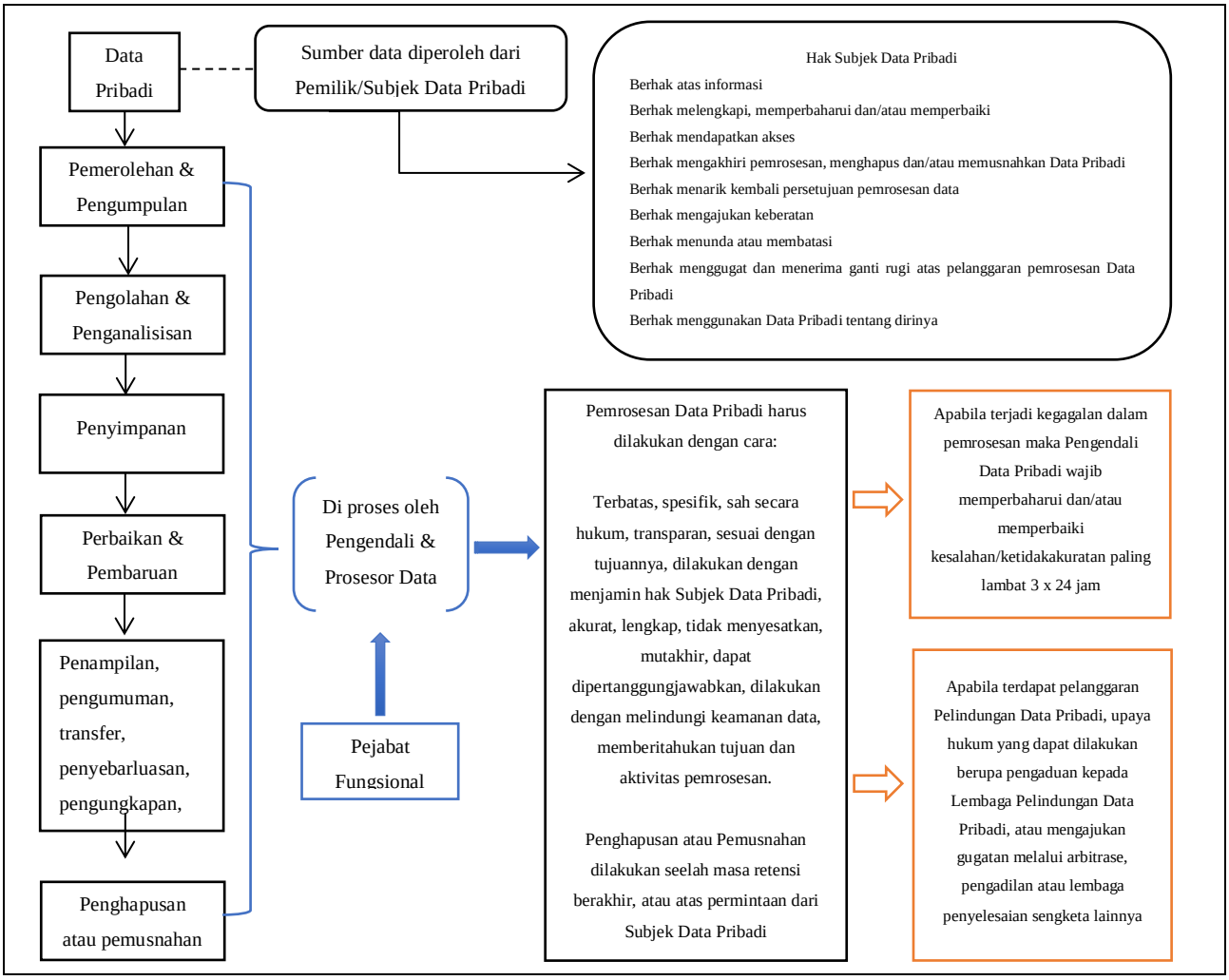
Selain hal tersebut, dalam bab ini juga terdapat analisis implikasi pemrosesan data pribadi terhadap Korporasi PSE lingkup privat, dengan menggunakan teknik analisis yang disebut *Regulatory Impact Assessment* (RIA). Keterkaitan dengan Korporasi PSE lingkup privat, karena korporasi ini dalam menjalankan kegiatan bisnisnya yang secara digital tidak terlepas dari pemrosesan data pribadi pelanggan.

III.1 Pemrosesan Data Pribadi

Berdasarkan Pasal 16 ayat (1) UU PDP Pemrosesan Data Pribadi dilakukan melalui beberapa tahapan yakni:

1. Pemerolehan dan pengumpulan;
2. Pengolahan dan penganalisisan;
3. Penyimpanan;
4. Perbaikan dan pembaruan;
5. Penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, dan/atau
6. Penghapusan atau pemusnahan.

Tabel III.1 Bagan Pemrosesan Data Pribadi Berdasarkan UU PDP



Tabel III.1 menggambarkan bahwa siklus pemrosesan Data Pribadi berdasarkan UU PDP, diawali dengan pengumpulan data yang diperoleh dari Subjek Data Pribadi, kemudian diproses oleh Pengendali Data Pribadi yang dibantu oleh Prosesor Data Pribadi. Pasal 19 UU PDP menyebutkan bahwa Setiap Orang, Badan Publik, dan Organisasi Internasional dapat menjadi Pengendali dan Prosesor Data Pribadi.

Pasal 20 ayat (1) UU PDP menyebutkan bahwa untuk melakukan pemrosesan Data Pribadi Pengendali Data Pribadi wajib memiliki dasar. Pasal 20 ayat (2) UU PDP menyebutkan dasar dari pemrosesan Data Pribadi berupa persetujuan yang sah secara eksplisit dari Subjek Data Pribadi,

pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian, pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan, pemenuhan pelindungan kepentingan vital Subjek Data Pribadi, pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi.

Dalam persetujuan yang dilakukan antara Subjek Data Pribadi dengan Pengendali Data Pribadi wajib menyampaikan informasi mengenai legalitas dari pemrosesan data pribadi; tujuan pemrosesan data pribadi; jenis dan relevansi data pribadi yang akan diproses; jangka waktu retensi dokumen yang memuat data pribadi; rincian mengenai informasi yang jangka waktu pemrosesan data pribadi; dan hak Subjek Data Pribadi. Dan apabila ada perubahan maka Pengendali Data Pribadi wajib memberitahukan hal tersebut kepada Subjek Data Pribadi sebelum terjadinya perubahan tersebut. Sesuai dengan Pasal 22 ayat (1) UU PDP pemrosesan ini dilakukan atas persetujuan Subjek Data sebelumnya tanpa adanya persetujuan yang tertulis maka data yang bersangkutan tidak boleh dilakukan pemrosesan apapun.

Pasal 23 UU PDP menyatakan apabila dalam tidak memuat persetujuan yang sah secara eksplisit dari Subjek Data Pribadi maka perjanjian pemrosesan Data Pribadi dinyatakan batal demi hukum. Pengendali Data Pribadi juga wajib menunjukan bukti persetujuan yang telah diberikan oleh Subjek Data Pribadi. Terdapat ketentuan khusus pada Pasal 25 dan Pasal 26 UU PDP apabila pemrosesan Data Pribadi terkait dengan data anak dan penyandang disabilitas maka

diselenggarakan secara khusus, dan wajib atas persetujuan orang tua atau wali serta persetujuan dari penyandang disabilitas atau wali darinya.

Dalam pemrosesan Data Pribadi Pengendali Data Pribadi wajib melakukan perekaman terhadap seluruh kegiatan tersebut dan memberikan akses kepada Subjek Data Pribadi terhadap rekam jejak itu paling lambat 3 x 24 jam terhitung sejak Pengendali Data Pribadi menerima Permintaan akses. Akan tetapi, pada Pasal 33 UU PDP Pengendali Data Pribadi dapat menolak untuk memberikan akses kepada Subjek Data Pribadi dalam hal membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/atau orang lain, berdampak pada pengungkapan Data Pribadi milik orang lain, dan/atau bertentangan dengan kepentingan pertahanan dan keamanan nasional.

Dalam UU PDP juga memuat konsep *Data Protection Impact Assessment* (DPIA) terkait dengan pemrosesan Data Pribadi. DPIA adalah sebuah konsep yang berasal dari ketentuan di dalam GDPR yang merupakan proses untuk merancang dan menggambarkan pemrosesan, menilai kebutuhan dan proporsionalitasnya, serta membantu mengelola risiko terhadap hak dan kebebasan orang perseorangan akibat pemrosesan data pribadi dengan menilai dan menentukan langkah langkah untuk mengatasinya. DPIA penting sebagai alat akuntabilitas, karena membantu Pengendali data pribadi tidak hanya untuk mematuhi persyaratan GDPR, tetapi juga untuk menunjukkan bahwa langkah-langkah yang tepat telah diambil untuk memastikan kepatuhan terhadap Peraturan pelindungan data pribadi[49].

[49] Directorate Fundamental Rights and Union Citizenship, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679" (Belgium: The European Commission, Directorate General Justice, 2017). hlm 4.

Hal tersebut tercantum dalam ketentuan Pasal 34 UU PDP yakni melakukan penilaian dampak Pelindungan Dat Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi. Pasal 34 ayat (2) UU PDP resiko tinggi yang dimaksud meliputi pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi, pemrosesan atas Data Pribadi yang bersifat spesifik; pemrosesan Data Pribadi dalam skala besar, pemrosesan Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi, pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data, penggunaan teknologi baru dalam pemrosesan Data Pribadi, dan/atau pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi. Akan tetapi ketentuan mengenai DPIA ini tidak dicantumkan secara spesifik di dalam UU PDP dan perlu dibuatkan peraturan pedoman.

Berdasarkan Pasal 36 hingga Pasal 45 UU PDP dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi memiliki kewajiban lainnya, seperti:

a. menjaga kerahasiaan Data Pribadi;
b. melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi di bawah kendali Pengendali Data Pribadi;
c. melindungi Data Pribadi dari pemrosesan yang tidak sah;
d. mencegah Data Pribadi diakses secara tidak sah;
e. menghentikan pemrosesan Data Pribadi dalam hal Subjek Data Pribadi menarik kembali persetujuan pemrosesan Data Pribadi;
f. melakukan penundaan dan pembatasan pemrosesan Data Fribadi baik sebagian maupun seluruhnya paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan penundaan dan pembatasan pemrosesan Data Pribadi;

g. memberitahukan telah dilaksanakan penundaan dan pembatasan pemrosesan Data Pribadi kepada Subjek Data Pribadi;
h. mengakhiri pemrosesan data pribadi dalam hal telah mencapai masa retensi, tujuan pemrosesan Data Pribadi telah tercapai atau terdapat permintaan dari Subjek Data Pribadi;
i. menghapus Data Pribadi dalam hal: Data Pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi, Subjek Data Pribadi telah melakukan penarikan kembali persetujuan pemrosesan Data Pribadi, terdapat permintaan dari Subjek Data Pribadi; atau, Data Pribadi diperoleh dan/atau diproses dengan cara melawan hukum;
j. memusnahkan Data Pribadi dalam hal: telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip, terdapat permintaan dari Subjek Data Pribadi, tidak berkaitan dengan penyelesaian proses hukum suatu perkara, dan/atau, Data Pribadi diperoleh dan/atau diproses dengan cara melawan hukum, dan
k. memberitahukan kepada Subjek Data Pribadi mengenai penghapusan dan/atau pemusnahan Data Pribadi.

Kewajiban Prosesor Data Pribadi dalam pemrosesan data pribadi sama dengan Pengendali Data Pribadi hanya saja Prosesor Data Pribadi bekerja dibawah perintah dari Pengendali Data Pribadi hal ini sesuai dengan ketentuan yang ada di dalam Pasal 51 dan 52 UU PDP.

Untuk benar-benar menjaga pelindungan privasi dari Data Pribadi Subjek yang bersangkutan memiliki sejumlah hak yang telah dijamin di dalam Pasal 5 sampai Pasal 13 UU PDP seperti hak atas informasi, hak melengkapi, memperbaharui dan/atau memperbaiki, hak mendapatkan akses, hak mengakhiri pemrosesan, menghapus dan/atau memusnahkan Data Pribadi, hak menarik kembali persetujuan pemrosesan data, hak mengajukan keberatan, hak menunda atau membatasi, hak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan

Data Pribadi, dan hak menggunakan Data Pribadi tentang dirinya. Hal tersebut menunjukan bahwa dalam UU PDP, subjek pribadi memiliki hak kontrol atas data dirinya, sesuai dengan teori privasi akses yang dipopulerkan oleh James Moor yang menempatkan fokus pada apa yang harus dipertimbangkan saat mengembangkan kebijakan untuk melindungi privasi, dalam menetapkan kebijakan untuk memberi individu sebanyak mungkin kontrol (*informed consent*) atas data pribadi secara realistis. orang yang berbeda diberikan tingkat akses yang berbeda untuk berbagai jenis informasi pada waktu yang berbeda.

UU PDP juga memuat Prinsip Publisitas (*The Publicity Principle*) secara implisit sesuai yang disampaikan pada teori privasi akses yakni berupa aturan atau ketentuan yang mengatur situasi Subjek Data Pribadi harus jelas. Hal ini bertujuan agar Subjek Data Pribadi dapat merencanakan untuk melindungi privasi dengan lebih baik jika yang bersangkutan mengetahui di mana zona privasi berada dan dalam kondisi apa dan kepada siapa informasi akan diberikan. Subjek Data Pribadi perlu diberikan pemahaman agar mengetahui data pribadi yang diberikan akan digunakan untuk apa, kepada siapa dan dampaknya apa terhadap dirinya, sehingga dirinya menjadi individu yang dapat mengontrol sebanyak mungkin data pribadi yang berkaitan dengannya. Ketentuan ini terdapat dalam Pasal 21 ayat (1) UU PDP yang mana dalam melakukan pemrosesan Data Pribadi perlu adanya persetujuan dari Subjek Data Pribadi dan Pengendali Data Pribadi perlu menginformasikan legalitas dari pemrosesan Data Pribadi; tujuan pemrosesan Data Pribadi; jenis dan relevansi Data Pribadi yang akan diproses; jangka waktu retensi dokumen yang memuat Data Pribadi; rincian mengenai Informasi yang jangka waktu pemrosesan Data Pribadi; dan hak Subjek Data Pribadi kepada Subjek Data Pribadi.

Dalam teori akses privasi terdapat Prinsip pengecualian (*The Justification of Exceptions Principle*) yang berarti bahwa pelanggaran terhadap Data Pribadi dibenarkan jika dan hanya ada

kemungkinan besar bahwa kerugian yang disebabkan oleh pengungkapan akan jauh lebih sedikit daripada kerugian yang dicegah oleh orang yang tidak memihak dalam mengizinkan pelanggaran. Hal ini termuat dalam Pasal 15 ayat (1) UU PDP Pelindungan Data Pribadi dikecualikan untuk tujuan kepentingan pertahanan dan keamanan nasional, kepentingan proses penegakan hukum, kepentingan umum dalam rangka penyelenggaraan negara, kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara atau kepentingan statistik, dan penelitian ilmiah.

Akan tetapi UU PDP tidak memuat Prinsip Penyesuaian padahal di dalam Teori akses privasi ketentuan Prinsip Pengecualian tersebut tidak dibarengi dengan Prinsip Penyesuaian (*The Adjustment Principle*), padahal ketentuan pengecualian diperlukan Prinsip Pengungkapan dan penyesuaian dalam pernyataan kebijakan itu sendiri. Jika keadaan khusus membenarkan pelanggaran data pribadi, maka perubahan itu harus menjadi bagian eksplisit dan publik dari aturan dan kondisi yang mengatur hal tersebut.

Selama melakukan tugasnya dalam pemrosesan data pribadi Pengendali dan Prosesor Data Pribadi diawasi oleh Pejabat Fungsional yang tugasnya sesuai dengan Pasal 54 UU PDP yakni, menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam Undang-Undang, memantau dan memastikan kepatuhan terhadap undang-undang ini dan kebljakan Pengendali Data Pribadi atau Prosesor Data Pribadi, memberikan saran mengenai penilaian dampak Pelindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi, serta berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi.

Pemrosesan Data Pribadi sesuai dengan Pasal 16 ayat (2) UU PDP harus dilakukan dengan cara terbatas, spesifik, sah secara hukum, transparan, sesuai dengan tujuannya, dilakukan dengan

menjamin hak Subjek Data Pribadi, akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dilakukan dengan melindungi keamanan data, memberitahukan tujuan dan aktivitas pemrosesan. Pasal 46 ayat (1) mencatumkan bahwa apabila terjadi kegagalan dalam pemrosesan maka Pengendali Data Pribadi wajib memperbaharui dan/atau memperbaiki kesalahan atau ketidakakuratan paling lambat 3 x 24 jam. Kemudian, apabila terdapat pelanggaran Pelindungan Data Pribadi, upaya hukum yang dapat dilakukan berupa pengaduan kepada Lembaga Pelindungan Data Pribadi, atau mengajukan gugatan melalui arbitrase, pengadilan atau lembaga penyelesaian sengketa lainnya.

Terkait dengan pemrosesan data sesuai dengan UU PDP, berdasarkan dari teori integritas kontekstual dari Hellen Nissenbaum perlu tiga prinsip yang mendominasi pertimbangan publik terhadap kebijakan privasi, yaitu *principle of Protecting Privacy of Individuals Against Intrusive Government Agents, principle of Restricting Access to Intimate, Sensitive, or Confidential Information, and principle of Curtailing Intrusions into Spaces or Spheres Deemed Private or Personal*. Prinsip-prinsip yang tersebut berkaitan dengan pembatasan pengawasan warga dan penggunaan informasi tentang mereka oleh agen pemerintah, pembatasan akses ke informasi intim, sensitif, rahasia dan pembatasan intrusi ke tempat-tempat yang dianggap pribadi.

Berdasarkan teori tersebut hal yang penting untuk diketahui adalah konteks-siapa yang mengumpulkan informasi, siapa yang menganalisisnya, siapa yang menyebarkannya dan kepada siapa, sifat informasi, hubungan antara berbagai pihak, dan keadaan kelembagaan. Dalam UU PDP penting diperhatikan konteks siapa yang mengumpulkan informasi dan yang menganalisisnya bisa dikatakan adalah Pengendali dan Prosesor Data Pribadi yang bekerja di bawah naungan Korporasi PSE lingkup privat, hubungan antara berbagai pihak seperti Subjek Data Pribadi sebagai pelanggan dari Korporasi PSE lingkup privat, sifat informasi yang diberikan kepada Korporasi PSE lingkup

privat harus jelas, serta siapa yang menyebarkan atau kepada siapa Data Pribadi ini akan dipergunakan harus diterangkan secara eksplisit kepada Subjek Data Pribadi sebagai Pemilik. Maka dari itu perlu diterapkan tiga prinsip diatas bahwa harus ada pembatasan dan pengawasan dari Subjek Data Pribadi terhadap data mereka yang digunakan oleh Korporasi PSE lingkup privat, kemudian Subjek Data Pribadi perlu melakukan pembatasan terhadap akses data yang bersifat intim, sensitif dan rahasia dan perlu adanya batasan bagi pemroses Data Pribadi terhadap ruang-ruang yang sekiranya dianggap pribadi oleh Subjek Data Pribadi.

III.2 Implikasi Pemrosesan Data Pribadi pada Korporasi PSE Lingkup Privat

Untuk melihat implikasi pemrosesan data pribadi yang terjadi terhadap Korporasi PSE lingkup privat akibat adanya UU PDP, penulis menggunakan teknik analisis RIA berupa *Soft-CBA*. Berdasarkan studi yang pernah dilakukan oleh SENADA *Competitiveness Project* yang berjudul *Regulatory Impact Asssessments and The Private Sector in Indonesia*, terdapat beberapa poin yang dapat dijadikan acuan dalam melakukan analisis ini yaitu, tujuan regulasi (*Objective of the Regulation*), fokus kebijakan (*Policy Focus of This Regulation*), alternatif regulasi (*Alternatives to This Regulation*), dampak langsung dan tidak langsung dari regulasi (*Direct and Indirect Impacts of The Regulation*), biaya kepatuhan terhadap regulasi (*Compliance Cost of This Regulation*), kepatuhan dan penegakan (*Compliance and Enforcement*), serta kualitas regulasi secara keseluruhan (*Overall Quality of The Regulation*).

Berikut ini adalah hasil dari analisis terkait dengan implikasi pemrosesan data pribadi terhadap Korporasi PSE lingkup privat berdasarkan UU PDP dengan menggunakan teknik analisis RIA *Soft-CBA*.

1. Tujuan Regulasi (*Objective of The Regulation*)

Mengacu pada bagian pertimbangan dibentuknya Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, tujuan dari UU PDP, yaitu:

a. bahwa Pelindungan Data Pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas Data Pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. bahwa Pelindungan Data Pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya Pelindungan Data Pribadi;
c. bahwa pengaturan Data Pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan Pelindungan Data Pribadi diperlukan pengaturan mengenai Pelindungan Data Pribadi dalam suatu undang-undang.

Berdasarkan hal tersebut dapat diketahui tujuan dari adanya UU PDP yaitu sebagai landasan hukum bagi pelindungan data pribadi, untuk menjamin hak warga negara atas pelindungan data pribadi dan untuk meningkatkan efektivitas dalam pelaksanaan Pelindungan Data Pribadi yang dibentuk dalam satu payung hukum yaitu undang-undang.

2. Fokus Kebijakan (*Policy Focus of This Regulation*)

Sebelum adanya UU PDP, regulasi terkait dengan Pelindungan Data Pribadi terdapat di berbagai aturan yang relevan dibawah level undang-undang, seperti:

a. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-undang Nomor 19 Tahun 2016 (“UU ITE”);

b. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP No. 71/2019");
c. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik ("PP No. 80/2019"); dan
d. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi Dalam Sistem Elektronik ("Permenkominfo No. 20/2016").

Namun demikian, UU PDP diharapkan lebih efektif dalam pelaksanaannya karena merupakan payung hukum pada level undang-undang yang secara khusus mengatur tentang Pelindungan Data Pribadi. Regulasi ini diundangkan karena adanya disharmonisasi pengaturan terkait dengan Pelindungan Data Pribadi.

3. Alternatif Regulasi (*Alternatives to This Regulation*)

Alternatif regulasi digunakan untuk dapat memastikan Pelindungan Data Pribadi dalam pemrosesan Data Pribadi berjalan dengan baik, dengan cara mengeluarkan pengaturan terkait dengan standar level keamanan sistem komputer yang digunakan untuk memproses Data Pribadi dan peraturan teknis terkait dengan pemrosesan Data Pribadi.

4. Dampak Langsung dan Tidak Langsung dari Regulasi (*Direct and Indirect Impacts of The Regulation*)

Regulasi ini baru akan sepenuhnya berjalan setelah dua tahun pengundangan selama itu maka ada masa transisi bagi para pengusaha dalam hal ini Korporasi PSE lingkup privat untuk bisa menyesuatkan dengan ketentuan yang ada di dalam UU PDP. Sesuai dengan ketentuan Pasal 74 Pengendali Data Pribadi, Prosesor Data Pribadi, dan pihak lain yang terkait dengan pemrosesan Data Pribadi, wajib menyesuaikan dengan ketentuan pemrosesan Data Pribadi

berdasarkan Undang-Undang ini paling lama 2 (dua) tahun sejak Undang-Undang ini diundangkan. Hal ini menjadi dampak yang tidak langsung, karena korporasi PSE lingkup privat masih diberikan waktu untuk menyesuaikan selama 2 tahun sebagai masa transisi.

Dampak langsung yang bisa dirasakan oleh korporasi PSE lingkup privat adalah UU PDP mengharuskan mereka untuk bisa mematuhi ketentuan yang ada, mematuhi prinsip Pelindungan Data Pribadi, mempekerjakan Pengendali dan Prosesor Data Pribadi, kemudian mempekerjakan pejabat fungsional agar pemrosesan data yang dilakukan oleh korporasi ini tetap bisa sah dan legal secara hukum.

5. Biaya Kepatuhan Terhadap Regulasi (*Compliance Cost of This Regulation*)

Analisis mengenai biaya kepatuhan terhadap UU PDP akan diuraikan melalui tabel dibawah ini.

Tabel III. 2 Biaya Kepatuhan terhadap UU PDP

Grup	**Potensi Manfaat (*Benefit*)**	**+**	**Potensi Biaya (*Cost*)**	**-**
Korporasi PSE lingkup privat	Memiliki kredibilitas yang baik di mata masyarakat/publik	+	Mempekerjakan Pengendali dan Prosesor Data Pribadi	-
	Kegiatan usaha tetap berjalan sebagaimana mestinya	+	Mempekerjakan Pejabat Fungsional	-
	Memperoleh peningkatan pasar, pelanggan, dan penghasilan karena tingginya kepercayaan publik	+	Memastikan pemenuhan hak Subjek Data Pribadi terkait dengan pemrosesan Data Pribadi	-
	Terhindar dari sanksi administratif maupun pidana	+	Mematuhi dan menyesuaikan dengan ketentuan terbaru Pidana tambahan secara berkala dalam pemrosesan Data Pribadi	-
			Pidana denda paling banyak 10x dari maksimal pidana yang diancamkan	-
			Pidana tambahan	-

Tabel III.2 menunjukan bahwa implikasi pemrosesan data pribadi terhadap Korporasi PSE lingkup privat berdasarkan UU PDP adalah biaya yang dikeluarkan oleh Korporasi PSE lingkup privat lebih besar dibandingkan dengan manfaat yang didapat. Biaya-biaya tersebut dikategorikan sebagai dampak negatif yang didapat oleh Koporasi PSE lingkup privat dikarenakan adanya ketentuan terkait dengan pelindungan data pribadi, seperti pengeluaran biaya untuk mempekerjakan Pengendali dan Prosesor Data Pribadi serta pejabat pengawas. Korporasi PSE lingkup privat juga dituntut untuk bisa memenuhi seluruh hak Subjek Data Pribadi dan bisa terus mengikuti pembaharuan kebijakan yang ada. Apabila hal tersebut tidak dilaksanakan dan terjadi pelanggaran data pribadi, Korporasi tersebut dapat terkena masalah seperti pemberian pidana denda dan pidana tambahan.

Dapat dibayangkan apabila sebuah Korporasi PSE lingkup privat tersandung masalah tindak pidana kebocoran data pribadi, korporasi tersebut bisa saja di jatuhi hukuman dua jenis sanksi pidana, yakni pidana denda dan pidana tambahan. Apabila diancam dengan pidana denda maka dapat dihitung penjatuhan sanksi pidana terhadap sebuah korporasi dengan ancaman denda maksimal Rp6.000.000.000 (enam miliar rupiah) seperti yang tercantum dalam ketentuan Pasal 68 UU PDP, dimungkinkan dapat dijatuhi sanksi maksimum sebanyak 10x lipat dari jumlah maksimal ancaman pidana denda, ini berarti suatu korporasi dapat dijatuhi pidana denda maksimum Rp60.000.000.000 (enam puluh miliar rupiah). Jumlah yang fantastis dan bisa sangat merugikan korporasi. Bukan hanya itu, korporasi tersebut juga dapat di jatuhi sanksi tambahan yang akan memberikan kerugian lainnya bisa sampai pada pembekuan atau sampai pada pembubaran korporasi.

Hal tersebut tentu menjadi sebuah rambu-rambu bagi setiap korporasi, terlebih lagi Korporasi PSE lingkup privat yang mana kegiatan bisnisnya dilakukan secara elektronik dan

erat kaitannya dengan pemrosesan data pribadi terhadap pelanggan. Apabila tidak berhati-hati dalam menerapkan dan mematuhi seluruh ketentuan pelindungan data pribadi, maka akan membawa dampak dan berpotensi merugikan terhadap kegiatan dan kelangsungan bisnisnya.

Sementara itu, bagi Korporasi PSE lingkup privat yang memenuhi ketentuan di dalam UU PDP akan mendapatkan potensi manfaat seperti, Korporasi PSE lingkup privat dipandang baik oleh masyarakat sebagai korporasi yang berintegritas, kegiatan usaha yang tetap bisa dilakukan yang berkaitan dengan pemrosesan data pribadi bagi pelanggan tetap sah secara hukum serta berpotensi memperoleh peningkatan pasar, pelanggan, dan penghasilan karena tingginya kepercayaan publik. Tingkat kepatuhan yang tinggi terhadap peraturan setidaknya akan menghindarkan Korporasi PSE lingkup privat dari pengeluaran biaya yang lebih besar seperti membayar denda atas pelanggaran pemrosesan data pribadi.

6. Kepatuhan dan Penegakan (*Compliance and Enforcement*)

Ketentuan penyelesaian sengketa dalam pelindungan data pribadi dapat dilakukan melalui upaya hukum sesuai dengan Pasal 67 UU PDP penyelesaian sengketa dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan dengan proses persidangan yang dilakukan secara tertutup.

Dalam UU PDP, terdapat 2 (dua) sanksi yang diatur yaitu sanksi administrasi dan sanksi pidana. Apabila korporasi melakukan pelanggaran pidana maka akan dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi. Pasal 70 UU PDP menyebutkan bahwa korporasi hanya bisa dijatuhkan pidana denda. Pidana denda paling banyak 10 kali dari maksimal pidana yang diancamkan dan pidana tambahan seperti:

a. perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
b. pembekuan seluruh atau sebagian usaha Korporasi;
c. pelarangan permanen melakukan perbuatan tertentu;
d. penutupan seluruh atau sebagian tempat usaha dan/ atau kegiatan Korporasi;
e. melaksanakan kewajiban yang telah dilalaikan;
f. pembayaran ganti kerugian;
g. pencabutan izin; dan/atau
h. pembubaran Korporasi.

Adanya ketentuan terkait dengan penyelesaian sengketa dan sanksi memberikan kepastian hukum bagi Subjek Data Pribadi. Namun, tingkat kepatuhan tinggi membutuhkan upaya penegakan hukum yang tinggi, kedua unsur ini perlu dilakukan dengan berimbang. Lembaga Pelindungan Data Pribadi yang diamanatkan dalam UU PDP akan menjadi pengawas dan penegak hukum administratif terhadap pelindungan data pribadi dalam setiap tahapan pemrosesan data pribadi. sedangkan penegakan hukum dalam penyelesaian sengketa pelindungan data pribadi yang bersifat tindak pidana akan diproses melalui pengadilan.

7. Kualitas Regulasi Secara Keseluruhan (*Overall Quality of The Regulation*)

Berdasarkan analisis diatas, implikasi pemrosesan data pribadi yang mengacu pada UU PDP menjadikan korporasi PSE lingkup privat harus menyediakan fitur yang memadai bagi kelangsungan pemrosesan data pribadi yang sesuai dengan aturan, seperti adanya Pengendali dan Prosesor Data Pribadi hingga keberadaan pejabat fungsional. Akan tetapi, ada kekhawatiran bahwa peraturan ini tidak dapat mencapai tujuan dalam memberikan kepastian

hukum kepada pemangku kepentingan, terutama pelaku usaha industri yaitu Korporasi PSE lingkup privat, karena masih ada kekurangan dalam UU PDP, seperti:

a. tidak adanya ketentuan standar level keamanan bagi sistem komputer yang digunakan untuk memproses Data Pribadi; dan
b. tidak terdapat ketentuan Prinsip Penyesuaian (*The Adjustment Principle*) bagi pengecualian Pelindungan Data Pribadi dalam pemrosesan Data Pribadi.

Bagi Korporasi PSE lingkup privat, tetap perlu mematuhi dan menyesuaikan dengan ketentuan pelindungan data pribadi secara berkala sedangkan masyarakat awam dapat menjadi *informed consent* dan percaya bahwa diri sendiri yang memegang kontrol penuh terhadap data pribadi serta berhati-hati untuk memberikan akses dan informasi terhadap data apapun kepada pihak manapun termasuk ketika menjadi pelanggan dari Korporasi PSE lingkup privat.

Untuk mengatasi kekurangan yang ada di dalam UU PDP maka penulis menyarankan adanya alternatif regulasi berupa peraturan terkait dengan strandar level keamanan sistem komputer yang digunakan untuk pemrosesan data pribadi. Hal ini guna memberikan Korporasi PSE lingkup privat gambaran standar level sistem komputer seperti apa yang digunakan, sehingga dapat menghindari atau meminimalisir kebocoran data dan apabila ada kebocoran yang diakibatkan dari tidak terpenuhinya standar sistem keamanan komputer yang digunakan korporasi PSE lingkup privat tersebut harus bertanggungjawab atas kebocoran yang terjadi.

Peraturan mengenai standar level sistem kemanan komputer dapat dibuatkan dalam dua cara, yakni sebagai berikut ini.

1. Pemenuhan sertifikasi standar internasional terkait keamanan sistem komputer

Terkait dengan hal ini, perlu dilakukan formulasi ketentuan yang menegaskan bahwa setiap Korporasi PSE lingkup privat perlu memenuhi sertifikasi standar internasional terkait dengan

keamanan sistem komputer, seperti ISO/IEC 27001 *Information Security Management Systems*. ISO/IEC 27001 adalah standar paling terkenal di dunia terkait dengan sistem manajemen keamanan informasi. Standar ISO/IEC 27001 merupakan panduan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi. Kesesuaian dengan ISO/IEC 27001 berarti bahwa organisasi dalam hal ini Korporasi PSE lingkup privat telah menerapkan sistem untuk mengelola risiko yang terkait dengan keamanan data yang dimiliki atau ditangani oleh korporasi.[50]

Ketika sebuah Korporasi PSE lingkup privat menerapkan kerangka kerja keamanan informasi yang ditentukan dalam standar ISO/IEC 27001, maka akan mendapatkan manfaat seperti:

a. Mengurangi risiko kerentanan terhadap ancaman *cyber*
b. Memastikan bahwa aset seperti laporan keuangan, kekayaan intelektual, data dan informasi karyawan yang dipercayakan oleh pihak ketiga tetap tidak rusak, rahasia, dan tersedia sesuai kebutuhan;
c. Menyediakan kerangka kerja yang dikelola secara terpusat yang mengamankan semua informasi di satu tempat;
d. Mengamankan informasi dalam segala bentuk, termasuk data berbasis kertas, berbasis *cloud*; dan
e. Menghemat pengeluaran dengan meningkatkan efisiensi dan mengurangi biaya untuk teknologi pertahanan yang tidak efektif.[51]

---

[50] ISO, "ISO/IEC 27001 Information Security Management Systems," *Iso.Org*, accessed August 8, 2023, https://www.iso.org/standard/27001.

[51] *Id*,.

Penggunaan standar sertifikasi ISO/IEC 27001 diterapakan sesuai dengan beberapa prinsip, diantaranya:

a. Kerahasiaan (*Confidentiality*)

   Prinsip ini menegaskan bahwa hanya orang yang tepat yang dapat mengakses informasi yang dimiliki oleh korporasi.

b. Integritas informasi (*Information integrity*)

   Data yang digunakan korporasi untuk menjalankan bisnisnya atau tetap aman untuk orang lain disimpan dengan andal dan tidak terhapus atau rusak. Hal ini untuk menghindari resiko seorang anggota staf secara tidak sengaja menghapus *file* atau data selama pemrosesan.

c. Ketersediaan data (*Availability of data*)

   Korporasi dan subjek data pribadi dapat mengakses informasi kapan pun diperlukan sehingga tujuan bisnis dan harapan pelanggan terpenuhi.[52]

Sistem manajemen keamanan informasi yang memenuhi persyaratan ISO/IEC 27001 menjaga kerahasiaan, integritas dan ketersediaan informasi dengan menerapkan proses manajemen risiko dan memberikan keyakinan kepada pihak yang berkepentingan bahwa risiko dikelola secara memadai.[53] Sertifikasi ISO/IEC 27001 adalah salah satu cara untuk menunjukkan kepada pelanggan bahwa Korporasi PSE lingkup privat berkomitmen dan mampu mengelola informasi/data pribadi secara aman, hal ini akan berdampak baik karena korporasi tersebut yang akan mendapatkan kepercayaan lebih dari pelanggan.

[52] *Id,.*

[53] *Id,.*

Sertifikasi ISO/IEC 27001 telah banyak digunakan sebanyak 140 negara dan dari berbagai sektor ekonomi, mulai seperti pertanian hingga manufaktur hingga layanan sosial.[54]

2. Pembuatan pengaturan terkait dengan keamanan sistem komputer

Selain pengaturan sertifikasi, perlu diatur juga ketentuan yang mengatur keamanan sistem komputer yang berkorelasi dan sertifikasi tersebut. Contoh demikian dapat ditemui misalnya UU Keamanan Komputer tahun 1987 (*Computer Security Act*) dari Amerika. Maksud dari undang-undang ini adalah untuk membuat program standar komputer bagi sistem komputer pada level federal, termasuk pedoman untuk keamanan sistem tersebut, menetapkan kewenangan pada level tersebut dalam menerapkan standar tersebut, mewajibkan agensi yang bersangkutan untuk menggunakan pedoman keamanan teknis sistem komputer yang dikembangkan oleh *National Security Agency* mengenai perlindungan informasi sensitif[55].

Jika *Computer Security Act* 1987 dibuat untuk sistem keamanan komputer yang digunakan oleh lembaga pemerintahan, maka dalam pembahasan penelitian ini, dapat dijadikan sebagai contoh bahwa telah ada peraturan tentang keamanan sistem komputer dalam mengelola data, hanya saja peraturan yang nantinya akan dibuat dikhususkan untuk Korporasi PSE lingkup privat dalam pemrosesan data pribadi pelanggan sebagai pemilik data

Selanjutnya, untuk kekurangan yang kedua dapat dibuatkan peraturan turunan/teknis yang terkait dengan pemrosesan data pribadi yang dikhususkan untuk Korporasi PSE lingkup privat. Adanya peraturan tersebut bisa menjadi acuan bagi Korporasi PSE lingkup privat ketika

---

[54] *Id*,.

[55] Congressional Research Service, "H.R.145 - Computer Security Act of 1987" (United States, 1987), https://www.congress.gov/bill/100th-congress/house-bill/145.

melakukan memproses data pribadi, dengan peraturan tersebut langkah pencegahan dan penanganan kebocoran data bisa dilakukan secara tepat dan efisien.

Pengimplementasian kedua peraturan yang diuraiakan dalam paragraf sebelumnya dapat dilakukan sesegera mungkin, apabila dalam waktu jangka pendek pemerintah belum kunjung mengeluarkan pengaturan terkait dengan hal tersebut maka Korporasi PSE lingkup privat bisa mengacu pada peraturan yang sudah ada. Korporasi juga perlu membuat peraturan internal sendiri dengan mengadopsi prinsip-prinsip ketentuan dalam UU PDP baru dan praktik terbaik (*best practices*) yang ada. Untuk jangka menengah, apabila terdapat peraturan turunan UU PDP yang sudah terbit, maka korporasi PSE perlu melakukan penyesuaian terhadap peraturan dimaksud terhadap peraturan internal yang mungkin sudah dibuat. Untuk jangka panjang, perlu dilakukan lagi analisa dan evaluasi atas norma-norma dalam UU PDP dan peraturan terkait lainnya terhadap praktik dan permasalahan yang ada untuk kemudian diusulkan pembaharuan terhadap UU PDP.