ATMA JAYA STUDIES ON
AVIATION, OUTER SPACE AND CYBER LAWS

MENGAWAL PELINDUNGAN DATA PRIBADI

(GLOBAL, REGIONAL DAN NASIONAL)

Undang-undang Republik Indonesia
Nomor 19 Tahun 2002 tentang Hak Cipta

Lingkup Hak Cipta
Pasal 2:

1. Hak Cipta merupakan hak eksklusif bagi Pencipta atau Pemegang Hak Cipta untuk mengumumkan atau memperbanyak, ciptaannya, yang timbul secara otomatis setelah suatu ciptaan dilahirkan tanpa mengurangi pembatasan menurut peraturan perundang-undangan yang berlaku.

Ketentuan Pidana
Pasal 72:

1. Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam pasal 2 ayat (1) atau pasal 49 ayat (1) dan ayat (2) dipidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp. 1.000.000,- (satu juta rupiah) atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,- (lima milyar rupiah).

2. Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud dalam ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,- (lima ratus juta rupiah).

ATMA JAYA STUDIES ON
AVIATION, OUTER SPACE AND CYBER LAWS

MENGAWAL PELINDUNGAN DATA PRIBADI

(GLOBAL, REGIONAL DAN NASIONAL)

PROF. DR. IDA BAGUS RAHMADI SUPANCANA
IDA BAGUS AYODHYA DIRGANTARA, SH., LL.M.

Penerbit Bintang Kejora
2024

Atma Jaya Studies on Aviation, Outer Space and Cyber Laws
MENGAWAL PELINDUNGAN DATA PRIBADI
(GLOBAL, REGIONAL DAN NASIONAL)

Penerbit Bintang Kejora
Mutiara Gading Timur Blok M15 No. 22
Bekasi 17158

Cetakan Pertama, Desember 2024

Penulis	:	Prof. Dr. Ida Bagus Rahmadi Supancana Ida Bagus Ayodhya Dirgantara, SH., LL.M.
Editor	:	Dr. Dra Yogi Widiawati M.Hum, Viranditha Koswara S.Tr.A.B
Layout Naskah	:	Grafindo
Desain Sampul	:	Grafindo
Gambar Sampul	:	https://www.theguardian.com/commentisfree/2018/jun/10/data-protection-press-freedom

Atma Jaya Studies on Aviation, Outer Space and Cyber Laws
MENGAWAL PELINDUNGAN DATA PRIBADI
(GLOBAL, REGIONAL DAN NASIONAL)

Penerbit Bintang Kejora, 2024
x + 172 hlm.; 17 x 25 cm
ISBN

KATA PENGANTAR

Berbagai Instrumen Internasional, baik *Hard Laws* maupun *Soft Laws* meneguhkan Privasi sebagai Hak Dasar Manusia yang harus dilindungi. Data Pribadi merupakan salah satu bentuk Privasi, yaitu *Information Privacy*, selain Privasi lain seperti *Communication Privacy, Territorial Privacy* dan *Bodily Privacy*. Pada tataran internasional, Pelindungan Data Pribadi telah diatur sejak tahun 1980 dan semakin hari pengaturannya semakin ketat. Ada hal utama yang harus dipahami dalam Mengawal Pelindungan Data Pribadi, yaitu harmoni antara Pelindungan Data Pribadi sebagai bentuk penghormatan atas hak-hak asasi manusia, dengan kebutuhan adanya *Cross Border Flow of Personal Data* untuk memfasilitasi globalisasi perdagangan, investasi, keuangan, dan lain-lain.

Buku ini disusun untuk memberikan gambaran secara menyeluruh namun ringkas mengenai berbagai langkah yang telah ditempuh, baik pada tataran Global, Regional, maupun Praktek Negara, serta Pengaturan Nasional di Indonesia dalam rangka Mengawal Pelindungan Data Pribadi.

Penyajian buku ini diawali dengan gambaran tentang Konsep-Konsep Dasar Pelindungan Data Pribadi yang meliputi: Privasi sebagai Hak-Hak Dasar yang dilindungi berdasarkan berbagai instrumen hukum yang berlaku; Cakupan Privasi; Privasi terkait Data dan Informasi Pribadi; gambaran faktual tentang Bentuk-Bentuk Pelanggaran terhadap Data Pribadi; Urgensi Pengaturan; serta Pentingnya Pelindungan Data Pribadi bagi Dunia Usaha. Selanjutnya sebagai

benchmarking (acuan) diuraikan Pengaturan Pelindungan Data Pribadi pada Tataran Internasional yang meliputi pengaturan di: Uni Eropa (EU); *Association of South East Asian Nations* (ASEAN); *Asia Pacific Economic Cooperation* (APEC); serta Pengaturan Pelindungan Data Pribadi di beberapa Negara. Perbandingan tersebut dimaksudkan untuk mengambil pembelajaran serta menarik unsur yang sama *(common elements)*, memahami standard yang berlaku dan praksis terbaik *(best practices)* sebagai bahan pertimbangan bagi pengaturan dan implementasinya di Indonesia.

Guna memberi gambaran tentang berbagai inisiatif yang telah ditempuh dalam Penyusunan dan Pembahasan Rancangan Undang-Undang tentang Pelindungan Data Pribadi, secara kronologis akan diuraikan: Studi Awal yang dimulai sejak tahun 2005 serta Konsultasi Awal pada tahun 2007; perkembangan Penyusunan dan Finalisasi Naskah Akademik; Penyusunan Rancangan Undang-Undang; serta Dinamika Pembahasan Rancangan Undang-Undang Pelindungan Data Pribadi di Komisi I DPR, hingga tercapainya Kesepakatan antara Pemerintah dan Dewan Perwakilan Rakyat untuk diundangkan. Setelah memberikan gambaran tentang Pokok-Pokok Pengaturan pada Undang-Undang tentang Pelindungan Data Pribadi, dilanjutkan dengan beberapa Analisa Kritis atas Isu-Isu tertentu yang membutuhkan perhatian, baik dari segi pengaturan maupun implementasinya. Untuk memastikan efektivitas pelaksanaan Undang-Undang tentang Pelindungan Data Pribadi, beberapa Isu penting perlu dijabarkan dalam Aturan Pelaksanaan berdasarkan mandat yang diberikan oleh Undang-Undang, baik dalam bentuk Peraturan Pemerintah maupun Peraturan Presiden. Berdasarkan praktek regulasi yang baik *(good regulatory practices),* harus ada keseimbangan antara *regulatory design, regulatory delivery* maupun *regulatory inspection*. Maknanya implementasi Undang-Undang tentang Pelindungan Data Pribadi harus dikawal, yang meliputi: Kesiapan Sektor Publik; Kesiapan Sektor Privat; Kesiapan dan Partisipasi Masyarakat; serta kesiapan Pengawasan dan Penegakan Hukumnya, . Untuk membantu kesiapan sektor publik, sektor privat, organisasi internasional maupun masyarakat dalam implementasi Undang-Undang tentang Pelindungan Data Pribadi, akan disajikan berbagai aspek praktis yang diharapkan dapat berguna sebagai semacam *checklist,* yang meliputi: *Privacy Policy; Gap Assessment*; *Data Processing Agreement*; *Data Sharing Agreement;*

Recording of Processing Activities (ROPA); Data Protection Impact Assessment (DPIA); Data Protection Officers (DPO); Software Compliance, Keamanan Data dan Penanganan *Data Breach;* Transfer Data; hingga Pengawasan dan Penegakan Hukum.

Melalui alur dan rangkaian penyajian sebagaimana tersebut di atas, semoga secara ringkas namun padat akan bermanfaat membantu para pembaca dalam memahami segala aspek yang terkait dengan berbagai upaya Mengawal Pelindungan Data Pribadi, baik secara konseptual, teoritis, akademis, historis, regulasi, hingga aspek-aspek praktis dan operasional, termasuk kasus-kasus terkait.

Semoga Naskah hasil kolaborasi antara Akademisi dengan Praktisi ini akan bermanfaat bagi semua kalangan yang terkait dengan pelaksanaan Undang-Undang Pelindungan Data Pribadi.

Jakarta, 12 Desember 2024
Para Penulis,

Ida Bagus Rahmadi Supancana
Ida Bagus Ayodhya Dirgantara

DAFTAR ISI

BAB I

KONSEP DASAR PELINDUNGAN DATA PRIBADI

Privasi adalah hak fundamental dari setiap individu yang harus dilindungi sebagai bentuk penghormatan terhadap hak-hak asasi manusia. Dalam Bab I ini akan diuraikan berbagai Sumber Hukum yang menjadi dasar bagi Pelindungan Data Pribadi, baik yang berdasarkan pada berbagai instrumen internasional, maupun yang bersumber pada Konstitusi Indonesia dan peraturan perundang-undangan lainnya. Bab ini juga akan menguraikan jenis-jenis Privasi, termasuk Data dan Informasi Pribadi yang menjadi dasar bagi Pelindungan Data Pribadi. Beberapa pengertian Privasi juga akan disajikan untuk memperoleh pengertian yang memadai. Hal lain yang juga penting untuk dipahami adalah tentang bentuk-bentuk Pelanggaran terhadap Data Pribadi, diikuti dengan uraian mengenai Urgensi Pengaturan tentang Pelindungan Data Pribadi. Terakhir, suatu penjelasan bahwa Pelindungan Data Pribadi ternyata mendukung kegiatan bisnis.

A. Privasi sebagai Hak-Hak Dasar yang Dilindungi

1. Pasal 28 G (1) UUD 1945 sebagaimana yang telah diamandemen
   "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda di bawah kekuasaannya, serta berhak atas rasa

aman dan perlindungan dari ancaman kesulitan untuk berbuat sesuatu atau tidak berbuat sesuatu yang merupakan hak asasi".

2. Undang-Undang No 39 Tahun 1999 tentang Hak-Hak Asasi Manusia
   Undang-Undang ini mengatur hal-hal pokok, yaitu: Ketentuan Umum; Asas-Asas Dasar; Hak Asasi Manusia dan Kebebasan Dasar Manusia; Kewajiban Dasar Manusia; Kewajiban dan Tanggung Jawab Pemerintah; Pembatasan dan Larangan; Komisi Nasional Hak Asasi Manusia; Partisipasi Masyarakat; Pengadilan Hak Asasi Manusia; Ketentuan Peralihan; dan Ketentuan Penutup.

   Ketentuan Pasal 29 ayat (1) menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya. Inti dari ketentuan pasal ini menyangkut pelindungan privasi sebagai hak dasar manusia.

3. *Universal Decalaration of Human Rights of 1945*
   Pasal 12 dari *The UN Universal Declaration of Human Rights menyatakan:* "*No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*".

   Inti dari ketentuan Pasal 12 dari Deklarasi Universal yang menjadi acuan utama dari pelindungan terhadap hak-hak asasi manusia di seluruh dunia adalah untuk menghormati dan melindungi privasi, keluarga, kediaman, serta korespondensi dari segala gangguan dan serangan terhadap kehormatan dan martabatnya. Setiap orang mempunyai hak untuk mendapatkan perlindungan terhadap segala bentuk gangguan atau serangan terhadap privasinya.

   Peran Negara sangat penting dalam memastikan pelindungan hak-hak dasar manusia, khususnya terhadap hak privasinya. Pelindungan yang diberikan termasuk dalam bentuk pelindungan hukum.

4. *The European Convention for the Protection of Human Rights Rights and Fundamental Freedoms 1950*
   Secara regional di Eropa juga ada instrumen hukum yang melindungan hak-hak asasi masnusia serta kebebasan dasarnya sebagaimana diatur dalam *The*

European Convention for the Protection of Human Rights and Fundamental Freedoms 1950. Salah satu pasalnya, yaitu Pasal 8 secara spesifik mengacu pada Pelindungan Privasi sebagaimana berikut ini:

Pasal 8:

"(1). Everyone has the right to respect his private and family life, his home and his correspondence.

(2). There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals or for the protection of the rights and freedoms of other."

Ketentuan di atas menekankan pada hak setiap orang untuk mendapatkan penghargaan atas privasi, kehidupan keluarga, kediaman maupun korespondensinya. Tidak boleh ada segala bentuk gangguan terhadap privasi seseorang oleh otoritas publik kecuali diperlukan atas dasar aturan hukum yang berlaku, baik untuk kepentingan keamanan nasional, keselamatan umum atau kesejahteraan bangsa, untuk mencegah ketidaktertiban karena tindak pidana, untuk melindungi kesehatan moral atau untuk perlindungan terhadap hak dan kebebasan orang lain.

Pengecualian terhadap pelindungan terhadap privasi seseorang hanya dapat dilakukan secara terbatas dan berdasarkan undang-undang sepanjang menyangkut kepentingan masyarakat yang lebih besar, baik keamanan, keselamatan umum, kesejahteraan bangsa dan menjaga moral masyarakat.

5. *The Arab Charter of Human Rights 2004*

Ketentuan pada lingkup regional lainnya dapat dicermati pada instrumen hukum seperti *The Arab Charter of Human Rights 2024* yang secara khusus juga mengatur tentang perlindungan Privasi sebagai salah satu hak dasar manusia yang harus dilindungi. Pasal 21 dari instrumen tersebut menyatakan:

Pasal 21:

"(1). No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation; and

(2). Everyone has a right to the protection of the law against such interference or attacks."

Piagam Hak Asasi Manusia dalam lingkup regional ini juga menekankan tentang pentingnya perlindungan terhadap privasi setiap orang, juga terhadap keluarga, kediaman dan korespondensinya dari tindakan sepihak yang melawan hukum ataupun bentuk-bentuk serangan terhadap kehormatan dan reputasinya. Oleh karenanya setiap orang mempunyai hak untuk mendapatkan perlindungan hukum dari serangan maupun gangguan tersebut.

6. *The Universal Declaration on Bio Ethics and Human Rights 2005*

Pengaturan dalam lingkup global dalam bentuk *soft law*s yang mengatur tentang *Bio Ethics* dan hak-hak asasi manusia juga mengandung ketentuan pelindungan privasi.

Pasal 9 merumuskan tentang privasi dan pelindungannya yaitu:

"The privacy of the persons concerned, and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law".

Rumusan yang ada pada Deklarasi ini secara spesifik menekankan pada penghormatan terhadap privasi seseorang terkait dengan kerahasiaan atas informasi pribadinya. Sejauh mungkin informasi pribadi tersebut tidak digunakan atau diungkap untuk tujuan-tujuan yang berbeda dengan tujuan pengumpulan data tersebut atau persetujuan yang diberikan. Hal ini sejalan dengan ketentuan-ketentuan Hukum Internasional, khususnya Hukum Internasional tentang Hak-Hak Asasi Manusia.

7. Amandemen Ke 4 Konstitusi Amerika Serikat

Amandemen Ke 4 dari Konstitusi Amerika Serikat juga mengatur tentang pelindungan terhadap Privasi Warganegara dari kemungkinan pelanggaran atau kesewenang-wenangan dengan rumusan: "*The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable*

cause, supportd by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

Isi ketentuan Amandemen Ke 4 Konstitusi AS yang disahkan pada tanggal 15 Desember 1791 ini berupaya untuk melindungi rakyat Amerika dari setiap bentuk penggeledahan dan penangkapan yang tidak memiliki dasar hukum yang kuat. Pada saat perumusan Amandemen Ke 4 atas Konstitusi Amerika tersebut adalah dalam rangka merespons meningkatnya pelanggaran atas Privasi[1].

8. Pidato Barrack Obama Saat Pencalonan Sebagai Presiden Amerika Serikat
   Pada saat penominasian Barrack Obama sebagai calon Presiden Amerika Serikat dari Partai Demokrat, salah satu isi pidato yang dianggap relevan dengan era informasi, termasuk kemungkinan dampaknya terhadap hak-hak Privasi serta arah kebijakan ke depan, dapat kita cermati dari kutipan kata-kata dalam pidatonya yang menyatakan:
   - *"The open information platforms of the twenty-first century can also temps institutions to violate the privacy of citizens. Dramatic increases in computing power, decreases in storage costs and huge flows of information that characterize the digital age bring enormous benefits, but also create risk of abuse. We need sensible safeguards that protect privacy in this dynamic new world ".*
   - *"…. but we disagree the privacy is not relevant or desirable, in this sensor driven, social everywhere, big data world that is heading towards. People today expect strong privacy protections because they are increasingly aware of, and concerned about, the digital trails they leave behind online and indeed there's plenty of evidence that people still can deeply about privacy"*[2].

   Pada pidato pencalonan Presiden Barrack Obama yang sangat terkenal tersebut ditekankan bahwa platform-platform informasi yang terbuka pada abad ke dua puluh satu juga menggoda institusi-institusi melanggar privasi warga Negara. Peningkatan yang dramatis atas kemampuan komputer

[1] Baca, "Constitutional Amendment-Amendment 4 The Privacy", www.reaganlibrary.gov, diunduh pada tanggal 6 Juli 2024.

[2] Barrack Obama, "Connecting and Empowering All American through Technology and Innovation", Presidential Announcement Speech in Spring Field, 2 October 2007.

serta semakin murahnya biaya penyimpanan data serta arus informasi yang sangat cepat dan besar yang menjadi karakteristik dari era digital, disatu sisi memberikan manfaat yang sangat besar, namun pada sisi lain menimbulkan resiko penyalahgunaan. Oleh karenanya diperlukan perlindungan privasi dalam dunia baru yang dinamis ini.

Lebih lanjut Obama menyampaikan bahwa ia tidak meyakini bahwa privasi tidak relevan atau tidak diinginkan dalam dunia Big Data dengan segala perubahan sosialnya yang dihadapi ke depan. Orang-orang saat ini membutuhkan perlindungan yang kuat atas privasinya karena kesadaran yang semakin besar atas jejak digitalnya yang mereka tinggalkan secara *online*, dan karenanya terdapat bukti yang kuat bahwa mereka sangat peduli terhadap privasinya.

9. *Black's Law Dictionary*

   Black's Law Dictionary merumuskan Privacy Rights sebagai:

   "*The right to be let alone; the right of a person tobe free of unwarranted publicity. The term "right of privacy" is generic term encompassing various rights recognized to be inherent inconcept of ordered liberty, and such rights prevents governments interference in intimate personal relationship or activities, freedom of individual to make fundamental choices involving himself, his family and his relationship with others*"[3].

   Dari rumusan di atas diperoleh pemahaman bahwa dalam pengertian umum hak privasi tersebut berkaitan dengan beberapa hak menyangkut kebebasan dan kemerdekaan manusia yang patut dilindungi, termasuk terhadap intrusi atau intervensi dari Pemerintah dalam hal-hal yang bersifat pribadi, keluarga maupun hubungannya dengan pihak lain.

10. Oxford Dictionary of Law

    Oxford Dictionary of Law merumuskan pengertian yang sejalan. Selanjutnya dinyatakan:

    "*The right includes privacy of communication (telephone call, correspondence, etc); privacy of home and office; environmental protection; the protection of physical integrity; and protection of unjustified prosecution and conviction of*

[3] Black, Henry Campbell, Black's Law Dictionary, Fifth Edition, West Publishing, USA, 1979, halaman 1075.

those engaged in consensual non violation of sexual activities. This right is a qualified right: as such, public interest can be used to justify interference with it providing that this is prescribed by law, designed for a legitimate purpose, and proportionate. Public authorites have limited but positive duty to protect privacy from interference by thirs parties"[4].

Hak yang ditambahkan pada rumusan di atas adalah berupa penjabaran atas hak privasi yang mencakup: komunikasi (melalui telepon, korespondensi, dll.), privasi atas rumah dan tempat kerja; perlindungan lingkungan, perlindungan atas integritas fisik; perlindungan atas tuntutan atau putusan yang berkaitan dengan kegiatan seksual pribadi. Hak-hak privasi adalah merupakan hak individual, namun dapat dibatasi oleh kepentingan umum, dimana dimungkinkan adanya campur tangan dan intervensi oleh Pemerintah, sepanjang hak tersebut ditetapkan oleh hukum, dirancang untuk maksud-maksud yang sah serta dilaksanakan secara proporsional. Dengan demikian Pemerintah memiliki kewajiban terbatas namun positif untuk melindungi privasi terhadap gangguan pihak ketiga.

B. Cakupan, Privasi[5]

Secara umum Privasi dapat dibagi atas:

1. Privasi atas Informasi *(Information Privacy):*
   Secara umum *information privacy* adalah informasi yang berkaitan dengan seseorang atau sekelompok orang yang mencerminkan rincian kehidupan seseorang dan karakteristik lain yang dapat berdampak kepadanya. Secara praktis pengaturan tentang *information privacy* berkaitan dengan perumusan aturan mengenai cara pengumpulan dan pengelolaan (penanganan) data pribadi seperti informasi kredit dan catatan kesehatan, dan lain-lain yang hanya dapat diakses oleh pihak-pihak yang berwenang atau memiliki otoritas atas *information privacy* tersebut.

---

4 Martin, Elizabeth A, Oxford Dictionary of Law, Oxford University Press, Fifth Edition, 2002, halaman 381.

5 Lihat Abu Bakar Munir dan Siti Hajar Mohd Yasin, Privacy and Data Protection, Sweet and Maxwell Asia, Hongkong, 2002, halaman 2.

Information privacy tersebut hanya dapat diakses dengan cara-cara tertentu seperti: *usernames* dan *password*, atau *biometric authentication*, atau dengan cara enkripsi, dan lain-lain. Bentuk perlindungan bagi *information privacy* dapat berupa langkah-langkah, seperti: memastikan bahwa data sensitif hanya dapat diakses oleh pihak-pihak yang memiliki wewenang untuk itu; mengenkripsi data untuk mencegah akses oleh pihak yang tidak berwenang; membatasi pengumpulan dan penggunaan data pribadi hanya sepanjang yang diperlukan saja; membuat mekanisme agar subjek data pribadi memiliki pengendalian atau kewenangan memodifikasi atas data pribadinya; mematuhi peraturan perundang-undangan yang berlaku terkait pelindungan atas data/informasi pribadi.

2. Privasi atas Komunikasi *(Communication Privacy)*:
   Aturan tentang *communication privacy* intinya membatasi kegiatan intersepsi, penggunaan dan pengungkapan komunikasi dan apa yang dapat dilakukan oleh penyedia jasa telekomunikasi terhadapnya. *Communication privacy* mencakup keamanan dan privasi atas surat, telepon, e*mail* dan bentuk-bentuk komunikasi lainnya[6].

   Di Amerika Serikat, pengaturan mengenai *communication privacy* dapat ditemukan pada: *The Cable Communication Policy Act*[7]*; The Electronic Communication Privacy Act*[8]*; The Telecommunication Act*[9]*; The Video Privacy Protection Act*[10].

   Di Indonesia, aturan tentang *communication privacy* diatur dalam Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi.

3. Privasi atas Wilayah *(Territorial Privcy)*:
   Territorial Privacy berkaitan dengan penetapan batas atas intrusi terhadap masalah dan lingkungan domestik seperti tempat kerja, tempat terbuka, dan

6 Baca: "Communication Privacy", epic.org, diunduh pada tanggal 7 Juli 2024.

7 Intinya membatasi penyedia jasa komunikasi via kabel untuk mengumpulkan, menyimpan, dan mengungkap komunikasi pelanggannya. Lihat Ibid.

8 Intinya membatasi kemampuan penyedia jasa elektronik untuk mengakses dan mengungkap isi dari komunikasi konsumen dan informasi lainnya terkait komunikasi elektronik pelanggan. Lihat Ibid.

9 Intinya membatasi penyedia jasa telekomunikasi untuk mengungkap informasi tentang jaringan informasi konsumen atau informasi konsumen yang berada pada penyedia jasa telekomunikasi, seperti calling plans dan informasi yang diperoleh konsumen yang dihasilkan dari penggunaan telepon. Lihat Ibid.

10 Intinya membatasi pengungkapan informasi rekaman video oleh konsumen. Lihat Ibid.

lain-lain[11]. Secara umum ada 4 (empat) konsep tentang territorial, yaitu: *attached territory, central territory, supporting territory, dan peripheral territory*.

Contoh-contoh umum terkait dengan perlindungan atas *territorial privacy* terkait dengan tindakan-tindakan seperti: *video surveillance, house and car searches, physical access. Territorial Privacy juga dapat meliputi tempat kerja (workplace)* atau ruang publik dan pertimbangan lingkungan.

4. Privasi atas Tubuh *(Bodily Privacy)*:
   Bodily Privacy berkaitan dengan perlindungan secara fisik terhadap seseorang, terhadap prosedur invasive seperti tes narkoba, penggeledahan. Contoh-contoh lain mencakup: *genetic testing, health research, drug test, and abortion rights.*

C. Privasi Terkait Data dan Informasi Pribadi

1. Pengertian Data Pribadi
   a. *EC Directive 95/46*
      "*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 of factors more specific to his physical, physiological, mental, economic, cultural or social identity*"[12]

      Dalam *Directive* yang merupakan salah satu bentuk aturan di samping *Regulation* yang berlaku di Uni Eropa dirumuskan pengertian Data Pribadi sebagai "setiap informasi terkait dengan seseorang (orang perorangan/individu) yang teridentifikasi atau dapat diidentifikasi yang disebut dengan Subjek Data Pribadi *(Data Subject)*. Seseorang yang teridentifikasi adalah seseorang yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, khususnya dengan mengacu pada nomor identifikasi atau terkait dengan faktor-faktor yang lebih spesifik tentang kondisi fisik, fisiologis, mental, ekonomi, kebudayaan atau identitas sosial.

---

[11] Lihat Australian Law Reform Commission, "The Meaning of Privacy", 16 Agustus 2010, www.airc.gov.au, diunduh pada tanggal 7 Juli 2024.

[12] Pasal 2 huruf (a)

b. OECD *Guidelines* 1980

"Personal data means any information relating to an identified or identifiable individual (data subject)".[13]

Berdasarkan *OECD Guidelines* yang merupakan instrumen internasional pertama yang mengatur Pelindungan Data Pribadi, Data Pribadi diartikan sebagai setiap informasi yang terkait dengan orang-perorangan (individu) yang terindentifikasi atau dapat diidentifikasi.

c. UK *Data Protection Act* 1998

"Data which relate to a living individual who can be identified: (a) from those data, or (b) from those data or other information, which is in the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual"[14].

UU Pelindungan Data Pribadi di Inggris tahun 1998 ini mendefinisikan Data Pribadi sebagai data seseorang yang hidup yang dapat diidentifikasi berdasarkan: dari data atau informasi lainnya yang berada pada kendali Pengendali Data, termasuk setiap bentuk ekspresi pandangan seseorang dan setiap indikasi atau maksud dari Pengendali Data atau terhadap orang lain terkait individu tertentu.

d. *European Union General Data Protection Regulation* (EU GDPR)

Personal data means 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 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[15].

Sementara itu menurut EU GDPR yang dianggap sebagai *Golden Rules* atau *Game Changer* dalam Pelindungan Data Pribadi di Dunia, dirumuskan pengertian Data Pribadi sebagai "setiap informasi tentang orang-perorangan yang teridentifikasi atau dapat diidentifikasi.

[13] Part one-General, Definitions 1 (b).
[14] UK Data Protection Act of 1998, Part I: Preliminary, 1 Basic Interpretation Provisions.
[15] EU GDPR, pasal 4 (1).

Seseorang yang dapat teridentifikasi adalah seseorang yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, khususnya mengacu pada hal-hal tertentu seperti: nama, nomor identifikasi, data lokasi, pengidentifikasi daring, atau beberapa faktor yang lebih spesifik seperti kondisi fisik, kondidi fisiologis, genetika, mental, ekonomi, kebudayaan atau identitas sosial dari yang bersangkutan".

2. Data Pribadi yang Bersifat Umum
   Data Pribadi yang bersifat umum meliputi namun tidak terbatas pada: nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang[16].

3. Data Pribadi yang Bersifat Spesifik (Sensitif)
   Data Pribadi yang bersifat spesifik atau sensitif dapat meliputi: data biometrik, data perbankan, catatan kesehatan, orientasi seksual, keanggotaan pada serikat pekerja, data kesehatan, pandangan politik, dan lain-lain[17].

D. Bentuk-bentuk Pelanggaran Terhadap Data Pribadi

1. Peretasan, Pencurian dan Pelanggaran atas Data Pribadi Konsumen
   Peretasan, pencurian dan pelanggaran atas Data Pribadi sangat marak terjadi di Indonesia. Beerapa kasus besar yang tercatat, antara lain:

   a. Kebocoran Data Tokopedia tahun 2020
      Pelaku menggunakan nama samaran *Shining Hunters.* Membocorkan 91 juta data pengguna Tokopedia dan 7 juta *data seller. Shining Hunters* menggunakan serangan *SQL Injection*. Terjadi karena kerentanan sistem *cloud* milik Tokopedia. Data tersebut dijual di *Dark Web*. Tokopedia mengklaim bahwa data pribadi spesifik/sensitif tetap aman.

   b. Kebocoran 26 Juta Data Pelanggan Indihome
      Data yang diduga bocor meliputi data histori penelusuran *(browsing*), KTP, email, nomor ponsel, kata kunci, domain, *platform*, dan URL.

[16] Lihat Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 4 ayat (3).

[17] Bandingkan dengan, Pasal 4 ayat (2) UU No 27 Tahun 2022 tentang Pelindungan Data Pribadi yang merumuskan bahwa Data Pribadi yang bersifat spesifik meliputi: data dan informasi kesehatan, data biometric, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan perundang-undangan.

Namun pihak Telkom menyangkal terjadinya kebocoran tersebut dengan menyatakan bahwa data yang diduga bocor tidak valid[18].

c. Kebocoran 1,3 Milyar Data Penduduk Yang Berasal Dari Pendaftaran SIM Card

Sebanyak 1,3 milyar data registrasi kartu SIM dengn kapasitas 87 GB dijual di situs gelap oleh *user BreachForums* dengan nama *Bjorka*. Mereka mematok harga US$ 50 ribu dengan menyertakan sampel data sebesar 2 GB. Diakui oleh Kominfo mengenai kecocokan data tersebut. Selanjutnya ditempuh langkah-langkah melalui kerjasama dengan: *Cyber Crime* Polri, Ditjen Dukcapil, BSSN dan seluruh operator seluler[19].

d. Kebocoran Data BPJS Kesehatan tahun 2021

Data yang bocor sebesar 22,5 juta data peserta BPJS Kesehatan. Data yang bocor meliputi: NIK, nama, alamat, nomor telepon, tanggal lahir, jenis kelamin, status pernikahan, golongan darah. Kasus terjadi karena adanya celah keamanan pada sistem informasi BPJS Kesehatan[20].

e. Kebocoran Data Polda Metro Jaya pada bulan September 2022, sebanyak 2,6 juta Data Personel POLRI dipasarkan di situs daring *"breached to*", dilakukan akun peretas bernama *"Meki"*.

f. Kebocoran 105 juta Data Penduduk dari Komisi Pemilihan Umum (KPU) pada bulan September 2022

Data dijual oleh *Hacker* berinisial *Bjorka* di laman *Breached Forum*. Data dijual dengan harga US$ 5 ribu. Semua data disimpan dalam file 20 GB *(uncompressed*) atau 4 GB *(compressed).* Data yang bocor meliputi: nama, NIK, kartu keluarga, tempat dan tanggal lahir, jenis kelamin dan umur.

g. Kebocoran Data PeduliLindungi tahun 2022

Pada bulan November 2022, 3,2 milyar data pengguna PeduliLindungi diretas oleh peretas Bjorka. Hal itu diketahui karena unggahan dalam situs

[18] Katadata.co.id, "Deretan BUMN dan Kementerian Alami Dugaan Kebocoran Data". 22 Agustus 2022, diakses tanggal 9 Juli 2024.

[19] Ditjen Aptika Kominfo, "Dugaan Kebocoran Data SIM Card, Kominfo Lakukan Koordinasi dengan Ekosistem Pengendali Data', 7 September 2022, diakses pada tanggal 9 Juli 2024.

[20] BPJS membantah serangan tersebut karena dianggap Hoaks.

Breached.to. Diantara data PeduliLindungi yang dibocorkan Bjorka dalam situs *BreachForums*, terdapat data beberapa pejabat penting dan selebritas seperti Menteri Komunikasi dan Informatika (saat itu dijabat Johny G Plate), Menko Kemaritiman dan Investasi (Luhut Binsar Pandjaitan) serta Deddy Corbuzier. Menurut Bjorka, data PeduliLindungi yang dibocorkan itu berjumlah 3.250.144.177, mencakup 48 Gigabite data terkompresi dan 157 Gigabyte data tak terkompresi. Data PeduliLindungi yang ada di tangan Bjorka meliputi data pengguna (94 Juta), akun yang diurutkan (94 juta), data vaksinasi (209 juta), riwayat check-in (1,3 milyar), dan riwayat pelacakan kontak (1,5 milyar)[21].

Bjorka menjual data Peduli Lindungi itu dengan harga US$ 100.000 (seratus ribu US dollar) dalam bentuk mata uang kripto Bitcoin.

h. Kebocoran Data Catatan Surat Presiden Joko Widodo dari Badan Intelejen Negara (BIN) pada bulan September 2022

Bjorka membocorkan rangkaian surat rahasia untuk Presiden Jokowi, termasuk dari BIN. Dari pernyataan Bjorka, dokumen yang dicuri pada September 2022 tersebut terdiri dari 679.180 data dengan kepasitas 40 MB *(compressed)* dan 189 MB *(uncompressed).* Data yang bocor meliputi: surat berjudul surat rahasia kepada Presiden dalam amplop tertutup dengan pengirim BIN dan penerima Presiden; surat rahasia kepada Mensesneg dalam amplop tetutup dengan pengirim BIN; permohonan jamuan snack dari Kepala Bagian Protokol dan Tata Usaha Pimpinan; permohonan dukungan sarana dan prasarana dengan pengirim Kepala Pusat Pendidikan dan Pelatihan; gladi bersih dan upacara bendera pada peringatan HUT ke 74 Proklamasi Kemedekaan dengan tujuan Kepala Biro Tata Usaha, dan seterusnya[22].

i. Kebocoran 15 Juta Data Nasabah dan Pegawai Bank Syariah Indonesia (BSI) Tahun 2023.

Kelompok peretas *Ransomware Lockbit 3.0* mengklaim bertanggung jawab. Dampak dari serangan tersebut mengakibatkan semua layanan

[21] Republika.co.id, "CISSRec: 3,2 Milyar Data Peduli Lindungi Bocor", 15 November 2022.

[22] BBC.Com, "Bjorka Klaim Retas Dokumen Presiden Jokowi, Pemerintah Bentuk Satgas dan Ungkap Motif," 14 September 2022.

BSI berhenti. Data lain yang diklaim dicuri adalah: dokumen keuangan, dokumen hukum hingga kata sandi *(password)* untuk semua layanan internal dan eksternal yang digunakan. Kebocoran BSI memuat sembilan (9) basis data, seperti: nama, alamat, informasi dokumen, nomor kartu, nomor telepon, transaksi[23].

j. Kasus Kebocoran Data DPT Pemilu 2024
Data diretas oleh akun *anonym "Jimbo*". Data yang bocor 204 juta dari website KPU. Dijual dengan nilai US$ 74 ribu. Data yang diretas meliputi: NIK, nomor KK, nomor paspor, nama lengkap, jenis kelamin, tanggal lahir, tempat lahir, status pernikahan dan alamat tinggal[24].

k. Serangan Ransomware Terhadap Pusat Data Nasional Sementara 2 (PDNS 2) di Surabaya pada tanggal 20 Juni 2024
Serangan *Ransomware Brain Chiper* yang merupakan varian dari *Lockbit 3.0* ini berdampak terhadap 210 instansi pemerintah, termasuk layanan imigrasi di bandara-bandara. Peretas meminta tebusan sebesar US$ 8 juta untuk memulihkan keadaan[25].

Atas kejadian ini Presiden memanggil Menteri-Menteri dan Pimpinan Lembaga yang terkait seperti Kementerian Kominfo, Badan Siber dan Sandi Negara (BSSN), Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PAN-RB), BPKP. Presiden meminta dilakukannya audit, termasuk audit forensik atas PDNS 2 untuk dicari sebab-sebab terjadinya kejadian ini serta untuk mencegah kejadian serupa terjadi di masa-masa yang akan datang.

Dalam Rapat Dengar Pendapat dengan DPR terkuak bahwa hanya 2% Data dari PDN yang punya cadangan *(back-up)* dan data yang telah tersanderakan terkategorikan hilang, termasuk Data Keimigrasian yang diserahkan ke PDN ikut tersandera[26].

---

23 Bisnis Tempo, "15 Juta Data Nasabah BSI diduga Bocor: Hati-Hati Serangan Phising", 16 Mei 2023.
24 www.bawaslu.go.id, "Bawaslu tegaskan Dugaan Kebocoran Data DPT Pemilu, 26 Februari 2024.
25 Dampak serangan Ransomware ke Pusat Data Nasional: gangguan pada sistem pelayanan publik; tingginya biaya pemulihan; resiko keamanan nasional; turunnya kepercayaan masyarakat pada Pemerintah.
26 Baca Lynda Ibrahim, "Baru Sekedar Mainan Digital", Kompas, 30 Juni 2024.

l. Data Ditjen Perhubungan Udara

Pada tanggal 6 Juni 2024 diperoleh informasi tentang kebocorn data pada Kementerian Perhubungan. Namun kebocoran data tersebut tidak terkait dengan peretasan PDNS2. Data-data yang bocor terdiri dari data pegawai hingga data penerbangan pesawat.

Setelah dilakukan pengecekan, data yang diduga mengalami kebocoran adalah data-data lama yang sudah tidak *update*, sehingga diduga kebocoran tersebut terjadi pada tahun 2022. Sebagai langkah ke depan dipersiapkan langkah-langkah memperkuat keamanan digital, termasuk: menyusun Sistem Pemerintah Berbasis Elektronik (SPBE), menyusun kebijakan satu data transportasi agar terwujud Tata Kelola Data dan Informasi di sektor transportasi; bekerjasama dengan BSSN meningkatkan keamanan *Critical Information Infrastructure*; segera memiliki *Disaster Recovery Plan (DRP);* dan *Disaster Recovery Center (DRC)*[27].

m. Data Kementerian Hukum dan Hak Aasasi Manusia (Kemenkumham)

Sebuah unggahan di Media Sosial yang viral pada tahun 2022 menampilkan adanya kebocoran data Kementerian Hukum dan Hak Asasi Manusia. Sebuah akun bernama *WaterAndCoffee* mengklaim memiliki lebih dari 85.000 data pegawai Kemenkumham dan 800 MB Data Pribadi. Data-data tersebut berisi Nomor Induk Pegawai (NIP), nama, Nomor Induk Kependudukan (NIK), ERP dan nomor rekening. Pihak Kemenkumham membantah kebocoran data tersebut karena setelah dilakukan pengecekan pada Sistem Informasi Kepegawaian (Simpeg), data tersebut adalah data arsip tahun 2020 dan bukan data krusial. Beberapa langkah yang ditempuh guna menangkal serangan siber mencakup: mengaktifkan fitur *blocking* pada *Advanced Web Application Firewall*; bekerjasama dengan BSSN membentuk *Computer Security Incident Response Team (CSIRT)*[28].

---

[27] Kompas.com, "Data Ditjen Perhubungan Udara, Kementrian Perhubungan Pastikan tidak ganggu Operasional", diakses tanggal 24 Juni 2024.

[28] Kompas.com, "Puluhan Ribu Data Pegawai Kemenkumham Diduga Bocor, Begini Penjelasannya", 28 Oktober 2022, diakses tanggal 9 Juli 2024.

n. Data Kementerian Koordinator Perekonomian (Kemenko Perekonomian)

Media Sosial diramaikan dengan unggahan yang mengklaim adanya kebocoran data pegawai Kementerian Koordinator Bidang Perekonomian. Informasi tersebut diungkap oleh akun *X (Twitter) @ anvie* pada tanggal 6 Juni 2024. Beberapa data yang tersebar memuat nomor rekening, nomor pokok wajib pajak (NPWP), dan daftar gaji. Kebocoran data tersebut dibenarkan oleh Kemenko Perekonomian, namun sudah dapat ditangani dengan baik dan dilakukan tindakan pencegahan[29].

o. Data Badan Usaha Milik Negara (BUMN)

Jutaan data pelanggan Perusahaan Listrik Negara (PLN), Indihome, Telkom juga mengalami kebocoran data. Lebih dari 17 juta data pelanggan PLN bocor sebagaimana diunggah laman *web breached. to* dengan akun bernama *"lolyta*" yang menjual data pribadi tersebut. Data-data yang dijual antara lain: ID lapangan, ID Pelanggan, nama pelanggan, tipe energi, *Kilo Watt Hour* (KWH), alamat rumah, nomor meteran, tipe meteran hingga nama unit UPI.

p. Data Aparatur Sipil Negara (ASN) Diretas dan Dijual di Darkweb

Peretasan dilakukan oleh oleh *Pseudonym TopiAx* yang mengklaim telah meretas 4,7 juta data ASN yang dijual di *Hacking Site Breach Forums*. Peretasan tersebut diketahui oleh *The Communication and Information System Security Research Center* (CISSRec) pada tanggal 12 Agustus 2024[30].

q. Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) pada Direktorat Jendral Pajak

Pada tanggal 18 September 2024 terjadi kebocoran data NPWP. Total data yang bocor sebanyak 6.663.379 yang dijual oleh peretas dengan nilai US$ 15.000 atau setara dengan Rp 153 juta. Data yang bocor, antara lain: Nomor Induk Kependudukan (NIK), NPWP, alamat, nomor

[29] Kompas.com, "Data Pegawainya disebut Bocor dan Beredar di Dark Web, Ini Penjelasan Kemenko Perekonomian", 11 Juni 2024, diakses pada tanggal 9 Juli 2024.

[30] Jakarta Post, "Fresh Breach Presses Government to form Data Privacy Agency", 14 Agustus 2024.

telepon seluler, email, status wajib pajak dan asal kantor pelayanan pajaknya. Ukuran data yang dibocorkan 2 Gigabites dan terkompresi menjadi 500 Megabites. NPWP yang tersebar meliputi Presiden dan Keluarganya serta Menteri dan Pejabat Negara lainnya[31].

Dari tahun 2019 hingga tahun 2024 Kementerian Komunikasi dan Informasi telah menangani sekitar 124 kasus dugaan pelanggaran data pribadi[32]. Sebanyak 111 kasus di antaranya tergolong kasus kebocoran data pribadi.

Setiap kasus kebocoran bisa melibatkan hingga ratusan juta data pribadi penduduk. Mayoritas kasus kebocoran data yang ditangani merupakan kumpulan data pribadi yang tidak dienkripsi. Kasus ini antara lain dialami penyelenggara sistem elektronik (PSE) lingkup publik. Dari kasus-kasus yang ada hanya 2 (dua) kasus yang ternyata data pribadi yang dikumpulkan telah melalui proses enkripsi[33].

Sejak tahun 2019 terdapat kecenderungan kenaikan kasus yang ditangani dari tahun ke tahun, dari 3 kasus tahun 2019, 21 kasus tahun 2020, 20 kasus tahun 2021, 35 kasus pada tahun 2022, dan 40 kasus pada tahun 2023. Dari Januari-14 Mei 2024 terdapat 5 kasus[34].

Rincian dari kasus-kasus tersebut terdiri dari: 111 kasus kebocoran data, 4 kasus terkait pengumuman data pribadi yang diduga tanpa persetujuan subjek data, 2 kasus pengungkapan data pribadi kepada pihak yang tidak sah, 3 kasus pengumpulan data pribadi yang tidak relevan dengan tujuan pemrosesan data, dan 4 kasus pelanggaran lainnya[35].

Dari sisi jenis PSE, 124 kasus dugaan pelanggaran pelindungan data pribadi yang ditangani Kementerian Kominfo berasal dari PSE privat sebanyak 85 kasus dan PSE publik sebanyak 39 kasus. Sementara itu terkait tahapan, 97 kasus selesai ditangani dan 27 kasus

---

31 Kompas, Kemenkominfo Usut Kebocoran Data Wajib Pajak", 23 September 2024.

32 Berita Kompas, "Kemenkominfo Tangani 124 Kasus Dugaan Pelanggaran Data Pribadi", 4 Juni 2024.

33 Ibid.

34 Ibid.

35 Ibid.

masih dalam proses penanganan[36]. Landasan hukum yang digunakan dalam penanganan kasus-kasus di atas masih berdasarkan Peraturan Kementerian Kominfo No 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Sanksi yang dikenakan bersifat administratif, dari peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, dan/atau pengumuman di laman.

Meskipun UU tentang Pelindungan Data Pribadi berlaku baik bagi sektor publik maupun sektor privat, namun dalam prakteknya masih terdapat perbedaan perlakuan, khususnya terkait dengan denda administratif yang baru dikenakan pada sektor privat, sementara belum ada kejelasan tentang sanksi serupa apabila pelanggaran itu dilakukan oleh institusi pemerintahan

2. Pencurian atas Data Pribadi sebagai bagian dari Tindak Pidana lainnya
   Tindakan kriminal berupa pencurian atas data pribadi dilakukan dengan menggunakan berbagai modus operandi, seperti: *phising, hacking, advance persistent threat (APT), Ransomware,* dan lain-lain. Melalui pencurian Data Pribadi, maka pelaku tindak pidana siber dapat menggunakan data tersebut untuk melakukan tindak pidana lainnya, meliputi, antara lain: memindahkan uang dari akun korban ke akun yang disiapkan pelaku; melakukan kejahatan asuransi; menggunakan data kesehatan yang dicuri untuk melakukan *assassination* (pembunuhan); dan lain-lain.

3. Pemalsuan Identitas
   Pemalsuan identitas juga banyak dilakukan oleh pelaku tindak pidana siber dengan maksud untuk menutupi identitas yang sebenarnya sehingga menyulitkan upaya pengungkapan tindak pidana yang dilakukan.

4. Penipuan dalam berbagai Dimensinya
   Banyak kegiatan penipuan di dunia siber dilakukan dengan menggunakan Data Pribadi yang diperoleh secara melawan hukum.

[36] Ibid.

5. *Doxing*

   Doxing adalah sebuah tindakan berbasis internet untuk meneliti dan menyebarluaskan informasi publik secara sepihak terhadap seorang individu atau organisasi. Metode ini digunakan untuk memperoleh informasi, termasuk mencari basis data yang tersedia untuk umum dan situs sosial media, meretas dan merekayasa sosial (Wikipedia).

   Yang menjadi sasaran dapat berupa informasi seperti nama asli korban, alamat rumah, tempat kerja, nomor telepon, informasi keuangan dan rincian informasi pribadi lainnya. Doxing merupakan tindakan yang melanggar, baik Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) maupun Undang-Undang Pelindungan Data Pribadi (UU PDP).

6. *Spoofing*

   Spoofing adalah bentuk kejahatan siber dengan modus penyamaran informasi sehingga pelaku seakan-akan sebagai pihak yang berwenang seperti dari bank atau institusi lainnya untuk memperoleh akses secara tidak sah ke suatu komputer, telepon seluler atau *handphone, email* maupun sistem informasi. Tujuannya adalah untuk mencuri data korban.

7. Soceng *(Social Engineering)*

   Adalah istilah yang digunakan bagi berbagai kegiatan jahat yang dilakukan melalui interaksi manusia. Dilakukan dengan menggunakan manipulasi psikologis untuk menjebak penggunanya sehingga melakukan kesalahan terkait keamanan data atau memberikan informasi sensitif. Serangan Soceng terjadi melalui satu langkah atau lebih.

E. Urgensi Pengaturan

Berdasarkan uraian di atas tentang pentingnya pengaturan Privasi, khususnya pelindungan Data Pribadi serta dengan memperhatikan berbagai kasus pelanggaran atau kejahatan terhadap Data Pribadi, maka memang terdapat urgensi untuk mengatur pelindungan Data Pribadi dalam suatu Undang-Undang. Adapun beberapa alasan pokok yang memperkuat urgensi tersebut, antara lain:

1. Belum Adanya Aturan yang Bersifat Spesifik dan Komprehensif tentang Pelindungan Data Pribadi

   Sebelum adanya Undang-Undang No 27 tahun 2022 tentang Pelindungan Data Pribadi pengaturan tentang Pelindungan Data Pribadi tersebar dalam berbagai peraturan perundang-undangan.

   Peraturan-peraturan tersebut bersifat parsial dan tersebar meliputi namun tidak terbatas pada:

   a. UU No 11 tahun 2008 sebagaimana diubah dengan UU No 19 tahun 2016 dan terakhir dengan UU No. 1 tahun 2024 tentang Informasi dan Transaksi Elektronik

      Pasal 26 ayat (1) UU tentang ITE menyatakan:

      "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan". Ketentuan ini menekankan tentang pentingnya persetujuan (*consent*) dari Subjek Data Pribadi atas penggunaan data pribadinya.

      Sementara itu ketentuan Pasal 26 ayat (2) menetapkan bahwa: "Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini".

   b. UU No 14 tahun 2008 tentang Keterbukaan Informasi Publik

      Pasal 6 ayat (3): "Informasi Publik yang tidak dapat diberikan oleh Badan Publik, sebagaimana dimaksud pada ayat (1) adalah:

      – Informasi yang dapat membahayakan Negara
      – Informasi yang berkaitan dengan kepentingan perlindungan usaha dan persaingan usaha tidak sehat
      – Informasi yang berkaitan dengan hak-hak pribadi
      – Informasi yang berkaitan dengan hak-hak jabatan; dan/atau
      – Informasi Publik yang diminta belum dikuasai atau didokumentasikan".

c. UU No 23 tahun 2006 sebagaimana diubah dengan UU No 24 tahun 2013 tentang Administrasi Kependudukan.
Pasal 95 A UU No 24 tahun 2013 menyatakan: "Setiap orang yang tanpa hak menyebarluaskan Data Kependudukan sebagaimana dimaksud dalam pasal 79 ayat (3) dan Data Pribadi sebagaimana dimaksud dalam pasal 86 ayat (1a) dipidana dengan pidana penjara paling lama 2 tahun dan/atau denda paling banyak Rp 25 juta rupiah".

d. UU No 36 tahun 1999 tentang Telekomunikasi
Pasal 40: "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun"

Pasal 36: "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun".

e. UU No 7 tahun 1992 sebagaimana diubah dengan UU No 10 tahun 1998 tentang Perbankan
Pasal 40 ayat (1): "Bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, kecuali sebagaimana dimaksud dalam Pasal 41, Pasal 41 A, Pasal 42, Pasal 44 dan Pasal 44 A"

Pasal 41 ayat (1): "Untuk kepentingan Perpajakan, Pimpinan Bank Indonesia atas Permintaan Kementerian Keuangan berwenang memberikan perintah tertulis kepada bank agar memberikan keterangan dan memperlihatkan bukti-bukti tertulis serta surat-surat mengenai keadaan keuangan Nasabah Penyimpan tertentu kepada pejabat bank "

Pasal 41 A ayat (1): "Untuk penyelesaian piutang bank yang sudah diserahkan kepada Badan Urusan Piutang dan Lelang Negara/Panitia Urusan Piutang Negara, Pimpinan Bank Indonesia memberikan izin kepada pejabat Badan Urusan Piutang dan Lelang Negara /Panitya Urusan Piutang Negara, untuk memperoleh keterangan dari bank mengenai Nasabah Debitur"

Pasal 42 ayat (1): Untuk kepentingan peradilan dalam perkara pidana, Pimpinan bank Indonesia dapat memberikan izin kepada polisi,

jaksa atau hakim untuk memperoleh keterangan dari bank mengenai simpanan tersangka atau terdakwa pada bank"

Pasal 44 ayat (1): "Dalam rangka tukar menukar informasi antar bank, direksi bank dapat memberitahukan keadaan keuangan nasabahnya kepada bank lain"

Pasal 44 A ayat (1): "Atas permintaan, persetujuan atau kuasa dari Nasabah Penyimpan yang dibuat secara tertulis, bank wajib memberikan keterangan mengenai simpanan Nasabah Penyimpan pada bank yang bersangkutan kepada pihak yang ditunjuk oleh Nasabah Penyimpan tersebut"

f. PP No 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Pasal 14 ayat (1): "Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi, meliputi:

- Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik (subjek) data pribadi.
- Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya.
- Pemrosesan Data Pribadi dilakukan dengan menjamin hak pemilik Data Pribadi.
- Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi.
- Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi.
- Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan Data Pribadi; dan

– Pemrosesan Data Pribadi dimusnakahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

g. PP No 80 tahun 2019 tentang Perdagangan Melalui Sistem Elektronik
Pasal 58: "(1). Setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau pelaku usaha yang bersangkutan. (2). Setiap pelaku usaha yang memperoleh data pribadi sebagaimana dimaksud pada ayat (1) wajib bertindak sebagai pengemban amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundang-undangan"

Pasal 59: "(1). Pelaku Usaha wajib menyimpan data pribadi sesuai standar perlindungan data pribadi atau kelaziman praktik bisnis yang berkembang. (2). Standar perlindungan data pribadi atau kelaziman sebagaimana dimaksud pada ayat (1) paling sedikit memenuhi kaidah perlindungan (prinsip perlindungan data pribadi), dst. (3). Dalam hal pemilik data pribadi menyatakan keluar, berhenti berlangganan atau berhenti menggunakan jasa dan sarana PMSE, maka pemilik data pribadi berhak meminta Pelaku Usaha untuk menghapus seluruh data pribadi yang bersangkutan. 4). Atas permintaan pemilik data pribadi sebagaimana dimaksud pada ayat (3), Pelaku Usaha harus menghapus data pribadi yang bersangkutan pada sistem yang dikelola Pelaku Usaha tersebut".

h. Permenkominfo No 20 tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik
Peraturan ini mengatur hal-hal meliputi: ketentuan umum; perlindungan (prinsip-prinsip); hak pemilik data pribadi; kewajiban pengguna; kewajiban penyelenggara sistem elektronik; penyelesaian sengketa; peran pemerintah dan masyarakat; pengawasan; sanksi administratif; ketentuan lain; ketentuan peralihan; dan ketentuan penutup.

i. Permenkominfo No 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi
Ketentuan-ketentuan pokok yang diatur dalam peraturan ini mencakup: Ketentuan Umum; Kategorisasi Sistem Elektronik; Standard Sistem

Manajemen Pengamanan Informasi; Penyelenggaraan; Lembaga Sertifikasi; Penerbitan Sertifikat, Pelaporan Hasil Sertifikasi, dan Pencabutan Sertifikat; Penilaian Mandiri; Pembinaan; Pengawasan; Sanksi; Ketentuan Peralihan; dan Ketentuan Penutup.

Dalam kaitan dengan Pelindungan Data Pribadi, salah satu aspeknya adalah keamanan data. Standard yang digunakan dalam keamanan data mengacu pada ISO 27001.

j. Permenkominfo No 5 tahun 2020 sebagaimana diubah dengan Permenkominfo No 10 tahun 2021 tentang Penyelenggaraan Sistem Elektronik Sektor Privat. Ketentuan-ketentuan pokok yang diatur meliputi: Ketentuan Umum; Pendaftaran Penyelenggara Sistem Elektronik Lingkup Privat; Tata Kelola dan Moderasi Informasi Elektronik dan/atau Dokumen Elektronik; Permohonan Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang Dilarang; Pemberian Akses terhadap Sistem Elektronik dan/atau Data Elektronik untuk Kepentingan Pengawasan dan Penegakan Hukum Pidana; Ketentuan Peralihan; Ketentuan Penutup.

   Ketentuan Pasal 43 ayat (2) dan Pasal 44 ayat (2) intinya menyatakan bahwa PSE lingkup privat dapat melakukan penilaian *(assessment)* mengenai dampak penggunaan akses terhadap Sistem Elektronik oleh Kementerian atau aparat penegak hukum terhadap: Pelindungan Data Pribadi dari Pengguna Sistem Elektronik.

k. Permenkominfo No 5 tahun 2021 tentang Penyelenggaraan Telekomunikasi

   Inti ketentuan Pasal 169 adalah terkait dengan kewajiban penyelenggara jasa telekomuikasi untuk menyampaikan laporan tiap 3 bulan terkait dengan data pelanggan jasa telekomunikasi prabayar aktif dan data pelanggan jasa telekomunikasi pasca bayar aktif. Dalam laporan tersebut paling sedikit memuat: identitas pelanggan jasa telekomunikasi yang melakukan registrasi, dan nomor MSISDN.

   Inti ketentuan Pasal 170 adalah kewajiban penyelenggara jasa telekomunikasi untuk menyediakan pusat data pelanggan jasa

telekomunikasi aktif secara real time terhubung dengan sistem monitoring registrasi Kementerian.

l. Peraturan Bank Indonesia (PBI) No 18 tahun 2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran
Ketentuan Pasal 34 huruf b menyatakan: Penyelenggara data dan informasi nasabah dilarang menyalahgunakan data dan informasi nasabah maupun data dan informasi transaksi pembayaran.

m. Peraturan Otoritas Jasa Keuangan (POJK) No 1 tahun 2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan
Peraturan ini terdiri dari: Ketentuan Umum; Ketentuan Perlindungan Konsumen Sektor Jasa Keuangan; Pengaduan Konsumen dan Pemberian Fasilitas Penyelesaian Pengaduan oleh Otoritas Jasa Keuangan; Pengendalian Internal; Pengawasan Perlindungan Konsumen Sektor Jasa Keuangan; Sanksi; Ketentuan Peralihan dan Ketentuan Penutup.

Ketentuan Pasal 31 dari POJK ini menyatakan bahwa Pelaku Usaha Jasa Keuangan dilarang dengan cara apapun, memberikan data dan/atau informasi mengenai konsumennya kepada pihak ketiga. Larangan tersebut dikecualikan dalam hal konsumen memberikan persetujuan tertulis dan/atau diwajibkan oleh peraturan perundang-undangan.

n. Surat Edaran (SE) OJK No 14 tahun 2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen
SE OJK ini berisi ketentuan-ketentuan tentang: Ketentuan Umum; Perlindungan Data dan/atau Informasi Pribadi Konsumen; Ketentuan lain-lain; Ketentuan Peralihan; dan Ketentuan Penutup.

Inti dari Perlindungan Data dan/atau Informasi Pribadi Konsumen adalah berupa larangan dengan cara apapun untuk memberikan data dan/atau informasi pribadi mengenai Konsumen kepada pihak ketiga, kecuali konsumen memberikan persetujuan tertulis, atau diwajibkan oleh peraturan perundang-undangan.

2. Untuk memfasilitasi *Cross Border Data Flow*
Meningkatnya volume perdagangan, investasi dan keuangan yang bersifat lintas batas nasional mempunyai konsekuensi dibutuhkannya lintas batas

data, termasuk lintas batas Data Pribadi. Kebutuhan lintas batas Data Pribadi perlu diakomodasikan melalui pengaturan, baik untuk kepentingan transfer data keluar Indonesia maupun dari luar ke Indonesia. Salah satu pertimbangan utamanya adalah untuk memastikan bahwa transfer Data Pribadi yang bersifat lintas batas nasional tersebut tidak merugikan kepentingan Subjek Data Pribadi.

3. Untuk menyesuaikan dengan Standard Internasional
   Pengaturan tentang Pelindungan Data Pribadi tersebar diberbagai Negara dan Kawasan. Standard yang berlaku tentu saja dikaitkan dengan karakteristik dan kebutuhan masing-masing negara atau kawasan. Saat ini pengaturan tentang Pelindungan Data Pribadi lebih dari 100-an Negara. Standard yang dianggap paling tinggi adalah apa yang berlaku di Uni Eropa, yaitu EU GDPR. Oleh karena itu banyak negara yang menjadikan EU GDPR sebagai rujukan *(benchmark)* dalam pengembangan pengaturan tentang Pelindungan Data Pribadi.

   Di samping EU GDPR, beberapa Kawasan lain juga memiliki standard dan aturan bersama seperti OECD, APEC, dan termasuk ASEAN. Dari standard yang berlaku secara internasional dapat ditarik unsur-unsur bersama *(common elements*) nya.

   Dengan mengacu pada *common elements* tersebut negara-negara (termasuk Indonesia) merumuskan aturan nasionalnya tentang Pelindungan Data Pribadi. Keuntungan dari pengaturan nasional yang sesuai dengan standard internasional adalah kemudahan dalam melakukan transfer data dari dan ke Indonesia, dengan demikian juga akan mampu memfasilitasi dunia usaha dalam melakukan komunikasi dan transaksi internasional. Hal yang sama juga berlaku bagi Negara.

4. Untuk Keseimbangan antara PDP dengan Hak-Hak Negara atas Data Pribadi
   Di satu sisi Pelindungan Data Pribadi pada dasarnya merupakan implementasi dari pelindungan terhadap hak-hak asasi manusia, khususnya terkait dengan privasi data. Pada sisi yang lain perlu ada keseimbangan dengan hak-hak Negara untuk memproses data pribadi untuk kepentingan

tertentu (keamanan nasional, kepentingan umum, keselamatan umum, dan lain-lain). Melalui keseimbangan tersebut, maka baik kepentingan Subjek Data Pribadi maupun kepentingan Negara akan dapat diakomodasikan secara harmonis dan proporsional.

F. Pentingnya PDP Bagi Dunia Usaha

Pelindungan Data Pribadi bukan semata-mata bentuk pelindungan terhadap data/informasi pribadi sebagai wujud penghormatan terhadap hak-hak asasi manusia, namun juga harus mampu mendorong *transboundary flow of personal data* yang diperlukan bagi dunia usaha. Oleh karena itu dapat dikatakan bahwa pelindungan data pribadi adalah baik bagi kepentingan dunia usaha. Ada beberapa alasan yang mendukung hal itu, antara lain:

1. Meningkatkan Kepercayaan Konsumen

   Melalui *Privacy Policy* yang melindungi Data Pribadi Konsumen, maka akan meningkatkan kepercayaan konsumen untuk memberikan persetujuan datanya dikumpulkan dan diproses. Hal ini juga menunjukkan transparansi yang diterapkan dalam pemrosesan dan penggunaan Data Pribadi Konsumen sesuai dengan peruntukannya. Meningkatnya kepercayaan konsumen pada akhirnya akan berdampak pada meningkatnya transaksi oleh konsumen serta juga meningkatnya reputasi korporasi.

2. Memiliki Keamanan Data yang Lebih Baik

   Pelanggaran terhadap keamanan data merupakan ancaman yang besar bagi korporasi. Melalui pengembangan sistem pelindungan data pribadi secara otomatis juga akan meningkatkan keamanan data. Melalui pembatasan akses data, termasuk *critical data*, hanya kepada beberapa professional di dalam korporasi/organisasi, maka akan lebih memastikan bahwa data tersebut tidak jatuh ke tangan yang salah yang berpotensi menyalahgunakannya.

3. Mengurangi Biaya Pemeliharaan

   Dengan mematuhi prinsip-prinsip Pelindungan Data Pribadi, maka akan secara signifikan mengurangi biaya pengumpulan data dengan

mengkonsolidasikan informasi yang sebelumnya disimpan dalam format yang inkonsisten menjadi format yang lebih konsisten dan mudah diakses serta digunakan.

4. Senantiasa Beradaptasi dengan Teknologi yang Berkembang
   Melalui kebijakan dan implementasi Pelindungan Data Pribadi, maka otomatis juga akan beradaptasi dengan berbagai teknologi baru seperti virtualisasi, *cloud computing, internet of things, artificial intelligence, big data, block chain*, yang pada akhirnya akan mampu mengelola secara lebih baik peningkatan kebutuhan akan data, disamping itu juga membuka kemungkinan yang lebih luas untuk menawarkan jasa kepada *end users* produk, jasa dan proses yang *augmented*.
5. Meningkatkan Pengambilan Putusan yang Lebih Baik
   Berdasarkan prinsip-prinsip Pelindungan Data Pribadi yang memberikan hak bagi subjek data untuk melakukan intervensi terhadap data pribadinya, maka akan mengurangi potensi pengambilan putusan yang keliru atau bermasalah.

BAB II

PELINDUNGAN DATA PRIBADI PADA TATARAN INTERNASIONAL SEBAGAI ACUAN

Sebagaimana yang telah disampaikan pada Bab I, Pengaturan tentang Pelindungan Data Pribadi di Indonesia mengacu pada berbagai standar internasional yang berlaku di Eropa, APEC, ASEAN, Amerika dan beberapa negara. Pengaturan Nasional dirumuskan berdasarkan *best practices* dan *common practices* yang berlaku pada tataran internasional. Pengaturan nasional yang berstandar internasional pada akhirnya akan memudahkan pelindungan Data Pribadi, baik dalam lingkup nasional maupun internasional.

A. Di Eropa

1. *OECD Guidelines 1980 on the Protection of Privacy and Transborder Flow of Personal Data 2013*

   OECD *Guidelines* 1980 merupakan prinsip-prinsip pertama tentang perlindungan privasi yang disepakati secara internasional. Prinsip-prinsipnya dirumuskan secara singkat namun padat dengan menggunakan bahasa yang bersifat netral teknologi yang secara signifikan memengaruhi kebijakan dan legislasi tentang pelindungan privasi baik bagi negara-negara anggota OECD maupun di luar negara-negara anggota OECD. Meskipun berbentuk *softlaw*

namun OECD *Guidelines* telah menjadi acuan dan dasar bagi pengembangan pengaturan tentang pelindungan *privacy* dan data pribadi.

Terdapat 4 (empat) pesan utama dari OECD *Guidelines*, yaitu: privasi adalah merupakan kunci bagi tumbuhnya kepercayaan dalam pengumpulan dan penggunaan data; privasi dan pelindungan data merupakan komponen yang esensial dari kebijakan digital; perkembangan teknologi yang meningkatkan perlindungan privasi dan data pribadi membutuhkan pedoman untuk menangani tantangan-tantangan regulasi, teknis, dan pengadopsiannya; akses pemerintah terhadap privasi dan data pribadi perlu dibatasi secara adil dan wajar.

OECD *Guidelines* ditetapkan sebagai sebuah rekomendasi dari OECD *Council* untuk mendukung prinsip-prinsip yang mengikat Negara-negara anggotanya, yaitu: demokrasi yang pluralistik, penghormatan terhadap hak-hak asasi manusia, serta ekonomi pasar terbuka.

Prinsip-prinsip yang diatur dalam OECD *Guidelines* mempunyai karakteristik: mengandung kejelasan dan fleksibilitas dalam rumusan dan penerapannya yang secara umum cukup luas sehingga mampu beradaptasi dengan perubahan teknologi. Prinsip-prinsip yang terkandung di dalamnya mencakup semua media terkait pemrosesan data individu, mencakup semua tipe pemrosesan data serta mencakup semua kategori data. Dalam kenyataannya prinsip-prinsip yang terkandung dalam OECD *Guidelines* telah diterapkan baik pada tataran nasional dan internasional[37]. OECD *Guidelines* 1980 ditindaklanjuti dengan *Declaration on Transborder Data Flows 1985 dan Ministerial Declaration on the Protection of Privacy of Global Networks 1998*.

Struktur OECD *Guidelines* terdiri dari beberapa bagian, yaitu: Umum (*General*) berisi beberapa definisi yang relevan serta cakupan berlakunya; Prinsip-prinsip Dasar dan Penerapan secara Nasional (*Basic Principles of National Application*); Prinsip-prinsip Dasar dan Penerapan pada Lingkup Internasional: Kebebasan Arus Data dan Pembatasan yang Sah (*Basic Principles of International Application*): *Free Flow and Legitimate Restrictions*);

[37] Lihat OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, www.oecd-library.org.

Implementasi Nasional (*National Implementation*); Kerjasama Internasional (*International Cooperation*). OECD *Guidelines* juga dilengkapi dengan *Explanatory Memorandum*.

a. Prinsip-Prinsip Dasar

   Beberapa Prinsip Dasar yang terkandung dalam OECD *Guidelines*, yaitu:

   – *Collection Limitation Principle*

     Berdasarkan prinsip ini harus ada pembatasan terhadap pengumpulan Data Pribadi dan Data tersebut harus diperoleh dengan cara-cara yang sah dan fair, dan sejauh mungkin atas dasar pengetahuan atau persetujuan Subjek Data Pribadi.

   – *Data Quality Principle*

     Data Pribadi harus relevan dengan tujuan-tujuan untuk mana data tersebut akan digunakan sejauh diperlukan bagi tujuan-tujuan tersebut dan harus akurat, lengkap dan mutakhir.

   – *Purpose Specification Principle*

     Data Pribadi dikumpulkan dan diproses hanya untuk maksud-maksud tertentu dan dibatasi penggunaannya terbatas sesuai dengan tujuan pengumpulan dan pemrosesannya

   – *Use Limitation Principle*

     Data Pribadi tidak dapat diungkap atau disediakan untuk maksud-maksud yang tidak sesuai dengan apa yang secara spesifik disepakati, kecuali atas persetujuan Subjek Data Pribadi atau atas dasar peraturan perundangan yang berlaku.

   – *Security Safeguards Principle*

     Data Pribadi harus dilindungi melalui langkah-langkah pengamanan terhadap kemungkinan terjadinya resiko seperti hilang atau akses tanpa wewenang, perusakan, penggunaan, modifikasi atau pengungkapan data secara tidak sah.

   – *Openness Principle*

     Harus ada kebijakan umum tentang keterbukaan dalam pengembangan praktek dan kebijakan terkait Data Pribadi. Harus

ada cara-cara informasi tentang eksistensi dan sifat Data Pribadi, tujuan penggunaannya, identitas dan tempat kedudukan Pengendali Data.

– *Individual Participation Principle*
  Subjek Data Pribadi memiliki hak untuk memperoleh informasi dari Pengendali Data apakah Pengendali Data memiliki datanya. Informasi atas Data Pribadi tersebut agar dapat diperoleh dalam jangka waktu yang wajar, apabila ada biaya tidaklah berlebihan, dengan cara yang sewajarnya, dalam wujud yang dapat dibaca. Jika ada penolakan dari Pengendali Data terhadap informasi Subjek Data Pribadi, agar diberikan alasan. Subjek Data juga memiliki hak untuk menghapus, memperbaiki, melengkapi atau mengubahnya.
– *Accountability Principle*
  Pengendali Data mempunyai kewajiban dan tanggung jawab untuk mematuhi prinsip-prinsip di atas melalui tindakan-tindakan yang nyata.

b. Revisi terhadap OECD *Guidelines*
  Pada saat peringatan 30 tahun OECD *Guidelines*, terdapat kesepakatan bahwa *Guidelines* membutuhkan revisi. Sebagai tindak lanjutnya pada tanggal 3 September 2013 OECD mempublikasikan versi revisi atas OECD *Guidelines* 1980. Terdapat 2 (dua) tema utama dari OECD *Guidelines* yang telah direvisi. Pertama, lebih difokuskan pada implementasi praktis dari Pelindungan Data Pribadi melalui pendekatan yang berbasis manajemen resiko. Kedua, adanya kebutuhan akan upaya yang lebih besar untuk mencakup dimensi Pelindungan Data Pribadi yang lebih global melalui perbaikan atas sistem *interoperability* nya.

  Daripada melakukan perubahan fundamental terhadap OECD *Guidelines*, revisi lebih diarahkan untuk memperkenalkan sejumlah konsep baru, seperti: *privacy management programmes, security breach notification, national privacy strategies, education and awareness*, serta *global interoperability*. Beberapa Aspek-aspek yang dimutakhirkan

dalam revisi menyangkut: *accountability, trans-border data flows*, dan *enforcement*.

Revisi atas *Guidelines* dimaksudkan untuk dapat digunakan sebagai dasar bagi legislasi nasional Negara-negara anggotanya, baik berupa legislasi baru maupun legislasi yang merupakan penyempurnaan dari yang sudah ada. Perubahan ini diharapkan diterima secara terbuka oleh kalangan dunia usaha karena adanya beberapa fleksibilitas, sehingga tidak bersifat "*one size fits all*"[38].

2. *The Council of Europe Convention of Personal Data Protection 1981* sebagaimana diubah menjadi *Convention 108* tahun 2018

Perjanjian awalnya dinegosiasikan pada tahun 1980 dan diadopsi pada tahun 1981. Konvensi ini dianggap sebagai instrumen internasional pertama yang bersifat mengikat yang melindungi individu atas penyalahgunaan Data Pribadinya terkait pemrosesan Data[39].

Pengadopsian Konvensi 108 didorong oleh kemajuan yang sangat pesat di bidang teknologi yang membutuhkan aturan yang lebih rinci untuk melindungi data pribadi individu. Disadari terjadinya defisiensi yang lebar terkait Pelindungan Data Pribadi dari perkembangan "*Electronic Data Banks*" ketika melibatkan perkembangan teknologi seperti *cloud computing* dan *storage*. Untuk menindaklanjutinya dihasilkan 2 (dua) resolusi, yaitu:

– Resolusi (73) 22 tentang pelindungan privasi individu *vis-à-vis electronic data banks* pada sektor privat.
– Resolusi (74) 29 tentang pelindungan privasi individu *vis-à-vis electronic data banks* pada sektor publik.

Pada tahun 2010 dibentuk "*Consultative Committee*" untuk merevisi Konvensi. Versi Konvensi yang baru dibuka untuk penandatanganan pada akhir tahun 2018. Alasan pemutakhiran Konvensi 108 didorong oleh adanya

38 Untuk analisis mengenai revisi terhadap OECD Guidelines, baca: Monika Kuschewksy, "Does the Revision of the OECD Privacy Guidelines Means for Business", dalam mLex AB EXTRA. Sebagaimana dikutip I B R Supancana dalam, Cyber Ethics dan Cyber Law: Kontribusinya bagi Dunia Bisnis, Penerbit Unika Atma Jaya, 2020, halaman 94-95.

39 Untuk selengkapnya, baca: Cecile de Terwagne, "Privacy and Personal Data Protection in Europe's Convention 108 + The European Union's GDPR", dalam Gloria Gonzales Fuster, Rosamunde van Brakel, dan Paul de Hert (Eds), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Edward Elgar Publisher, Cheltenham, UK, 2022, halaman 10-35.

kebutuhan untuk menyesuaikan dengan GDPR yang dibentuk oleh tatanan supranasional di Eropa, yaitu EU.

Karena berisi banyak ide-ide mendasar, *Convention 108* sering menjadi dasar bagi penyusunan legislasi tentang Pelindungan Data Pribadi di berbagai Negara, bahkan ada yang menyatakannya sebagai pendahulu dari EU GDPR. Oleh karenanya tidak mengherankan jika *Convention 108* memiliki berbagai persamaan dengan EU GDPR. Pentingnya *Convention 108* ditunjukkan dengan fakta bahwa *Convention 108* mampu menjembatani dicapainya *adequacy decisions* antara negara-negara anggota EU GDPR dengan Negara Ketiga. Menurut *recital 105* dari EU GDPR, aksesi terhadap *Convention 108* akan menjadi pertimbangan untuk mencapai tingkat *adequacy decisions*. Tidaklah mengherankan jika ada yang mengatakan bahwa jika EU GDPR merupakan *Gold Rules*, maka *Convention 108* dianggap sebagai *Global Standard* dalam pelindungan data pribadi.

3. *EC Directives 94/95*

   a. *Directives* ini meletakkan suatu kerangka regulasi guna menyeimbangkan antara pelindungan privasi individu tingkat tinggi dengan kebebasan pergerakan data pribadi bagi negara-negara anggota EU.

   b. Prinsip-prinsip yang diletakkan
      - *lawful and fair processing of personal data*
      - *specific, explicit and valid consent of data collection and processing in accordance with its purpose*
      - *sufficient and relevant data collection and processing*
      - *accurate and updated*
      - *data storage within reasonable time*

   c. Pada bulan Mei 2009 Komisi Eropa memulai suatu proses untuk melakukan *review* terhadap kerangka hukum di Eropa menyangkut Pelindungan Data Pribadi untuk menyesuaikan dengan perkembangan teknologi dan globalisasi. Disimpulkan bahwa prinsip-prinsip yang terdapat pada *EU Directives* masih valid namun perlu difokuskan kepada aspek implementasi dari prinsip-prinsip tersebut.

d. Peta jalan bagi masa depan pelindungan privasi atas data pribadi dirumuskan antara lain: mendukung penerapan standar global sesuai dengan Resolusi Madrid 2009, termasuk *privacy by design* sebagai suatu kewajiban bagi semua aktor pada sektor *information and communication technology*; memberdayakan warganegara masing-masing dengan kemampuan untuk melakukan penegakan hukum atas aturan-aturan tentang *privacy*; termasuk penerapan gugatan *class action* serta menggunakan mekanisme *Alternative Dispute Resolution* (ADR).

4. *European Union General Data Protection Regulation* (EU GDPR) 2016

a. Pentingnya EU GDPR sebagai *Golden Rules* dan *Game Changer*
EU GDPR telah efektif berlaku sejak 25 Mei 2018. EU GDPR meletakkan Standar yang sangat tinggi (*golden rules*) dalam Pelindungan Data Pribadi dan juga merupakan *a "game changer"*. Berlaku tidak hanya kepada anggota EU, tapi juga terhadap mitra dagang (*counter part*)nya.

b. Karakteristik
EU GDPR mempunyai beberapa karakteristik yang juga menjadi benchmark dalam proses legislasi nasional di berbagai Negara. Ada beberapa karakteristik yang perlu dicermati, yaitu[40]:
- merupakan instrumen tunggal
- memperluas berlakunya ke luar anggota EU
- Menambah Klasifikasi Data Sensitif/Spesifik
- Menegaskan perlunya *explicit consent*
- Menambah kewajiban-kewajiban bagi Pengendali Data dan Pemroses Data
- Kepatuhan terhadap EU GDPR harus dapat diuji/diverifikasi
- Adanya kewajiban menunjuk *Data Protection Officer* (DPO)
- Adanya persyaratan melakukan *Data Protection Impact Assessment* (DPIA)
- Adanya persyaratan pemrosesan data yang harus dipenuhi

[40] Paul Voigt and Axel van den Bussche, The European Union General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing AG, 2017.

c. Ketentuan Pokok

Ketentuan-ketentuan Pokok dari EU GDPR pada garis besarnya terdiri dari:

– Ketentuan Umum

Ketentuan Umun berisi ketentuan-ketentuan tentang: *subject matter and objectives*[41]; *material scope*[42]; *territorial scope*[43] *and Definitions*[44]

EU GDPR meletakkan aturan yang terkait dengan perlindungan terhadap hak-hak orang perorangan terkait dengan Pemrosesan Data Pribadi dan aturan-aturan yang terkait dengan kebebasan pergerakan atas data. Peraturan ini juga melindungi hak-hak dan kebebasan fundamental orang perorangan, khususnya hak untuk mendapatkan Perlindungan atas Data Pribadinya. Kebebasan pergerakan Data Pribadi di Uni Eropa tetap didorong, sementara tetap memberikan pelindungan terhadap data pribadi.

Dari cakupan secara material, EU GDPR berlaku bagi kegiatan pemrosesan data yang secara keseluruhan atau sebagian dilakukan secara otomatis serta pemrosesan data yang tidak dilakukan secara otomatis yang membentuk bagian dari sistem kearsipan atau dimaksudkan untuk membentuk bagian dari suatu sistem kearsipan.

Ketentuan-ketentuan EU GDPR tidak berlaku bagi kegiatan pemrosesan data yang: kegiatannya dilakukan di luar Uni Eropa; yang dilakukan oleh negara-negara anggota Uni Eropa yang melakukan kegiatan yang termasuk dalam cakupan sebagaimana diatur pada *Chapter 2 of Title V of the TEU*; dilakukan oleh seseorang untuk hal-hal yang dilakukan murni bersifat pribadi atau yang bersifat urusan rumah tangga; atau dilakukan oleh otoritas yang berwenang untuk tujuan pencegahan, investigasi, deteksi atau penuntutan atas tindak pidana atau dalam rangka eksekusi hukuman pidana, termasuk pengamanan terhadap atau pencegahan bentuk-bentuk ancaman terhadap keamanan publik.

41 EU GDPR, op.cit, pasal 1.
42 Ibid, pasal 2.
43 Ibid, pasal 3.
44 Ibid, pasal 4.

Dari cakupan teritorial, peraturan ini berlaku bagi: kegiatan pemrosesan data dalam konteks kegiatan dimana tempat kedudukan Pengendali Data dan Pemroses Data berada di Uni Eropa, tanpa memandang apakah pemrosesan tersebut dilakukan di Uni Eropa atau bukan; regulasi ini juga berlaku dalam Pemrosesan Data Pribadi dari Subjek Data Pribadi yang terkait dengan Pengendali Data dan Pemroses Data yang tidak berkedudukan di Uni Eropa di mana pemrosesan data pribadi tersebut terkait dengan kegiatan: menawarkan barang dan jasa, tanpa melihat apakah suatu pembayaran oleh Subjek Data diperlukan terhadap Subjek Data pada Uni Eropa; atau pemantauan perilaku sejauh perilaku tersebut berlangsung di wilayah Uni Eropa.

Ketentuan Umum juga memuat 26 istilah yang digunakan, seperti: personal data, pemrosesan data, pembatasan terhadap pemrosesan; profiling; pseudonymisation; filing system; consent; third party; personal data breach; genetic data; biometric data; data concerning health; binding corporate rules; *supervisory authority*.

– Prinsip-prinsip
  Beberapa prinsip-prinsip pokok yang diatur meliputi: *lawful, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability*. Di samping itu untuk memudahkan pemahaman juga dielaborasi faktor-faktor yang menjadi dasar apakah suatu kegiatan pemrosesan disebut *"lawfulness of processing"*; bagaimana persyaratan adanya "*consent*"; bagaimana persyaratan yang berlaku untuk "*consent*" kepada anak-anak; tata cara pemrosesan terhadap "*special categories of data*"; pemrosesan data terkait dengan tindak pidana dan pelanggaran lainnya; serta pemrosesan yang tidak memerlukan identifikasi[45].

– Hak-hak Subjek Data Pribadi

[45] EU GDPR, Pasal 5-11.

Hak-hak Subjek Data pribadi yang diatur dalam EU GDPR, mencakup: hak atas informasi dan akses atas data pribadi subjek data; hak untuk melakukan pembetulan (*right to rectification*); hak untuk meminta penghapusan data (*right to erasure/right to be forgotten*); hak untuk membatasi pemrosesan (*right to restriction of processing*); *right to data portability; right to object and automated individual decision making*[46].

– Pengendali Data dan Pemroses Data
  Bab IV dari EU GDPR antara lain mengatur tentang: Tanggung Jawab (Data) *Controller*, *Joint Controller;* Perwakilan *Data Controller* dan *Data Processor* yang tidak didirikan di EU; tentang *Processor*, pemrosesan data atas otorisasi *Data Controller* dan *Data Processor; Recording of Processing Activities* (ROPA) meliputi, kerjasama dengan *Supervisory Authority*, keamanan pemrosesan; notifikasi adanya kebocoran data kepada *Supervisory Authority;* komunikasi tentang kebocoran data kepada *Data Subject*; *Data Protection Impact Assessment* (DPIA); konsultasi; penunjukan *Data Protection Officer* (DPO), kedudukan DPO termasuk tugas DPO, aturan perilaku bagi DPO, pemantauan aturan perilaku yang telah disetujui, sertifikasi dan lembaga sertifikasi[47].

– Transfer Data Pribadi ke Negara Ketiga atau Organisasi Internasional
  Ketentuan-ketentuan tentang Transfer Data Pribadi ke Negara Ketiga atau Organisasi Internasional, meliputi: prinsip-prinsip utama transfer; transfer atas dasar *Adequacy Decision*; transfer dengan pengamanan yang memadai (*Appropriate Safeguards*); transfer berdasarkan *Binding Corporate Rules* (BCR); transfer atau pengungkapan data yang tidak berdasar pada otorisasi UE; *derogations* dalam situasi-situasi tertentu; serta kerjasama internasional dalam Pelindungan Data Pribadi[48].

[46] EU GDPR, Pasal 12-23.
[47] EU GDPR, pasal 24-43, untuk analisis selengkapnya, baca: Christopher Kuner, Lee A Bygrave, Christopher Docksey (Eds), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2017, halaman 555-754.
[48] Ibid, halaman 755-862, EU GDPR Bab V Pasal 44-50.

– *Independent Supervisory Authority*
  Supervisory Authority yang independen dinyatakan secara tegas dalam EU GDPR, termasuk dalam persyaratan umum untuk menjadi anggota serta aturan pembentukan *Certification Authority*, demikian pula aturan tentang tugas, kompetensi dan kekuasaan *Supervisory Authority*[49].

– Kerjasama dan Konsistensi
  Kerjasama dan Konsistensi diatur dalam Bab VII EU GDPR, terutama dari Pasal 60-76. Kerjasama meliputi: kerjasama antara *Lead Supervisory Authority dengan Supervisory Authority* terkait lainnya; bantuan timbal balik; serta kerjasama operasi antar *Supervisory Authority*. Konsistensi mencakup: mekanisme konsistensi; opini dari *Board*; prosedur urgensi serta pertukaran informasi. Sementara itu juga diatur tentang *European Data Protection Board* (EDPB); termasuk independensinya, tugasnya, pelaporan, prosedur, ketua, tugas ketua, sekretariat serta kerahasiaan[50].

– *Remedies, Liabilities and Penalties*
  Chapter VIII yang mengatur tentang *Remedies, Liabilities and Penalties* antara lain mengatur tentang: hak untuk mengajukan komplain melalui *Supervisory Authority*; hak untuk mengajukan *Judicial Remedy* terhadap *Supervisory Authority*; hak untuk mengajukan *Judicial Remedy* kepada *Data Controller* dan *Data Processor*; perwakilan Subjek Data Pribadi; penangguhan; hak atas kompensasi dan ganti rugi; prinsip-prinsip umum bagi pengenaan denda; dan penalti[51].

– Ketentuan tentang Situasi Pemrosesan Khusus
  Ketentuan tentang situasi pemrosesan khusus sebagaimana diatur dalam Bab IX, Pasal 85-91 mencakup substansi, antara lain: pemrosesan dikaitkan dengan kebebasan berekspresi dan komunikasi; pemrosesan dan akses publik terhadap dokumen resmi;

[49] Ibid, halaman 862-952, EU GDPR Bab VI, Pasal 51-59.
[50] Ibid, halaman 953-1116.
[51] Ibid, halaman 1117-1201.

pemrosesan nomor identitas nasional; pemrosesan yang terkait dengan *employment*; pengamanan yang terkait dengan pemrosesan untuk kepentingan umum; kewajiban menjaga kerahasiaan; aturan PDP tentang asosiasi gereja dan asosiasi keagamaan[52].

– *Delegated Acts and Implementing Acts*
  Ketentuan tentang *Delegated Acts dan Implementing Act* sebagaimana diatur dalam Bab X, pasal 92-93 yang difokuskan kepada pelaksanaan delegasi dan prosedur komisi[53].

– Ketentuan Penutup
  Ketentuan Penutup sebagaimana yang diatur dalam Bab XI, pasal 94-99 intinya mengatur tentang: *repeal of Directive 94/96/EC* serta hubungan dengan *Directive 2002/58/EC*; hubungan dengan perjanjian sebelumnya; laporan komisi; serta *review* terhadap tindakan EU lainnya terkait PDP; serta mulai berlakunya dan penerapan EU GDPR[54].

d. Kasus-Kasus Pelanggaran terhadap EU GDPR dan Denda yang Dijatuhkan
  Pada tahun 2023, jumlah denda meningkat tajam sebagai konsekuensi pelanggaran terhadap EU GDPR. Ada beberapa kasus yang menggambarkan denda terbesar yang pernah dikenakan kepada korporasi yang melanggar EU GDPR, meliputi:

– ***Meta, 2023***
  Pada bulan Mei 2023, Meta dikenakan denda sebesar Euro 1,2 milyar oleh *Irish Data Protection Commission* (DPC), denda itu dikenakan karena Meta tidak *comply* terhadap EU GDPR terkait kegiatan transfer data dari Subjek Data Pribadi di Uni Eropa ke Amerika Serikat.

– ***Amazon, 2021***

52 Ibid, halaman 1202-1267.
53 Ibid, halaman 1268-1277.
54 Ibid, halaman 1268-1322.

Pada bulan Juli 2021 Amazon didenda oleh *Luxembourg National Commission for Data Protection* (CNDP) sebesar Euro 746 juta. Denda itu dikenakan atas dasar aduan yang diajukan oleh 10.000 orang terhadap Amazon pada bulan Mei tahun 2018 melalui suatu kelompok (LSM) tentang *Privacy Rights* di Perancis yang mendorong dan membela hak dan kebebasan di dunia digital (*La Quadratur du Net*). Atas aduan tersebut CNPD melakukan investigasi tentang bagaimana Amazon memproses data konsumennya. Hasilnya, ditemukan adanya pelanggaran oleh *Amazon advertising targeting system* yang melakukan pemrosesan tanpa persetujuan yang memadai.

– ***Meta, 2022***

  Pada bulan September 2022 dikenai denda sebesar Euro 405 juta oleh *Irelands Data Protection Commission* (DPC) terkait pelanggaran dalam pemrosesan data anak-anak dalam melaksanakan suatu kontrak dan atas dasar legitimate interests. Investigasi DPC difokuskan pada data anak remaja usia 13-17 tahun, pengoperasian akun bisnis Instagram, dan bagaimana akun tersebut secara otomatis menyajikan informasi kontak anak-anak tersebut (seperti: *email address*, nomor telepon, dll.) secara terbuka. Menurut DPC Meta telah gagal mengambil langkah-langkah yang seharusnya untuk memberi informasi kepada anak-anak dalam rentang usia tersebut dengan menggunakan kata-kata yang jelas dan lugas, kurang melakukan *appropriate technical and organizational measures*, dan tidak melakukan DPIA terhadap pemrosesan data yang dapat menimbulkan resiko yang tinggi tekait hak dan kebebasan anak-anak tersebut.

– ***Meta Platform Ireland Ltd, 2024***

  Dalam kasus yang terjadi pada tahun 2024 ini *Meta Platform Ireland Ltd* dikenai denda sebesar Euro 390 juta karena dianggap melakukan pelanggaran terhadap beberapa pasal pada EU GDPR, yaitu Pasal 5 (1) A), Pasal 6 (1), Pasal 12, Pasal 13 (1) EU GDPR.

Meta Platform Ireland ltd dikenai denda karena meminta penggunaan Data Pribadi untuk iklan di Facebook dan Instagram dengan cara melanggar hukum. Regulator menyatakan bahwa Meta seharusnya tidak boleh memaksakan persetujuan konsumen dengan cara meminta konsumen untuk memberi persetujuan atau jika persetujuan tidak diberikan maka diminta untuk keluar dari *Platform*. Selama investigasi yang dilakukan oleh *The Irish Data Protection Commission* (DPC) ditemukan fakta bahwa Meta memiliki kebijakan tentang Pelindungan Data Pribadi yang tidak jelas, terutama bagaimana mereka akan menggunakan Data Nasabah atau Pengguna.

– ***Tik Tok Ltd, 2023***

Pada tahun 2023 Tik Tok dikenakan denda sebesar Euro 345 juta karena dianggap melanggar pasal-pasal EU GDPR, yaitu: Pasal 5 (1) c), Pasal 5 (1) f), Pasal 12 (1), Pasal 13 (1) c), Pasal 24 (1), Pasal 25 (1) (2).

Menurut *Irish Data Protection Commission* (DPC), bentuk pelanggaran *Tik Tok Ltd* termasuk menaruh *data User* anak-anak berusia 13-17 tahun pada *Default Public Setting* (DPS). Kegagalan melindungi data anak-anak di bawah umur, ditambah dengan kegagalan mensuplai anak-anak ini dengan informasi yang transparan serta tidak melakukan pengecekan apakah orang dewasa yang dipasangkan dengan anak-anak dalam skema pasangan keluarga apakah benar-benar orang tuanya. Lebih jauh telah ditemukan fakta bahwa tidak memperhitungkan resiko yang dimiliki anak di bawah umur yang mengakses ke platform.

– ***WhatsApp Ireland, 2021***

Pada tahun 2021 *WhatsApp Ireland* telah dikenakan denda sebesar 225 juta Euro karena melanggar beberapa ketentuan EU GDPR, terutama pelanggaran terhadap beberapa pasal, yaitu: Pasal 5, Pasal 12, Pasal 13 dan Pasal 14.

Otoritas Data di Ireland mengenaan denda kepada *WhatsApp Ireland* dengan jumlah di atas karena dianggap telah melanggar standard privasi. Denda ini merupakan salah satu denda terbesar yang dijatuhkan oleh *Data Protection Commission* (DPC).

Inti kasus ini, pada tahun 2018 suatu investigasi yang dilakukan oleh DPC menemukan bahwa *WhatsApp* tidak cukup transparan kepada konsumen perihal bagaimana *WhatsApp* mengumpulkan, mengelola, dan memproses Data Konsumen. Setelah melalui proses investigasi yang cukup panjang dan komprehensif, kemudian DPC menjatuhkan sanksi denda sebagaimana tersebut di atas dan telah mengkomunikasikan keputusannya kepada *Regulator* lain sebagaimana dipersyaratkan berdasar EU GDPR, *WhatsApp* juga mendapatkan komplain dari 4 (empat) negara, termasuk Jerman, Perancis dan Italia.

– ***Google LLC, 2019***

Pada tahun 2019 Google mendapatkan denda dari Regulator Data di Perancis sebesar 50 juta Euro karena disangkakan melanggar ketentuan Pasal 5, Pasal 12, Pasal 13, dan Pasal 14 EU GDPR.

Denda dikenakan karena kurangnya transparansi, kurangnya informasi dan kurang validnya persetujuan (*consent*) terkait personalisasi iklan. Info personalisasi iklan didilusi melalui beberapa dokumen sehingga menyulitkan *Users* untuk mengetahui secara penuh isinya. Sebagai tambahan, pilihan untuk menerima personalisasi iklan yang dibuat secara "*pre-ticket*" pada saat membuka akun, sehingga secara langsung dapat dikatakan *defying* EU GDPR.

– ***CRITEO, 2023***

Pada tahun 2023 Otoritas PDP di Perancis (CNIL) telah mendenda CRITEO sebesar 40 juta Euro karena melanggar pasal-pasal EU GDPR, yaitu: Pasal 7 (1), (3), Pasal 12, Pasal 13, Pasal 15 (1), Pasal 17 (1) dan Pasal 26.

CRITEO adalah spesialis di bidang iklan *on-line*. Komplain kepada CRITEO diajukan oleh sebuah *Non-Governmental*

Organization (NGO) yang bernama *Privacy International and Non of Your Business* (NOYB).

Dalam putusannya CNIL menganggap bahwa CRITEO telah gagal menjamin mitranya seperti penerbit untuk: memperoleh persetujuan Subjek Data Pribadi (penggunanya) untuk menggunakan *Cookies* dari CRITEO. Meskipun mitranya yang seharusnya bertanggung jawab untuk memperoleh persetujuan dari penggunanya, namun CNIL tetap menganggap CRITEO bertanggung jawab untuk memverifikasi persetujuan dan penggunanya. Denda sebesar 40 juta Euro tersebut setara dengan 2% *global revenue* CRITEO, jumlah mana lebih rendah dari perhitungan CNIL sebelumnya, yaitu sebesar 60 juta Euro.

– ***H&M, 2020***

Pada tahun 2020 Otoritas PDP Hambourg mengenakan denda kepada *H&M* sebesar 35.25 juta Euro karena telah melakukan *surveillance* (mata-mata) terhadap karyawannya.

Modus yang digunakan adalah terhadap karyawan yang mengambil cuti atau cuti sakit, pada saat masuk kembali karyawan tersebut mengikuti *program Return to Work*. Pada saat *program Return to Work* tersebut dilakukan perusahaan melakukan perekaman dan datanya kemudian dapat diakses oleh sekitar 50 Manajer *H&M*. Hasilnya, perusahaan memiliki rekaman yang berlebihan dari karyawan, termasuk keluarga, agama, penyakit karyawan yang disimpan pada *Nurenberg Service Center*. Kemudian perusahaan menggunakan data tersebut untuk mengevaluasi kinerja karyawan dan membuat berbagai putusan terkait dengan karyawan. Tindakan yang dilakukan oleh *H&M* dianggap melanggar ketentuan Pasal 5 dan 6 EU GDPR.

– ***TIM, 2020***

Pada tahun 2020 Regulator PDP Itali yaitu *Garante* telah mengenakan denda kepada perusahaan jasa telekomunikasi yaitu *TIM* denda sebesar 27,8 Juta Euro karena melakukan pelanggaran

berupa penggunaan data pribadi Subjek Data untuk melakukan telemarketing serta pelanggaran terhadap ketentuan-ketentuan EU GDPR lainnya. Pertama, *TIM* mengirim ratusan ribu *unsolicited communication* tanpa persetujuan Subjek Data. Dalam satu kasus bahkan Subjek Data bisa dihubungi sampai 155 kali per orang. Kedua, *Privacy Policy* dari *TIM Apps and Promotion* tidak transparan dan tidak jelas, terutama mengapa mereka menggunakan Data Pribadi Subjek Data tanpa persetujuan mereka, bahkan data tersebut dikelola secara tidak benar, bahkan tidak sah, di mana satu persetujuan digunakan untuk banyak tujuan. Ketentuan tentang Retensi Data juga berlebihan, kadang-kadang bisa mencapai hingga 10 tahun. Tindakan-tindakan *TIM* sebagaimana disebut di atas dianggap melanggar ketentuan-ketentuan Pasal 5, Pasal 6, Pasal 7, Pasal 17, Pasal 21, dan Pasal 32 EU GDPR.

– ***British Airways, 2020***

  Karena melanggar ketentuan Pasal 5 (1) EU GDPR, maka *British Airways* pada tahun 2020 dikenakan denda sebesar 22,4 juta Euro karena telah gagal melindungi Data lebih dari 400.000 konsumennya. Hasil investigasi menemukan bahwa British Airways telah melakukan pemrosesan Data Pribadi yang cukup besar.

e. Pembelajaran yang Dapat Dipetik

Dari kasus-kasus terkait PDP sebagaimana tersebut di atas, pembelajaran utama yang dapat dipetik adalah perlunya peningkatan kesadaran dan kepatuhan atas aturan PDP yang semakin lama semakin ketat. Selanjutnya, dari kasus-kasus tersebut setidak-tidaknya dapat dicermati bentuk-bentuk pelanggaran apa saja yang paling banyak terjadi, bagaimana penafsirannya dan bagaimana penegakannya. Bagi Indonesia pembelajaran tersebut sangat bermanfaat untuk mengantisipasi implementasi penuh dari Undang-Undang PDP yang berlaku efektif pada bulan Oktober 2024. Apalagi dari kasus-kasus tersebut akan dapat dipahami bagaimana implementasi dan penegakan ketentuan-ketentuan tentang PDP yang perlu diperhatikan oleh *Data Controller*,

Data Processor dan bahkan *Data Subject*, serta Lembaga Pengawas yang segera dibentuk.

5. *EU-US Data Privacy* Framework (DPF)

   EU-US DPF dikembangkan untuk memfasilitasi kegiatan perdagangan di kawasan Trans-Atlantik dengan menyediakan suatu mekanisme yang terpercaya yang dapat digunakan oleh organisasi/korporasi di Amerika Serikat untuk mentransfer data pribadi dari Uni Eropa ke Amerika Serikat. DPF berlaku secara efektif pada tanggal 10 Juli 2023 bersamaan dengan the *European Commission's Adequacy Decision*. Prinsip-prinsip DPF terdiri dari *Supplemental Principles dan Annex I to the Principles*. *The Adequacy Decision* memungkinkan dilakukannya transfer data pribadi dari Uni Eropa ke organisasi/korporasi di Amerika Serikat.

   Program DPF dilaksanakan oleh *International Trade Administration* (ITA) yang menjadi salah satu bagian dari *US Department of Commerce*. DPF membuka peluang bagi organisasi/korporasi di Amerika Serikat yang memenuhi syarat untuk melakukan sertifikasi secara mandiri (*self certify*) terkait kepatuhan mereka terhadap EU-US DPF. Untuk dapat berpartisipasi dalam program DPF tersebut, maka organisasi/korporasi tersebut harus menunjukkan kepatuhannya terhadap EU-US DPF melalui proses kepatuhan yang bersifat sukarela. Sekali suatu organisasi/korporasi melakukan *Self-Certification* melalui ITA dan menyatakan kepatuhannya terhadap DPF, maka komitmen tersebut dapat ditegakkan berdasarkan hukum yang berlaku di Amerika Serikat. Bagi organisasi/korporasi yang telah melakukannya, maka akan terdaftar di DPF *List* dan hal itu tetap berlangsung hingga organisasi/ korporasi tersebut menarik diri dari DPF. Organisasi/korporasi yang telah menarik diri, maka akan dikeluarkan dari DPF List dan karenanya harus menghentikan untuk mengklaim berpartisipasi atau patuh terhadap EU-US DPF. Sementara itu selama organisasi/korporasi tersebut menjadi partisipan dari EU-US DPF, maka harus tetap menerapkan EU-US DPF dalam setiap kegiatan menerima atau mengimport informasi berdasarkan EU-US DPF.

6. EU–ASEAN *Privacy* (*Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*)

   Merupakan model klausula Pelindungan Data yang dapat diinkorporasikan, baik oleh eksportir maupun importir data dalam pengaturan kontraktual mereka sebagai dasar untuk melakukan transfer Data Pribadi yang bersifat lintas batas nasional. Klausula tersebut merupakan sarana sukarela untuk memastikan Data Pribadi terus mendapatkan perlindungan tingkat tinggi dalam hal transfer data bersifat lintas batas Negara, khususnya untuk memastikan kepatuhan terhadap persyaratan hukum yang berlaku bagi transfer data internasional. Klausula tersebut mercerminkan persyaratan Pelindungan Data yang bersumber kepada *ASEAN Framework on Personal Data Protection (2016)* dan EU GDPR.

   Pedoman Bersama ini terdiri dari 2 (dua) dokumen: *Reference Guide* dan *Implementation Guide. Reference Guide* memuat garis besar perbandingan yang menggambarkan perbedaan dan persamaan antara ASEAN MCCs dengan EU SCCs. Sementara itu *Implementation Guide* berisi praksis terbaik dari perusahaan-perusahaan yang memenuhi persyaratan, baik ASEAN MCCs maupun EU SCCs.

   Tujuan dari Pedoman Bersama ini adalah untuk membantu perusahaan-perusahaan yang beroperasi di kawasan ASEAN maupun EU (baik *Data Exporter* maupun *Data Importer*) untuk dapat memahami perbedaan maupun persamaan antara ke 2 (dua) klausula tersebut, untuk memfasilitasi kepatuhan terhadap ketentuan yang berlaku bagi ASEAN MCCs dan EU SCCs. Pedoman ini juga mempermudah berbagai kalangan untuk melakukan transfer data, khusus antara Uni Eropa ke ASEAN dan sebaliknya.

B. *Association of Southeast Asian Nations* (ASEAN)

Dalam lingkup ASEAN ada beberapa instrumen hukum dan etika yang mengatur tentang Pelindungan Data Pribadi, meskipun instrumen-instrumen tersebut lebih bersifat *soft laws,* mengingat tingkat Pelindungan Data Pribadi di antara negara-negara anggota ASEAN masih beragam tingkatannya. Di bawah ini beberapa instrumen yang relevan, yaitu:

1. ASEAN *Framework on Personal Data Protection* (ASEAN *Privacy Framework*) 2016[55]

   ASEAN *Privacy Framework* ditetapkan dalam pertemuan Menteri-menteri Telekomunikasi (TELMIN) ASEAN pada tanggal 25 November 2016. Tujuan *ASEAN Framework on PDP* adalah untuk penguatan Pelindungan Data Pribadi di ASEAN dan untuk memfasilitasi kerjasama di antara para pihak agar berkontribusi terhadap peningkatan dan pertumbuhan perdagangan regional dan global serta arus informasi.

   ASEAN *Privacy* Framework ini bersifat sukareala dan digunakan sebagai catatan maksud dari para pihak, meskipun tidak mempunyai daya mengikat secara hukum. Cakupan *ASEAN Privacy Framework* ini adalah untuk kepentingan pengaturan nasional di masing-masing negara anggota. Implementasinya sangat tergantung kepada kesiapan masing-masing negara. Hal-hal lain yang diatur meliputi: pengaturan keuangan, kerahasiaan, amandemen, penyelesaian sengketa, perwakilan dan alamat masing-masing pihak serta ketentuan Penutup.

   Prinsip-prinsip Pelindungan Data Pribadi yang diatur dalam ASEAN *Privacy* Framework meliputi:
   - *Consent, Notification and Purpose*
   - *Accuracy of Personal Data*
   - *Security Safeguards*
   - *Access and Correction*
   - *Transfer to another country or territory*
   - *Retention*
   - *Accountability*

2. *ASEAN Model Contractual Clauses for Cross Border Data Flows* (MCCs)

   MCCs merupakan persyaratan kontraktual yang terdapat dalam binding legal agreements diantara para pihak yang mentransfer data pribadi yang bersifat lintas batas Negara di ASEAN. MCCs melindungi Data Pribadi dan menciptakan kepercayaan diantara para Pihak yang terkait. MCCs

[55] ASEAN Privacy Framework dihasilkan melalui pertemuan Menteri-Menteri Telekomunikasi di ASEAN (ASEAN TELMIN).

merupakan standard yang bersifat sukarela yang dirancang sebagai pedoman dan pertimbangan dalam melakukan transfer data lintas Negara.

ASEAN MCC's merupakan turunan dari *ASEAN Privacy Framework 2016*. Kewajiban yang diletakkan oleh ASEAN MCC's bersumber dari ketentuan kontraktual yang menggarisbawahi kewajiban pelindungan data-data kunci dalam kontrak komersial di antara para pihak dalam hal dilakukan transfer data. Kewajiban-kewajiban tersebut meliputi: dasar hukum yang jelas dan memadai tentang pengumpulan, penggunaan dan pengungkapan data; *baseline* klausula Pelindungan Data; serta mekanisme notifikasi dalam hal terjadinya kebocoran data.

Berdasarkan ASEAN MCC's terdapat 2 modul perihal hubungan di antara para pihak yang melakukan transfer data, baik antara *Data Controler* dengan *Data Controller* maupun antara *Data Controller* dengan *Data Processor*.

Isi dari Modul 1 yang mengatur hubungan antara *Data Controller* dengan *Data Controller* meliputi: definisi, kewajiban *data exporter*, kewajiban data importer, pilihan hukum (dalam sengketa), penangguhan transfer, pengakhiran kontrak, *general undertakings*, variasi, serta deskripsi tentang transfer.

Sementara itu Modul 2 yang mengatur hubungan antara Data Controller dengan *Data Processor* memiliki elemen ketentuan yang serupa.

Di samping Modul 1 dan Modul 2, juga terdapat *Appendix A*, yaitu *Template for Data Exporters and Importers to describe Purposes for the transfer of personal data*. ASEAN MCC's juga mengatur persyaratan dan ketentuan bagi penerapan MCC's.

3. *ASEAN Data Management Framework (DMF), 2018*

The ASEAN Data Management Framework di endorsed oleh Pertemuan Menteri-Menteri Telekomunikasi (TELMIN) ASEAN pada persidangannya yang ke 18 di tahun 2018. Kegiatan utamanya adalah menetapkan prioritas, prinsip-prinsip dan inisiatif sebagai pedoman bagi Negara-negara anggota ASEAN (ASEAN *Member States*/AMS) dalam pendekatan kebijakan dan regulasi ke arah tata kelola digital pada ekonomi digital.

Priotitas strategisnya meliputi: siklus dan ekosistem data (*data life cycles and ecosystem*), arus data lintas batas (*cross boder data flows*), digitalisasi dan teknologi baru (*digitalization and emerging technologies*), aspek hukum dan regulasi (*legal and regulatory*). Hal-hal yang ingin dihasilkan dari prioritas-prioritas strategis tersebut, antara lain: adanya tata kelola data sepanjang siklusnya (dari pengumpulan, penggunaan, akses, penyimpanan); perlindungan yang memadai bagi setiap tipe data; kepastian usaha terkait *cross border data flows*; tidak ada pembatasan yang tidak perlu terhadap arus data; pengembangan kapasitas data (baik infrastruktur maupun ketrampilan); *leverage* terhadap teknologi baru; harmonisasi lanskap hukum dan regulasi di ASEAN (termasuk Pelindungan Data Pribadi); pengembangan dan pengadopsian praksis terbaik[56].

Berdasarkan prioritas strategis dan hasil yang ingin dicapai sebagaimana tersebut di atas, dirumuskan beberapa inisiatif, antara lain: *ASEAN Data Classification Framework*; *ASEAN Cross Border Data Flows Mechanism; ASEAN Digital Innovation Forum*; serta *ASEAN Data Protection and Policy Forum*.

C. *Asia Pacific Economic Cooperation* (APEC)

1. APEC *Privacy Framework 2004*

APEC *Privacy Framework* ditetapkan dalam suatu pertemuan tingkat menteri APEC pada tahun 2004. Ada 9 (sembilan) prinsip PDP yang diletakkan dalam dokumen tersebut, yaitu: *preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguard, access and correction, dan accountability*. Dalam penerapannya masing-masing negara diberi kebebasan untuk menggunakan berbagai pendekatan, seperti: *legislative, administrative, industry self-regulatory,* atau kombinasi dari berbagai pendekatan tersebut.

2. APEC *Data Privacy Pathfinder 2007*

Pada tahun 2007 Menteri-menteri APEC mengendorse "APEC *Data Privacy Pathfinders*". *Pathfinders* adalah wujud kerjasama di antara Negara-negara

[56] Asean-org, "ASEAN Data Management Framework (Data Governance and Protection Throughout the Data Lifecycle)", Final Copy Endorsed by the First ASEAN Digital Senior Official Meeting (ADGSOM), January 2021.

yang menjadi anggotanya. Maksud dari *Data Privacy Pathfinders* adalah berupa proyek-proyek kerjasama diantara negara-negara anggota APEC serta untuk mengembangkan suatu *sistem Cross-Border Privacy Rules* (CBPR) yang dapat digunakan oleh negara-negara anggotanya untuk melindungi privasi di bidang informasi di antara sesama negara-negara anggotanya.

3. APEC *Privacy Framework 2015*

   Pada tahun 2015 disepakati APEC *Privacy Framework* yang memuat: preambul, cakupan, APEC *Privacy Information Principles*, serta implementasinya, baik yang bersifat domestik maupun internasional. Ketentuan APEC *Principles* terdiri dari: *Preventing Harms; Notice; Collection Limitation; Uses of Personal Information; Choice; Integrity of Personal Information; Security Safeguards; Access and Correction; and Accountability.*

   Mengenai pedoman bagi *domestic implementation* harus memperhatikan berbagai konsep dasar seperti: *maximizing benefits of privacy protection and information flows; giving effect to* APEC *Privacy Framework; privacy management programmes; promotion of technical measures to protect privacy; public education and communication; cooperation within and between the public and private sectors; providing for appropriate remedies in a situation where privacy protection are violated; and mechanism for domestic implementation of the* APEC *Privacy Framework*.

   Sementara itu *Guidance for International Implementation* meliputi: *information sharing among member economies; cross-border cooperation in investigation and enforcements; cross border privacy mechanism; cross border transfers; and interoperability between privacy frameworks*.

4. APEC *Cross Border Privacy Rules* (CBPR)

   CBPR dimaksudkan untuk memberikan *minimum level of protection* terhadap Data Pribadi.

   Implementasi CBPR melibatkan perusahaan-perusahaan besar untuk mengembangkan dan mengimplementasikan *privacy policies* yang sejalan dengan APEC *Privacy Framework*. Maksud dari APEC CBPR adalah untuk mengembangkan perlindungan privasi yang efektif untuk menghindari

hambatan arus informasi dan untuk menjamin keberlangsungan pertumbuhan perdagangan dan perekonomian di kawasan APEC.

APEC *Cross-Border Privacy Rules System, Policies, Rules and Guidelines*. Beberapa Isi utamanya adalah: Pengembangan *CBPR System;* Pengoperasian *CBPR System*[57]; *CBPR Process Overview*[58]; *the CBPR System and Domestic Laws and Regulations; Governance of the CBPR System*[59]; *Success Criteria for CBPR System*[60]. Dilengkapi dengan *Annex A* yaitu *Charter of the APEC Cross Border Privacy Rules System joint oversight panel.*

D. Pengaturan PDP di Beberapa Negara

1. *Hongkong Personal Data (Privacy) Ordinance*, Sebagaimana Diubah Tahun 2013

   Pengaturan tentang PDP di Hongkong SAR dapat ditemukan pada *The Personal Data* (*Privacy*) *Ordinance* yang mengatur tentang pengumpulan dan penanganan data. Ordonansi ini telah berlaku sejak tahun 1996, namun mengalami perubahan yang signifikan pada tahun 2012/2013, khususnya terkait dengan *direct marketing*. *The Personal Data* (*Privacy*) berlaku pada bulan Oktober 2021 dan memperkenalkan suatu bentuk kejahatan terhadap Data Pribadi yang disebut *Doxxing* berikut aturan-aturan pidananya[61].

   Pada tahapan rancangan *Amendment Ordinance* terdapat sejumlah usulan perubahan (dalam *consultation paper*), antara lain: memperkenalkan *mandatory data breach notification mechanism*, mempersyaratkan kepada *Data User* untuk memformulasikan *Data Retention Policy*, pemberdayaan/ The *Privacy Commissioner for Personal Data* (PCPD) untuk menjatuhkan denda administratif yang dikaitkan dengan *annual turn over*, serta mengatur

---

57 Terdiri dari elemen-elemen: CBPR system self assessment; compliance review; recognition/ acceptance; dispute resolution and enforcement.

58 Terdiri dari elemen-elemen: process for participation and discontinuation of participation by APEC Economies in the CBPR system; process for recognition of accountability agent; process for certification of organizations; role of privacy enforcement authority.

59 Terdiri dari: objectives; functions and the governance model; joint oversight panel.

60 Dengan cara menginkorporasikan prinsip-prinsip utama dari APEC, yaitu: voluntarism, comprehensiveness, consensus0based decision making, flexibility, transparency, regionalism and differential implementation timetables for developed and developing economies.

61 Baca DLApiperdataprotection.com, "Data Protection Laws of the World: Hongkong SAR", terakhir dimodifikasi tanggal 11 Januari, 2024.

secara langsung tentang *Data Processor*. Dalam laporan PCPD ke *Legislative Council* pada bulan February 2023, PCPD mengkaji lebih lanjut amandemen terhadap Ordonansi dengan Pemerintah Hongkong SAR untuk penguatan penegakan PDP dan mengatasi tantangan-tantangan yang dihadapi, termasuk tantangan yang muncul dari perkembangan teknologi.

Ketentuan-ketentuan pokok yang diatur *Hongkong Personal Data* (*Privacy*) *Ordinance* meliputi: definisi, *authority, registration, Data Protection Officer, collection and processing, transfer, security, breach notification, enforcement, electronic marketing, online privacy and contacts.*

Beberapa definisi yang dirumuskan khususnya tentang *personal data* dan *sensitive personal data*. Otoritas yang menjalankan Ordonansi adalah *the Office of the Privacy Commissioner for Personal Data* (PCPD). Ordonansi ini berlaku bagi sektor publik, perbankan, asuransi dan industri telekomunikasi, organisasi dengan *data base* anggota yang besar (misalnya *customer loyalty system*).

Meskipun tidak ada kewajiban *Data User (Controller)* untuk menunjuk DPO, namun pada tahun 2014 dan 2019 PCPD menetapkan *best practice guide* yang menghimbau agar *Data Controller (User)* menunjuk orang yang bertanggung jawab memastikan kepatuhan *Data Controller* terhadap aturan Ordonansi. Namun tidak ada ketentuan tentang penalti dalam hal *Data Controller* tidak menunjuk seorang DPO.

Ordonansi ini juga mengatur prinsip-prinsip Pelindungan Data Pribadi. PCPD juga mengeluarkan himbauan untuk melakukan "*privacy impact assessment*" yang disebut "*ethical data impact assessment*". Pada tahun 2021 PCPD mempublikasikan "*the Guidance on Ethical Development and Use of Artificial Intelligent*" yang bertujuan untuk membantu organisasi (baik publik maupun privat) untuk menghadapi masalah privasi dan resiko etis yang terkait dengan perkembangan dan penggunaan AI.

Transfer data hanya dapat dilakukan apabila: Negara penerima termasuk "*whitelist jurisdiction*", atau diperoleh persetujuan secara sukarela dari Subjek Data Pribadi; dan adanya perjanjian transfer data yang dapat ditegakkan.

Pada tanggal 13 Desember 2023 dihasilkan *standard contract for the cross-boundary flow of personal information* antara *Guangdong-Hongkong-Macau Greater Bay Area* (GBA).

Ordonansi baru mengatur tentang larangan melakukan *Doxxing*. *Doxxing* didefinisikan sebagai "*an offence to disclose, without the Data Subject's consent, any personal data with an intent to cause harm to the Data Subject or any family member of the Data Subject*". Penalti yang dapat dikenakan untuk tindakan melakukan *Doxxing* adalah: denda pada level 6 (100.000 HK Dollar) dan hukuman kurungan 2 tahun; denda sebesar 1.000.000 HK Dollar dan penjara 5 tahun jika pengungkapan data tersebut menyebabkan kerugian kepada Subjek Data Pribadi atau keluarganya.

PCPD juga diberi wewenang untuk melakukan *criminal investigation* terhadap tindakan Doxxing. Wewenang tersebut mencakup: mengakses data, mengeluarkan perintah, memasuki premises, melakukan penyitaan, dan lain-lain. Ketentuan anti Doxxing bersifat extra territorial.

Sejak *Amendment Ordinance* berlaku pada tanggal 31 Oktober 2023, PCPD telah melakukan 221 kali investigasi kriminal, menangkap 40 orang dalam 39 kasus di mana 13 orang didakwa melakukan Doxxing dan 11 di antaranya dipidana. PCPD juga melakukan perintah penghentian pemrosesan data sebanyak 1800 kali, penghentian 41 *online platforms*, memerintahkan memindahkan 27.000 pesan Doxxing dengan tingkat kepatuhan 95%.

2. UK *Data Protection Act of*[62]

The Data Protection Act 2018 adalah implementasi EU GDPR. Setiap pihak yang bertanggungjawab dalam pemrosesan data harus tunduk pada *Data Protection Principles. Data Protection Act* juga mengatur prinsip-prinsip PDP yang pada intinya serupa dengan EU GDPR. Demikian juga mengatur hak-hak Subjek Data Pribadi.

Tujuan dari *Data Protection Act* adalah untuk memberdayakan individu untuk memegang kendali atas data pribadinya dan untuk mendukung organisasi/korporasi (publik dan privat) untk melakukan kegiatan pemrosesan data secara sah berdasarkan hukum yang berlaku. DPA 2018 berisi ketentuan-ketentuan PDP yang ketat yang melindungi individu dari

[62] Untuk analisis rinci, baca: Susan Singleton, Data Protection, Jordan Publishing Limited, UK, 1998. Baca juga PeterCarey (ed), Data Protection: A Practical Guide to UK and EU Law, fifth Edition, Oxford University Press, 2018.

penyalahgunaan data pribadinya atau tindakan yang mengeksploitasi atau penyalahgunaan data pribadi orang perorangan. Sebelum diberlakukannya *Data Protection Act 2018* yang berlaku adalah *Data Protection Act 1998* yang berlaku hanya bagi organisasi/korporasi di UK, sementara itu *Data Protection Act 2018* juga berlaku keluar. Ketentuan-ketentuan Pokok pada *Data Protection Act 2018* meliputi: *preliminary, general processing, law enforcement processing, intelligence service processing, the information commissioner,* dan *enforcement*.

Personal Data Protection Act 2018 juga menekankan pada perlindungan lebih kepada Data Pribadi *Sensitive/Specific* seperti: ras, latar belakang etnik, pandangan politik, keyakinan agama, keanggotaan pada serikat pekerja, data genetika, data biometrik, rekam medis, kehidupan dan orientasi seksual.

Prinsip-prinsip utama yang dirumuskan pada *Data Protection Act 2018* adalah: *lawfulness, fairness* dan transparansi, *accuracy*, *storage limitation*, *integrity and confidentiality (security)* dan *accountability*. *Data Protection Act 2018* berlaku bagi setiap pihak yang melakukan pemrosesan terhadap data pribadi. Aturan tersebut juga mengatur tentang "*consent*" yang mensyaratkan bahwa "*consent*" diberikan secara "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by a statement or by clear affirmative action signifies agreement to the processing of personal data relating to him or her*"[63].

Berdasarkan *Data Protection Act 2018* ada hal-hal yang dilarang, seperti: *unauthorized surveillance or profiling by Governments or third parties or used for unconnected purposes without consent*. Ada 7 (tujuh) *golden rules* terkait Pelindungan Data Pribadi yaitu: *necessary, proportionate, relevant, adequate, accurate, timely and secure*. Ada beberapa tips yang ditekankan untuk meningkatkan keamanan data dengan cara: mengenkripsi data, memutakhirkan *software* yang digunakan, melakukan *back-up* terhadap data secara teratur, membuat *password* yang kuat dan sering mengubahnya, serta berupaya mencari *software* anti virus yang handal.

[63] Lihat Pasal 4 (11) Data Protection Acts 2018.

3. *Japan Act on the Protection of Personal Information* (APPI)
   Peraturan ini dirancang untuk melindungi informasi pribadi warganegara Jepang. Siapapun yang menerima data pribadi warganegara Jepang wajib mematuhi ketentuan ini atau akan menghadapi resiko hukum. Peraturan ini semula diundangkan pada tahun 2005. Pemberlakuannya menandai suatu shift yang penting informasi pribadi dilindungi. Sebelumnya perusahaan-perusahaan swasta dipantau oleh beberapa Kementerian dan otoritas lainnya. Ketika terjadi kebocoran data subjek data pribadi (korban) dapat mengajukan tuntutan ganti rugi berdasarkan aturan tentang perbuatan melawan hukum.

   APPI mengkonsolidasikan pengawasan terhadap pelindungan data pribadi melalui Komisi Pelindungan Informasi Pribadi (PPC). PPC ditugaskan untuk menyusun *guidelined* (pedoman) kepada semua sektor usaha, dengan pedoman tambahan pada bidang-bidang seperti: pelayanan kesehatan, keuangan, dan telekomunikasi. APPI memiliki banyak persamaan dengan standard EU-GDPR. Sejak diundangkan telah mengalami berbagai perubahan, yaitu melalui pemutakhiran pada tahun 2015 dan 2020. Sejalan dengan perkembangan, baik di dunia bisnis maupun maupun di dunia digital. Amandemen 2015 difokuskan pada penerapan skema "*opt out*" serta memaksa dunia usaha untuk memperoleh persetujuan dari subjek data pribadi. Sementara itu amandemen 2020 lebih difokuskan pada penigkatan penalty atas ketidakpatuhan yang terjadi.

   Ada beberapa cara yang dapat digunakan untuk memenuhi kepatuhan atas *Act* ini, melalui: memutakhirkan standard meng updates sistem legasi; menerapkan pengendalian akses; menunjuk DPO; membatasi transfer data; dan lain-lain[64].

4. *Malaysia Personal Data Protection Act (PDPA) 2010*
   Malaysia memiliki The Personal Data Protection Act sejak tahun 2010. Peraturan ini mengatur pemrosesan Data Pribadi yang terkait dengan transaksi komersial. PDPA 2010 hanya berlaku bagi sektor privat.

[64] https://www.delphix.com.

7 (tujuh) prinsip dasar dalam Pelindungan Data Pribadi 2010 meliputi: *general, notice and choice, disclosure, security, retention, data integrity* dan akses. PDPA tidak mempersyaratkan penunjukan DPO oleh *Data Controller*, tapi diberlakukan semacam *code of practice*. PDPA mulai berlaku pada tanggal 5 November 2013.

Pengawasan untuk pelaksanaan PDPA dilakukan oleh Personal *Data Protection Commissioner* (PDPC) di bawah Kementerian Komunikasi dan Multimedia. Pada tanggal 23 Desember 2015 PDPC mempublikasikan *Personal Data Protection Standard* (Standard) yang berisi persyaratan minimal (standard), meliputi: standar keamanan data (baik elektronik maupun biasa); standar retensi untuk pemrosesan data, baik secara elektronik mapun non-elektronik. PDPA juga mengatur tentang: transfer data, keamanan data, *data breach notification, enforcement, electronic marketing*, *online privacy* dan *contacts*.

Pada bulan Oktober 2023 draft revisi PDPA mencapai fase finalisasi dan telah disetujui Parlemen pada bulan Juli tahun 2024. Dalam revisi PDPA terdapat beberapa isu utama, termasuk terkait pemberlakuannya, baik bagi sektor privat maupun sektor publik, demikian pula usul adanya kewajiban penunjukan DPO.

Berdasarkan PDPA, ada kelas-kelas data yang harus diregistrasi, seperti: komunikasi, bank dan lembaga keuangan, asuransi, kesehatan, pariwisata dan hospitality, transportasi, pendidikan, *direct selling*, jasa, *real estate*, *utilities, pawn broker,* dan *money lender*.

5. *Taiwan Personal Data Protection Act 2010* sebagaimana diubah pada tahun 2023

   PDPA Taiwan mengatur hal-hal sebagai berikut: ketentuan umum; pengumpulan, pemrosesan dan penggunaan data oleh badan-badan pemerintah; pengumpulan, pemrosesan dan penggunaan oleh badan-badan non-pemerintah; tentang kerugian dan *class-action; penalty;* ketentun pelengkap. Secara keseluruhan terdiri dari 59 pasal[65].

[65] Informasi selengkapnya dapat dilihat pada https://law.moj.gov.tw>Eng

6. *Korea Personal Information Protection Act 2011* sebagaimana diamandemen tahun 2023

   Beberapa hal yang direvisi meliputi: penetapan prosedur untuk melaksanakan hak-hak Subjek Data Pribadi terkait pengambilan putusan secara otomatis (*automated decisions*); penunjukan dan kualifikasi *Personal Information Protection Officer*; memperbaiki cakupan yang tunduk pada jaminan tanggung jawab ganti rugi; menetapkan standard dan prosedur dalam mengevaluasi perlindungan informasi pribadi pada sektor publik; pengungkapan data pribadi dalam keadaan darurat dan penyelesaian sengketa melalui mediasi; standar perfilman yang terkait data pribadi; pemrosesan data pribadi secara *daring* dan *luring*[66].

7. *Singapore Personal Data Protection Act 2012*

   Singapore PDPA pertamakali diundangkan pada tahun 2012. Ketentuan-ketentuan pokoknya terdiri dari: pengantar, dan tujuan; penerapan undang-undang; Komisi PDP dan pengadministrasiannya; ketentuan umum tentang pelindungan dan akuntabilitas bagi data pribadi; pengumpulan, penggunaan dan pengungkapan data pribadi; akses dan pembetulan atas data pribadi; perlindungan dan keakurasion data pribadi; notifikasi terkait kebocoran data; dan lain-lain[67].

8. *Philipines Data Privacy Act 2012*

   Philipines Data Privacy Act 2012 bertujuan untuk melindungi hak-hak asasi manusia yang fundamental terkait dengan privasi, terkait dengan komunikasi dengan tetap menjamin kebebasan arus informasi untuk meningkatkan pertumbuhan dan inovasi. Pada tahun 2016 dibentuk *Data Privacy Commission* (DPC) yang kemudian menyusun aturan pelaksanaan terkait pengumpulan, pemrosesan dan penggunaan data pribadi[68].

---

66 Hasil amandemen tersebut mulai berlaku pada tanggal 15 Maret 2024. Untuk selengkapnya, baca: https://www.private-ai.com

67 Untuk selengkapnya, lihat: https://sso.agc.gov.sg>Act

68 Untuk analisis dan informasi selengkapnya, baca: https://clym.io>regulations

9. *Thailand Personal Data Protection Act* (PDPA) 2019

PDPA merupakan legislasi kunci di Thailand dan menyajikan pelindungan yang komprehensif terhadap data pribadi. Badan hukum lokal maupun asing yang mengumpulkan, menggunakan atau mengungkap data pribadi dari Subjek Data Pribadi di Thailand tunduk pada PDPA.

Ketentuan-ketentuan pokok pada PDPA Thailand, yang terdiri dari 7 (tujuh) Bab dan 96 sections meliputi pengaturan tentang: Komite Pelindungan Data Pribadi; Pelindungan Data Pribadi; Hak-hak Subjek Data Pribadi; Kantor Komite Pelindungan Data Pribadi; Keluhan (*Complaints*); Tanggung Jawab Keperdataan; dan Penalti.

10. *The United States of Amerika* (USA)

Pengaturan tentang PDP di Amerika Serikat (AS) terdiri dari seperangkat aturan, baik pada tingkat Federal, Negara Bagian hingga Kota. Pada tingkat *Federal the US Federal Trade Commission* (FTC) menggunakan otoritasnya untuk melindungi atas praktik yang tidak adil dan *deceptive*, terutama untuk mengambil langkah penindakan hukum terhadap praktik bisnis yang tidak adil dalam kaitas dengan *privacy* dan keamanan data.

Beberapa aturan lain yang relevan pada tingkat Federal, antara lain: *Driver's Privacy Protection Act* (1994); *Children's Online Privacy Protection Act* (COPPA); *Privacy Act* (1974); *Fair Credit Reporting Act* (1970); *Communications Act* (1934); *Federal Trade Commission Act* (1914); dan lain-lain[69]. Pada tahun 2022 suatu rancangan undang-undang, yaitu *The America Data Privacy and Protection Act* diusulkan, namun mendapatkan banyak tantangan dari beberapa senator, sehingga sulit diharapkan akan disepakati dalam jangka waktu yang singkat.

Pada tingkat Negara Bagian, California sangat aktif dengan memiliki sekitar 25 aturan Negara Bagian tentang *Privacy*, seperti: *California Consumer Privacy Act* (CCPA); *California Privacy Rights Act* (CPRA). Beberapa Negara Bagian juga telah memiliki aturan yang komprehensif tentang *Privacy*, seperti: Florida (2024); Oregon (2024); Texas (2024); Montana (2024)[70].

69 Lihat https://epic,org. diunduh pada tanggal 1 Oktober 2024.

70 Untuk uraian selengkapnya, baca: https://www.diapiperdataprotection.com, diunduh tanggal 1 Oktober 2024.

11. Republik Rakyat Tiongkok (RRT)

Personal Information Privacy Law (PIPL) adalah salah satu aturan utama dalam Pelindungan Data Pribadi di RRT. Undang-Undang ini ditetapkan oleh *Standing Committee of the National People's Congress* pada tanggal 20 Oktober 2021 dan efektif berlaku sejak 1 November 2021. Undang-Undang ini mengatur tentang pemrosesan informasi pribadi dan melindungi hak-hak dan kepentingan individu yang terkait dengan informasi pribadi. Undang-Undang ini menegaskan bahwa pemrosesan informasi pribadi harus terikat dengan prinsip-prinsip: legalitas; keadilan; integritas; minimum *necessity*; keterbukaan dan transparansi; dan tujuan pemrosesan harus dinyatakan secara eksplisit dan beralasan.

Hak-hak Subjek Data Pribadi juga diatur, meliputi: hak akses; hak memperoleh salinan; hak untuk memperbaiki dan meminta penghapusan data; *data compatibility*, dan lain-lain. Dalam hal memproses informasi pribadi anak-anak di bawah usia 14 tahun, pemroses data harus meminta persetujuan dari orang tua atau walinya, serta harus memiliki formula khusus tentang pemrosesan informasi pribadi.

PIPL melarang penggunaan sistem otomasi dalam pengambilan putusan yang didasarkan atas informasi pribadi seseorang yang berpotensi merugikan orang tersebut, misalnya terkait dengan penerapan harga yang diskriminatif. Individu juga harus diberikan hak *opt-out* terkait penggunaan informasi pribadinya untuk kepentingan pemasaran secara otomatis.

Dalam hal transfer data pribadi ke luar wilayah RRT (*mainland*), maka harus didasarkan atas persetujuan terpisah oleh subjek data pribadi, disamping memenuhi persyaratan lainnya seperti lulus penilaian keamanan yang dilakukan oleh otoritas siber nasional, memperoleh sertifikasi dari lembaga professional terkait serta berdasarkan kontrak standard yang dirumuskan oleh *national cyberspace authorities*.

PIPL juga memuat ketentuan hukuman denda atas pelanggaran terhadap ketentuan PIPL dengan denda maksimal 50 juta RMB atau 5% dari pendapatan tahunan atau juga dalam bentuk perintah penangguhan operasi bisnis atau pencabutan ijin atau lisensi yang dimiliki.

Highlights pengaturan PIPL meliputi: tujuan legislasi; target pengaturan; penerapan ekstra territorial; definisi informasi pribadi; definisi informasi pribadi sensitf; transparansi; pengumpulan, penggunaan dan pengungkapan informasi pribadi; persetujuan (*consent*); keakurasian; keamanan; periode retensi; akuntabilitas dan tata kelola; kewajiban *platform internet*; notifikasi kebocoran data; transfer data lintas batas negara; pengambilan putusan secara otomatis; hak akses dan pembetulan data; portabilitas informasi pribadi; hak menghapus, membatasi dan menolak pemrosesan informasi pribadi; hak untuk memperoleh informasi; otoritas penegakan hukum; penalty; kompensasi dan litigasi[71].

12. India

Perkembangan pengaturan Pelindungan Data Pribadi di India dimulai dari *The Information Technology Act* (IT *Act*) tahun 2000. Kemudian berkembang menjadi *Privacy Rules* tahun 2011. Pada tahun 2017, sembilan (9) Hakim pada pada Mahkamah Konstitusi di India menegaskan bahwa privasi merupakan hak fundamental yang diatur dalam Pasal 21 Konstitusi. Penegasan ini memberi arah bagi perumusan kerangka pengaturan yang komprehensif mengenai Pelindungan Data Pribadi. Setelah melalui proses yang cukup panjang dan atas rekomendasi dari Kementerian Elektronik dan Teknologi Informasi (MeitY), maka Pemerintah India merelease *the Draft of the Digital Personal Data Protection Bill* (DPDP Bill) pada tahun 2022.

Setelah melalui pembahasan atas DPDP Bill, pada tanggal 11 Agustus 2023 Pemerintah India mempublikasikan *Digital Personal Data Protection Act* (DPDP *Act*). DPDP *Act* menetapkan perlunya kepatuhan yang terkait dengan kegiatan pengumpulan, pemrosesan, penyimpanan dan transfer data pribadi digital. Namun demikian diperlukan langkah-langkah lebih lanjut guna mengefektifkan DPDP *Act*, termasuk aturan pelaksanaan bagi upaya implementasi dan penegakannya. DPDP *Act* hanya berlaku bagi data pribadi dalam bentuk digital. Dengan demikian maka pengumpulan dan penanganan data pribadi non-digital masih belum diatur di India[72].

---

71 Lihat https://www,pcpd.org.hk, diunduh tanggal 1 Oktober 2024.

72 Lihat https://www.dlapiperdataprotection.com versi 9 Januari 2024.

Prinsip-prinsip Pelindungan Data Pribadi pada DPDP *Act* umumnya sama dengan aturan, baik EU GDPR, aturan regional maupun aturan nasional di berbagai Negara. DPDP *Act* berlaku, baik terhadap pemrosesan data di India maupun yang bersifat ekstra territorial.

E. Pembelajaran dari Pengaturan Internasional

Dari pengaturan tentang PDP, baik dalam lingkup global, regional maupun nasional di beberapa Negara sebagaimana diuraikan di atas, dapat ditarik adanya standard dan unsur-unsur yang sama (common elements) sebagai berikut:

1. Unsur-Unsur yang Sama (*Common Elements*) dalam PDP yang pada umumnya mengatur tentang:

    a. Prinsip-Prinsip PDP (*Data Protection Principles*)
    Setiap pengaturan tentang PDP selalu mencantumkan prinsip-prinsip PDP seperti: pemrosesan data yang berdasarkan hukum, adil dan transparan; pembatasan pemrosesan data sesuai dengan tujuannya; pemrosesan data seminimal mungkin; keakurasian dan kemutakhiran data; pembatasan terhadap penyimpanan data; dijaminnya integritas, kerahasiaan dan keamanan data; akuntabilitas; pelindungan *data by design* dan *by default*.

    b. Hak-Hak Subjek Data Pribadi (*Rights of Data Subject*)
    Hak-hak Subjek Data Pribadi yang dilindungi meliputi, namun tidak terbatas pada: hak akses; hak atas informasi; hak untuk melakukan pembetulan; hak untuk mengajukan keberatan terkait penggunaan data pribadi untuk kepentingan pemasaran langsung; hak untuk meminta penghapusan data pribadi; hak untuk membatasi pemrosesan; hak untuk mengajukan keberatan terkait pemrosesan data secara otomatis; ha katas ganti rugi; hak pemulihan melalui proses judisial; serta hak untuk mengajukan keluhan melalui lembaga pengawas.

    c. Kewajiban Pengendali Data dan Pemroses Data (*Obligations of Data Controller and Data Processor*)

Sebagian besar pengaturan tentang PDP terkait dengan kewajiban dan tanggung jawab Pengendali Data yang mencakup: kewajiban memiliki kebijakan privasi; kewajiban menunjukkan persetujuan dan Subjek Data Pribadi; kewajiban menyampaikan informasi kepada Subjek Data Pribadi dalam terjadi perubahan informasi; menghentikan pemrosesan data jika Subjek Data Pribadi menarik kembali persetujuannya; menunda atau membatasi pemrosesan; melindungi Data Pribadi; melindungi data pribadi dari pemrosesan illegal; mencegah pemrosesan illegal; serta merekam semua kegiatan pemrosesan (*recording of processing activities*/ ROPA).

d. Adanya Lembaga Pengawas untuk Menegakkan Aturan PDP (*Special Enforcement Entity*)

Pada umumnya pengaturan tentang Lembaga Pengawas mencakup hal-hal seperti: sifat independen dari lembaga pengawas untuk melaksanakan tugasnya; adanya berbagai kewenangan, baik kewenangan investigasi, kewenangan pengawasan, kewenangan korekftif, kewenangan advisory hingga kewenangan penegakan aturan PDP.

Lembaga Pengawas mempunyai tugas-tugas yang cukup luas: dari memantau dan menegakkan aturan, meningkatkan kesadaran dan pemahaman; memberikan advis; kewenangan memberikan advis kepada Subjek Data Pribadi mengenai hak-haknya; menangani keluhan/aduan Subjek Data Pribadi; memantau perkembangan teknologi komunikasi dan informasi terkait PDP; menyusun check-list terkait *Data Protection Impact Assessment* (DPIA) mendorong penyusunan aturan perilaku (*code of conduct*) serta mendorong sertifikasi PDP.

Lembaga Pengawas dapat mengeluarkan peringatan, teguran hingga mengenakan denda terhadap pelanggaran atas ketentuan PDP.

e. Pemberitahuan kepada Subjek Data Pribadi dalam hal terjadinya Kebocoran Data (Data Breach Notification to Data Subject)

Dalam hal terjadinya kebocoran data, Pengendali Data dan Pemroses Data wajib untuk menyampaikan pengumuman kepada Subjek Data Pribadi tentang kebocoran data, termasuk upaya mitigasi serta pemulihannya.

Demikian pula informasi tentang dampak yang ditimbulkan terhadap hak-hak Subjek Data Pribadi.

f. Laporan kepada Otoritas yang Berwenang (Reporting to Authority)
Hampir semua pengaturan tentang PDP juga memuat ketentuan tentang kewajiban pelaporan terhadap Otoritas yang berwenang mengenai hal-hal yang terkait dengan kebocoran data atau hal-hal lain yang dipandang perlu.

g. Membedakan Antara Data Pribadi yang bersifat Umum dengan Data Pribadi Sensitif/Spesifik (*Differentiate Personal Data and Sensitive/ Specific Data*)
Pengaturan tentang PDP pada umumnya juga membedakan antara Data Pribadi yang bersifat Umum dengan Data Pribadi yang spesifik/sensitif. Meskipun salah satu prinsip utama PDP adalah Minimum Disclosure, namun biasanya pengaturan terhadap Data Pribadi Spesifik/Sensitif lebih ketat dan kadang-kadang membutuhkan persetujuan secara tegas dari Subjek Data Pribadi.

h. Mekanisme ADR dalam Penyelesaian Sengketa (*ADR Mechanism to Resolve Dispute*)
Dalam melaksanakan PDP selalu terbuka kemungkinan terjadinya sengketa. Untuk menyelesaikan sengketa tersebut diperlukan adanya mekanisme yang efektif yang memungkinkan para pihak yang bersengketa menyelesaikan melalui Alternatif Penyelesaian Sengketa (APS/ADR), termasuk melalui Mediasi. Di samping itu penyelesaian sengketa melalui Arbitrase atau bahkan melalui proses peradilan. Pada umumnya pada berbagai yurisdiksi mekanisme tersebut tersedia.

i. Kewajiban untuk Memiliki DPO (*Obligation to Have* DPO)
Berdasarkan ketentuan yang terdapat pada EU GDPR maupun praktek Negara-negara, dalam hal dilakukan pemrosesan Data Pribadi pada skala besar atau menyangkut Data Pribadi Spesifik/Sensitif dipersyaratkan ditunjukkan *Data Protection Officer* (DPO) yang memastikan bahwa kegiatan Pemrosesan Data mematuhi prinsip-prinsip PDP serta menghormati Hak-Hak Subjek Data Pribadi.

j. Upaya Pemulihan baik yang Bersifat Perdata Maupun Pidana (*Civil and Criminal Remedies*)
Dalam hal terjadi pelanggaran terhadap aturan PDP maupun Hak-Hak Subjek Data Pribadi, maka terbuka adanya upaya-upaya hukum untuk memulihkan hak-hak Subjek Data Pribadi, baik yang bersifat Perdata (melalui ganti rugi/kompensasi) atau yang bersifat Pidana (pidana denda maupun pidana kurungan atau bahkan pidana tambahan).

k. Analisis Dampak Pelindungan Data (*Data Protection Impact Assessment*/ DPIA)
Secara umum dalam rangka PDP, maka terhadap rencana kegiatan atau kegiatan yang dapat menimbulkan dampak terhadap Hak-Hak Subjek Data Pribadi, wajib dilakukan DPIA yang bertujuan untuk menghilangkan atau memitigasi dampak yang mungkin ditimbulkan. Pengaturan regional maupun praktek egara-negara juga menerapkan kewajiban melakukan DPIA bagi kegiatan-kegiatan pemrosesan data tertentu.

l. Denda Finansial yang diterapkan oleh Regulator (*Financial Penalty Imposed by Regulator*)
Terhadap pelanggaran atas aturan PDP serta Hak-Hak Subjek Data Pribadi, maka lembaga pengawas dapat mengenakan denda, baik terhadap Pengendali Data, Pemroses Data maupun pihak-pihak lain yang terkait. Dalam berbagai kasus jumlah denda yang dikenakan cukup besar.

m. Penerapan PDP pada Sektor Publik maupun Privat (*The Application to Public and Private Sector*)
Mengenai cakupan berlakunya aturan tentang PDP, sebagian besar berlaku, baik bagi sektor publik maupun sektor privat. Hanya beberapa negara yang memberlakukan aturan PDP bagi sektor privat saja.

2. Standard Internasional, Standar Industri dan Standar Nasional
Di samping Standar Nasional PDP sebagaimana yang dapat kita cermati di berbagai negara maupun Kawasan (*region*), standar PDP juga dapat kita

cermati pada lingkup Internasional maupun Industri. Di bawah ini diuraikan secara singkat berbagai standar yang dikenal.

a. Standar Internasional (*International Standard*)
International Association of Privacy Professionals (IAPP) adalah komunitas informasi global yang terbesar yang didirikan pada tahun 2000. IAPP adalah merupakan organisasi nirlaba bagi para profesional untuk mengembangkan dirinya dengan memajukan karirnya. IAPP merupakan wadah berkumpulnya para profesional privasi, juga merupakan sarana dan praksis pengelolaan informasi global yang dibutuhkan dalam perkembangan ekonomi informasi yang berkembang pesat. IAPP berpusat di Portsmouth, New Hampshire, Amerika Serikat.

Dalam ekonomi informasi, data adalah semacam mata uang yang sangat berharga dan resiko yang terkait dengan data juga sangat meningkat. Para profesional yang memahami resiko dalam era pengelolaan informasi global senantiasa berupaya mengamankan data dari berbagai resiko yang mengancam.

Dalam menjalankan organisasinya IAPP menyelenggarakan pelatihan berbasis kompetensi berserta sertifikasinya yang dirancang secara khusus bagi para profesional yang pekerjaannya terkait dengan pengelolaan, analisis, penanganan dan akses terhadap data sensitif yang merupakan tuntutan dalam menunaikan tugasnya. Sertifikasi yang dikeluarkan, yaitu sebagai *Certified International Privacy Professionals* (CIPP) sangat cocok bagi professional yang bertanggung jawab atas persoalan hukum, kepatuhan, pengelolaan informasi, tata kelola data, serta pengembangan sumber daya manusia. CIPP dirancang untuk kompetensi yang difokuskan pada aspek-aspek hukum dan regulasi pelindungan Data Pribadi dan bagaimana menerapkannya. Dengan demikian melalui pelatihan tersebut para profesional akan mampu menunjukkan penguasaan terhadap aspek hukum dari model-model penerapan yurisdiksi, regulasi dan penegakan, serta berbagai persyaratan hukum menangani dan mentransfer data.

Terdapat 4 (empat) pusat CIPP di berbagai kawasan, seperti: Asia (CIPP/A); Kanada (CIPP/C); Eropa (CIPP/E); US, yang terdiri dari US Private sector (CIPP/US) dan US Government (CIPP/G).

IAPP bukan merupakan organisasi yang bersifat supra-nasional, namun merupakan salah satu organisasi yang berupaya untuk memajukan profesi para profesional di bidang Pelindungan Data Pribadi.

b. Standar Industri (*Industrial Standard*)

Standar Industri dalam PDP juga tersebar dalam Standar ISO yang lebih rinci dan lebih teknis. Beberapa standar ISO yang dapat menjadi rujukan, antara lain:

– ISO 27001: *Information Security Management System* (ISMS) *Requirements*:

Ditetapkan pada tahun 2005 sebagai hasil kolaborasi antara ISO dan IEC. Nama lengkap dari ISO 27001 adalah: *information-technology-security tecniques-information security management systems-requirements*. ISO 27001 berlaku untuk semua tipe organisasi, baik *commercial enterprises, government agencies,* maupun *non-profit organizations.*

ISO 27001 secara khusus mempersyaratkan tentang: *establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System* (ISMS) dalam suatu *organisasi for adequate and proportionate security controls and to protect all information assets and give confidence to interested parties about their security.*

Manfaat dari penerapan ISO 27001 antara lain: melindungi kerahasiaan, integritas dan ketersediaan informasi (*protecting confidentiality, integrity, and availability of information*); melindungi asset dan informasi sensitif (*protection of assets and sensitive information*); mengurangi resiko keamanan informasi (*reduce information security risks*); keuntungan kompetitif (*competitive advantage*); serta meningkatkan reputasi dan menambah keyakinan konsumen (*improving reputation and increasing customer confidence*).

– ISO 27000

Berbagai standard yang dipublikasi terkait ISO 27000, adalah: *overview and vocabulary* (ISO 27000); *Requirements* (ISO 27001); *Code of Practice* (ISO 27002); *Information Security Management Measurements* (ISO 27004); *Information Security Risk Management* (ISO 27005); *Requirements for Certification Bodies* (ISO 27006); *Guidelines for Telecommunications Organizations* (ISO 27011); *Guidelines for Business Continuity* ((ISO 27031); *Network Security, Overview and Concepts* (ISO 27033-1); *Network Security, Networking Scenarios* (ISO 27033-3); *Information Security Management in Health* (ISO 27799).

– ISO 27002

Adalah standar yang mendukung keseluruhan implementasi sistem manajemen keamanan informasi (*information security management system*). Standar ini dipublikasikan oleh ISO (*International Organization for Standardization*) dan IEC (*International Electronical Commission*). Seiring dengan teknologi yang terus berkembang, standar ini juga terus dikembangkan untuk mengatasi perubahan persyaratan keamanan informasi di berbagai industri dan lingkungan.

ISO 27002 berfungsi sebagai acuan keamanan informasi yang dirancang untuk membantu perusahaan dalam memilih, menerapkan, dan memelihara Sistem Manajemen Keamanan Informasi (SMKI). Standar ini digunakan sebagai standar pelengkap pada ISO 27000 series, khususnya untuk seri utama 27001. ISO 27002 digunakan sebagai panduan yang lebih spesifik dari kerangka kerja ISO 27001 untuk memilih kontrol keamanan yang sesuai dalam menerapkan ISMS yang efektif.

Standar ISO 27002 memberikan berbagai referensi terkait kontrol keamanan informasi secara umum, termasuk panduan implementasinya yang dirancang untuk organisasi dalam rangka: penerapan sistem keamanan informasi berdasarkan ISO 27001;

untuk menerapkan kontrol keamanan informasi berdasarkan praktik terbaik yang diakui secara internasional; untuk mengembangkan pedoman manajemen keamanan informasi khusus organisasi.

ISO 270022 (022) menyediakan kerangka kerja keamanan informasi yang terdiri dari 14 (empat belas) Bab dengan topik yang mencakup kebijakan dan keamanan: kebijakan keamanan informasi; manajemen pengembangan dan pemeliharaan; pengelolaan asset; informasi organisasi; sumber daya manusia; akses; operasional; komunikasi; sistem penyedia layanan; persyaratan pemrosesan transaksi; persyaratan aplikasi; lingkungan; persyaratan pengembangan sistem; dan persyaratan manajemen pengiriman[73].

– ISO 29100 (*Privacy Framework*)
  ISO 29100 adalah merupakan kerangka privasi: menerapkan terminology privasi yang umum; menetapkan para pihak terkait beserta perannya masing-masing dalam memproses *personally identifiable information* (PII); menggambarkan pertimbangan bagi pengamanan privasi; memberikan referensi bagi prinsip-prinsip privasi bagi teknologi informasi. ISO 29100 berlaku bagi orang-perorangan maupun organisasi yang terlibat dalam kegiatan specifying, pengadaan, merancang, mengembangkan, melakukan pengetesan, menjaga, mengadministrasikan dan mengoperasikan sistem teknologi informasi dan komunikasi atau jasa-jasa lain dimana pengendalian data diperlukan bagi pemrosesan PII[74].
– ISO 29151 (PII *Protection Code of Practice*)
  Intinya memberikan panduan untuk melindungi PII. Standard ini menjelaskan pengendalian keamanan yang dapat diterapkan oleh setiap organisasi untuk menjaga integritas, kerahasiaan, dan ketersediaan PII.
– ISO 29134 (*Privacy Impact Assessment*)
  Privacy Impact Assessment (PIA) adalah suatu instrumen untuk: menilai potensi dampak privasi dari suatu kegiatan pemrosesan,

[73] Baca, kualitaskonsultan.com, diunduh tanggal 1 Juni 2024.
[74] Lihat https://www.iso.org/standard/45123.html.

sistem informasi, program, modul perangkat lunak, peralatan atau inisiatif lainnya yang memproses informasi pribadi yang dapat diidentifikasi; mengambil langkah-langkah yang diperlukan melalui konsultasi dengan pemangku kepentingan, untuk mengatasi resiko privasi[75].

Laporan PIA dapat mencakup dokumentasi tentang tindakan-tindakan yang dilakukan sebagai bentuk penanganan resiko, misalnya penanganan masalah resiko-resiko yang timbul dari penggunaan *information security management system* (ISMS) pada ISO 27001. PIA lebih dari sekedar tool, tetapi merupakan proses yang dimulai seawal mungkin dari suatu inisiatif, jika masih ada kesempatan untuk untuk memengaruhi hasilnya, yang oleh karenanya akan memastikan perlindungan *privacy by design*. PIA adalah merupakan suatu proses yang terus berlangsung dan bahkan hingga setelah proyek tersebut digelar.

Dasar pertimbangan dalam melakukan PIA, meliputi: manfaat yang dapat diperoleh dari kegiatan melakukan PIA; tujuan pelaporan PIA; akuntabilitas dalam melakukan PIA; serta skala dalam melakukan PIA[76].

Beberapa pedoman dalam melakukan PIA, intinya: melakukan threshold analysis untuk mengetahui apakah PIA perlu dilakukan; melakukan persiapan untuk melakukan PIA (misalnya: membentuk tim dan mempersiapkan arahan, menyiapkan perencanaan PIA, menggambarkan apa yang akan dinilai, pelibatan pemangku kepentingan); pelaksanaan PIA (misalnya: mengidentifikasi alur informasi, menganalisis implikasinya, menentukan persyaratan pengamanan informasi yang relevan, menilai resiko privasi, penyiapan untuk mengatasi resiko privasi); menindaklanjuti PIA (penyiapan laporan, publikasi, implementasi rencana penanganan resiko, *review* dan/atau audit, merefleksikan perubahan pada proses).

[75] Lihat ISO, "Information Technology-Security Techniques-Guidelines for Privacy Impact Assessment", Edisi ke 2, tahun 2023.

[76] Ibid.

Terkait dengan Laporan, hal-hal yang harus diperhatikan mencakup: struktur laporan; cakupan PIA (proses yang sedang dievaluasi, kriteria resiko, sumber daya dilibatkan dalam PIA, konsultasi dengan pemangku kepentingan); persyaratan privasi; penilaian resiko (sumber-sumber resiko, ancaman dan semacamnya, konsekuensi dan tingkat dampaknya, evaluasi resiko, analisis kepatuhan); rencana penanganan resiko; kesimpulan dan putusan yang diambil; ringkasan umum PIA[77].

– ISO 27035 (*Information Security Incident Management*)
ISO 27035 merupakan standard yang difokuskan pada manajemen insiden keamanan informasi. Standard ini memberikan panduan bagi organisasi untuk merencanakan, mendeteksi, menilai, dan merespons insiden keamanan informasi, serta meningkatkan perlindungan dari insiden di masa depan.

– ISO 27018
ISO 2708 adalah aturan praksis yang difokuskan pada pelindungan data pada cloud. Pada prinsipnya didasarkan atas ISO 27002 (*information security standard*) dan memberikan pedoman implementasi pengendalian atas public cloud PII.

– ISO 27701: *Privacy* Management Information System (PMIS)
Adalah standar mengenai Sistem Manajemen Informasi Privasi (*Privacy Management Information System*) yang memberikan pedoman untuk pelindungan privasi dan penanganan Data Pribadi. Standar ini membantu untuk menunjukkan kepatuhan terhadap peraturan Pelindungan Data di seluruh dunia. Proses ISO 27701 meliputi: *confidentiality; analyse risk; responsibility; identify processor requirements; identify controller's requirements; record keeping; internal process and training*.

ISO 27701 merupakan perluasan dari ISO 27001 dan ISO 27002. Manfaat dari penerapan ISO 27701 adalah: memperbaiki privasi (*improvement privacy*); pelindungan dari kebocoran data

[77] Ibid.

(*protection from data breached*); meningkatkan kepuasan konsumen (*improved customer satisfaction*); untuk pemasaran (*marketing*); serta meningkatkan pengakuan internasional (*increased international recognition*).

c. Standar Nasional (*National Standard*)

– Standard Kompetensi Kerja Nasional Indonesia (SKKNI)
Berdasarkan Undang-Undang No 13 tahun 2003 tentang Ketenagakerjaan, terdapat standard kompetensi kerja nasional Indonesia (SKKNI) yang harus diperhatikan dalam rangka pengembangan kompetensi kerja tenaga kerja yang sesuai dengan kebutuhan dunia usaha, dunia industri dan dunia kerja (Dudika). Sebagai acuan dalam pengembangan kompetensi tenaga kerja, terutama pada sektor Pelindungan Data Pribadi, perlu diperhatikan beberapa peraturan yang relevan, antara lain: Peraturan Pemerintah No 31 tahun 2006 tentang Sistem Pelatihan Kerja Nasional (Sislatkernas); Peraturan Pemerintah No 10 tahun 2018 tentang Badan Nasional Sertifikasi Profesi (BNSP); Peraturan Menteri Ketenagakerjaan No 2 tahun 2016 tentang Sistem Standardisasi Kompetensi Kerja Nasional Indonesia (SKKNI); dan Keputusan Menteri Ketenagakerjaan No 102 tahun 2023 tentang Penetapan SKKNI Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan yang Berhubungan dengan itu Bidang Keahlian Pelindungan Data Pribadi.

– Kerangka Kualifikasi Nasional Indonesia (KKNI)
Menurut Peraturan Presiden No 8 tahun 2012 tentang KKNI, dinyatakan bahwa KKNI adalah kerangka penjenjangan kualifikasi kompetensi yang dapat menyandingkan, menyetarakan dan mengintegrasikan antara bidang pendidikan dan bidang pelatihan kerja serta pengalaman kerja dalam rangka memberikan pengakuan kompetensi kerja sesuai dengan struktur pekerjaan di berbagai sektor.

KKNI menetapkan 9 (ssembilan) jenjang kualifikasi dari tingkat operator (jenjang 1-3), tingkat teknis/analis (jenjang4-6), tingkat ahli (jenjang 7-9). Jenjang-jenjang tersebut dapat dicapai, baik melalui pendidikan, pelatihan kerja atau pengalaman kerja.

Jenjang KKNI DPO diperkirakan pada level 6 (spesialis dan analis monodisipliner), level 7 (supervisi dan analis mono disipliner), dan level 8 (inter dan multidisipliner).

– Peta Okupasi

Peta Okupasi terkait PPDP minimal mencakup 15 okupasi, yaitu: DPO, *privacy program manager*, *privacy product development*, *privacy auditor, chief privacy officer, data protection executives, data protection authority, privacy council, privacy analist, director of privacy, privacy manager, privacy engineer, privacy specialist, privacy delegates/liaison, privacy technologist*[78].

[78] Lihat, Kominfo, Grand Design Pembentukan Ekosistem DPO, 2021.

BAB III

INISIATIF AWAL, PERUMUSAN DAN PEMBAHASAN RANCANGAN UNDANG-UNDANG PELINDUNGAN DATA PRIBADI

A. Insiatif Awal

Inisiatif awal dalam upaya perumusan pengaturan tentang PDP dalam lingkup nasional, mencakup:

1. Studi yang diinisiasi Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi

   Studi awal diinisiasi oleh Kementerian Pemberdayaan Aparatur Negara dan Reformasi Birokrasi sebagai upaya untuk menciptakan *Good Governance and Clean Government* melalui pengembangan *Single Identification number*. Penulis (IBR Supancana) bersama-sama dengan Prof Abu Bakar Munir *(University of Malaya),* Prof Siti Hajar *(Mara Technological University*, Malaysia), Dr Sonny Zulhuda *(International Islamic University,* Malaysia) mendapatkan tugas untuk menyusun suatu kajian sebagai cikal bakal pengaturan lebih lanjut dalam suatu undang-undang khusus.

2. Hasil Kajian

Hasil kajian diselesaikan pada tahun 2007 dengan judul "Harmonisasi dan Sinkronisasi Konsepsi Hukum Perlindungan Data dan Informasi Pribadi". Isi pokok dari kajian tersebut adalah: latar belakang; kerangka konsepsi hukum perlindungan data dan informasi pribadi; pemetaan peraturan perundang-undangan yang mengatur penghimpunan data dan informasi; perbandingan pengaturan internasional tentang privasi atas data dan informasi pribadi; implikasi atas keberadaan pengaturan yang memberikan perlindungan atas data dan informasi pribadi; pembangunan kesisteman dalam rangka pembuatan *Indonesian National Id Card*; serta Penutup[79].

Latar belakang dari studi ini menyoroti tentang kemajuan ilmu pengetahuan dan teknologi informasi dan komunikasi serta berbagai peluang dan tantangan yang menjadi implikasinya. Salah satu hak dasar yang penting untuk dilindungi adalah privasi, terutama *information privacy*. Saat itu belum ada pengaturan yang sifatnya komprehensif terkait Perlindungan Data dan Informasi Pribadi. Akibat belum adanya pengaturan tersebut menimbulkan berbagai permasalahan, meliputi: terjadinya penyalahgunaan terhadap data dan informasi pelanggan yang digunakan sebagai persyaratan transaksi bisnis; terjadinya kasus kartu tanda penduduk yang berlainan dengan data dan informasi dari yang sebenarnya; terjadinya kejahatan yang bermula dari pencarian data dan informasi seseorang; penghilangan identitas atas data dan informasi dari pelaku kejahatan seperti *illegal logging, illegal fishing, illegal mining* dan *money laundering*, praktek perbankan illegal dan lain sebagainya; pelanggaran privasi atas data dan informasi seseorang. Latar belakang tersebut juga menjadikan adanya kebutuhan suatu undang-undang yang mampu menjamin pelindungan bagi seseorang atas data dan informasinya[80].

Dalam Bab II tentang Kerangka Konsepsi Hukum Pelindungan Data dan Informasi Pribadi, diperjelas berbagai peristilahan dan konsep kunci, seperti: konsepsi privasi; konsepsi hak; konsepsi hak atas privasi; konsepsi pelindungan privasi, khususnya data dan informasi pribadi; konsepsi data

[79] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, Harmonisasi dan Sinkronisasi Konsepsi Hukum Perlindungan Data Pribadi: Menuju Hukum yang Adil, Program Penerapan Ke Pemerintahan yang Baik, 2007.

[80] Ibid, halaman 1-6.

pribadi dan pelindungannya; kecenderungan atas pengaturan privasi data dan informasi pribadi; arti penting pengaturan dan pelindungan data dan informasi pribadi; landasan pengaturan pelindungan data dan informasi pribadi; serta materi pengaturan pelindungan data dan informasi pribadi[81].

Dalam Bab III tentang Peraturan Perundang-Undangan yang mengatur Penghimpunan Data dan Informasi Pribadi, dibahas beberapa hal penting, seperti: jenis-jenis pelayanan; dan ketentuan peraturan perundangan terkait[82].

Dalam Bab IV tentang Perbandingan Pengaturan Internasional tentang Privasi atas Data dan Informasi Pribadi, digambarkan beberapa hal, seperti: kerjasama multilateral; pengaturan di berbagai Negara; respons atas arah dan kecenderungan pengaturan Pelindungan Data dan Informasi Pribadi dalam perspektif Indonesia[83].

Bab V yang membahas Implikasi atas Keberadaan Pengaturan yang memberikan Pelindungan Privasi atas Data dan Informasi Pribadi, mengkajinya baik dari aspek implikasi eksternal (internasional) maupun implikasi internal (domestik)[84].

Pada Bab VI tentang Pembangunan Kesisteman dalam rangka Pembuatan *Indonesia National Id Card* dibahas beberapa aspek yang relevan, antara lain: landasan konstitusional; layanan pemerintah; kesisteman; *single identity number*; masalah pengelolaan data; kebutuhan adanya identitas warganegara; serta instansi pengelola identitas warga Negara[85].

Bab VII yaitu Bab Penutup menyajikan beberapa kesimpulan serta saran[86].

3. Konsultasi Awal

Konsultasi awal terhadap hasil kajian yang dilakukan Tim dibahas dalam suatu kegiatan konsultasi publik pada tanggal 4 September 2007 yang melibatkan baik kementerian dan lembaga terkait, akademisi, dunia usaha dan perwakilan masyarakat.

81 Ibid, halaman 7-50.
82 Ibid, halaman 51-70.
83 Ibid, halaman 71-94.
84 Ibid, halaman 95-114.
85 Ibid, halaman 115-124.
86 Ibid, halaman 125-130.

B. Naskah Akademik dan Draft Final

1. Naskah Akademis Tahun 2015

   Naskah Akademis 2015 disusun setelah ada kepastian penugasan kepada Kementerian Kominfo untuk mengawal penyusunan RUU PDP. Sebagaimana diketahui sejak tahun 2008 belum dicapai kesepakatan instansi mana yang ditunjuk sebagai inisiator dari RUU PDP. Ada 3 (tiga) Kementerian yang sebelumnya berpotensi menjadi inisiator, yaitu Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi yang merupakan inisiator awal, Kementerian Kominfo yang berhasil menginisiasi Undang-Undang ITE dan Undang-Undang Keterbukaan Informasi Publik, serta Kementerian Dalam Negeri yang menginisiasi Undang-Undang tentang Kependudukan dan Catatan Sipil.

   Naskah Akademis tahun 2015 merupakan hasil pemutakhiran dari hasil kajian sebelumnya. Naskah Akademis ini terdiri dari 5 (lima) Bab, yaitu: Bab Pendahuluan; Bab Kajian Teoritis dan Praktek Empiris; Bab tentang Evaluasi dan Analisis Peraturan Perundang-undangan Terkait; Bab tentang Landasan Filosofis, Sosiologis dan Yuridis; Bab tentang Jangkauan, Arah Pengaturan, dan Ruang Lingkup Materi Muatan Rancangan Undang-Undang; dan Penutup.

   Secara Yuridis Formal isi dari Naskah Akademis tahun 2015 memang telah memenuhi persyaratan sebagaimana diatur dalam Undang-Undang Nomor 12 tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan, namun secara substansi ada beberapa hal yang perlu dicermati, antara lain: perlu ada analisis dari perspektif bisnis internasional; perlu disesuaikan dengan standar internasional mutakhir; perlu *benchmark* internasional tentang penerapan PDP dari kasus-kasus yang terjadi; perlu pemutakhiran kepustakaan; harmonisasi terhadap peraturan perundang-undangan juga perlu dimutakhirkan; analisis dampak regulasi masih sangat sederhana dan minimalis; serta masih adanya penggunaan isitilah yang kurang tepat[87].

[87] Mengenai analisa kritis terhadap Naskah Akademis 2015, baca: I B R Supancana, "Menuju Undang-Undang Perlindungan Data Pribadi yang Modern, Mengakomodasikan Kepentingan Nasional dan Berstandar Internasional", materi disampaikan pada Brownbag Discussion Proyeksi Kebijakan Perlindungan Data Pribadi, Jakarta 7 Juli 2020.

2. Draft Rancangan Undang-Undang PDP tahun 2020

Rancangan Undang-Undang tentang PDP terdiri dari XVI Bab dan 80 Pasal. Ketentuan-ketentuan Pokok yang diatur meliputi: ketentuan umum; asas, prinsip dan tujuan; jenis data pribadi; hak pemilik data pribadi; pemrosesan data pribadi; kewajiban Pengendali Data Pribadi, Prosesor Data Pribadi dan pihak ketiga dalam pemrosesan data pribadi; transfer dan pengalihan data pribadi; larangan dalam penggunaan data pribadi; pembentukan pedoman perilaku Pengendali Data Pribadi; Pengeculaian terhadap PDP; penyelesaian sengketa; kerjasama internasional; peran Pemerintah dan masyarakat; ketentuan pidana; ketentuan peralihan; dan penutup.

Terhadap RUU tersebut ada beberapa hal yang pada saat itu perlu dicermati, antara lain: penggunaan istilah yang kurang tepat (misalnya isitilah Pemilik Data Pribadi); batasan yang terlalu sederhana dan tidak operasional (bandingkan dengan EU GDPR); tujuan belum menunjukkan keseimbangan antara hak Subjek Data Pribadi dengan Pemerintah; tidak konsisten dengan Naskah Akademik (data sensitif vs data pribadi yang bersifat spesifik); hak Subjek Data Pribadi kurang diimbangi dengan kewajiban; tidak jelas fungsi pihak ketiga dan pejabat pelindungan data pribadi; mengapa pejabat pelindungan data pribadi diatur dengan Peraturan Menteri? Padahal seharusnya independen; belum tampak fungsi badan penyelesaian sengketa di luar pengadilan, terutama terkait keluhan Subjek Data Pribadi kepada Pengendali Data; tidak diatur secara khusus mengenai Komisi Independen[88].

C. Pembahasan di DPR

1. Amanat Presiden

Atas Dasar Naskah Akademis dan RUU PDP, maka Presiden menyampaikan Amanat (Surat Presiden) ke DPR untuk pembahasan RUU PDP sebagai Prolegnas Prioritas yang direncanakan dapat diselesaikan pada tahun 2020.

[88] Lihat, Ibid.

2. Daftar Inventarisasi Masalah (DIM)
   Pemerintah dan Komisi I DPR menyepakati Daftar Inventarisasi Masalah yang terdiri dari kluster sebagai berikut: Fix Proposal sebanyak 66; Fix Proposal dengan beberapa catatan sebanyak 49; usulan amandemen/ perubahan sebanyak 179; usulan perubahan atas rumusan/formulasi sebanyak 9; dan usulan baru sebanyak 68.

3. Pembahasan Antara Eksekutif dan Legilatif
   Pembahasan awal RUU PDP dimulai pada bulan September 2020 dan direncanakan dapat diselesaikan dalam maksimal 3 kali masa sidang. Pada Rapat Paripurna DPR yang ke 21 masa sidang ke V DPR RI masa sidang 2020-2021 pada tanggal 22 Juni 2021 dicapai kesepakatan untuk menyelesaikan pembahasan, bahkan dilakukan konsinyering pada tanggal 29-30 Juni 2021, namun terjadi deadlock, sehingga target penyelesaian pada tanggal 16 Juli 2021 tidak tercapai.

4. Isu-isu yang Krusial Dalam Pembahasan
   Terdapat beberapa isu krusial yang menyebabkan sulitnya dicapai kesepakatan. Isu-isu krusial tersebut meliputi: tentang Lembaga Pengawas; tentang Pengendali Data; tentang *Transboundary Flow of Personal Data*; tentang penyelesaian sengketa; serta perlakuan terhadap data elektronik dan data non-elektronik.

   Isu yang paling alot dibahas adalah tentang Lembaga Pengawas PDP. Sikap Komisi I DPR yang didukung 8 Fraksi intinya menyatakan bahwa Lembaga Pengawas seharusnya bersifat independen karena UU PDP nantinya berlaku baik bagi sektor publik maupun sektor privat. Hal itu juga didukung oleh standard dan praksis terbaik internasional dimana sekitar 114 negara menempatkan lembaga pengawas sebagai lembaga independen. Hanya beberapa negara (termasuk Malaysia dan Singapura) yang menempatkan lembaga pengawas pada Pemerintah, karena UU PDP di Malaysia dan Singapura pada saat itu hanya berlaku untuk sektor privat. Pandangan fraksi-fraksi di DPR tersebut juga didukung oleh para pakar, LSM dan publik.

Sementara itu Pemerintah yang didukung oleh 1 fraksi, yaitu Fraksi Nasdem (Fraksi Menkominfo pada saat itu) menginginkan agar Lembaga Pengawas berada di bawah Kemenkominfo. Alasannya antara lain: alasan efektivitas serta ketersediaan sumber daya serta semangat untuk tidak membentuk badan baru (moratorium), serta telah dipraktekkan di beberapa negara (hanya sekitar 10 dari 140 negara).

Untuk mengatasi kebuntuan dalam pembahasan yang sangat penting tersebut telah dilakukan upaya-upaya terobosan, seperti: menggunakan standar internasional tentang Lembaga Pengawas; setuju tidak membentuk badan baru, namun memperluas kewenangan badan yang ada (misalnya memperluas kewenangan Komisi Informasi menjadi 2 kamar); serta harus ada intervensi Presiden karena Indonesia akan menjadi tuan rumah G-20 Summit. Dari anggota G-20 ada desakan Indonesia segera menyelesaikan pembahasan RUU PDP, karena adanya UU PDP disamping sebagai perwujudan penghormatan hak-hak asasi manusia terkait privasi, juga harus memfasilitasi *cross-border data flow* untuk kepentingan bisnis, investasi, perdagangan, dan keuangan.

5. Kesepakatan yang dicapai

   Untuk menyongsong pelaksanaan G-20 *Summit* di Bali pada tahun 2022, akhirnya antara Pemerintah dan DPR menyepakati bahwa Lembaga Pengawas tersebut akan berada di bawah Presiden yang rinciannya akan diatur dalam aturan pelaksanaan UU PDP.

BAB IV

ANALISA KRITIS TERHADAP KETENTUAN-KETENTUAN UNDANG-UNDANG PELINDUNGAN DATA PRIBADI

A. Ketentuan-ketentuan Pokok yang Diatur

1. Ketentuan Umum

   Dalam Ketentuan Umum dirumuskan beberapa peristilahan yang digunakan dalam Undang-Undang ini beserta pengertiannya, seperti: Data Pribadi; Pelindungan Data Pribadi; Informasi; Pengendali Data Pribadi; Prosesor Data Pribadi; Subjek Data Pribadi[89]. Dalam Ketentuan Umum juga diatur ruang lingkup berlakunya Undang-Undang ini, baik yang berada di wilayah hukum negara Republik Indonesia maupun yang di luar wilayah hukum negara Republik Indonesia sepanjang akibat hukum terjadi di wilayah hukum negara Republik Indonesia dan/atau dampaknya terhadap Subjek Data Pribadi di luar wilayah hukum negara Republik Indonesia[90].

89 Pasal 1 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
90 Ibid, Pasal 2 ayat 1.

2. Asas

   Beberapa asas penting menjadi dasar bagi Undang-Undang ini, yaitu: pelindungan; kepastian hukum; kepentingan umum; kemanfaatan; kehati-hatian; keseimbangan; pertanggungjawaban; dan kerahasiaan[91].

3. Pengertian dan Jenis-jenis Data Pribadi

   Secara umum Data Pribadi dibagi atas: Data Pribadi yang bersifat spesifik dan Data Pribadi yang bersifat umum[92]. Data Pribadi yang bersifat spesifik terdiri dari: data dan informasi kesehatan; data biometrik; data genetika; catatan kejahatan; data anak; data keuangan pribadi; dan atau lainnya sesuai dengan ketentuan peraturan perundang-undangan[93]. Sementara itu data pribadi yang bersifat umum, meliputi: nama lengkap; jenis kelamin; kewarganegaraan; agama; status perkawinan; dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang[94].

4. Hak-hak Subjek Data

   Dalam Undang-Undang ini, hak-hak dari Subjek Data Pribadi, mencakup: hak untuk mendapatkan informasi[95]; hak melakukan pembetulan atas Data Pribadi nya[96]; hak akses[97]; hak mengakhiri dan menghapus pemrosesan Data Pribadi[98]; hak menarik kembali persetujuan[99]; hak mengajukan keberatan atas pemrosesan data secara otomatis[100]; hak menunda atau membatasi pemrosesan Data Pribadi[101]; hak menggugat dan memperoleh ganti rugi[102]; hak portabilitas[103].

---

91 Ibid, Pasal 3.
92 Ibid, Pasal 4 ayat (1).
93 Ibid. Pasal 4 ayat (2).
94 Ibid, Pasal 4 ayat (3).
95 Ibid, Pasal 5.
96 Ibid, Pasal 6.
97 Ibid, Pasal 7.
98 Ibid, Pasal 8.
99 Ibid, Pasal 9.
100 Ibid, Pasal 10.
101 Ibid, Pasal 11.
102 Ibid, Pasal 12.
103 Ibid, Pasal 13.

Dalam hal-hal tertentu, pelaksanaan hak Subjek Data Pribadi, khususnya sebagaimana dimaksud dalam Pasal 6 sampai 11 diajukan melalui permohonan tercatat yang disampaikan secara elektronik atau non-elektronik kepada Pengendali Data Pribadi[104].

Terdapat beberapa pengecualian terkait pelaksanaanhak-hak Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 8, 9, 10, 11 ayat (1), dan 13 ayat 1. Pengecualian tersebut dalam hal: kepentingan pertahanan dan keamanan Negara; 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; dan kepentingan statistik dan penelitian ilmiah[105].

5. Pemrosesan Data Pribadi

   Pemrosesan data pribadi meliputi kegiatan-kegiatan yang cakupannya sangat luas dan rinci, seperti: pemerolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan atau pengangkapan; dan/atau penghapusan atau pemusnakan[106]. Dalam melakukan kegiatan pemrosesan data pribadi harus dilakukan dengan mematuhi prinsip-prinsip: dilakukan secara terbatas dan spesifik, sah secara hukum dan transparan; dilakukan dengan menjamin hak-hak Subjek Data Pribadi; dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan; memastikan keamanan dan integritas data; memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Pelindungan Data Pribadi; menghapus atau memusnahkan data atas permintaan Subjek Data Pribadi; serta dilakukan secara bertanggungjawab[107].

6. Kewajiban Pengendali Data dan Pemroses Data

   Ketentuan tentang kewajiban Pengendali Data dan Pemroses Data yang diatur dalam Undang-Undang Pelindungan Data Pribadi cukup banyak

[104] Ibid, Pasal 14.
[105] Ibid, Pasal 15.
[106] Ibid, Pasal 16 ayat (1).
[107] Ibid, Pasal 16 ayat (2).

tersebar dari Pasal 19 sampai Pasal 54. Boleh dikatakan hampir 50% ketentuan yang terdapat dalam Undang-Undang tentang Pelindungan Data Pribadi menyangkut tentang Kewajiban Pengendal Data dan Pemroses Data.

Kewajiban Pengendali Data meliputi, antara lain: kewajiban memiliki dasar pemrosesan[108]; kewajiban menyampaikan informasi tentang legalitas, tujan, jenis dan relevansi, jangka waktu retensi, rincian informasi, jangka waktu pemrosesan, hak subjek data pribadi[109] kewajiban menunjukkan persetujuan[110]; kewajiban memperoleh persetujuan dalam pemrosesan data pribadi penyandang disabilitas[111]; kewajiban melakukan pemrosesan data secara spesifik, sah dan transparan[112]; kewajiban melakukan pemrosesan sesuai dengan tujuannya[113]; kewajiban memastikan akurasi, kelengkapan dan konsistensi data pribadi[114]; kewajiban memperbarui atau memperbaiki kesalahan[115]; kewajiban melakukan perekaman pemrosesan[116]; kewajiban melakukan analisis dampak PDP[117]; kewajiban menjamin keamanan[118]; kewajiban menjaga kerahasiaan[119]; kewajiban melakukan pengawasan[120]; kewajiban melindungi Data Pribadi dari pemrosesan yang tidak sah[121]; kewajiban mencegah akses Data Pribadi yang tidak sah[122]; kewajiban menghentikan pemrosesan data karena penarikan persetujuan[123].

7. Pejabat Pelindungan Data Pribadi (PPDP)
   Dalam keadaan-keadaan tertentu Pengendali Data wajib menunjuk Pejabat Pelindungan Data Pribadi (PPDP), dalam hal: melakukan pemrosesan data

[108] Ibid, Pasal 20 ayat (1).
[109] Ibid, Pasal 21 (1).
[110] Ibid, Pasal 24.
[111] Ibid, Pasal 26.
[112] Ibid, Pasal 27.
[113] Ibid, Pasal 28.
[114] Ibid, Pasal 29 ayat (1).
[115] Ibid, Pasal 30 ayat (1).
[116] Ibid, Pasal 31.
[117] Ibid, Pasal 34 ayat (1).
[118] Ibid, Pasal 35.
[119] Ibid, Pasal 36.
[120] Ibid, Pasal 37.
[121] Ibid, Pasal 38.
[122] Ibid, Pasal 39 ayat (1).
[123] Ibid, Pasal 40 ayat (1).

pribadi untuk kepentingan pelayanan publik; kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; kegiatan inti Pengendali Data terdiri dari pemrosesan data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana[124].

PPDP wajib memiliki kualifikasi, setidak-tidaknya: berdasarkan profesionalitas; pengetahuan mengenai hukum; praktik pelindungan Data Pribadi; serta kemampuan untuk memenuhi tugas-tugasnya[125].

Tugas minimal PPDP adalah: menginformasikan dan memberikan saran kepada Pengendali Data Pribadi dan Prosesor Data Pribadi agar mematuhi ketentuan dalam Undang-Undang PDP; memantau dan memastikan kepatuhan terhadap Undang-Undang PDP dan kebijakan Pengendali Data Pribadi atau Prosesor Data Pribadi; memberikan saran mengenai penilaian dampak PDP dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi; berkoordinasi dan bertindak sebagai nara hubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi[126].

8. Transfer Data Pribadi

Transfer Data dapat berlangsung baik dalam wilayah hukum Republik Indonesia maupun Transfer Data ke luar wilayah hukum Republik Indonesia. Pengendali Data Pribadi dapat melakukan transfer data pribadi lainnya dalam wilayah hukum Republik Indonesia[127]. Pengendali Data Pribadi yang melakukan transfer maupun yang menerima transfer data pribadi wajib melakukan pelindungan data pribadi.

Untuk Transfer Data ke luar wilayah Hukum Republik Indonesia, maka berlaku ketentuan: dalam melakukan transfer data, Pengendali Data Pribadi wajib memastikan negara tempat kedudukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari ketentuan UU PDP; dalam hal Negara

[124] Ibid, Pasal 53 ayat (1).
[125] Ibid, Pasal 53 ayat (2).
[126] Ibid, Pasal 54 ayat (1).
[127] Ibid, Pasal 55.

Penerima tidak memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi, harus dipastikan terdapat tingkat Pelindungan Data Pribadi yang memadai yang bersifat mengikat; dalam hal ketentuan yang setara atau lebih tinggi serta tingkat Pelindungan Data Pribadi yang memadai dan mengikat tidak terpenuhi, maka Pengendali Data Pribadi wajib memperoleh persetujuan Subjek Data Pribadi[128].

9. *Data Breach Notification*

   Dalam hal terjadi kegagalan, Pengendali Data wajib menyampaikan pemberitahuan tertulis paling lama 3 kali 24 jam kepada Subjek Data Pribadi dan Lembaga[129]. Pemberitahuan tersebut minimal memuat data pribadi yang terungkap; kapan dan bagaimana data pribadi terungkap; dan upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh Pengendali Data Pribadi[130]

10. Sanksi Administratif

    Undang-Undang tentang Pelindungan Data Pribadi juga mengatur tentang sanksi administratif yang mencakup: peringatan tertulis; penghentian sementara kegiatan pemrosesan data pribadi; penghapusan atau pemusnahan data pribadi; serta denda administratif[131].

11. Kelembagaan

    Lembaga ditetapkan oleh Presiden dan bertanggung jawab kepada Presiden dan akan diatur lebih lanjut dalam Peraturan Presiden[132]. Tugas Lembaga: perumusan dan penetapan kebijakan dan strategi PDP; pengawasan penegakan hukum administratif; fasilitasi penyelesaian sengketa di luar pengadilan[133]. Wewenang Lembaga ditambah dengan: membantu penegak hukum; kerjasama dengan lembaga di luar negeri; penilaian pemenuhan persyaratan transfer data; melakukan perintah untuk tindak lanjut hasil

[128] Ibid, Pasal 56.
[129] Ibid, Pasal 46 ayat (1).
[130] Ibid, Pasal 46 ayat (2).
[131] Ibid, Pasal 57 ayat (2).
[132] Ibid, Pasal 58.
[133] Ibid, Pasal 59.

pengawasan; publikasi hasil pengawasan; menerima aduan/laporan; melakukan pemeriksaan dan penelusuran; memanggil dan menghadirkan, meminta keterangan, memanggil dan menghadirkan ahli; pemeriksaan dan penelusuran secara elektronik; serta meminta bantuan hukum kepada Kejaksaan[134]. Ketentuan tentang tata cara pelaksanaan wewenang Lembaga akan diatur dengan Peraturan Pemerintah[135].

12. Kerjasama Internasional

    Kerjasama internasional dilakukan oleh Pemerintah dengan pemerintah Negara lain atau Organisasi Internasional terkait dengan Pelindungan Data Pribadi[136]. Kerjasama Internasional dalam rangka pelaksanaan Undang-Undang PDP dilakukan sesuai dengan peraturan perundang-undangan dan prinsip Hukum Internasional[137].

13. Partisipasi Masyarakat

    Prtisipasi Masyarakat untuk terselenggaranya Pelindungan Data Pribadi dapat dilakukan, baik secara langsung maupun tidak langsung[138]. Partisipasi Masyarakat tersebut mencakup kegiatan-kegiatan, seperti: pendidikan, pelatihan, advokasi, sosialisasi, dan/atau pengawasan sesuai dengan ketentuan peraturan perundang-undangan[139].

14. Penyelesaian Sengketa dan Hukum Acara

    Dalam hal terjadi sengketa, maka penyelesaiannya dapat dilakukan, baik melalui pengadilan, arbitrase, maupun alternatif penyelesaian sengketa lainnya. Alat bukti yang digunakan, baik yang bersifat konvensional sesuai Hukum Acara, ditambah dengan alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik. Persidangan terkait sengketa menyangkut data Pribadi dimungkinkan bersifat tertutup[140]

134 Ibid, Pasal 60.
135 Ibid, Pasal 61.
136 Ibid, Pasal 62 ayat (1).
137 Ibid, Pasal 62 ayat (2).
138 Ibid, Pasal 63 ayat (1).
139 Ibid, Pasal 63 ayat (2).
140 Ibid, Pasal 64.

15. Larangan dan Ketentuan Pidana

    Ada beberapa perbuatan melawan hukum yang dilarang dalam Undang-Undang PDP terkait dengan kegiatan seperti: memperoleh atau mengumpulkan[141], mengungkapkan[142], menggunakan[143], serta membuat Data Pribadi Palsu atau memalsukan[144], yang dilakukan untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian pada Subjek Data Pribadi. Terhadap pelanggaran atas larangan-larangan yang telah ditetapkan dikenai Sanksi Pidana, baik Pidana Denda, Pidana Kurungan dan Pidana Tambahan. Apabila tindakan melanggar larangan tersebut dilakukan oleh korporasi, maka ancaman pidana dendanya diperberat.

16. Ketentuan Peralihan

    Pada saat Undang-Undang PDP berlaku, kepada Pengendali Data, Prosesor Data maupun pihak-pihak lain yang melakukan pemrosesan data wajib menyesuaikan dengan ketentuan Undang-Undang paling lama 2 (dua) tahun sejak diundangkan[145]. Pada saat Undang-Undang PDP berlaku, semua ketentuan perundang-undangan yang mengatur mengenai Pelindungan Data Pribadi, dinyatakan masih berlaku sepanjang tidak bertentangan dengan Undang-Undang ini[146].

17. Ketentuan Penutup

    Undang-Undang PDP berlaku sejak saat diundangkan[147].

18. Penjelasan

    Penjelasan UU PDP meliputi baik Penjelasan Umum maupun Penjelasan Pasal demi Pasal.

---

141 Ibid, Pasal 65 ayat (1).
142 Ibid, Pasal 65 ayat (2).
143 Ibid, Pasal 65 ayat (3).
144 Ibid, Pasal 66.
145 Ibid, Pasal 74.
146 Ibid, Pasal 75.
147 Ibid, Pasal 76.

B. Beberapa Analisa Kritis terhadap UU PDP

1. Tentang Pengertian dan Batasan

   Banyak pengertian dan batasan yang terlalu umum dan tidak rinci dan karenanya menyulitkan operasionalisasinya. Jika dibandingkan dengan EU GDPR misalnya, selalu ada elaborasi atas pengertian dan berbagai terminologi yang digunakan, sehingga mudah memahami dan mengimplementasikannya karena ada ukuran dan panduan yang jelas untuk menerapkannya. Oleh karena itu diharapkan aturan pelaksanaan sebagaimana yang dimandatkan oleh Undang-Undang No 27 tahun 2022 tentang PDP dapat mengakomodasikan kekurangan tersebut sehingga diharapkan akan efektif dalam pelaksanaannya.

2. Tentang Data Pribadi Umum dan Data Pribadi Spesifik

   Mengenai pembagian Data Pribadi menjadi Data Pribadi Umum dan Data Pribadi Spesifik, dalam beberapa hal ada beberapa perbedaan dengan praktek internasional yang berlaku. Agama, misalnya berdasarkan UU PDP menjadi bagian dari Data Pribadi Umum, sementara pada mayoritas Negara-negara yang memiliki Undang-Undang PDP agama dianggap sebagai Data Pribadi Spesifik karena menyangkut hak fundamental yang bersifat universal yaitu *Freedom of Religion*. Demikian pula dengan status perkawinan *(marital status),* pada beberapa negara dianggap sebagai Data Pribadi Spesifik, sementara di Indonesia merupakan Data Pribadi Umum. Dalam praktek banyak Negara, pandangan politik *(political opinion)* serta keanggotaan pada serikat pekerja *(trade union)* juga merupakan Data Pribadi Spesifik. Selebihnya pembagian atas Data Pribadi Umum dan Data Pribadi Spesifik yang diterapkan oleh UU PDP sama dengan yang berlaku secara internasional. Yang menarik, UU PDP juga memasukkan Data Anak dan Data Penyandang Disabilitas sebagai Data Pribadi Spesifik. Meskipun UU PDP telah membagi Data Pribadi menjadi Data Pribadi Umum dan Data Pribadi Spesifik, namun tidak diatur secara jelas bagaimana perbedaan perlakuannya, khususnya yang terkait dengan persetujuan *(consent)* Subjek Data Pribadi untuk melakukan pemrosesan Data Pribadinya.

3. Tentang Hak-hak Subjek Data

   Hak-hak Subjek Data Pribadi yang diatur dalam UU PDP secara garis besarnya banyak mengacu pada ketentuan-ketentuan EU GDPR. Hanya hak-hak tertentu dari Subjek Data Pribadi yang tidak diatur secara khusus dalam UU PDP, khususnya yang berkaitan dengan pengajuan keberatan dalam hal dilakukan pemrosesan data secara otomatis tanpa keterlibatan maupun pengawasan dari manusia. Dengan semakin berkembangnya teknologi seperti *Artificial Intelligent (AI),* khususnya *Machine Learning (ML)* yang lebih besar menggunakan AI, maka potensi pelanggaran terhadap Subjek Data Pribadi juga semakin besar. Contoh kongkritnya adalah penggunaan AI dan ML untuk kepentingan *Credit Scoring* atau untuk kepentingan *Job Recruitment* yang semata-mata dilakukan melalui cara otomasi, maka hal itu akan berpotensi merugikan kepentingan calon nasabah (bank) maupun kepentingan pelamar kerja.

4. Tentang Prinsip-Prinsip PDP

   Secara umum prinsip-prinsip PDP yang diatur dalam UU PDP serupa dengan prinsip-prinsip yang diatur dalam EU GDPR maupun aturan nasional pada banyak negara. Namun dalam UU PDP maupun dalam RPP tentang Peraturan Pelaksanaan UU PDP masih belum memberikan kejelasan baik konsep maupun operasionalisasi prinsip-prinsip tersebut. Berdasarkan pengalaman dalam implementasi EU GDPR dibuat serangkaian *Guidelines* yang dapat digunakan oleh semua pihak yang terkait dengan pemrosesan data pribadi untuk mengimplementasikan prinsip-prinsip PDP yang diatur dalam EU GDPR. Praktek beberapa negara juga menunjukkan hal serupa. Melalui *guidelines* ini, bagi Pengendali Data maupun Pemroses Data ada kejelasan tentang hal-hal apa yang dapat dilakukan dan sebaliknya hal-hal apa yang tidak boleh dilakukan. Hal ini pada akhirnya akan menimbulkan kepastian bagi semua pihak, termasuk bagi Subjek Data Pribadi sehingga ketika mereka memberikan *consent* kepada Pengendali Data dan Pemroses Data untuk memproses data pribadinya, tidak ada lagi keraguan mereka. Bagi *Supervisory Authority*, transparansi mengenai pelaksanaan prinsip-prinsip PDP juga akan memudahkan mereka dalam melakukan upaya-upaya

penegakan prinsip-prinsip PDP. Hal serupa juga dapat menjadi pegangan bagi aparatur penegak hukum untuk melakukan penegakan hukum dalam hal terjadi pelanggaran terhadap prinsip-prinsip PDP.

5. Tentang Kewajiban Pengendali Data dan Pemroses Data
   Seperti yang diuraikan di atas, ketentuan-ketentuan tentang kewajiban Pengendali Data dan Pemroses Data mencakup sekitar 50% dari UU PDP. Pada intinya ketentuan-ketentuan tersebut untuk memastikan bahwa Pengendali Data dan Pemroses Data harus menghormati, baik prinsip-prinsip PDP maupun hak-hak Subjek Data Pribadi. Mengingat UU PDP relative baru dan selama ini tidak ada aturan yang komprehensif mengenai PDP, maka harus dilakukan *benchmarking* terhadap aturan-aturan pada tataran internasional. Salah satu hal yang perlu diperhatikan adalah perlunya pengaturan dalam bentuk pedoman (guidelines) untuk implementasi UU PDP, khususnya menyangkut kewajiban Pengendali Data dan Pemroses Data. Sebagai contoh, berdasarkan EU GDPR, terdapat beberapa Guidelines terkait dengan Prinsip-Prinsip PDP dan Hak-Hak Subjek Data Pribadi, misalnya: *Guidelines 01/2022 on Data Subject's Rights-Right of Access, version 2.0, adopted on March 28, 2023; Guidelines on the Right of Data Portability, adopted on 13 December 2016, as last revised and adopted on 5 April 2017; Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1) version 2.0, adopted on 7 July 2020; etc.*

   Dengan adanya *Guidelines* seperti contoh di atas, maka akan semakin memperjelas semua pihak tentang bagaimana mengoperasionalkan norma-norma yang ada dalam UU PDP dalam penerapan sehari-hari.

6. Tentang Kerjasama Internasional
   Mengingat PDP tidak hanya sekedar merupakan bentuk pelindungan terhadap hak-hak asasi manusia, khususnya terkait privasi atas data pribadi, namun PDP juga berupaya mendorong *cross-border data flow* untuk berbagai kepentingan, maka diperlukan adanya kerjasama internasional. Dalam mendorong kerjasama internasional atas persoalan-persoalan menyangkut

PDP, maka mekanisme maupun kesepakatan perjanjian internasional harus bertumpu pada kepentingan nasional serta menghormati *legitimate rights* dan standard internasional yang berlaku. Dalam setiap perjanjian yang menyangkut kerjasama internasional harus memperhatikan prinsip-prinsip kerjasama internasional, seperti: prinsip manfaat timbal balik, prinsip resiprositas, prinsip kesetraan, prinsip sukarela, dan lain-lain.

Aturan pelaksanaan atas UU PDP seyogyanya disamping memperhatikan prinsip kerjasama internasional, juga memberikan pedoman *(guidelines*) yang jelas dan operasional tentang pelaksanaan kerjasama internasional, baik menyangkut kelembagaan, mekanisme kerjasama, dan lain-lain.

7. Tentang Kelembagaan

Masalah Kelembagaan, dalam hal ini Lembaga PDP, merupakan masalah yang sangat krusial untuk memastikan efektivitas implementasi UU PDP. Hal itu tidak mengherankan karena UU PDP memberikan kewenangan yang sangat luas kepada Lembaga, dari kewenangan investigasi, kewenangan *advisory,* kewenangan dalam perumusan kebijakan umum, kewenangan terkait dengan sertifikasi, kewenangan menetapkan standard, hingga kewenangan dalam penyelesaian sengketa serta melakukan penegakan terhadap aturan UU PDP, termasuk dalam memberikan peringatan dan bahkan menjatuhkan sanksi berupa Pidana denda kepada Pengendali Data maupun Pemroses Data yang melanggar aturan-aturan UU PDP.

Tugas, Fungsi dan Kewenangan yang luas tentu membutuhkan struktur organisasi, kapasitas sumber daya manusia, sarana dan prasarana serta dukungan pembiayaan yang memadai. Mengingat UU PDP berlaku baik bagi sektor publik, sektor privat dan bahkan organisasi internasional, maka dibutuhkan independensi, netralitas dan profesionalisme yang tinggi, termasuk dalam hal keanggotaan lembaga harus terdiri dari berbagai unsur dalam masyarakat, tidak hanya dari unsur birokrasi, tetapi juga unsur industri, akademisi, ahli di bidang *cyber security*, ahli di bidang tata kelola data dan informasi, kelompok advokasi maupun kelompok kepentingan. Dengan pendekatan yang melibatkan multi sektor tersebut, maka setiap bentuk kebijakan, regulasi, *guidelines* dan hal-hal lain yang disusun dan

diimplementasikan akan bersifat komprehensif dan dapat dilaksanakan secara efektif. Patut dicatat bahwa PDP harus dianggap merupakan suatu gerakan *(movement)* sehingga sedapat mungkin melibatkan berbagai kalangan yang relevan.

8. Tentang Transfer Data

   Transfer data pribadi adalah merupakan suatu kebutuhan, baik untuk memfasilitasi kegiatan bisnis, investasi, perdagangan, keuangan dan lain-lain. Oleh karena itu aturan tentang transfer data harus lebih fleksibel tanpa mengorbankan hak-hak dasar subjek data pribadi. Berbagai praksis terbaik internasional terkait transfer data seperti *adequacy decision, appropriate safeguard, binding corporate rules, cross border privacy rules, contractual clauses* yang intinya memberikan standard PDP perlu menjadi perhatian dan pertimbangan dalam aturan pelaksanaan tentang transfer data.

9. Tentang Mekanisme Penyelesaian Sengketa

   Dalam implementasi PDP, terbuka kemungkinan terjadinya sengketa, baik antara *Data Controller* dengan *Data Processor*, *Data Controller* dengan Subjek Data Pribadi dan lain-lain. Oleh karena itu diperlukan suatu mekanisme penyelesaian sengketa yang cepat, efektif, proporsional dan terjangkau untuk menjamin keadilan, kemanfaatan dan kepastian hukum. Dalam upaya mengembangkan mekanisme penyelesaian sengketa sebagaimana tersebut di atas, maka perlu dibuka seluas-luasnya cara-cara penyelesaian sengketa, baik melalui proses litigasi maupun melalui cara-cara di luar pengadilan, baik arbitrase maupun alternatif penyelesaian sengketa (APS). Pemahaman yang komprehensif mengenai berbagai cara penyelesaian sengketa sebagaimana yang berkembang pada tataran internasional akan sangat membantu menciptakan cara penyelesaian sengketa yang ideal sebagaimana digambarkan di atas. Jenis-jenis APS misalnya yang diatur dalam UU No 30 tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa masih sangat terbatas pada negosiasi, konsultasi, mediasi, konsiliasi, dan *expert determination* saja, itupun tanpa elaborasi tentang bagaimana cara-cara penyelesaian sengketa itu dilaksanakan. Sementara itu alternatif penyelesaian sengketa pada tataran

internasional telah sangat berkembang, termasuk namun tidak terbatas pada *dispute boards, ombudsman, grievances, mini trials* dan cara-cara penyelesaian sengketa yang bersifat *hybrid* seperti *Arb-Med-Arb*, dan lain-lain.

Jika dicermati aturan penyelesaian sengketa yang diatur pada UU PDP masih sangat terbatas dan kurang operasional karena disamping miskinnya keragaman dalam cara penyelesaian sengketa, juga kurang elaborasi agar lebih operasional. Ketentuannya sangat bersifat normatif. Di masa yang akan datang harus juga dibuka kemungkinan penyelesaian sengketa yang bersifat *online* yang lebih mempercepat penyelesaian sengketa, termasuk dengan menerapkan teknologi sebagai *enabler* seperti pemanfaatan AI, meskipun tetap harus ada kendali dan intervensi manusia. Mekanisme penyelesaian sengketa juga harus terbuka untuk dikembangkan secara spesifik pada sektor-sektor tertentu seperti sektor jasa keuangan, dan lain-lain.

10. Tentang Sanksi Administratif dan Sanksi Pidana

Dalam rangka memastikan kepatuhan terhadap UU PDP, telah diatur mekanisme dan berbagai bentuk sanksi yang dapat dikenakan terhadap pelanggarnya, baik melalui sanksi administratif maupun sanksi pidana. Suatu hal yang patut dicatat, berbagai bentuk sanksi yang diterapkan seyogyanya bersifat edukatif untuk meningkatkan kesadaran dan kepatuhan terhadap aturan-aturan UU PDP. Dari berbagai kasus yang berkembang pada tataran internasional, dapat kita cermati bahwa sanksi administratif terutama denda yang dikenakan terhadap pelanggar relatif besar, tentu saja dikaitkan dengan tingkat pelanggaran dan ukuran dari organisasi/korporasi yang melakukan pelanggaran.

Penerapan sanksi, baik sanksi administratif maupun sanksi pidana juga harus diterapkan secara non-diskriminatif, baik terhadap sektor publik maupun privat. Disamping itu juga perlu ditegakkan bentuk-bentuk *restorative justice* dalam penerapan sanksi. Jangan sampai sanksi yang diterapkan menggambarkan *Draconian Law* (hukum yang terlalu keras dan tegas) yang pada akhirnya akan berdampak negatif terhadap transfer data, termasuk *cross border data flow*, yang pada akhirnya akan mengurangi *data flow* yang sebenarnya dibutuhkan dalam dunia bisnis, perdagangan, investasi, keuangan, dan lain-lain.

11. Tentang Pejabat Pelindungan Data Pribadi

    Dalam mengawal PDP, peranan Pejabat Pelindungan Data Pribadi (PPDP) sangat penting. Tugas utama dari PPDP adalah untuk mendorong dan memastikan kepatuhan terhadap UU PDP. Tentu saja dibutuhkan kualifikasi tertentu bagi seorang PPDP. Pada tataran internasional yang dimaksud dengan PPDP adalah *Data Protection Officer (DPO)* yang tugasnya sangat jelas dan kualifikasinya juga sangat jelas. Namun dalam *Grand Design* Ekosistem PPDP yang disusun oleh Kemenkominfo dan SKKNI yang dibangun, ternyata PPDP mencakup Peta Okupasi yang sangat luas, dimana DPO hanya merupakan salah satu dari 15 (lima belas) Peta Okupasi yang ada. Hasilnya, timbul kebingungan tentang apa yang harus menjadi kompetensi PPDP, apakah harus memenuhi seluruh kompetensi dari 15 (lima belas) Peta Okupasi tersebut, atau hanya terbatas pada DPO saja. Kerancuan pengaturan tentang PPDP ini berpotensi menyulitkan efektivitas implementasi UU PDP.

BAB V

TANTANGAN PENUNTASAN ATURAN PELAKSANAAN

A. Isu-Isu Penting yang Harus Diselesaikan

1. Masalah Kelembagaan

   Salah satu masalah yang paling krusial yang mewarnai pembahasan RUU PDP adalah tentang Lembaga Pengawas. Pembahasan yang alot serta tarik menarik diantara berbagai kepentingan menjadikan pembahasannya berlarut-larut hingga terpaksa dicapainya kompromi bahwa Lembaga berada di bawah Presiden. Tantangan selanjutnya adalah bagaimana menerjemahkan kata-kata di bawah Presiden? Apakah Lembaga Khusus Non-Kementerian? Lembaga independen *(independent regulatory body).* Semua pilihan yang ada tentu saja tidak terlepas dari untung-ruginya. Oleh karena itu perlu dilakukan semacam *Cost and Benefit Analysis* (CBA) serta *Cost Effective Analysis* (CEA) untuk mendapatkan pilihan yang paling baik dan paling efisien. Sesuatu hal yang harus dipastikan adalah Kelembagaan tersebut harus independen dan professional, mengingat luasnya kewenangan yang dimiliki.

2. Masalah Penegakan Hukum

   Salah satu aspek yang merupakan tantangan yang sangat besar dalam implementasi UU PDP adalah terkait dengan Penegakan Hukum. Jika

menilik pada data kasus-kasus kebocoran data serta pelanggaran Data Pribadi sebagaimana yang telah diuraikan pada Bab sebelumnya, sangat banyak pelanggaran yang tidak terungkap dan/atau pelakunya dihukum. Alasan bahwa kelemahan penegakan hukum karena belum selesainya aturan pelaksanaan serta belum terbentuknya Lembaga Pengawas tidak dapat diterima. Prinsipnya ketika terjadi suatu tindak pidana terkait dengan pelanggaran atau kejahatan terhadap data pribadi, tidak ada alasan untuk tidak melakukan penegakan hukum karena adanya kekosongan hukum. Dalam situasi apapun seharusnya aturan hukum serta kelembagaan yang ada harus berfungsi dalam rangka melakukan penegakan hukum sesuai dengan kewenangan masing-masing. Dalam kasus BSI misalnya, terdapat beberapa instansi yang dapat melakukan pengawasan dan penegakan hukum, seperti Kepolisian BSSN, OJK, Kemenkominfo dan lain-lain.

Kepolisian dengan segala kemampuan dan fasilitas yang dimiliki seperti laboratorium forensik telematik serta adanya mekanisme kerjasama internasional seperti Interpol seharusnya dapat melakukan langkah-langkah tertentu untuk mencegah dan menanggulangi kejahatan terhadap Data Pribadi. BSSN dengan kapasitasnya di bidang *Cyber Security* juga sepatutnya mampu menerapkan langkah-langkah keamanan data yang komprehensif, baik yang bersifat pencegahan maupun penanggulangan, termasuk dalam mengidentifikasi pelaku kejahatan atau pelanggaran terhadap Data Pribadi. Kemenkominfo (sekarang Kementerian Komunikasi dan Digital) juga memiliki kewenangan dan kapasitas untuk menanganinya. Untuk Sektor Jasa Keuangan ada lembaga yang dapat mengawasi pelaku usaha Sektor Jasa Keuangan, baik dalam konteks pelindungan konsumen, serta khususnya terkait PDP. OJK mempunyai kewenangan untuk menerapkan sanksi.

Penegakan Hukum terkait PDP juga perlu dilengkapi dengan Penegakan Etika yang bisa melibatkan unsur-unsur non-pemerintah, baik asosiasi, praktisi, professional, akademisi dan masyarakat umum. Penegakan aturan PDP tidak bisa hanya dibebankan kepada Pemerintah dengan segala keterbatasannya, baik dari aspek sumber daya manusia, peralatan, pendanaan, struktur organisasi, dan lain-lain. Pendekatan etika bisa dilakukan secara

Self Regulatory yang sanksinya juga dapat diterapkan oleh komunitas terkait sesuai dengan sektor dan kegiatannya.

3. Masalah Sanksi Pidana yang terlalu Tegas dan Keras *(Draconian Law)*
   Salah satu aspek yang perlu diperhatikan untuk mengefektifkan implementasi UU PDP adalah dengan penerapan Sanksi Pidana. Namun demikian, seyogyanya ancaman pidana seharusnya lebih bersifat mengedukasi daripada bersifat menghukum atau membalas dendam. Penerapan sanksi Pidana yang terlalu keras dan tegas *(Draconian Law)* berpotensi merugikan kebutuhan akan transfer data, baik dalam lingkungan domestic maupun yang bersifat internasional.

4. Masalah Literasi Pada Masyarakat
   PDP harus merupakan suatu gerakan *(movement)* yang melibatkan seluruh komponen masyarakat serta mencakup sektor publik maupun privat dan masyarakat luas. Aspek literasi menjadi sangat penting untuk meningkatkan kesadartahuan *(awareness)* dari setiap individu untuk menjaga dan melindungi Data Pribadinya. Literasi dan edukasi harus dilaksanakan sedini mungkin. Etika dalam penerapan PDP harus selalu diutamakan, sementara penegakan hukum hanya dilaksanakan jika cara-cara yang bersifat *persuasive* dan *self regulatory* tidak efektif. Dalam konteks ini hukum hanya sebagai obat terakhir (ultimum remedium).

5. Masalah Penyelesaian Sengketa
   Ketentuan tentang penyelesaian sengketa yang diatur dalam UU PDP bersifat sangat umum dan tidak operasional. Sepatutnya dielaborasikan dan diklasifikasi jenis-jenis sengketa terkait PDP beserta mekanisme penyelesaian sengketa yang bisa berbeda-beda. Misalnya sengketa antara Subjek Data Pribadi dengan *Data Controller* dapat berbeda mekanisme penyelesaian sengketanya dengan sengketa antara *Data Controller* dengan *Data Processor*, atau antar *Data Controller* dan antar *Data Processor*. Sengketa yang terjadi juga bisa bersifat domestik, namun juga bersifat internasional atau trans-nasional.

Mekanisme penyelesaian sengketa yang lebih rinci akan sangat membantu para pihak yang bersengketa untuk mencari solusi terbaik atas sengketa yang timbul. Penyelesaian sengketa melalui Arbitrase misalnya, bisa dilakukan melalui institutional arbitration maupun *ad.hoc Arbitration*. Penyelesaian sengketa melalui mekanisme ADR seharusnya dibuka luas meliputi berbagai jenis ADR, seperti: Negosiasi. Konsultasi, Mediasi, Konsiliasi, *Good Offices*, maupun cara-cara penyelesaian sengketa yang bersifat *hybrid* seperti *Arb-Med-Arb, Med-Arb, Mini Trial*, dan lain-lain. Salah satu kendalanya adalah UU No 30 tahun 1999 tentang Arbitrase dan ADR lebih dari 90% mengatur tentang Arbitrase, dan hanya kurang dari 10% mengatur tentang ADR, itupun tanpa penjelasan yang rinci, baik tentang konsep maupun tata caranya. Untuk mengatasi hal itu, ada baiknya dilakukan *benchmarkin*g terhadap mekanisme penyelesaian sengketa yang ideal untuk sengketa di bidang PDP, terutama kemungkinan diterapkan di Indonesia dengan penyesuaian seperlunya.

6. Masalah *Grace Period* yang terlalu singkat

   UU No 27 tahun 2022 tentang PDP secara normatif telah efektif berlaku sejak tanggal 17 Oktober 2024 sebagaimana yang ditetapkan oleh UU PDP sendiri. Namun demikian, sampai dengan tanggal tersebut 2 (dua) aturan pelaksanaan yang sangat penting yaitu PP tentang Pelaksanaan UU PDP dan Perpres tentang Kelembagaan belum juga selesai. Secara umum, baik pada EU GDPR maupun UU PDP di beberapa Negara lain memang *grace period*nya rata-rata 2 (dua) tahun, namun dalam konteks Indonesia waktu 2 (dua) tahun tersebut dipandang terlalu singkat. Di samping itu persiapan implementasi UU PDP juga termasuk minimal. Berdasarkan praktek regulasi yang baik *(good regulatory practices*) efektivitas suatu peraturan perundang-undangan sangat tergantung dari persiapan implementasinya. Persiapan implementasi meliputi namun tidak terbatas pada: struktur organisasi, sumber daya manusia, sosialisasi maupun dukungan pendanaan yang memadai. Aspek lain yang perlu diperhatikan adalah dalam setiap pembentukan peraturan perundang-undangan aspek konsultasi publik yang inklusif dan substantif harus dilakukan, yang melibatkan baik pemangku

kepentingan utama *(main stakeholders*), kelompok advokasi, kelompok kepentingan maupun masyarakat luas. Dari pengalaman yang ada di Indonesia, kegagalan dalam memenuhi konsultasi publik yang insklusif dan substantif berujung pada Kegagalan Regulasi. Kegagalan regulasi berarti apa yang menjadi tujuan pembentukan regulasi tidak tercapai.

B. Mandat Pengaturan dalam Peraturan Pelaksanaan

1. Dengan Peraturan Pemerintah

   Undang-Undang PDP memberi mandat penyusunan peraturan pelaksanaan yang harus diatur dalam bentuk Peraturan Pemerintah.

   Materi muatan yang perlu diatur dalam aturan pelaksanaan pada jenjang Peraturan Pemerintah tersebut mencakup:

   a. Tugas dan Wewenang Lembaga[148]
   b. Ketentuan Sanksi[149]
   c. Transfer Data Pribadi[150]
   d. PPDP (DPO)[151]
   e. Tata Cara Pemberitahuan tentang Merger dan Akuisisi[152]
   f. DPIA[153]
   g. Pemrosesan Data[154]
   h. Hak-Hak Subjek Data[155]
   i. Ganti Rugi bagi
   j. Pelanggaran terkait Pemrosesan Data Pribadi[156].

2. Dengan Peraturan Presiden

   Salah satu aspek yang sangat krusial dalam memastikan efektivitas implementasi Undang-Undang tentang Pelindungan Data Pribadi

[148] Mandat dari ketentuan Pasal 61 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[149] Mandat dari ketentuan Pasal 57 ayat 5 UU No 27 tahun 2022 tentang Pelindungan Data PribadI.
[150] Mandat dari ketentuan Pasal 54 ayat 4 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[151] Mandat dari Pasal 54 ayat 3 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[152] Mandat dari ketentuan Pasal 48 ayat 5 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[153] Mandat dari ketentuan Pasal 34 ayat 3 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[154] Mandat dari ketentuan Pasal 16 ayat 3 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[155] Mandat dari Pasal 13 ayat 3 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.
[156] Mandat dari ketentuan Pasal 12 ayat 2 UU No 27 tahun 2022 tentang Pelindungan Data Pribadi.

adalah terkait dengan desain dan penyiapan serta pengaturan tentang Kelembagaan. Apabila desain Kelembagaan yang dilengkapi dengan segala tugas, fungsi dan wewenangnya dirumuskan secara tepat, besar harapannya bahwa Undang-Undang ini akan efektif berlaku dan tujuan intervensi dalam bentuk pengaturannya akan dapat dicapai. Sebaliknya, kegagalan dalam pembentukan Kelembagaan yang tepat akan berpotensi mengurangi efektivitas dan bahkan dapat menjadi regulasi yang gagal.

C. Rancangan Peraturan Pemerintah tentang Peraturan Pelaksanaan UU PDP

1. Pengantar

   RPP tentang Peraturan Pelaksanaan UU No 27 tahun 2022 tentang Pelindungan Data Pribadi terdiri dari 10 Bab dan 245 Pasal. Pada Ketentuan Umum ada sekitar 25 definisi dari istilah-istilah yang digunakan. Terdapat ketentuan kepada siapa dan dimana peraturan ini berlaku, serta pengecualian berlakunya.

2. Ketentuan Pokok yang Diatur

   Dalam Konsiderans RPP dinyatakan bahwa RPP disusun berdasarkan amanat pasal-pasal dari UU No 27 tahun 2022 tentang PDP, yaitu: Pasal 10 Ayat 2; Pasal 12 Ayat 2; Pasal 16 Ayat 3; Pasal 34 Ayat 3; Pasal 48 Ayat 5; Pasal 48 Ayat 5; Pasal 54 Ayat 3; Pasal 56 Ayat 5; dan Pasal 61.

   Hal-hal pokok yang diatur dalam RPP ini, meliputi: data pribadi; pemrosesan data pribadi; hak-hak dan kewajiban; transfer data pribadi; kerjasama internasional; kewenangan lembaga pelindungan data pribadi; sanksi administratif; penyelesaian sengketa dan hukum acara.

3. Analisis

   Idealnya isi dari RPP tentang Peraturan Pelaksanaan UU No 27 tahun 2022 tentang Pelindungan Data Pribadi adalah menjabarkan dan mengoperasionalkan ketentuan-ketentuan yang terdapat dalam UU No 27 tahun 2022 tentang PDP, namun dalam kenyataannya masih banyak

pengulangan terhadap ketentuan-ketentuan dari UU PDP dan belum memberikan penjelasan yang operasional, sehingga RPP ini tidak serta merta mampu dijadikan pedoman operasional bagi berbagai pihak yang harus melaksanakan ketentuan-ketentuan UU PDP.

Dalam Konsiderans RPP ini, yang tidak ada perintahnya berdasarkan UU PDP adalah tentang Sanksi Administratif serta Penyelesaian Sengketa dan Hukum Acara, serta tentang Kerjasama Internasional.

D. Peraturan Presiden tentang Lembaga Pengawas PDP

1. Latar Belakang,
   Persoalan pembentukan lembaga merupakan isu yang paling hangat dalam pembahasan. Delapan (8) dari Sembilan (9) Fraksi yang ada pada Komisi I DPR mengingatkan agar Lembaga PDP merupakan Lembaga yang Independen *(independent regulatory body)* mengingat UU PDP berlaku baik bagi sektor public maupun sektor privat. Menjelang G-20 Summit di Bali pada tahun 2022, terdapat desakan yang kuat untuk menuntaskan pembahasan RUU PDP, yang disepakati pada bulan September di DPR dan menjadi UU pada bulan Oktober tahun 2022.

2. Praksis Internasional sebagai Acuan
   Ada beberapa acuan tentang Lembaga Pengawas PDP, baik yang mengacu pada EU GDPR maupun Praktek beberapa Negara, yaitu:

   a. EU GDPR
      Berdasarkan EU GDPR Lembaga Pengawas PDP *(Supervisory Authority)* memiliki status yang independen serta memiliki kewenangan, tugas dan kekuasaan yang sangat luas.

      Mengenai independensi *Supervisory Authority* dinyatakan bahwa *Supervisory Authority* harus bertindak sepenuhnya independen dalam melaksanakan tugas serta kewenangannya sesuai dengan EU GDPR, tetap bebas dari pengaruh dari luar, baik secara langsung maupun tidak langsung, serta tidak mencari maupun menerima instruksi dari siapapun[157]. *Supervisory Authority* juga harus menahan diri dari setiap

[157] EU GDOR, Pasal 52.

tindakan yang tidak sesuai dengan tugasnya dan selama menjabat tidak terlibat dalam pekerjaan apapun, yang tidak sesuai dengan jabatannya, baik dibayar maupun tidak dibayar[158].

Supervisory Authority haruslah memiliki kompetensi dalam melaksanakan tugas-tugas yang diembannya dan melaksanakan tugasnya sesuai dengan ketentuan EU GDPR. Namun demikian *Supervisory Authority* tidak berwenang mengawasi kegiatan pemrosesan data yang terkait dengan pengadilan dalam kapasitas judisialnya[159].

Supervisory Authority mempunyai tugas yang sangat luas, yang meliputi: memantau dan menegakkan penerapan EU GDPR; meningkatkan kesadartahuan publik serta pemahaman akan berbagai resiko, peraturan serta pengamanan hak-hak Subjek Data Pribadi yang terkait dengan pemrosesan datanya; memberikan advis yang terkait dengan perlindungan hak dan kebebasan seseorang terkait pemrosesan Data Pribadinya; meningkatkan kesadartahuan Pengendali Data dan Pemroses Data tentang kewajiban-kewajibannya; atas permintaan Subjek Data Pribadi, memberikan informasi tentang hak-hak Subjek Data Pribadi; menangani keluhan yang diajukan oleh Subjek Data Pribadi, badan hukum, organisasi atau asosiasi serta melakukan investigasi atas hal yang dikeluhkan serta memberikan informasi tentang kemajuan dan hasil investigasinya dalam jangka waktu yang layak, terutama apabila investigasi dan koordinasi lebih lanjut diperlukan; memantau setiap perkembangan yang dapat berdampak terhadap Pelindungan Data Pribadi, khususnya yang terkait dengan perkembangan teknologi informasi dan komunikasi serta praksis komersial; mengadopsi standard klausula kontraktual; menetapkan dan memelihara daftar yang terkait dengan persyaratan dalam melakukan DPIA; mendorong pengembangan semacam aturan perilaku *(code of conduct*); mendorong pengembangan sertifikasi terkait pelindungan data[160].

158 Ibid.
159 Ibid, Pasal 56.
160 Ibid, Pasal 57.

Supervisory Authority memiliki berbagai kekuasaan, dari kekuasaan investigasi, kekuasaan korektif, kekuasaan untuk memberikan otorisasi atau advis, serta kekuasaan untuk menegakkan aturan EU GDPR.

Supervisory Authority diberikan kekuasaan investigatif yang cukup luas, kekuasaan ini meliputi: kekuasaan untuk memerintahkan pihak-pihak tertentu untuk memberikan informasi; untuk melakukan investigasi dalam bentuk audit; untuk *mereview* sertifikasi pelindungan data yang diberikan kepada suatu organisasi; untuk memperoleh informasi yang diperlukan dari Pengendali data dan Pemroses Data dalam rangka melaksanakan tugasnya; dan bahkan berhak untuk mengakses tempat dan peralatan yang dimiliki oleh Pengendali Data dan Pengelola Data.

Supervisory Authority juga memiliki kewenangan korektif yang meliputi: memberikan peringatan jika pemrosesan data berpotensi melanggar EU GDPR; menyampaikan teguran jika pemrosesan nyata-nyata melanggar EU GDPR; memerintahkan Pengendali Data dan Pemroses Data untuk mematuhi permintaan Subjek Data Pribadi untuk melaksanakan hak-haknya; memerintahkan agar pemrosesan data mematuhi aturan yang berlaku, termasuk untuk mengambil langkah-langkah tertentu dalam jangka waktu tertentu; memerintahkan agar Subjek Data Pribadi mendapatkan informasi terkait terjadinya kebocoran data pribadinya; mengeluarkan larangan sementara atau tetap melakukan pemrosesan data; memerintahkan pembetulan atau penghapusan data pribadi; menarik kembali sertifikasi pelindungan data; mengenakan denda; memerintahkan penangguhan transfer data internasional.

Sementara itu kekuasaan atau kewenangan otorisasi dan advis yang dapat dilakukan oleh *Supervisory Authority* meliputi: memberikan advis kepada Pengendali Data berdasarkan prosedur konsultasi yang telah dilakukan sebelumnya; memberikan otorisasi untuk pemrosesan data; menyampaikan pendapat dan menyetujui rancangan aturan perilaku *(code of conduct)*; melakukan akreditasi terhadap lembaga sertifikasi;

mengadopsi klausula standar; memberikan otorisasi terkait klausula kontraktual; menyetujui *binding corporate rules*.

Supervisory Authority juga diberikan kekuasaan/kewenangan untuk menegakkan aturan EU-GDPR, yang berkisar dari menyampaikan peringatan atau teguran, hingga mengenakan denda.

b. Korea Selatan

Di Korea Selatan *the Personal Information Protection Commission (PIPC)* merupakan otoritas PDP berdasarkan aturan yang berlaku. PIPC dibentuk sebagai Badan Independen pada tahun 2011 berdasarkan *Personal Information Protection Act (PIPA).* Komisi ini terdiri dari 9 (sembilan) Komisioner yang diketuai oleh seseorang yang ditunjuk oleh Presiden Korea Selatan.

Sebelumnya PIPC hanya bersifat *advisory*, tapi sejak tahun 2020 telah diubah menjadi *Independent Regulatory Agency.*

Dalam kiprahnya PIPC telah mendenda Facebook sebesar US$ 6,1 juta pada tahun 2020, Google sebesar US$ 150 juta (2022), Meta sebesar US$ 22 juta karena melanggar aturan Privasi di Korea Selatan.

Ketua PIPC mempunyai kedudukan setingkat Menteri, sementara anggota Komisioner yang lain terdiri dari: 2 direkomendasikan oleh Ketua; 2 direkomendasikan oleh partai yang berkuasa; dan 3 direkomendasikan oleh partai oposisi.

c. Republik Rakyat Tiongkok (RRT)

Personal Information Privacy Law (PIPL) di RRT diundangkan pada bulan Agustus 2021 dan efektif berlaku pada 1 November 2021. Dalam banyak hal PIPL serupa dengan EU GDPR, namun memiliki persyaratan yang unik sendiri. *Cyber Administration of China (CAC)* merupakan regulator di bidang ini. CAC pernah mengenakan denda ke Didi *(China's largest ride service*) sebesar US$ 1,2 milyar karena pelanggaran terhadap aturan *Data Privacy, Data Security* dan *Cyber Security Law*.

d. Thailand

Office of the Personal Data Committee melekat pada Kementerian Ekonomi Digital dan Masyarakat (Ministry of Digital Economy and

Society). Lembaga ini dipimpin oleh seorang Ketua dengan *Permanent Secretary* adalah Menteri Ekonomi Digital dan Masyarakat, serta Ex Officio direktur adalah Sekretaris Jendral Kementerian[161].

e. Philipina

Di Philipina Lembaga Pengawas PDP adalah *National Privacy Commission*. Lembaga ini bersifat Independen. Komisi dipimpin oleh seorang Komisioner Privasi, dengan dibantu dengan 2 wakil komisioner. Komisioner Privasi ditunjuk oleh Presiden Philipina untuk masa jabatan 3 tahun[162].

f. Malaysia

Lembaga PDP di Malaysia bernama Pesuruh Jaya Perlindungan Data Pribadi yang dalam melaksanakan tugasnya hanya mengawassi sektor privat, karena UU PDP Malaysia semula hanya berlaku untuk sektor privat saja. Komisioner ditunjuk, dilantik dan bertanggung jawab kepada Menteri. Komisioner dapat menunjuk sejumlah pejabat publik sebagai wakil Komisioner dan sejumlah orang sebagai wakil Komisioner[163]. Dengan revisi terhadap UU PDP di Malaysia yang diberlakukan baik bagi sektor privat maupun sektor publik, maka konsekuensinya Lembaga Pengawas juga mengalami penyesuaian.

g. Singapura

Di Singapura *Personal Data Protection Commission (PDPC)* menjadi lembaga yang melekat pada *The Info-Communication and Media Development Authority (IMDA).* PDPC dibentuk oleh menteri terkait yang keanggotaannya tak kurang dari 6 anggota dan tak lebih dari 20 anggota. Selain PDPC, UU PDP Singapura juga mengatur mengenai Komisi Banding Pelindungan Data[164].

3. Pengaturan yang Ideal

Jika menghendaki suatu pengaturan yang ideal tentang tugas, fungsi, kompetensi, wewenang dan kekuasaan Lembaga PDP, maka acuan yang

[161] Untuk selengkapnya, baca: Rumadi Ahmad, "Lembaga Perlindungan Data Pribadi", Kompas 22 Juli 2024.
[162] Ibid.
[163] Ibid.
[164] Lihat, Ibid.

paling ideal adalah *Supervisory Authority* yang diatur oleh EU GDPR. Hal itu mengingat luasnya wewenang *Supervisory Authority* dan kedudukannya yang independen dan professional. Praksis terbaik dari berbagai Negara juga meneguhkan bahwa Lembaga PDP harus bersifat Independen, meskipun sesuai mandatnya berada di bawah Presiden.

4. Usulan Pengaturan

Dalam pembahasan tentang pembentukan Lembaga PDP yang dilaksanakan pada Kantor Sekretariat Presiden pada 7 Mei 2024 yang mengundang berbagai kalangan, baik kalangan industri, asosiasi profesi PDP, akademisi, Kemenkominfo, BSSN, pakar keamanan data, penggiat HAM dan lain-lain, terdapat berbagai usulan, terutama untuk menjabarkan kesepakatan DPR dan Pemerintah pada saat pembahasan UU PDP dimana disepakati Lembaga PDP berada di bawah Presiden, persoalannya adalah bagaimana menerjemahkannya sehingga badan tersebut tetap dapat independen, professional, dan efektif? Hal itu mengingat bahwa Lembaga PDP di bawah Presiden tersebut bisa merupakan Lembaga Non-Struktural (LNS) maupun Lembaga Pemerintah Non Kementerian (LPNK).

Beberapa kalangan yang menghadiri pembahasan tentang Pembentukan Lembaga PDP pada KSP tanggal 7 Mei 2024, menyampaikan berbagai pandangan yang intinya sebagai berikut:

- Lembaga PDP yang akan dibentuk diharapkan mampu melaksanakan tugas, fungsi dan wewenangnya secara independen, professional dan inklusif
- Independensi juga mencakup independensi fungsional
- Apapun bentuk kelembagaan nanti, apakah lembaga, badan otorita maupun komisi, tetap harus dipastikan independensinya
- Untuk menjamin independensinya perlu dipertimbangkan kemungkinan pendanaan Lembaga PDP tidak bersumber dari APBN, tapi mandiri seperti OJK
- Lembaga yang dibentuk harus otonom, mandiri, kompeten, transparan dengan mandate yang jelas da nada perlindungan hukum dalam pelaksanaan tugasnya

- Perlu ada Penjabaran tugas, fungsi dan wewenang Lembaga PDP secara rinci dan operasional serta disosialisasikan agar mudah dipahami, diimplementasikan dan dipatuhi oleh berbagai kalangan, baik pada sektor public maupun sektor privat
- Lembaga harus kuat dan independen, mengingat besarnya ancaman serangan siber, terutama banyaknya serangan siber di Indonesia
- Struktur kelembagaannya harus bersifat kolektif, kolegial
- Anggota Lembaga yang akan direkrut harus terdiri dari berbagai unsur dalam masyarakat, baik pemerintah, kelompok pemangku kepentingan utama, kelompok advokasi, kelompok kepentingan, dunia usaha, dunia industri, dunia kerja, para pakar maupun masyakat umum
- BSSN harus jadi tulang punggung Enkripsi
- Dalam struktur organisasi harus ada komisi PDP dan Badan Otorita PDP

E. Keputusan Menteri Ketenagakerjaan No 103 tahun 2023 tentang Penetapan SKKNI Kategori Informasi dan Komunikasi Golongan Pokok Pemrograman, Konsultasi Komputer dan Kegiatan yang Berhubungan dengan itu (YBD) Bidang Keahlian Pelindungan Data Pribadi

1. Konsiderans

   Dalam Konsiderans Menimbang mengacu pada ketentuan Pasal 31 Permenaker No 3 tahun 2016 tentang Penetapan SKKNI. Demikian pula mengacu pada Kesepakatan Konvensi Nasional tanggal 10 November 2022.

   Konsiderans Mengingat mengacu pada beberapa ketentuan, yaitu: Undang-Undang No 13 tahun 2013 tentang Ketenagakerjaan; Peraturan Pemerintah No 31 tahun 2006 tentang Sistem Latihan Kerja Nasional (Sislatkernas); Peraturan Presiden No 8 tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (KKNI); Permenaker No 21 tahun 2014 tentang Pedoman Penerapan KKNI; Permenaker No 3 tahun 2016 tentang Tata Cara Penerapan SKKNI.

2. Keputusan

   Inti Kepmenaker No 103 tahun 2013 adalah: menetapkan SKKNI dan seterusnya sebagaimana tercantum dalam lampiran; SKKNI menjadi acuan dalam menyusun jenjang kualifikasi nasional, penyelenggaraan pendidikan dan latihan serta sertifikasi kompetensi; pemberlakuan SKKNI ditetapkan oleh Kemenkominfo da/atau Kementerian/Lembaga teknis terkait sesuai dengan tugas dan fungsinya; SKKNI dikaji ulang setiap 5 (lima) tahun.

3. Lampiran

   Pada Bab I Lampiran, yaitu Pendahuluan, khususnya pada Latar Belakang dinyatakan bahwa ketentuan pasal 53 (1) UU No 27 tahun 2022 tentang PDP terkait penunjukan Pejabat Pelindungan Data Pribadi (PPDP) yang wajib memiliki kualitas professional, pengetahuan hukum dan praktek PDP serta kemampuan untuk memenuhi tugas-tugasnya yang dibuktikan melalui sertifikasi terhadap kompetensi dan pengalaman kerja. Ada 15 (lima belas) Peta Okupasi di bidang PDP, yaitu: *Data Protection Officer (DPO); Privacy Program Manager; Privacy Product Development; Privacy Auditor; Chief Privacy Officer; Data Protection Executives; Data Protection Authority; Privacy Counsel; Privacy Analist; Director of Privacy; Data Privacy Manager; Privacy Engineer; Privacy Specialist; Privacy Delegates (liaison); dan Privacy Technologis*t. Disebutkan pula bahwa diperkirakan kebutuhan PPDP di Indonesia sekitar 127.000 orang. Ditekankan pula tentang perlunya penyusunan SKKNI berdasar Permenaker No 3 tahun 2016 tentang Tata Cara Penerapan SKKNI.

   Pada Bab I Lampiran, tentang Pendahuluan juga dielaborasi beberapa hal penting seperti: pengertian; penggunaan SKKNI; Komite Standar Kompetensi; Tim Perumus RSKKNI bidang PDP; serta Tim Verifikasi RSKKNI.

   Beberapa pengertian pokok yang terkait meliputi: Data Pribadi; PDP; Informasi; Pengendali Data Pribadi; Prosesor Data Pribadi; Subjek Data Pribadi; PPDP; Fungsi Organisasi PDP (tata kelola kepatuhan, manajemen, teknis operasional, pengawasan); Lingkup Pemrosesan Data Pribadi; Prinsip PDP; Dasar Pemrosesan Data Pribadi; serta Insiden Kegagalan PDP.

Sementara itu ditekankan tentang penggunaan SKKNI, misalnya berlaku: bagi institusi pendidikan dan pelatihan (digunakan sebagai informasi program dan kurikulum); acuan dalam penyelenggaraan pelatihan; penilaian dan sertifikasi); bagi dunia usaha, dunia industri, dan dunia kerja (DUDIKA); bagi institusi penyelenggara pengujian dan sertifikasi (sebagai acuan perumusan paket-paket program sertifikasi sesuai dengan kualifikasi dan levelnya, sebagai acuan dalam penyelenggaraan pelatihan, penilaian dan sertifikasi).

Pada Bab II tentang SKKNI memuat hal-hal penting seperti Pemetaan Standar Kompetensi serta Daftar Unit Kompetensi.

Tujuan utama dari Pemetaan Standar Kompetensi adalah untuk melaksanakan fungsi PDP dalam organisasi sesuai dengan ketentuan. Sementara Fungsi Utamanya adalah: untuk merencanakan program kerja PDP; mengelola program kerja PDP; menjaga kelangsungan PDP; serta merespons permintaan informasi dalam insiden kegagalan PDP.

Daftar Unit Kompetensi meliputi Kode Unit dan Judul Unit Kompetensi. Judul Unit Kompetensi mencakup: menentukan landasan program kerja PDP; menentukan kerangka kerja PDP; mengidentifikasi peraturan perundang-undangan terkait PDP; melakukan penilaian dampak PDP; menyusun tata kelola PDP (termasuk ROPA); menerapkan program kerja PDP; merumuskan saran kepada manajemen terkait; mengelola audit berkaitan dengan program kerja PDP; merumuskan proses peroleh persetujuan pemrosesan Data Pribadi; memberikan respons terhadap permintaan informasi Data Pribadi sesuai ketentuan; memastikan PDP telah terintegrasi dalam manajemen respons insiden; serta merumuskan berjalannya manajemen respons insiden terkait kegagalan PDP.

Masing-masing Kode Unit beserta elemen kompetensi dan kriteria unjuk kerjanya dielaborasi dalam Kepmenaker No 103 tahun 2023 termasuk batasan variabel dan panduan penilaiannya.

4. Analisis

Sepintas Kepmenaker No 103 tahun 2023 ini mengandung hal-hal yang sangat ideal, namun luasnya peta okupasi terkait PPDP yang terdiri dari 15

(lima belas) Peta Okupasi, dimana DPO hanya merupakan salah satu dari ke 15 (lima belas) Peta Okupasi tersebut tentu saja menimbulkan kebingungan. Dalam praktek di berbagai Negara dan di Uni Eropa, DPO identik dengan PPDP yang tugasnya adalah untuk memastikan kepatihan tekait PDP, disamping tugas-tugas lainnya. Ketidakjelasan dan perbedaan Kemmenaker ini dengan standar internasional yang berlaku sepanjang menyangkut DPO akan menyulitkan untuk merumuskan kompetensi DPO yang tidak identik dengan PPDP.

Hal lain yang memerlukan perhatian adalah tentang Kode Unit dan Judul Unit Kompetensi yang secara umum sebenarnya hampir sama dengan kompetensi yang dibutuhkan oleh DPO yang berlaku secara internasional dan berdasarkan praksis terbaik. Namun jika Kode Unit dan Judul Unit Kompetensi tersebut hampir sama dengan kompetensi DPO, bagaimana kemudian dengan 15 (lima belas) Peta Okupasinya di luar DPO? Kompetensi apa yang harus dimiliki? Bagaimana kurikulum pendidikan dan pelatihannya?

Persoalan selanjutnya terkait dengan kualifikasi DPO. Berdasarkan hasil penelitian tentang perbandingan antara DPO di Uni Eropa dengan di Indonesia yang dilaksanakan di Universitas Leiden, Belanda, DPO tidak mempersyaratkan sertifikasi tertentu sepanjang dapat melaksanakan kompetensinya sesuai dengan aturan yang berlaku. Sementara di Indonesia mempersyaratkan sertifikasi kompetensi, namun dengan persyaratan kompetensi yang terlalu luas yang tidak mungkin dipenuhi oleh seorang DPO.

Permasalahan lain adalah tentang siapa lembaga yang punya wewenang untuk merumuskan dan menyetujui SKKNI? Apakah Kominfo atau lembaga lain dengan tugas dan fungsi yang sama, ataukah juga mencakup Lembaga Pengawas PDP yang dibentuk dengan Peraturan Presiden berdasarkan mandate dari UU PDP? Di Uni Eropa fungsi itu ada pada Supervisory Authority yang independen dan professional, sementara di Indonesia Lembaga Pengawas yang disepakati di bawah Presiden mempunyai penafsiran yang berbeda. Di satu sisi kalangan dunia industri pada umumnya mengharapkan adanya perlakuan yang sama dengan sektor publik dalam

pengimplementasian UU PDP, sehingga diharapkan lembaga tersebut merupakan Independent Supervisory Body yang benar-benar independen, sementara itu dari kalangan Pemerintah cenderung menafsirkannya sebagai lembaga yang melekat pada kewenangan eksekutif yang bertanggung jawab kepada Presiden.

Pertanyaan selanjutnya menyangkut Kurikulum pelatihan dan pendidikan, uji kompetensi dan sertifikasi seperti apa yang akan diterapkan dan lembaga mana yang mempunyai wewenang untuk mengkoordinasikannya?

5. Tindak Lanjut

Untuk memperjelas implementasi SKKNI memerlukan tindak lanjut yang kongkrit, realistis dana dapat dilaksanakan secara efektif. Jawaban yang tepat atas pertanyaan-pertanyaan di atas akan membantu dalam menindaklanjuti penetapan dan penerapan SKKNI.

BAB VI

MENGAWAL IMPLEMENTASI UU PDP

A. Pentingnya Persiapan Implementasi

Dalam praktek regulasi yang baik *(good regulatory practices)*, regulasi yang baik tidak hanya terbatas pada rumusan aturan *(regulatory design*), namun juga menyangkut efektivitas implementasi *(regulatory delivery)*, maupun pengawasan terhadap kepatuhan *(regulatory inspection*[165]*)*.

Tahapan *regulatory design*, dalam arti pembentukan UU tentang PDP sudah selesai dan bahkan 2 (dua) tahun setelah diundangkan pada tahun 2022 sudah seharusnya efektif berlaku mulai tanggal 17 Oktober 2024. Namun demikian belum selesainya aturan pelaksanaan, baik dalam bentuk Peraturan Pemerintah maupun dalam bentuk Peraturan Presiden berpotensi menghambat efektivitas implementasi UU PDP. Yang tidak boleh diabaikan dalam penuntasan regulasi adalah pentingnya proses konsultasi publik yang substantif dan inklusif. Konsultasi publik yang substantif dan inklusif serta dikawal dalam setiap tahapan pembentukan perundang-undangan akan mampu meningkatkan tingkat kepatuhan, yang pada gilirannya akan meningkatkan efektivitas implementasi, sehingga pada akhirnya alan mampu mencapai tujuan dari intervensi regulasi. Lebih jauh terbentuknya Lembaga PDP yang telah lama dinantikan, dengan kewenangan yang luas, independen, professional dan kompeten juga sangat mendesak.

---

[165] Baca: I B R Supancana, Sebuah Gagasan tentang Grand Design Reformasi Regulasi Indonesia, Penerbit Unika Atma Jaya, 2017, halaman 25-28.

Tantangan dalam implementasi UU PDP disamping dari sisi finalisasi peraturan, yang tak kalah pentingnya adalah persiapan implementasi. Banyak regulasi yang tidak efektif dalam implementasinya karena lemah dalam persiapan implementasinya. Persiapan implementasi meliputi: sosialisasi, kesiapan struktur organisasi, kesiapan sumber daya manusia, kesiapan dukungan pendanaan.

Jika pada saat penyusunan peraturan perundang-undangan sangat membutuhkan konsultasi publik yang substantif dan inklusif, pada saat peraturan diundangkan aspek sosialisasi menjadi sangat penting. Sosialisasi dapat meliputi edukasi dan peningkatan kesadartahuan *(awareness raising)* tentang pentingnya menjaga data pribadi sebagai upaya preventif. Implementasi UU PDP tidak dapat mengandalkan semata kepada Pemerintah, tapi harus merupakan suatu gerakan *(movement)* bersama. Dunia usaha juga punya peran penting untuk mengembangkan dan menegakkan norma-norma terkait perlakuan terhadap Data Pribadi dengan menggunakan pendekatan *self regulatory* pada tataran etika. Etika tentang PDP perlu dikembangkan sebagai suatu bentuk *soft laws* dengan mekanisme yang ditegakkan oleh komunitas terkait.

Dalam rangka persiapan implementasi, selain langkah-langkah sosialisasi juga harus dilengkapi dengan penataan dan kesiapan organisasi untuk melaksanakannya. Struktur organisasi, baik pada sektor publik maupun sektor privat harus dipersiapkan. Penyiapan struktur organisasi tersebut dalam rangka pelaksanaan dan kepatuhan terhadap aturan-aturan PDP. Struktur organisasi yang relevan harus didukung oleh sumber daya manusia, baik secara kuantitatif maupun secara kualitatif. Berbagai upaya untuk meningkatkan kapasitas institusi maupun individual harus dilakukan, termasuk dengan pelatihan dan pendidikan berbasis kompetensi, yang dilakukan oleh lembaga-lembaga pelatihan publik maupun atas dasar swadaya masyarakat. Untuk mengefektifkan implementasi harus didukung oleh pendanaan yang memadai. Pendanaan tersebut dapat bersumber pada anggaran Negara maupun melalui sumber-sumber lain yang sah.

B. Kesiapan Sektor Publik

Mengingat UU PDP berlaku, baik bagi sektor publik maupun privat, maka sektor publik juga perlu mempersiapkan langkah-langkah yang memadai.

Selama ini banyak kebocoran data justru terjadi pada sektor publik, namun atas kejadian tersebut banyak yang tidak terungkap dan tidak mendapatkan penindakan hukum secara sepadan. Dalam rangka mengimplementasikan UU PDP secara penuh, sektor publik perlu melakukan penyiapan langkah-langkah, sebagai berikut:

1. Struktur Organisasi dan Kelembagaan
   Penataan organisasi pada sektor publik idealnya sudah dipersiapkan sedini mungkin sebelum berlakunya UU PDP. Namun dalam kenyataannya justru tidak menunjukkan kesiapan yang memadai. Institusi-insitusi yang ada pada Pemerintah terlihat gamang dalam menghadapi implementasi UU PDP sebelum terbentuknya Lembaga PDP. Atas kasus-kasus yang terjadi, koordinasi diantara instansi yang terkait tampak lemah sehingga gagal melakukan penindakan tegas terhadap pelaku kebocoran data serta bentuk-bentuk kejahatan terhadap Data Pribadi lainnya. Kementerian Komunikasi dan Digital, BSSN, Kepolisian, OJK serta lembaga-lembaga yang ada seharusnya dapat berkerjasama sesuai dengan tugas dan fungsi masing-masing.

2. Sumber Daya Manusia
   Mengingat pesatnya perkembangan teknologi dan beragam serta kompleksnya permasalahan terkait dengan PDP, tentu saja membutuhkan kesiapan dari aspek sumber daya manusia. Kesiapan sumber daya manusia pada sektor publik harus dilakukan sedini mungkin, baik dari aspek kualitas kompetensi maupun kuantitasnya. Dari aspek kualitas perlu dilakukan peningkatan kompetensi dari PPDP pada sektor publik dapat melalui pelatihan berbasis kompetensi, *re-skilling, up-skilling*, dan lain-lain. Tanpa kompetensi yang memadai, maka akan berpengaruh terhadap implementasi UU PDP. Secara kuantatif juga perlu dilakukan perekrutan terhadap personil untuk mengimplementasikan dan menegakkan UU PDP pada sektor publik. Perekrutan tersebut dilakukan dengan mempertimbangkan berbagai disiplin ilmu terkait. Secara berkelanjutan juga perlu dilakukan pembinaan dan tentu saja dengan jenjang karir yang jelas dan kesejahteraan yang memadai.

3. Sarana dan Prasarana

   Seiring dengan perkembangan teknologi, dibutuhkan dukungan sarana dan prasarana untuk mendukung peran badan-badan publik dalam mengimplementasikan UU PDP. Teknologi yang terus berkembang dan semakin menantang memerlukan penyesuaian dari sisi ketersediaan sarana dan prasarana.

4. Pendanaan

   Semua kebijakan yang terkait dengan implementasi UU PDP, baik kegiatan sosialisasi, pengembangan sumber daya manusia, pengadaan sarana dan prasarana tentu saja membutuhkan dukungan pendanaan. Mengingat implementasi UU PDP merupakan suatu gerakan bersama, tentu juga harus dipahami bahwa sumber pendanaannya tidak terbatas pada sumber pendanaan Pemerintah, tapi juga dapat bersumber pada sumber pendanaan lain, termasuk sumber pendanaan swasta dan sumber-sumber lain yang sah. Cara pendanaan membutuhkan kreatifitas dan inovasi, sepanjang sah dan diperbolehkan oleh peraturan perundang-undangan yang berlaku.

5. Pembinaan dan Pengawasan

   Sebagai bagian dari *Regulatory Inspection* perlu dilakukan Pembinaan dan Pengawasan yang berkelanjutan. Dalam melakukan Pembinaan dan Pengawasan peran dari Lembaga PDP sangat krusial. Pembinaan dan Pengawasan dilakukan baik kepada sektor publik maupun sektor privat melalui: bantuan teknis; pendidikan dan pelatihan; pedoman (*guidelines*); *advisory*; menetapkan standard; menyelenggarakan sertifikasi; memberikan peringatan lisan maupun tertulis; hingga pengenaan denda administratif.

6. Penegakan Hukum

   Salah satu unsur dari bekerjanya sistem hukum adalah penegakan hukum yang konsisten dan tanpa pandang bulu. Penegakan hukum yang baik harus ditopang oleh sumber daya manusia yang memiliki karakteristik: moral integritas yang tinggi; kemampuan professional yang mumpuni; kematangan intelektual; serta kearifan. Idealnya penegakan hukum

dilakukan dengan pendekatan *restorative justice*, tidak bersifat menghukum atau membalas dendam, namun lebih bersifat memulihkan keadaan atau harmoni dalam masyarakat, serta bersifat persuasif dan edukatif. Dengan demikian diharapkan terciptanya kesadaran hukum dalam masyarakat perihal kepatuhan terhadap UU PDP. Jadi kepatuhan yang bukan didasarkan atas ketakutan karena sanksi hukumnya, tetapi karena kesadaran dalam masyarakat tentang pentingnya PDP sebagai wujud pengormatan terhadap hak-hak asasi manusia, terutama terhadap hak-hak atas informasi pribadinya.

C. Kesiapan Sektor Privat

1. Antisipasi Implementasi UU PDP

   Sejak diundangkannya UU No 27 tahun 2022, meskipun belum dilengkapi dengan peraturan pelaksanaannya, sektor swasta justru menunjukkan upaya persiapan dan kepatuhan yang paling aktif dan antisipatif. Banyak sekali perusahaan pada skala besar dan global maupun regional yang mempersiapkan diri untuk mematuhi standard PDP melalui berbagai aktivitas, mencakup: melakukan audit, melakukan *gap assessment*, menyesuaikan *privacy policy*, melakukan DPIA, menunjuk DPO, menyesuaikan struktur organisasi, menyiapkan standard kontrak terkait transfer data, pemrosesan data dan sharing data, menyiapkan *data breach management plan* dan *data breach notification*, dan lain-lain. Jauh-jauh hari sebelum berakhirnya *grace period* dan menyongsong efektif berlakunya UU PDP secara normative.

2. Mengembangkan *Common Practices* and *Best Practices*

   Dalam mengawal PDP sepatutnya tidak dapat semata-mata diartikan kepatuhan hanya terhadap UU PDP saja, tetapi harus berpikir *Beyond Compliance* terhadap UU PDP. Artinya menggunakan kepatuhan terhadap UU PDP sebagai kepatuhan dasar, sementara itu kepatuhan dalam mengawal PDP melebihi kepatuhan terhadap UU PDP. Sebagai contoh Perusahaan/ Korporasi yang jangkauan usahanya juga mencakup lintas negara, termasuk Uni Eropa, selayaknya mengembangkan praktek PDP yang setara dengan aturan EU GDPR. Jika menerapkan standar kepatuhan terhadap EU GDPR berdasarkan *common practices* dan *best practices*, maka otomatis akan mampu

menunjukkan kepatuhan terhadap UU PDP. Sesuai dengan desain UU PDP yang menganut *co-regulatory approach*, maka industri terkait, sesuai dengan sektor dan kebutuhannya dapat mengembangkan *common practices* dan *best practices* dalam komunitas mereka sebagai cerminan *self-regulatoy approach* yang berbentuk *soft laws* yang tidak mengikat secara hukum namun mengikat secara etika diantara komunitas atau sektornya.

3. Menyiapkan Hal-Hal yang Praktis

   Dalam upaya mematuhi aturan-aturan tentang PDP, perlu dikembangkan dan diterapkan hal-hal yang bersifat praktis sebagai petunjuk atau pedoman dalam menjalankan kepatuhan. Petunjuk dan pedoman praktis tersebut sangat diperlukan agar sektor privat, terutama perusahaan/korporasi dapat mempersiapkan, merencanakan, melaksanakan, mengevaluasi, melakukan *self-assessment*, memperbaiki/menyempurnakan kepatuhan terhadap UU PDP.

   Selama ini, bahkan sebelum UU PDP berlaku secara efektif, perusahaan/korporasi telah melakukan langkah-langkah nyata ke arah kepatuhan terhadap UU PDP. Dalam upaya menunjukkan kepatuhan tersebut mereka melakukan penataan terhadap internal organisasi, melakukan *mappin*g terhadap *existing conditions*, melakukan audit kepatuhan, melakukan *self-assessment*, untuk selanjutnya menyiapkan atau menyempurnakan *privacy policy*, melakukan DPIA terhadap proyek yang diperkirakan berdampak terhadap hak-hak subjek data pribadi, melakukan ROPA, menyusun *binding corporate rules*, menyiapkan kontrak standard terkait sharing data maupun pemrosesan data, hingga mengembangkan *software* kepatuhan.

4. Menyiapkan DPO

   DPO memainkan peranan yang sangat penting dalam memantau dan memastikan kepatuhan terhadap UU PDP. DPO juga berperan memberikan advis terhadap kepatuhan, membantu menyiapkan *privacy policy*, membantu melakukan DPIA, menjadi nara hubung dengan regulator, dan lain-lain. Demikian pentingnya peranan DPO dalam suatu perusahaan/korporasi, termasuk dalam setiap proses pengambilan keputusan yang menyangkut

pemrosesan data pribadi, menjadikan DPO sering juga disebut sebagai mini-CEO. Untuk menyiapkan DPO yang dapat melaksanakan tugasnya dengan sebaik-baiknya, terutama membantu Pengendali Data dan Pemroses Data dalam mematuhi UU PDP, maka diperlukan pelatihan maupun pendidikan yang berbasis kompetensi. Idealnya pelatihan maupun pendidikan yang berbasis kompetensi tersebut dikembangkan berdasarkan, baik standar internasional, standar nasional maupun standar industri.

Oleh karena itu kurikulum maupun modul pelatihan dan pendidikan harus mencerminkan kompetensi yang harus dikuasai, tidak hanya terkait pengetahuan, namun juga ketrampilan dan sikap yang patut. Disamping pelatihan atau pendidikan berbasis kompetensi, juga diikuti dengan uji kompetensi dan sertifikasi. Meskipun pada dasarnya salah satu persyaratan dari seorang DPO adalah pengetahuan di bidang hukum, khususnya Hukum Pelindungan Data Pribadi, namun juga dibutuhkan kemampuan lain yang bersifat lintas disiplin ilmu yang saling melengkapi, pengalaman, serta kemampuan untuk berkoordinasi dalam internal organisasi/korporasi. Mengingat kebutuhan DPO yang cukup besar di Indonesia, maka Pemerintah selayaknya mendorong dan mendukung upaya-upaya peningkatan kapasitas sebagai DPO melalui pelatihan dan pendidikan bersertifikasi, baik atas inisiatif Pemerintah maupun inisiatif sektor privat.

D. Kesiapan dan Partisipasi Masyarakat

1. Meningkatkan *Awareness* tentang Perlunya Melindungi Data Pribadi Masing-masing

   Efektivitas implementasi dan meningkatnya kepatuhan terhadap UU PDP juga sangat tergantung kepada kesiapan masyarakat. Kesiapan masyarakat akan semakin meningkat jika ditopang oleh sosialisasi dan kampanye tentang perlunya pelindungan PDP, baik sebagai bentuk penghormatan terhadap hak-hak asasi manusia terkait data pribadinya, maupun untuk mendukung transfer data seiring dengan perkembangan globalisasi, terutama untuk mendukung bisnis perdagangan, investasi, jasa, keuangan, dan lain-lain.

   Sosialisasi dan kampanye untuk meningkatkan *awareness* di kalangan masyarakat tentang pentingnya PDP, harus diarahkan pada *awareness*

dari setiap individu. Dimulai dari hal-hal yang sederhana seperti perilaku tidak mengumbar informasi pribadi, baik di dunia nyata maupun dunia maya, termasuk menghormati privasi orang lain. Jika tingkat awareness dari masyarakat luas semakin meningkat, maka tingkat kepatuhan juga diharapkan meningkat, yang pada akhirnya akan berkontribusi pada efektivitas implementasi UU PDP.

Komponen-komponen dalam masyarakat seperti kelompok advokasi, kelompok kepentingan, lembaga pendidikan, lembaga swadaya masyarakat, dan lain-lain perlu didorong untuk mengambil peran dalam upaya meningkatkan *awareness* di kalangan masyarakat.

2. Memberikan Pendidikan dan Pelatihan

   Di samping peningkatan *awareness* pada masyarakat, upaya meningkatkan kesiapan masyarakat dalam rangka kepatuhan terhadap UU PDP juga perlu ditopang dengan inisiatif dari komponen-komponen dalam masyarakat dalam wujud pendidikan dan pelatihan. Hal itu dapat dilakukan dari bentuk non-formal, informal, sampai dengan yang formal. Ini menggambarkan bahwa peningkatan kepatuhan terhadap UU PDP merupakan suatu gerakan bersama *(movement)* yang juga melibatkan masyarakat. Oleh karena itu, dalam setiap kebijakan dan regulasi yang dibuat, maka konsultasi publik yang dilakukan harus menyentuh seluruh komponen dalam masyarakat secara inklusif. Demikian pula partisipasi unsur masyarakat juga harus tercermin dalam susunan keangotaan Lembaga Pengawas.

3. Memahami Hak-Hak Subjek Data Pribadi dan Bagaimana Mengaplikasikannya

   Inti dari pemahaman tentang PDP pada hakekatnya adalah pemahaman tentang: prinsip-prinsip PDP; Hak-Hak Subjek Data Pribadi; Kewajiban Pengendali Data dan Pemroses Data; Tugas, Fungsi dan Wewenang Lembaga Pengawas; Perbuatan yang Dilarang; Ketentuan Pidana; dan lain-lain. Oleh karena itu semua komponen dalam masyarakat berhak mendapatkan informasi, sosialisasi tentang UU PDP, termasuk pemahaman tentang Hak-Hak Subjek Data Pribadi yang harus dihormati. Hak-hak Subjek Data

Pribadi tentu tidak hanya sebagai pengetahuan, namun juga bagaimana mengaplikasikannya dalam kehidupan sehari-hari. Contoh sederhana misalnya tidak meng *up-load content* yang terkait data pribadi, apalagi data pribadi yang sensitif; tidak men*shar*e data pribadi orang lain di luar *consent* yang diberikan; tidak memberikan data pribadi yang tidak relevan atau berlebihan, dan lain-lain.

4. Partisipasi Masyarakat

   Dalam mendukung meningkatnya kepatuhan terhadap UU PDP, partisipasi masyarakat sejak awal seharusnya telah dilibatkan, baik melalui konsultasi publik untuk menjaring kepentingan dan aspirasi masyarakat; pengakomodasian kepentingan masyarakat pada setiap tahapan pembuatan kebijakan atau pembentukan peraturan perundang-undangan; sosialisasi atas UU PDP; pelibatan perwakilan komponen masyarakat dalam pembentukan dan pelaksanaan tugas, fungsi dan wewenang Lembaga Pengawas, dan lain-lain.

E. Antisipasi Terhadap Perkembangan Teknologi yang Berimplikasi pada PDP

1. Pengantar

   Setiap upaya untuk Pelindungan Data Pribadi seyogyanya juga mengantisipasi perkembangan teknologi, baik sekarang maupun di masa yang akan datang, yang diperkirakan berimplikasi terhadap hak-hak Subjek Data Pribadi. Pada saat ini berkembang teknologi-teknologi tertentu yang diperkirakan berimplikasi terhadap hak-hak Subjek Data Pribadi. Teknologi-teknologi tersebut mencakup: *Artificial Intelligence (AI); Big Data; Cloud Computing; Face Recognition; Face Scanning Smart Glassess,* dan lain-lain. Di bawah ini akan diuraikan secara singkat tentang perkembangan, penerapan serta implikasi teknologi-teknologi tersebut terhadap hak-hak Subjek Data Pribadi.

2. *Artificial Intelligence (AI)*

   Secara teknis AI dirumuskan sebagai: *"It rely more on the idea of intelligent machine, which-as flexible rational agent-perceives its environment and take*

*actions that maximize its chance of success at an arbitrary goa*l"[166] Ada beberapa kategori dari AI, yaitu: *Narrow AI, True AI, General AI, Machine Learning, Deep Learning*. Terdapat beberapa cakupan kemampuan dari AI, antara lain[167]:

- Kemampuan untuk memprediksi dan mengantisipasi keadaan yang akan datang berbasis analisis data.
- Dapat menjalankan berbagai fungsi intelejensia manusia[168].
- Melakukan pengamatan *(surveillance)* yang dilakukan oleh Pemerintah.
- Menerjemahkan bahasa.
- Mengendarai kendaraan secara *autonomous*.
- Melakukan pengenalan wajah.
- Melakukan profiling terhadap seseorang.
- Dan lain-lain.

Banyak manfaat yang dapat dipetik dari AI, demikian pula berbagai konsekuensi yang menyertainya. Manfaat yang bisa dipetik, antara lain *customer support, virtual assistance, content generation, digital surveillance, using AI during Work, employment*, dan lain-lain[169]. Sementara itu konsekuensi yang dapat ditimbulkan oleh pemanfaatan AI, terutama terkait data pribadi, mencakup: secara potensial berdampak terhadap kepentingan Subjek Data Pribadi, secara hukum dapat mempunyai efek hukum terhadap Subjek Data Pribadi terutama dalam pemrosesan data pribadi dan pengambilan putusan yang sepenuhnya dilakukan secara *automated* yang dapat berdampak terhadap pelaksanaan hak-hak Subjek Data Pribadi[170].

Pemanfaatan AI yang secara khusus mempunyai implikasi hukum terhadap PDP, yaitu: *automated decision making (credit scoring, e-recruitment); discriminatory effect (for example based on ethnicity); the use of special category*

166 Russel S and Norvig P, Artificial Intelligence: A Modern Approach, Prentice Hall, 2003, halaman 23.

167 Baca: I B R Supancana, "Legal and Ethical Issues on the Utilization of Artificial Intelligence and its Implications Towards Personal Data Protection", Disampaikan pada Seminar Nasional tentang "Filling the Legal Vacuum Concerning Unlawful Actions by Artificial Intelligence", diselenggarakan Fakultas Hukum Unika Atma Jaya Jakarta, 26 Mei 2024.

168 Mencakup fungsi-fungsi seperti: reasoning, problem solving, pattern recognition, perception, cognition, understanding, learning. Baca: Ibid.

169 Lihat, Ibid.

170 Ibid.

of data to audit the AI system; legal basis for processing data entirely conducted by AI; information duties and data subject rights in the context of AI use; further obligations under data protection law[171].

Dengan mencermati manfaat maupun implikasi hukum pemanfaatan AI maka perlu ada penyelesaian, baik melalui pendekatan hukum maupun pendekatan etika. Secara internasional maupun berdasarkan hukum nasional terdapat banyak instrumen hukum tekait pemanfaatan AI, seperti: *EU AI Act 2024, China's Interim Measures for the Administration of Generative AI Services in China 2023, Italian Supervisory Authority Requirements for Opean AI,* dan lain-lain. Sementara itu di Indonesia sudah ada prinsip-prinsip Etika pemanfaatan AI yang meliputi: inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, PDP, pengembangan dan kelanjutan lingkungan, serta perlindungan hak-hak kekayaan intelektual[172].

3. *Big Data*

Salah satu perkembangan teknologi yang perlu dicermati adalah *Big Data*[173]. Karena jumlah data yang sangat besar dan kompleks, maka cara-cara pemrosesan data secara tradisional tidak mampu menanganinya sesuai dengan skala dan kecepatannya. Dalam penerapan *Big Data* ada 3 (tiga) resiko yang dapat ditimbulkan terkait dengan privasi data, yaitu: pelanggaran/ kebocoran data *(data breach), data brokerage* dan *data discrimination.* Oleh karena itu tata kelola data *(data governance)* dan integrasi data sangat vital bagi kepatuhan terhadap PDP dan *privacy management.*

Terdapat banyak contoh *big data analytic* yang melibatkan pemrosesan data pribadi yang bersumber dari: media sosial, *loyalty cards* dan *sensors in clinical trials.* Salah satu persyaratan pelindungan data kunci adalah memastikan pemrosesan data pribadi harus *fair,* ini khususnya sangat penting dalam hal *big data* digunakan untuk membuat putusan yang mempengaruhi

[171] Ibid.

[172] Cermati Surat Edaran Kementerian Komunikasi dan Informasi No 3 tahun 2023 tentang Aspek-Aspek Etika Kecerdasan Buatan (Artificial Intelligence).

[173] Secara umum Big Data didefinisikan sebagai: "Big Data is high-volume, high-velocity and high-variety of information assets that demands cost-effective, innovative forms of information processing for enhanced insight and decision making".

kepentingan individu sebagai Subjek Data Pribadi. Karen*a big data* menggunakan semua data yang tersedia, maka berpotensi bertentangan dengan prinsip *data minimization.*

4. *Cloud Computing*

Pengembangan cloud computing saat ini telah menjadi bagian dari kehidupan ari-hari. Data-data Publik maupun Privat dapat disimpan melalui cloud computing. Pelayanan jasa *cloud computing* bisa dilaksanakan secara domestic maupun di luar Negara. Mengingat cloud computing bisa menyimpan semua jenis data, termasuk data pribadi, maka perlu ada perlindungan terhadap data pribadi., termasuk keamanan terhadap data pribadi. Untuk memastikan kepatuhan terhadap UU PDP dalam pemanfaatan *cloud computing*, ada beberapa langkah yang dapat ditempuh, antara lain: melakukan audit dan pemantauan terhadap lingkungan penyimpanan data cloud; menerapkan enkripsi maupun pengendalian akses; melakukan penilaian terhadap keamanan data secara regular termasuk *vulnerability scans*; menerapkan *multi-factor authentication;* melakukan pelatihan terhadap karyawan tentang *data protection best practices*[174].

Sebagai *best practices* terkait *cloud data privacy*, disarankan dilakukan langkah-langkah seperti: melakukan *risk assessment*; menerapkan *privacy by design principles*; menggunakan *softwar*e pengaman.

5. *Face Recognition*

Dalam bidang-bidang tertentu, termasuk bidang transportasi, baik darat, laut maupun udara, pemanfaatan alat pengenalan wajah *(Face Recognition)* merupakan hal yang biasa. Mengingat wajah seseorang adalah merupakan data pribadi, khususnya data biometrik yang merupakan data pribadi spesifik atau sensitif, maka pemanfaatan *Face Recognition* seharusnya didahului dengan melakukan DPIA. Hasil DPIA tersebut kemudian digunakan untuk mengantisipasi dan mempersiapkan langkah-langkah selanjutnya untuk mencegah maupun memitigasi dampak negatif terhadap Subjek Data Pribadi.

[174] Lihat https://www.hivenet.com, diunduh tanggal 18 November 2024.

Terkait pedoman pemanfaatan *Face Recognition, Council of Europe* telah menerbitkan suatu dokumen, yaitu *Guidelines on Facial Recognition. Guidelines* tersebut ditujukan kepada: Legislator dan Pengambil Keputusan; Pengembang, Produsen dan Penyedia Jasa; Pelaku Usaha yang menggunakan teknologi *Face Recognition*[175].

Bagi Legislator dan Pengambil Putusan misalnya, berlaku prinsip-prinsip: *lawfulness, necessary involvement of supervisory authorities, certification; and raising awareness*. Bagi Pengembang, Produsen dan Penyedia Jasa, berlaku prinsip-prinsip: *quality of data and algorithms, reliability of the tools used, awareness, and accountability*. Sementara bagi Pelaku Usaha yang menggunakan teknologi *Face Recognition* berlaku prinsip: *legitimacy of data processing and quality of data, data security, accountability, and ethical frameworks*. Bagi semua kategori di atas, dalam penerapan *Face Recognition* harus menghormati hak-hak Subjek Data Pribadi[176].

6. *Face Scanning Smart Glasses*

Teknologi ini dikembangkan oleh 2 (dua) mahasiswa *Harvard University*, yaitu Caine Ardayfio dan AnhPhu Nguyen, dimana keduanya mengadaptasi kacamata *Ray-Ban Meta* serta *computer software* untuk menciptakan kacamata yang memungkinkan penggunanya mengidentifikasi orang yang ditemuinya secara *real time* dengan memanfaatkan teknologi *Augmented Reality (AR).* Kacamata tersebut akan dapat mengungkap nama dan identitas orang yang ditemuinya secara *real time* hanya dalam waktu 2 menit dengan menggunakan *public facial recognition search engine* dan *artificial intelligence* dan dikombinasikan dengan berbagai teknologi yang ada lainnya. Diakui oleh para penemunya bahwa temuannya sangat powerful tapi juga sekaligus memunculkan permasalahan *privacy*. Mereka menyadari akan potensi dampak yang akan ditimbulkan terhadap *privacy* jika temuan teknologi mereka dikomersialkan. Para aktivis HAM juga menyampaikan keprihatinannya tentang dampak yang mungkin ditimbulkan, terutama terhadap wanita dan kelompok minoritas. Teknologi ini tidak hanya mampu mengindentifikasi

[175] Council of Europe, Guidelines on Facial Recognition, June 2021, https://rm.coe.int
[176] Ibid.

nama seseorang, tetapi juga data pribadi lainnya, termasuk data pribadi yang sensitif[177]. Penerapan teknologi ini akan menimbulkan persoalan etika dan persoalan hukum.

F. Persoalan Ancaman terhadap *Cyber Security*

Salah satu persoalan yang mendesak untuk ditangani adalah persoalan ancaman terhadap *Cyber Security*. Berbagai bentuk kebocoran dan kejahatan data telah dialami, baik pada sektor-sektor publik maupun sektor privat. Sampai saat ini belum ada pedoman yang jelas tentang hal-hal apa yang harus dilakukan, baik dalam perspektif pencegahan maupun dalam perspektif penanggulangan terkait ancaman terhadap *Cyber Security*. Ancaman terhadap *Cyber Security* ini juga dapat berdampak terhadap PDP, terutama Subjek Data Pribadi. Uraian di bawah ini akan menggambarkan beberapa hal yang terkait dengan *Cyber Security*, baik konsep, *tools*, kebijakan, kerangka regulasi, upaya pencegahan dan penanggulangan ancaman terhadap *Cyber Security*, khususnya yang terkait dengan Data Pribadi.

Berikut uraian singkat tentang isu-isu sekitar *Cyber Security*, khususnya yang terkait dengan PDP:

1. Konsep *Cyber-Security*

   European Commission High Representatives merumuskan *Cyber Security* sebagai: *"Cyber Security commonly referred to the safeguard and action that can be used to protect the cyber domain, both in the civilian and military fied, from those threat that are associated with or that may harm its independent networks and information infrastructure. Cyber Security strives to preserve the availability and integrity of the networks and infrastructure, and the confidentiality of the information contained therein"*[178].

   Sementara itu *US Department of Homeland Security merumuskan Cybr Security,* sebagai*: "The prevention of damage to, the protection of, and the*

[177] Adam Smith, "Are Face-Scanning Smart Glassess a Problem or a Prophecy?", The Jakarta Post, 13 November 2024.

[178] Baca: I B R Supancana, "Legal Aspects of Cyber Security", disampaikan pada Loka Karya tentang Cyber Security, diselenggarakan oleh Kementerian Pertahanan RI bekerjasama dengan Kedutaan Amerika Serikat di Indonesia, Jakarta 25 Februari 2019.

restoration of computers, electronic communications systems, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and no repudiation"[179].

2. Jenis-jenis *Tools* yang Dapat Jadi Ancaman Terhadap *Cyber Security*
   Jenis-jenis *tools* yang berpotensi dimanfaatkan untuk mengancam *Cyber Security* meliputi, antara lain *backdoors, botnets, denial of service attacks, key loggers, logic bomb, malware, pharming, phising, rootkits, smurfing, spoofing, spyware, Trojan horses, viruses, wamrs, zombies, exploits, sniffers*[180].

3. Potensi Ancaman Terhadap *Cyber Security*
   Potensi ancaman terhadap *Cyber Security* dapat berupa*: cyber crime, cyber terrorism, cyber war, hacking, hactivism, cyber espionage, advance persistent treath,* dan lain-lain.

4. Upaya Pencegahan
   Di praktek beberapa Negara seperti di Perancis sebagai upaya untuk mencegah terjadinya *Cyber Security Incident*, baik organisasi maupun korporasi perlu melakukan langkah-langkah, seperti[181]:
   - Meningkatkan kesadartahuan *(raise awareness)*
   - Secara teratur memutakhirkan sistem TI-nya
   - Membatasi akses dan mendorong penggunaan otentikasi yang kuat
   - Melakukan audit
   - Melakukan enkripsi terhadap data-data yang sensitif, terutama ketika data tersebut akan ditransfer
   - Melakukan desentralisasi terhadap jaringan

5. Upaya Penanggulangan
   Jika teridentifikasi terjadinya kebocoran, maka langkah-langkah yang dapat dilakukan meliputi:

---

179 Ibid.
180 Ibid.
181 Baca: ADSTO (avocats a la cour), "At Glance: Cyber Security Best Practices in France", Lexology, 13 Februari 2023

- Memutus sistem IT yang terdampak dari jaringan yang ada
- Menyampaikan informasi tentang *incident* tersebut kepada *local computer emergency response team*
- Membuat *clone copy* atas *hard disk drive*
- Memngumpulkan bukti-bukti dan mencari jejak digitalnya
- Melaporkan kepada Polisi

6. Pengaturan di Indonesia

   Pada tahun 2022 OJK menerbitkan Peraturan OJK (POJK) nNo 11/POJK-03/2022 tentang Implementasi Teknologi Informasi oleh Bank Komersial. Regulasi ini merupakan bagian dari revolusi OJK terkait regulasi tentang: data, teknologi, manajemen resiko, kolaborasi, dan kelembagaan (penataan). Semua itu dirancang untuk meningkatkan akselerasitransformasi digital perbankan.

   POJK No 11 sebagaimana tersebut di atas ditindaklanjuti dengan Surat Edaran (SE) OJK No 29/SEOJK.03/2022 tentang *Cyber Security* serta ketahanannya pada Bank-bank komersial. Inti Surat Edaran ini, antara lain[182]:

   - Melakukan serangkaian *self-assessment rating* tentang proses pengamanan yang diterapkan secara reguler (tahunan)
   - Melaporkan hasil *self-assessment rating* tersebut kepada OJK
   - Melaporkan jika terjadi *Cyber Incident* kepada OJK dan
   - Membuat *Cyber Security Structure* yang baru
   - *Cyber Security Assessment* dilakukan dengan melakukan *assessment* terhadap *Inherent Risk*[183] dan *Cyber Security Maturity*[184]
   - Melakukan *Cyber Security Testing*[185]
   - Memiliki *Cyber Security Unit*[186]
   - Menyampaikan *Cyber Incident Report*[187]

[182] Rajah & Tan, "OJK Sets New Cyber Security Best Practices for the Banking Industry", Lexology, 6 April 2023.

[183] Inherent Risk Assessment meliputi: technology, banking products, organization characteristics serta cyber incidents track record. Baca: Ibid.

[184] Maturity Risk Assessment meliputi, baik Risk Management Aspects maupun Resilience Processes.

[185] Cyber Security Testing meliputi: vulnerability analysis; scenario-based testing, dan other pro-active measures.

[186] Keberadaan Cyber Security Unit dibuthkan untuk mengelola keamanan dan ketahanan siber (Cyber Security and Resilience).

[187] Cyber Incident Report meliputi: an initial notification report, yang meliputi informasi dasar tentang

G. Perlunya Pedoman Implementasi PDP yang Lebih Rinci

Jika dicermati, UU PDP berisi ketentuan-ketentuan yang sangat umum dan tidak seoperasional EU GDPR misalnya, demikian pula Rancangan Peraturan Pemerintahnyapun kurang memberikan pedoman secara rinci tentang bagaimana penerapan ketentuan-ketentuan UU PDP dalam kehidupan sehari-hari. Sebagai acuan untuk mendapatkan gambaran secara utuh terhadap implementasi suatu aturan, khususnya PDP di Uni Eropa, dapat dicermati penerapan tersebut dari putusan atas berbagai kasus yang ada serta banyaknya *Guidelines* yang dikeluarkan oleh *European Data Protection Board (EPDB)*.

insiden yang terjadi; serta a cyber incident report yang berisi informasi rinci tentang insiden yang terjadi.

BAB VII

ASPEK-ASPEK PRAKTIS DALAM IMPLEMENTASI UNDANG-UNDANG PELINDUNGAN DATA PRIBADI

Dalam Bab ini akan dibahas aspek-aspek praktis dalam rangka implementasi UU PDP, baik oleh sektor publik, sektor privat. Hal-hal praktis tersebut meliputi: melakukan *gap assessment*; menyiapkan *privacy policy*; melakukan *Recording of Processing Activities* (ROPA); melakukan *Data Protection Impact Assessment* (DPIA); merumuskan *data processing agreement*; merumuskan *data sharing agreement*; menyusun *data breach management plan* serta *data breach notification*; melakukan transfer data; menunjuk DPO; meningkatkan keamanan data; dan lain-lain.

A. Menyusun *Gap Assessment*

Sebagai langkah awal dalam rangka kepatuhan *(compliance)* terhadap UU PDP, khususnya untuk menilai kesenjangan antara kondisi awal dan kondisi idealnya, maka perlu dilakukan *Gap Assesment*. Berdasarkan *Gap Assessment* tersebut kemudian dapat dirumuskan semacam *transformation road map* ke arah *compliance.*

Dalam rangka melakukan *Gap Assessment*, ada pertanyaan-pertanyaan dasar yang perlu diajukan kepada organisasi/korporasi, antara lain:

1. Bagaimana struktur organisasi/korporasi?
2. Bagaimana struktur satuan kerja yang menangani PDP pada organisasi/korporasi?
3. Bagaimana mekanisme koordinasi antar satuan kerja dalam penanganan PDP pada organisasi/korporasi?
4. Mohon dijelaskan SDM yang menanganai PDP pada organisasi (jumlah maupun kualifikasinya)?
5. Adakah fungsi pada satuan kerja semacam DPO?
6. Apakah organisasi/korporasi mempunyai *Privacy Policy?*
7. Apa saja yang dimuat dalam *Privacy Policy* tersebut?
8. Apakah ada pemrosesan data yang melibatkan data spesifik (misalnya *face recognition*) atau menggunakan teknologi yang inovatif (misalnya AI)?
9. Jika ada, pernah dilakukan DPIA?
10. Jika sudah dilakukan DPIA, langkah-langkah apa saja yang tercakup dalam kegiatan DPIA tersebut?
11. Apakah organisasi/korporasi sudah mulai menerapkan ROPA?
12. Langkah-langkah apa yang telah ditempuh dalam melakukan ROPA?
13. Apakah penerapan ROPA pada Organisasi/Korporasi telah dikonsultasikan dan disosialisasikan secara internal?
14. Apakah dalam melakukan ROPA telah memperhatikan prinsip-prinsip PDP dan Hak-hak Subjek Data?
15. Apa saja cakupan kegiatan dalam melakukan ROPA?
16. Hal-hal apa saja yang di*record* dalam melakukan ROPA?
17. Apakah organisasi/korporasi menerapkan *Data Breach Management Plan?* Jika ada meliputi hal-hal apa saja?
18. Ketika terjadi kebocoran data, apakah ada *Data Breach Notification?*
19. Bagaimana kebijakan pengamanan data pada organisasi/korporasi?
20. Apakah rujukan pengaturan tentang pengamanan data?
21. Apakah organisasi/korporasi melakukan transfer data, baik domestik maupun internasional?
22. Adakah kebijakan-kebijakan pokok dalam transfer data?
23. Apakah rujukan dalam transfer data?
24. Apakah ada *safeguard* dalam transfer data?

25. Apakah ada *corporate binding rules* terkait transfer data?
26. Apakah ada *Standard contractual clauses* dalam transfer data?
27. Apakah diterapkan *cross border privacy rules*?
28. Apakah kegiatan pemrosesan data dilakukan sendiri atau dilakukan oleh pemroses data?
29. Jika dilakukan sendiri apakah disadari bahwa organisasi/korporasi bertindak sebagai pengendali data?
30. Jika dilakukan oleh pemroses data, apakah ada semacam *data processing agreement* dengan pemroses data?
31. Hal-hal apa saja yang diatur dalam *data processing agreement*?
32. Apakah data-data yang diproses pemroses data dishare kepada pihak lain?
33. Apakah organisasi memiliki *data sharing agreement*?
34. Apa isi ketentuan-ketentuan pokok pada *data sharing agreement?*

Jawaban atas pertanyaan-pertanyaan dasar tersebut agar disusun dalam tabel dan dilakukan *assessment* secara menyeluruh untuk selanjutnya didiskusikan langkah-langkah selanjutnya ke arah *compliance.*

B. Menyusun *Privacy Policy*

1. Definisi

   Data Protection Policy/Privacy Notice adalah merupakan dokumen publik/terbuka dari suatu organisasi/korporasi tentang bagaimana mereka memproses Data Pribadi dan bagaimana penerapan prinsip-prinsip Pelindungan Data Pribadi.

2. Hal-hal Pokok yang Diatur

   Menurut Pasal 21 Undang-Undang tentang Pelindungan Data Pribadi, ada hal-hal pokok yang dimuat dalam *Privacy Policy*, yaitu:

   a. Legalitas pemrosesan Data Pribadi.
   b. Tujuan pemrosesan Data Pribadi.
   c. Jenis dan relevansi Data Pribadi yang akan diproses.
   d. Jangka waktu Retensi Data yang memuat Data Pribadi.

e. Rincian mengenai informasi yang dikumpulkan.
f. Jangka waktu pemrosesan Data Pribadi.
g. Hak-hak Subjek Data Pribadi.

3. *International Best Practices*

Berdasarkan *International Best Practices Privacy Policy* setidak-tidaknya memcakup[186]:

a. Identitas dan nomor kontak Pengendali Data, serta DPOnya.
b. Tujuan memproses Data Pribadi dan Dasar Hukumnya.
c. Kepentingan yang sah dari Pengendali Data untuk memproses data.
d. Setiap penerima data atau kategorisasi penerima data secara individu.
e. Informasi rinci tentang transfer Data Pribadi ke Negara Ketiga dan pengamanan yang dilakukan.
f. Periode retensi atau kriteria yang digunakan untuk menentukan periode retensi data.
g. Pelaksanaan atas setiap hak dari Subjek Data.
h. Hak untuk menarik kembali persetujuan pemrosesan setiap saat (jika diperlukan).
i. Hak untuk mengajukan complain kepada Pengendali Data/Pemroses Data melalui *Supervisory Authority*.
j. Informasi apakah ketentuan tentang Data Pribadi merupakan bagian dari pelaksanaan peraturan perundang-undangan atau pelaksanaan persyaratan kontraktual, atau berdasarkan kewajiban kontraktual, disertai informasi mengenai kemungkinan konsekuensinya dalam hal gagal menyediakan Data Pribadi.
k. Informasi dalam hal adanya sistem pengambilan putusan secara otomatis, termasuk melakukan profiling, dan informasi bagaimana sistem tersebut dipasang, serta informasi, baik manfaatnya maupun konsekuensinya.

4. Cara Mengembangkan Privacy Policy yang Baik[187]
   a. Singkat tapi Komprehensif *(concise)*

[186] Baca: Abu Bakar Munir, Module 6: Collection Notice and Privacy Policy, Materi Pelatihan DPO diselenggarakan oleh APPDI bekerjasama dengan Schinder Law Firm, 2024.
[187] Ibid.

b. Transparan *(truthful)*
c. Mudah diakses *(easily accessible)*
d. Menggunakan bahasa yang sederhana, namun jelas dan mudah dipahami *(uses clear and plain languages)*

5. Contoh *Privacy Policy* yang Baik

a. *WhatsApp*

WhatsApp pada tahun 2023 memuat *Privacy Policy* baru yang membuat pesan data bersifat *end-to-end encrypted* dan aplikasi ini tidak mempunyai akses terhadap *chat* pribadi atau mengakses lokasi.

Hal-hal yang terdapat pada *privacy policy* dari *WhtasApp*, antara lain:

– *WhatsApp legal info*
– *Information we collect*
– *Information you provide; your account info; your message; undelivered message; media forwarding; your connection; status info; transaction and payment data; customer support and other*
– *Automated collected info; usage and log into device and connection info; location info; cookies*
– *Third party information: infor others provide you; user reports; business on WhatsApp; third party service provider; third party services.*
– *How we use information: our services; safety, security and integrity.*
– *Receive and share information with Fcebook, as part of the Facebook companies.*

b. 5 (lima) *Privacy Policy* terbaik lainnya terkait *compliance* terhadap *GDPR,* antara lain*: Disney's Privacy Policy; Outbrain's Privacy Policy; Uber's Privacy Policy; Google's Privacy Policy; dan Twitter's Privacy Policy*[188].

c. Dari 5 (lima) *Privacy Policy* terbaik tersebut, maka ada beberapa *common elements* yang dapat ditarik, yaitu[189]:

– *Data processing must be fair to the data subject*

[188] Ironclad Journal, "GDPR: 5 Best Examples Privacy Policy Examples", ironcladapp.com, diunduh tanggal 12 Nopember 2024.
[189] Ibid.

- *Data must only be processed for specific and legitimate purposes, outlined In the Privacy Policy*
- *Don't collect more data than you need*
- *Make sure the data that you collect is accurate*
- *Don't store personal data longer than needed for specific purposes*
- *Process data in a way that ensures security, integrity, and confidentiality*
- *Be able to demonstrate compliance with this principle*

C. *Data Processing Agreement*

Dalam *Data Processing Agreement*, ada beberapa hal yang harus diperhatikan:

1. Hubungan antara Pengendali Data dengan Pemroses Data
   Pengendali Data adalah pihak yang menentukan tujuan dan cara pemrosesan data. Pemroses Data bertindak untuk dan atas nama Pengendali Data sesuai dengan instruksi yang diberikan.

   Pada dasarnya Pengendali Data yang bertanggung jawab atas apa yang dilakukan oleh Pemroses Data sepanjang Pemroses Data melakukan kegiatan pemrosesan sesuai dengan instruksi yang diberikan oleh Pengendali Data. Pemroses Data dapat dimintakan pertanggungjawabannya jika melakukan pemrosesan data yang tidak sesuai dengan instruksi yang diberikan oleh Pengendali Data.

2. Pentingnya Kontrak antara Pengendali Data dengan Pemroses Data
   Kontrak antara Pengendali Data dan Pemroses Data diperlukan untuk[190]:
   a. Memformalkan hubungan.
   b. Agar para pihak mengetahui kewajiban dan tanggung jawab masing-masing.
   c. Untuk menunjukkan kepatuhan kepada aturan pelindungan data pribadi.

[190] Baca: Abu bakar Munir, Module 5: Data Protection Rules and Obligations of Organizations, Materi Pelatihan DPO diselenggarakan oleh APPDI bekerjasama dengan Schinder Law Firm, 2024.

3. Ketentuan-ketentuan Pokok pada *Data Processing Agreement*
   Ketentuan-ketentuan pokok pada *Data Processing Agreement,* minimal meliputi[191]:
   a. Hal-hal yang diproses dan jangka waktunya.
   b. Sifat dan tipe pemrosesan.
   c. Tipe data pribadi.
   d. Kategori Subjek Data.
   e. Hak-hak dan kewajiban Pengendali Data.
   f. Hak-hak Subjek Data.
   g. Pelibatan Sub-Prosesor.
   h. Tindakan pengamanan yang memadai.
   i. *Duty of confidence*.
   j. Pemrosesan hanya dilakukan berdasarkan instruksi Pengendali Data.
   k. Bantuan terhadap Pengendali Data.
   l. Audit dan Pengawasan.
   m. Ketentuan tentang pengakhiran kontrak.

4. Tips- untuk memilih Pemroses Data[192]
   a. Pilih Pemroses Data yang mempunyai reputasi baik.
   b. Pastikan bahwa kontrak dapat ditegakkan di Indonesia dan dimana Pemroses Data berdomisili.
   c. Pastikan bahwa calon Pemroses Data mempunyai sistem pengamanan data yang memadai.
   d. Pastikan calon Pemroses Data telah melakukan pengecekan yang memadai terhadap stafnya.
   e. Lakukan audit terhadap calon Pemroses Data.
   f. Minta (sebagai syarat) kepada Pemroses Data untuk melaporkan setiap kebocoran data atau permasalahan lain yang timbul.
   g. Memiliki prosedur yang berlaku (pada Pengendali Data) untuk bisa bertindak secara memadai ketika menerima laporan.
   h. Secara teratur mereview proses dan prosedur yang berlaku.

[191] Ibid.
[192] Ibid.

D. *Recording of Processing Activities (ROPA)*

Salah satu bentuk kepatuhan terhadap regulasi terhadap PDP adalah melakukan perekaman terhadap kegiatan pemrosesan data pribadi *(ROPA).* Dalam melaksanan *ROPA,* ada beberapa aspek yang perlu dicermati:

1. Kewajiban melakukan ROPA
   Pengendali Data mempunyai kewajiban untuk melakukan ROPA. Undang-undang Pelindungan Data Pribadi mengatur kewajiban ROPA sebagaimana diatur dalam Pasal 31, yang rumusannya menyatakan "Pengendali Data wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan data".

2. Hal-hal yang direkam *(record)*[193]
   a. Nama dan nomor kontak Pengendali Data.
   b. Tujuan Pemrosesan
   c. Kategori Subjek Data
   d. Kategori penerima data
   e. Transfer data pribadi ke Negara Ketiga
   f. Masa Retensi
   g. Tindakan pengamanan, baik secara tertulis maupun secara operasional.

3. Langkah-langkah Untuk Menyiapkan ROPA[194]
   a. Lakukan audit informasi atau pemetaan data untuk memperjelas data apa yang dimiliki dan dimana.
   b. Tempatkan dan *review* semua kebijakan *(privacy),* prosedur maupun kontrak serta perjanjian-perjanjian yang ada.

4. Bagaimana Perekaman dilakukan[195]
   a. Harus tertulis (baik menggunakan kertas maupun secara elektronik).
   b. Ada beberapa keuntungan menggunakan cara elektronik, yaitu mudah ditambah, diubah atau dipindah.

[193] Ibid.
[194] Ibid.
[195] Ibid.

c. Kegiatan pemrosesan harus didokumentasikan secara *granular* (*detail*/ rinci) dan *meaningful* (berarti).
d. Harus mencerminkan perbedaan antara kategori data yang berbeda.
e. Adanya suatu daftar umum tentang bagian-bagian informasi yang kurang memiliki kaitan diantara mereka, atau tidak memenuhi persyaratan hukum yang berlaku.

5. Tips untuk melakukan ROPA
   a. Bukan merupakan *a one-off exercise.*
   b. Harus mencerminkan situasi yang sebenarnya.
   c. DPO harus memperlakukan rekaman pemrosesan sebagai suatu *living document* yang memerlukan pemutakhiran jika diperlukan.
   d. DPO harus melakukan *review* secara teratur terhadap data/informasi yang diproses.

E. *Data Protection Impact Assessment (DPIA)*

1. Pengertian DPIA

   The International Association for Impact Assessment merumuskan DPIA *sebagai "the identification of future consequence of a current proposed action*". Maknanya adalah: DPIA merupakan suatu proses sistematis untuk mengevaluasi suatu proposal (proyek) dari aspek dampaknya terhadap privasi. DPIA merupakan suatu proses untuk membantu suatu organisasi/ korporasi dalam mengidentifikasi dan meminimalkan resiko terkait dengan pelindungan data dalam suatu proyek. DPIA merupakan suatu penilaian sistematis terhadap suatu proyek dengan mengidentifikasi dampak dari proyek tersebut terhadap privasi individu, serta merancang rekomendasi untuk mengelola, meminimalisasi dan menghilangkan dampaknya[196].

2. Mengapa Perlu Dilakukan DPIA?

   Pelaksanaan DPIA akan membantu organisasi/korporasi untuk[197]:

[196] Lihat Abu Bakar Munir, Module 1, Data Protection Officer: Duties and Functions, Materi Pelatihan CDPO yang diselenggarakan oleh APPDI bekerjasama dengan Schinder Law Firm, 2024.
[197] Ibid.

a. Memberikan gambaran tentang arus informasi/data pribadi pada proyek yang dilakukan.
b. Menganalisis kemungkinan dampak terhadap data/informasi pribadi.
c. Mengidentifikasi dan merekomendasi opsi-opsi yang ada dalam rangka penghindaran, minimalisasi atau memitigasi dampak negatif dari proyek tersebut terhadap privasi.
d. Mengembangkan berbagai pertimbangan privasi dalam perancangan proyek.
e. Mencapai tujuan proyek dengan meminimalisasi dampak negatif, semetara meningkatkan dampak positif terhadap privasi.

3. Apa Resiko Jika Tidak Melakukan DPIA?
   Beberapa resiko yang dapat diidentifikasi apabila tidak melakukan DPIA, antara lain:
   a. Ketidakpatuhan terhadap aturan PDP secara potensial akan mengarah kepada kebocoran data serta publisitas negatif.
   b. Hilangnya kredibilitas karena kurangnya transparansi dalam merespons harapan publik dalam penanganan data/informasi pribadi.
   c. Rusaknya reputasi organisasi/korporasi apabila proyek gagal memenuhi ekspektasi tentang bagaimana informasi pribadi akan dilindungi.
   d. Identifikasi resiko privasi pada tahapan berikutnya dalam pengembangan atau implementasi proyek akan menjadi beban biaya yang tidak perlu atau solusi yang tidak tepat[198].

4. Manfaat Melakukan DPIA
   a. memastikan kepatuhan proyek terhadap aturan PDP.
   b. Mencerminkan nilai-nilai masyarakat terkait privasi data dan informasi pribadi dalam perancangan proyek.
   c. Mengurangi biaya di kemudian hari terkait manajemen, biaya hukum serta potensi publisitas negatif.
   d. Mengidentifikasi strategi untuk mencapai tujuan proyek tanpa berdampak terhadap privasi.

[198] Ibid.

e. Menunjukkan kepada pemangku kepentingan bahwa proyek dirancang dengan kesadaran akan perlindungan privasi.
f. Meningkatkan kesadartahuan dan pemahaman dalam masalah-masalah privasi dalam perusahaan.
g. Membangun kesadaran masyarakat serta penerimaan terhadap proyek melalui konsultasi publik.

5. Proyek Mana yang Memerlukan DPIA?
   a. Jika menggunakan teknologi yang bersifat inovatif.
   b. Menggunakan profiling atau kategori data khusus untuk memutuskan akses terhadap suatu pelayanan.
   c. Melakukan profiling terhadap individu (Subjek Data) dalam skala besar.
   d. Memproses data biometrik.
   e. Memproses data genetika.
   f. Memadukan data atau mengkombinasikan serangkaian data dari sumber-sumber yang berbeda.
   g. Menumpulkan data pribadi dari sumber-sumber yang tidak bersifat individual.
   h. Melacak lokasi dan perilaku individual.
   i. Memprofile anak-anak atau target pemasaran atau jasa *online* pada mereka.
   j. Memproses data yang dapat membahayakan kesehatan fisik individu serta keselamatan individu[199].

6. Kapan Perlu Melakukan DPIA?
   a. DPIA harus menjadi bagian integral dari proses perencanaan proyek.
   b. Perlu dilakukan seawal mungkin dalam pengembangan proyek sehingga masih memungkinkan memengaruhi rancangan proyek, atau jika mempunyai dampak privasi yang bersifat negatif, dapat dipertimbangkan untuk memikirkan kembali kelanjutan proyek.
   c. DPIA dilakukan dalam keseluruhan tahapan perencanaan proyek.

[199] Ibid.

d. Melakukan DPIA harus dilihat sebagai proses yang tidak berakhir pada saat publikasi laporan DPIA.

7. Apakah Tahapan-tahapan Dalam Melakukan DPIA?
   a. Melakukan *threshold assessment*
   b. Merancang DPIA.
   c. Memberikan gambaran tentang proyek.
   d. Melakukan identifikasi terhadap pemangku kepentingan dan berkonsultasi kepada mereka.
   e. Memetakan arus informasi.
   f. Melakukan analisis dampak terhadap privasi serta mengecek kepatuhannya.
   g. Pengelolaan privasi untuk mengatasi resiko.
   h. Rekomendasi.
   i. Pelaporan.
   j. Merespons dan mereview[200].

F. *Data Protection Officer (DPO)*

1. Dasar Pengaturan tentang DPO di Indonesia
   a. Undang-undang No 27 tahun 2022 tentang Pelindungan Data Pribadi.
   b. Undang-Undang No 11 tahun 2008 sebagaimana diubah dengan Undang-Undang No 19 tahun 2016, terakhir diubah dengan Undang-Undang No 1 tahun 2024 tentang Informasi dan Transaksi Elektronik.
   c. Undang-Undang No 20 tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian.
   d. Undang-Undang No 13 tahun 2003 tentang Ketenagakerjaan.
   e. Peraturan Pemerintah No 31 tahun 2006 tentang Sistem Pelatihan Kerja Nasional (SISLATKERNAS).
   f. Peraturan Pemerintah No 10 tahun 2018 tentang Badan Nasional Sertifikasi Profesi (BNSP).

[200] Ibid.

g. Keputusan Presiden No 78 tahun 2001 tentang Komite Akreditasi Nasional.
h. Peraturan Presiden No 8 tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (KKNI).
i. Peraturan Menteri Ketenagakerjaan No 2 tahun 2016 tentang Sistem Standardisasi Kompetensi Kerja Nasional Indonesia (SKKNI)
j. Peraturan Menteri Komunikasi dan Indonesiasi No 24 tahun 2015 tentang Pemberlakuan SKKNI Komunikasi Informatika
k. Peraturan Menteri Komunikasi dan Informasi No 20 tahun 2016 tentang Perlindungan Data Pribadi pada Sistem Elektronik.
l. Keputusan Menteri Ketenagakerjaan No 103 tahun 2023 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Informasi dan Komunikasi Golongan Pokok Aktivitas Pemrograman, Konsultasi Komputer dan Kegiatan yang Berhubungan dengan Bidang Keahlian Pelindungan Data Pribadi.

2. Kebutuhan DPO di Indonesia

Berdasarkan *Grand Design* Pembentukan Ekosistem *Data Protection Officer (DPO)* Indonesia yang disusun oleh Direktorat Jenderal Informatika Kementerian Komunikasi dan Informasi pada tahun 2021, dibutuhkan sekitar 155.000 DPO di Indonesia.

DPO yang dimaksud harus memenuhi kompetensi tertentu, baik dari aspek pengetahuan, ketrampilan maupun perilakunya sesuai dengan peraturan perundang-undangan yang berlaku.

3. Kualifikasi DPO

a. Memiliki kualifikasi profesional, dan khususnya pengalaman dan pengetahuan serta keahlian di bidang Hukum Pelindungan Data Pribadi.
b. Berdasarkan praksis terbaik, pengetahuan dan ketrampilan yang dimiliki seorang DPO harus proporsional dengan tipe pemrosesan, dengan memperhatikan tingkat perlindungan data pribadi yang dibutuhkan.

c. Dalam hal pemrosesan data pribadi bersifat kompleks atau beresiko, maka pengetahuan dan kemampuan yang perlu dimiliki oleh seorang DPO harus memadai untuk melakukan pengawasan yang efektif.
d. Seorang DPO juga perlu memiliki pemahaman yang cukup tentang tindakan teknis dan operasional yang dibutuhkan serta pemahaman tentang teknologi informasi dan keamanan data.

4. Tugas dan Fungsi DPO
   a. Menyampaikan informasi dan saran-saran bagi Pengendali data atau Pemroses Data untuk mematuhi peraturan perundang-undangan yang berlaku.
   b. Memantau dan memastikan kepatuhan terhadap peraturan yang berlaku.
   c. Membantu dalam melakukan *Data Protection Impact Assessment (DPIA).*
   d. Bertindak sebagai narahubung antara Pengendali Data/Pemroses Data dengan regulator, termasuk melakukan mitigasi resiko.

G. Keamanan Data dan Penanganan *Data Breach*

Masalah Keamanan Data dan *Data Breach* merupakan hal yang penting, mengingat banyaknya terjadi kebocoran data. Selain itu juga perlu dipahami tentang kewajiban Pengendali dan Pemroses Data untuk memastikan keamanan data. Lebih jauh, untuk mengantisipasi terjadinya Data Breach, perlu dilakukan langkah-langkah berupa penyiapan *Data Breach Management Plan* sehingga jika terjadi *Data Breach* sudah ada panduan tentang hal-hal yang harus dilakukan, termasuk melakukan *Data Breach Notification.* Berikut beberapa uraian singkat tentang hal-hal di atas:

1. Kasus-Kasus Kebocoran Data
   a. 12 juta data pengguna Bukalapak (2019)
   b. 90 juta data pengguna Tokopedia (2020)
   c. 279 juta data BPJS Kesehatan (Mei 2021)
   d. 195 juta data penduduk pada situs KPU (September 2022)

e. 26 juta data pelanggan Idihome (Agustus 2022)
f. 1,3 miliar data penduduk dari pendaftaran SIM Card (Agustus 2022)
g. Kasus Kebocoran Data Bank Syariah Indonesia (BSI) pada tahun 2023
h. Kasus Serangan Ransomware terhadap Pusat Data Nasional Sementara 2 tahun 2024
i. Kasus Kebocoran Data NPWP tahun 2024
j. Dan lain-lain.

2. Kewajiban Pengendali Data terkait Keamanan Data
   a. Pasal 35 Undang-Undang PDP
      "Pengendali Data Pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya dengan melakukan:
      – Penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi yang perundang-undangan bertentangan dengan ketentuan peraturan.
      – Penentuan tingkat keamanan data dengan memperhatikan sifat dan resiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi "
   b. Pasal 36 Undang-Undang PDP
      "Dalam melakukan pemrosesan data pribadi, Pengendali Data wajib menjaga kerahasiaan data pribadi".

3. *Data Breach Management Plan*[201]
   a. *Data Breach Management Plan* merupakan suatu perencanaan yang melibatkan peran dan tanggung jawab berbagai pihak dalam menangani kebocoran data.
   b. *Data Breach Management Plan* juga menggambarkan langkah-langkah yang harus dilakukan suatu organisasi/korporasi ketika terjadi kebocoran data.
   c. *Data Breach Management Plan* harus dibuat secara tertulis untuk memastikan agar semua staf yang terkait memahami apa yang harus dilakukan dalam hal terjadinya kebocoran data.

[201] Baca: Abu Bakar Munir, Module 8: Security Processing and Managing Data Breach, Materi Pelatihan DPO, diselenggarakan oleh APPDI bekerjasama dengan Schinder Law Firm, 2024.

4. *Data Breach Notification*
   Mengenai *Data Breach Notification*, diatur dalam Pasal 46 Undang-Undang Pelindungan Data Pribadi yang rumusannya, sebagai berikut:

   a. Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi Wajib menyampaikan pemberitahuan secara tertulis plaing lambat 3 x 24 jam kepada: a, Subjek Data Pribadi; b. Lembaga.

   b. Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat: a. data pribadi yang terungkap; b. kapan dan bagaimana data pribadi terungkap; dan c. upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh Pengendali Data Pribadi.

   c. Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan data pribadi.

H. *Transfer Data*

1. Pelindungan Data Pribadi dan Transfer Data
   Pengaturan tentang pelindungan data pribadi merupakan keseimbangan antara pelindungan data pribadi di satu pihak, dengan upaya memfasilitasi *cross-border flow of personal data* yang dibutuhkan dalam kegiatan bisnis, baik di bidang perdagangan, investasi dan keuangan.

2. Pengaturan Transfer Data Menurut PDP

   a. Pasal 55 UU PDP
      "Transfer data dalam wilayah Indonesia wajib melakukan pelindungan data pribadi".

   b. Pasal 56 UU PDP
      Transfer data ke luar wilayah Indonesia, Pengendali Data wajib memastikan bahwa negara tempat penerima memiliki tingkat Pelindungan Data Pribadi yang lebih tinggi atau setara. Jika tidak lebih tinggi atau setara, wajib memastikan terdapat Pelindungan Data Pribadi yang memadai dan bersifat mengikat, Jika tidak terpenuhi, maka wajib mendapat persetujuan dari Subjek Data.

3. Pengaturan Transfer Data Menurut EU GDPR

   Pengaturan mengenai Transfer Data menurut EU-GDPR dapat ditemukan pada Pasal 44-47. Intinya adalah bahwa transfer data tersebut dapat dilakukan apabila dapat dijamin tingkat pelindungan data yang memadai *(adequate level of protection),* serta adanya pengamanan yang memadai *(providing adequate safeguards).*

   Pelindungan data yang memadai meliputi: adanya ketentuan yang relevan *(relevant provision),* yang lebih tinggi atau minimal setara; dan adanya unsur-unsur untk menilai tingkat pelindungan data yang memadai *(the elements for assessing Adequate Level of Protection).*

   Mengenai tindakan pengamanan yang memadai berdasarkan EU GDPR intinya mencakup:

   a. Adanya instrumen yang mengikat secara hukum dan dapat ditegakkan antara otoritas pelindungan data dan badan-badan lain yang terkait.
   b. Adanya *binding corporate rules* sebagaimana diatur dalam Pasal 47 EU GDPR.
   c. Adanya klausula standard tentang pelindungan data pribadi yang ditetapkan oleh *European Commission*.
   d. Adanya klausula pelindungan data pribadi yang standard yang ditetapkan oleh suatu *Supervisory Authority* yang disetujui oleh *European Commission*.
   e. Adanya aturan perilaku yang disepakati.
   f. Adanya mekanisme sertifikasi yang disepakati.
   g. Adanya klausula kontraktual antara Pengendali Data dan Pemroses Data.

I. Penggunaan *Software* atau Perangkat Lunak Kepatuhan Pelindungan Data Pribadi

Perkembangan PDP di dunia telah memberikan peluang kepada perusahaan-perusahaan di dunia untuk melakukan inovasi dengan meluncurkan produk-

produk *software* kepatuhan *(compliance software)* PDP yang ditawarkan kepada seluruh pasar di dunia. Sebagai contoh, Perusahaan yang telah meluncurkan produk *software* kepatuhan PDP adalah: *One Trust, TrustArc, Securiti, Microsoft Purview Compliance Manager, IBM Security Guardium*, dan lain-lain.

Penggunaan *software* PDP dapat membentu perusahaan atau organisasi yang sedang melakukan usaha kepatuhan data pribadi terhadap UU PDP dan regulasi PDP lainnya di luar negeri dalam beberapa cara, antara lain:

1. Otomatisasi Proses Manajemen Data

    a. Penemuan dan Klasifikasi Data
    Software ini memindai sistem organisasi, termasuk penyimpanan cloud, basis data, dan penyimpanan lokal, untuk mengidentifikasi dan mengklasifikasikan data berdasarkan sensitivitas dan persyaratan kepatuhannya. Ini mungkin melibatkan penandaan data pribadi, keuangan atau kesehatan untuk memastikan data ditangani dengan benar.

    b. Pemetaan dan Inventaris Data
    Membuat peta data memungkinkan organisasi memahami dimana data disimpan, diproses, dan ditransfer di dalam dan di luar organisasi. Ini sangat penting untuk kepatuhan UU PDP, dimana UU PDP mewajibkan organisasi untuk mendokumantasikan dan menunjukkan aktivitas pemrosesan data mereka.

2. Memfasilitasi Kepatuhan terhadap Regulasi

    a. Menyusun dan Memantau Implementasi Manajemen Kebijakan/ *Privacy Policy*
    Software kepatuhan dapat membantu menegakkan kebijakan pelindungan data, memastikan bahwa data diproses dan disimpan sesuai dengan persyaratan peraturan. Ini mencakup penetapan kebijakan retensi data, control akses, dan langkah-langkah keamanan.

    b. Penilaian Dampak Pelindungan Data Pribadi *(Data Protection Impact Assessment/DPIAs)*

Software kepatuhan juga seringkali menyertakan alat untuk melakukan DPIA, yaitu penilaian resiko untuk proyek-proyek yang melibatkan data pribadi. Penilaian ini sangat penting di bawah UU PDP, karena mereka mengidentifikasi resiko terhadap privasi data dan membantu organisasi mengatasi resiko sebelum masalah muncul.

c. *Audit Trails* dan Pencatatan atau *Recording of Processing Activities (ROPA)*
Software kepatuhan memiliki kemampuan untuk mencatat aktivitas pemrosesan data, yang memungkinkan organisasi untuk mempertahankan catatan yang membuktikan kepatuhan.Ini dapat membantu selama audit, dan menunjukkan kepada regulator jejak yang jelas tentang bagaimana data dikelola.

3. Menegakkan Akses Data dan Langkah-langkah Keamanan

a. Kontrol Akses dan Manajemen Pengguna
Software ini membatasi akses ke data sensitif berdasarkan peran dan izin pengguna, memastikan hanya personil yang berwenang yang dapat melihat atau memanipulasi data. Ini sangat penting untuk meminimalkan ancaman dari dalam dan memenuhi kewajiban hukum untuk melindungi data pribadi.

b. Enkripsi dan Anonimisasi
Banyak *platform* kepatuhan menawarkan alat enkripsi dan anonimisasi bawaan, memastikan bahwa data pribadi atau data pribadi sensitif dilindungi saat disimpan atau ditransfer. Ini sangat berguna untuk memenuhi standar seperti persyaratan UU PDP untuk melindungi data pribadi.

c. Deteksi Insiden dan Respon
Software ini mencakup alat untuk memantau pelanggaran data atau aktivitas mencurigakan, memungkinkan respons cepat tehadap insiden keamanan potensial. *Software* ini juga memberikan panduan prosedur respons dan pemberitahuan untuk memenuhi kewajiban hukum dalam hal pelaporan pelanggaran.

4. Memfasilitasi Manajemen Hak Subjek Data

    a. Permintaan Akses Subjek Data atau *Data Subject Access Requests (DSARs) Software* kepatuhan memungkinkan individu untuk menggunakan hak mereka (seperti mengakses, memperbaiki, atau menghapus data pribadi) dengan memfasilitasi permintaan akses subjek data pribadi. *Software* ini dapat mengelola permintaan ini dengan cara yang sesuai, menyediakan alur kerja otomatis untuk mengambil, memverifikasi, dan memproses informasi yang berkaitan dengan permintaan tersebut.

    b. Manajemen Persetujuan
    Software dapat melacak dan mengelola persetujuan pengguna untuk pengumpulan dan pemrosesan data, yang sangat penting untuk mematuhi UU yang mengharuskan persetujuan pengguna (misalnya UU PDP, GDPR, CCPA). Fitur ini memungkinkan organisasi dengan mudah mengambil dan mendokumentasikan preferensi persetujuan, membuat kepatuhan lebih mudah jika ada permintaan pengguna untuk mencabut persetujuan.

5. Menyediakan Pelaporan dan Analisis

    a. Dasbor Kepatuhan
    Dasbor ini menyajikan tampilan terpusat dari upaya pelindungan data organisasi, memungkinkan tim kepatuhan untuk memantau *metric* utama. Mengidentifikasi area resiko, dan melacak proses penanganan data.

    b. Pelaporan Regulasi dan Laporan Kepatuhan
    Software dapat menghasilkan laporan standar yang seringkali diwajibkan oleh regulator untuk menunjukkan upaya kepatuhan yang sedang berlangsung. Laporan-laporan ini mmerinci praktek manajemen data, langkah-langkah keamanan dan status kepatuhan organisasi.

6. Mengurangi Resiko dan Memastikan Kepatuhan Berkelanjutan
    a. Penilaian Resiko dan Penilaian Skor

Software kepatuhan dapat menilai resiko yang terkait dengan aktivitas pemrosesan data dan memberikan skor resiko. Dengan mengidentifikasi area beresiko tinggi, organisasi dapat menerapkan tindakan untuk mengurangi resiko tersebut.

b. Pembaruan dan Penyesuaian Regulasi
Hukum pelindungan data terus berkembang, dan *software* kepatuhan seringkali menyertakan pembaruan untuk menyesuaikan dengan persyaratan regulasi yang baru. Hal ini penting bagi organisasi/ korporasi berskala multi nasional yang tunduk pada berbagai peraturan pelindungan data yang sering diperbarui.

7. Manfaat *Software* Kepatuhan PDP

a. Peningkatan Efisiensi
Melakukan otomatisasi dapan mengefisienkan proses kepatuhan, mengurangi waktu dan upaya yang dibutuhkan untuk mengelola kewajiban dan persyaratan pelindungan data.

b. Keamanan Data yang lebih baik
Memperkuat pelindungan data dengan menerapkan kebijakan keamanan, enkripsi, dan kontrol akses.

c. Mengurangi Denda dan Resiko Hukum
Membantu mencegah denda akibat ketidakpatuhan dengan memastikan praktek pelindungan data yang memenuhi standar hukum yang berlaku.

d. Skalabilitas
Saat organisasi berkembang, *software* kepatuhan dapat menyesuaikan diri dengan data yang lebih besar, aliran data yang lebih kompleks, dan persyaratan regulasi tambahan.

e. Meningkatkan Kepercayaan dan Reputasi
Menunjukkan kepatuhan terhadap regulasi pelindungan data akan meningkatkan kepercayaan pelanggan dan memperkuat komitmen perusahaan terhadap privasi.

Kesimpulannya, *software* kepatuhan pelindungan data adalah alat yang kuat yang tidak hanya membantu memenuhi persyaratan regulasi, tapi juga meningkatkan strategi tata kelola data organisasi secara keseluruhan. Mengingat meningkatnya perhatian tehadap privasi data di seluruh dunia, penggunaan software semacam ini akan menjadi semakin penting bagi organisasi/korporasi dari berbagai ukuran.

J. Pengawasan dan Penegakan Hukum

Guna memastikan efektivitas PDP, maka diperlukan sistem pengawasan dan penegakan hukum yang mumpuni. Untuk memahami sistem pengawasan yang ideal, ada baiknya melakukan *benchmarking* terhadap sistem pengawasan yang berbasis EU GDPR, yang kemudian dibandingkan dengan pengaturan berdasarkan UU PDP. Hasil benchmarking tersebut akan dapat digunakan untuk mengembangkan sistem pengawasan yang ideal di Indonesia**.**

1. Pengawasan
    a. Menurut EU GDPR

        Inti pengaturan tentang pengawasan berdasarkan EU GDPR, mencakup:
        - Dilaksanakan oleh *Supervisory Authority* yang bersifat independen.
        - *Supervisory Authority* memiliki kewenangan untuk melaksanakan tugas-tugas yang diberikan sesuai dengan ketentuan EU GDPR.
        - Tugas *Supervisory Authority*, antara lain: memantau dan menegakkan penerapan aturan GDPR; meningkatkan kesadaran dan pemahaman; memberikan advis; memberikan informasi kepada Subjek Data tentang hak-haknya; menangani keluhan yang disampaikan oleh Subjek Data; memantau perkembangan teknologi informasi dan komunikasi terkait dengan Pelindungan Data Pribadi; menyusun *check list* terkait dengan *Data Protection Impact Assessment (DPIA*); mendorong penyusunan *code of conduct*; mendorong sertifikasi Pelindungan Data Pribadi.
        - Dalam menjalankan tugasnya, *Supervisory Authority* memiliki kekuasaan investigatif, kekuasaan korektif maupun kekuasaan otorisasi dan advisory.

- *Advisory Authority* dapat mengeluarkan peringatan, teguran, hingga mengenakan denda kepada pelanggaran terhadap Pelindungan Data Pribadi.

b. Menurut UU PDP

Dalam Undang-Undang Pelindungan Data Pribadi mengenai kewenangan pengawasan diatur dalam ketentuan Pasal 58-61, yang intinya:

- Kewenangan Pengawasan dalam implementasi UU PDP akan dilakukan oleh Lembaga yang akan dibentuk berdasarkan Peraturan Presiden yang bertanggung jawab kepada Presiden (Pasal 58).
- Tugas utama Lembaga adalah merumuskan dan menetapkan kebijakan dan strategi Pelindungan Data Pribadi; melakukan pengawasan terhadap penyelenggaraan Pelindungan Data Pribadi; penegakan hukum administratif; memfasilitas penyelesaian sengketa di luar pengadilan (Pasal 59).
- Lembaga memiliki kewenangan yang cukup luas (Pasal 60).
- Ketentuan tentang tata cara pelaksanaan kewenangan Lembaga akan diatur dalam Peraturan Pemerintah (Pasal 61).

2. Penegakan Hukum

a. Perbuatan yang Dilarang

Ada beberapa perbuatan yang dilarang berdasarkan Undang-Undang Pelindungan Data Pribadi sebagaimana diatur pada Pasal 65 dan Pasal 66 Undang-Undang Pelindungan Data Pribadi. Perbuatan-perbuatan yang dilarang meliputi: memperoleh dan mengumpulkan Data Pribadi secara melawan hukum; mengungkapkan Data Pribadi secara melawan hukum; menggunakan Data Pribadi secara melawan hukum (Pasal 65). Perbuatan lain yang dilarang adalah membuat Data Pribadi palsu atau memalsukan (Pasal 66).

b. Ketentuan Pidana

Beberapa Ketentuan Pidana yang diatur dalam Pasal 65-67 Undang-undang Pelindungan Data Pribadi adalah:

- Pelanggaran ketentuan terkait Pasal 65 (1) yaitu memperoleh atau mengumpulkan Data Pribadi secara melawan hukum diancam pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp 5 milyar (Pasal 67 ayat 1).
- Pelanggaran terhadap ketentuan Pasal 65 ayat (2) yaitu mengungkapkan Data Pribadi secara melawan hukum diancam pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp 4 milyar (Pasal 67 ayat 2).
- Pelanggaran hukum terhadap ketentuan Pasal 65 ayat (3) yaitu menggunakan Data Pribadi secara melawan hukum, diancam pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp 5 milyar (Pasal 67 ayat 3).
- Pelanggaran terhadap ketentuan Pasal 66, yaitu membuat Data Pribadi Palsu atau memalsukan Data Pribadi secara melawan hukum diancam pidana penjara 6 tahun dan/atau denda paling banyak Rp 6 milyar.

DAFTAR SINGKATAN

–	APEC	:	Asia Pacific Economic Cooperation
–	ASEAN	:	Association of South East Asian Nations
–	BCR	:	Binding Corporate Rules
–	BPJS	:	Badan Pengelola Jaminan Sosial
–	BSI	:	Bank Syariah Indonesia
–	CIPP	:	Certified International Privacy Professionals
–	CBPR	:	Cross Border Privacy Rules
–	DMF	:	Data Management Framework
–	DPA	:	Data Protection Authority
–	DPIA	:	Data Protection Impact Assessment
–	DPO	:	Data Protection Officer
–	EDPB	:	European Data Protection Board
–	EU	:	European Union
–	EU SCC	:	European Union Standard Contractual Clauses
–	GDPR	:	General Data Protection Regulation
–	IACC	:	International Association of Privacy Professionals
–	IEC	:	International Electronical Commission

- ISMS : International Security Management System
- ISO : International Organization for Standardization
- KKNI : Kerangka Kualifikasi Nasional Indonesia
- KPU : Komisi Pemilihan Umum
- MCC's : Model Contractual Clauses
- OECD : Organization Economic Cooperation and Development
- PDP : Personal Data Protection
- PIA : Privacy Impact Assessment
- PMIS : Privacy Management Information System
- POLRI : Polisi Republik Indonesia
- PPDP : Pejabat Pelindungan Data Pribadi
- ROPA : Recording of Processing Activities
- RRT : Republik Rakyat Tiongkok
- SKKNI : Standar Kompetensi Kerja Nasional Indonesia
- SMKI : Sistem Management Keamanan Informasi
- UK : United Kingdom
- UN : United Nations
- UUD : Undang-Undang Dasar
- UU PDP : Undang-Undang Pelindungan Data Pribadi
- USA : United States of America

DAFTAR SELECTED BIBILIOGRAPHY

- Ahmad Rumadi, "Lembaga Pelindungan Data Pribadi", Kompas 22 Juli 2024;
- Amedi, Azeem Marhendra, "Navigating the Future of Data Privacy in Indonesia", Jakarta Post, 18 Mei 2024;
- APPDI, "Perspektif Industri Terkait Pembentukan Lembaga Pelindungan Data Pribadi", disampaikan pada FGD tentang Pembentukan Lembaga Pelindungan Data Pribadi, diselenggarakan oleh Kantor Staf Presiden (KSP), 7 Mei 2024;
- ASEAN Digital Senior Official Meeting (ADGSOM), "ASEAN Model Contractual Clauses for Cross Border Data Flows", Januari 2021;
- Basten, "Disrupting Notions of Protected Health Informasion", Jakarta Post, 30 Agustus 2023;
- Carey, Peter (ed), Data Protection and Practical Guide to UK & EU Law, Oxford University Press Press, 2018 (Fifth Edition);
- Dirgantara, Ida Bagus Ayodhya, A Comparative Study on the Designation and Practical Role of DPO in the Netherlands and The Republic of Indonesia, Master Thesis, Law and Digital Technology, Law Faculty, Leiden University, 2023;

- EU Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 2018 edition;
- Fadhli, Miftah, Thinking Beyond Data Protection: The Regulatory Gaps in the Use of AI in Government Surveillance (A Reflection on the Clearview AI Case), Master of Law Thesis, Leiden University, 2023;
- Frans, Rico Usthavia, "Data Nasabah Perbankan", Kompas, 21 Mei 2024;
- Fratucello, Fabio, "The Rise of Identity Attacks and How to Defend Against Them", Jakarta Post, 17 October 2023;
- Fuster, Gloria Gonzales, Rosamunde van Brakel & Paul De Hart, Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Edward Elgar, 2022;
- Hallinan Dara, Ronald Henes, & Paul De Hert (eds), Data Protection and Privacy: Enforcing Rights in a Changing World, Hart Publishing, 2022;
- Harvard Business Review, Customer Data and Privacy, HBR Press, 2020;
- Juniarto, Cornel, "Ujian Jelang Implementasi Undang-Undang Pelindungan Data Pribadi", Kompas 27 Juni 2024;
- Juniarto, Cornel, "Why a Personal Data Protection Agency Matters?", Jakarta Post, 8 Juli, 2024;
- Kansil, Amanda Herodita, Comparative Analysis on the DPIA Provisions Under the EU GDPR and The Indonesian PDP Law, Master of Law Thesis, Leiden University, 2023;
- Kasir, Romeo F, Handbook Certified Data Protection Officer: Practical Workplan Guidance, Dataprotectionbook.com, 2021;
- Kiergaard (ed), Cyber Law Security & Privacy, Proceedings of the Second Legal Security and Privacy in IT (LSPI) Conference , Beijing, 5–7 December 2007;
- KOMINFO, "Grand Design Pembentukan Ekosistem DPO (Data Protection Officer)", 2021;
- Kompas, "DPR Minta ada Lembaga Pengawas Pelindungan Data Pribadi", 13 Agustus 2024;

- Kompas, "Penindakan Pelanggaran Data Pribadi Perlu Dipantau", 21 Agustus 2024;
- Kompas, "Pengecualian Pada UU PDP Dipersoalkan", 9 November 2022;
- Kuner, Christopher, Lea Bygrave, Christopher Doksey, The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020;
- Lambert, Paul, The Data Protection Officer: Profession, Rules and Role, CRC Press, Tailor and Francis Group, 2017;
- Manthovani, Reda, Penyadapan vs Privasi, Bhuana Ilmu Populer Press, 2015;
- Munir, Abu Bakar & Siti Hajar Mohd Yasin, Privacy and Data Protection, Sweet and Maxwell Asia, 2002;
- Munir, Abu Bakar & Siti Hajar Mohd Yasin, MD Ershadul Karim, Data Protection Law in Asia, Sweet and Maxwell, 2014;
- Munir, Abu Bakar & Siti Hajar Mohd Yasin, Personal Data Protection in Malaysia, Sweet and Maxwell Asia, 2010;
- Perdana, Arif & Baru Arifin, "Finding a Fix for Indonesia's Data Protection Problems", 13 Desember 2023;
- Pfefferkorn, Riana & Callum Voge, "Curbing Government Internet Surveillance", Jakarta Post, 25 October 2023;
- Pollit, Piersleigh & James Mullock, The Point of Law Data Protection Act Explained, Third Edition, Stationary Office, The Official Publisher of the Acts, 2001;
- Putri, Astrella Maryadi, A Comparative Study on Cross–Border Data Transfer in the EU and Indonesia: Analysis of Adequacy Decision, Standard, Contractual Clauses, and Binding Corporate Rules, Thesis Master pada Universitas Leiden, 2023;
- Rahmawati, Meity, Formulasi Sanksi Pidana yang Ideal dalam Regulasi PDP, Disertasi, Fakultas Hukum UPH Jakarta, 2024;
- Regina Damaris, "Baby Steps: Indonesia's Progress in Online Child Protection Regulation", Jakarta Post, 30 Juli 2024;

- Samson, "Data Breach: Are You Prepared or Paying?", Jakarta Post, 17 Pebruari 2023;
- Sharma, "Protecting People's Health Data is an Urgent Priority", Jakarta Post 28 Desember 2023;
- Singleton, Susan, Data Protection, Jordan Publishing Limited, 1998;
- Sudin, Putri Prameswari, Children's PDP in Online Trageted Advertising: A Comparison between GDPR and Indonesia PDP Law, Master of Law Thesis, Leiden University, 2023;
- Supancana, I B R, "Beberapa Tanggapan terhadap RUU PDP (versi 4 Juni 2015)", disampaikan pada Rapat Pembahasan tanggal 23 Juni 2015, Ruang Rapat Maladi, Kementerian Kominfo;
- Supancana, I B R, "The Concepts and Efforts to Formulate PDP Law in Indonesia", Lecture at Kobe University Summer Course, Kobe, 25 August 2015;
- Supancana, I B R, "Pengakomodasian Standar Internasional dalam Legislasi Nasional di Bidang PDP", disampaikan pada Seminar Dimensi Internasional pada Konsepsi PDP di Indonesia, Bandung, 29 September 2015;
- Supancana, I B R, "Menuju UU PDP yang Berstandar Internasional dan Efektif", disampaikan dalam Seminar Refleksi Hukum PDP dalam Menyongsong Masyarakat Ekonomi ASEAN, Jakarta, 8 Desember 2015; organized by Untag Surabaya, 31 March 2016;
- Supancana, I B R, "Legal Protection of Information Privacy Under Indonesian Draft Law on PDP", Presented at the International Seminar on PDP
- Supancana, I B R, " How the Management of Digital Identity in the Big Data Era Protect Sensitive Personal Data?" Presented at the International Conference on the Digital Economy Security and Privacy in the Big Data Era, organized by Padjadjaran Alumni Club, Jakarta 26–27 April 2017;
- Supancana, I B R, "The Concepts and Efforts to Formulate PDP Law in Indonesia", An Introduction to Data Protection Law Workshop, Organized by Schinder Law Firm, Jakarta, 28 April 2017;

- Supancana, I B R, "PDP: Conceptual Framework, Ecosystems and Instruments", Presented at PDP Training Organized by Law faculty, Catholic University of Atma Jaya, Jakarta, 28 March 2019;
- Supancana, I B R, Cyber Ethics dan Cyber Law: Kontribusinya bagi Dunia Bisnis, Seri Atma Jaya Studies on Aviation, Outer Space and Cyber Laws, Penerbit Bintang Kejora, 2020;
- Supancana, I B R, "Menuju UU PDP yang Modern, Mengakomodasikan Kepentingan Nasional dan Berstandar Internasional", disampaikan pada Brownbag Discussion Proyeksi Kebijakan PDP, diselenggarakan oleh FH Unika Atma Jaya, 7 Juli 2020;
- Supancana, I B R, "PDP: Conceptual Framework, International Standards and Legislation Process in Indonesia", presented at Training Organized by PPHBI, March 19th 2021;
- Supancana, I B R, "Perlunya Terobosan dalam Penuntasan RUU PDP", disampaikan pada Webinar diselenggarakan oleh APPDI bekerjasama dengan Schinder Law Firm dan Investree, 5 Agustus 2021;
- Supancana, I B R, "Standar Internasional PDP dan Upaya Pengaturannya di Indonesia", disampaikan pada Webinar diselenggarakan Mahasiswa Program Doktor Ilmu Hukum Angkatan 40 FH Untag Surabaya, 19 September 2021;
- Supancana, I B R, "Pemrosesan Data Pribadi: Kewajiban dan Tanggung Jawab Pengendali/Pemroses Data", disampaikan pada Webinar diselenggarakan oleh Young Lawyer Community, PERADI Denpasar, 7 Januari 2022;
- Supancana, I B R, "DPO sebagai Profesi Baru pada Era Digital: Arah Pengaturannya di Indonesia", disampaikan pada Webinar diselenggarakan APPDI bekerjasama dengan FH UPH, Jakarta 18 Maret 2022;
- Supancana, I B R, "Kewajiban dan Tanggung Jawab Pengendali Data dan Pemroses Data dalam Melindungi Hak–Hak Subjek Data Pribadi", disampaikan pada Diskusi bersama PT Asuransi Allianz Life Indonesia, 12 April 2022;

- Supancana, I B R, "Prinsip–prinsip Pelindungan Data Pribadi dan Pelindungan Hak–Hak Subjek Data Pribadi", disampaikan pada Workshop diselenggarakan oleh LPPM Unika Atma Jaya, 29 Agustus 2022;
- Supancana, I B R, "The Challenges of Implementing PDP Law in Relations with Existing Laws and Regulations", presented at Seminar Organized by APPDI, Jakarta 3 Oktober 2022;
- Supancana, I B R, "Undang–Undang No 27 tahun 2022 tentang Pelindungan Data Pribadi: Formulasi dan Tantangan Implementasinya", 25 November 2022;
- Supancana, I B R, "Hal–Hal Praktis yang Perlu Diperhatikan Oleh Organisasi/Korporasi terkait PDP", disampaikan pada Seminar yang diselenggarakan PT Kalbe Farma, 20 Juli 2023;
- Supancana, I B R, "AI–Based Automated Processing and the Protection of Data Subject's Rights", presented on Webinar on AI & Data Protection Law, Organized by Law Faculty UPH Surabaya, 1 December 2023;
- Supancana, I B R, "Legal and Ethical Issues on the Utilization of AI and Its Implications Toward PDP", presented at National Seminar on Filling the Legal Vacuum Concerning Unlawful Actions by AI, organized by Law Faculty Atma Jaya University, 26 Mei 2024;
- Supancana, I B R, "Perspektif Industri Terkait Pembentukan Lembaga Pelindungan Data Pribadi", disampaikan pada FGD tentang Pembentukan Lembaga Pelindungan Data Pribadi, diselenggarakan oleh KSP, Jakarta, 7 Mei 2024;
- Supancana, I B R, "Pelindungan Konsumen dan PDP pada E–Commerce", disampaikan pada Seminar yang Diselenggarakan Kalbe Farma Group, Jakarta 6 Juni 2024;
- Tundang, Ronald Eberhard, Genomic Data, Privacy and Equity in Health Law", Jakarta Post, 29 Agustus 2023;
- Ustaran, Eduardo (ed), European Data Protection Law and Practice, IAPP, 2018;

– Voigt, Paul & Axel von den Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Spring International Publishing AG, 2017

BIOGRAFI PENULIS

Prof. Dr. Ida Bagus Rahmadi Supancana adalah Guru Besar dan Koordinator *Atma Jaya Studies on Aviation, Outer Space and Cyber Laws*. Mendalami *Cyber Laws* dan *Personal Data Protection* sejak tahun 1990-an. Bersama-sama dengan Prof Abu Bakar Munir, Prof. Siti Hajar, dan Dr Sonny Zulhuda pada tahun 2005-2007 membuat kajian tentang Pelindungan Data Pribadi atas permintaan Kementerian Aparatur Negara dan Reformasi Birokrasi dalam rangka penerapan *Single Identity Number* guna menunjang *Good Governance and Clean Government*. Kajian tersebut menjadi cikal bakal penyusunan Rancangan Undang-Undang tentang Pelindungan Data Pribadi.

Sebagai *Co-Founder* dari Asosiasi Profesional Privasi Data Indonesia (APPDI) bertandem dengan Prof Abu Bakar Munir aktif memberikan pelatihan calon *Certified Data Protection Officer (CDPO)* dengan Modul yang mengadopsi Standar Internasional, Standar Industri dan berdasarkan *Best Practices* dari berbagai Negara serta sesuai dengan Undang-Undang no 27 tahun 2022 tentang Pelindungan Data Pribadi. Pelatihan yang telah dilaksanakan sejak tahun 2020

hingga penerbitan Buku ini telah berlangsung 19 *batches* pelatihan dengan peserta sekitar 1000 peserta dari berbagai latar belakang, seperti: *Lawyers, Bankers, Insurance Companies, Fintech Companies, Consultants, Trading Companies, Industries*, *Telecommunication Companies*, BUMN, Institusi Pemerintahan, Organisasi Internasional, Akademisi, dan Praktisi Pelindungan Data Pribadi.

Pada tahun 2020 menerbitkan Buku berjudul "*Cyber Laws and Cyber Ethics*: Kontribusinya bagi Dunia Bisnis" yang bersumber dari materi perkuliahan pada Program Magister Manajemen Universitas Airlangga sejak tahun 2005 hingga kini. Pendidikan Sarjana Hukum diselesaikan pada Universitas Padjadjaran (1983), Magister Hukum di Universitas Indonesia (1990), dan Doktor Ilmu Hukum dari Universitas Leiden, Belanda (1998).