BAB I

PENDAHULUAN

1.1 Latar Belakang

Setiap orang mempunyai hak konstitusional beserta kedudukannya yang dijamin oleh Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 ("**UUD NRI 1945**"), yaitu negara berperan penting dalam memberikan jaminan konstitusional kepada setiap warga negara. Hal ini terdapat dalam Pembukaan UUD NRI 1945 alinea ke-4, yang mengemukakan bahwa negara berkewajiban melindungi segenap bangsa Indonesia dengan cara meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa dan memajukan kemerdekaan berdasarkan perdamaian dunia dan keadilan sosial.

Secara historis, hakikat Hak Asasi Manusia (HAM) berkisar pada hubungan antara individu dengan komunitas politik yang disebut negara. Meskipun Hak Asasi Manusia sudah ada sejak manusia lahir, penegakan dan perjuangannya hanya tumbuh saat manusia dihadapkan pada ancaman dari kekuasaan negara. Penegakan Hak Asasi Manusia memicu perselisihan antara dua hak dasar, yakni Hak Asasi Manusia dan kekuasaan yang melekat pada negara.[1]

Sejak masa kemerdekaan Republik Indonesia, telah mengakui pentingnya Hak Asasi Manusia (HAM) dalam kerangka kehidupan berbangsa dan bernegara. Dalam konteks ini, salah satu langkah strategis yang diambil adalah memasukkan

[1] Koentjoro Poerbopranoto, *Hak-hak Asasi Manusia dan Pancasila,* (Jakarta: Pradnya Paramita, 1960), hal. 16 – 17.

ketentuan HAM ke dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945). Langkah ini tidak hanya mencerminkan komitmen bangsa Indonesia terhadap perlindungan dan penghormatan HAM, tetapi juga menjadi landasan bagi seluruh hukum dan kebijakan yang berlaku di negara ini.

Pembukaan UUD NRI 1945 tidak secara khusus menyebutkan HAM dengan mengatakan bahwa *"sesungguhnya kemerdekaan adalah hak segala bangsa..."*. Oleh karena itu, penjabaran konsep perlindungan hukum Hak Asasi Manusia diatur dalam batang tubuh UUD NRI 1945 (setelah amandemen), yaitu dalam Pasal 28A-J, Pasal 29, Pasal 30, Pasal 31, dan Pasal 34. Hak asasi manusia adalah hak yang diakui hakikat dan hakikatnya sebagai Hak Asasi Manusia yang melekat. Salah satu hak yang paling mendasar yaitu hak atas kebebasan. Tanpa hak atas kebebasan, tidak mungkin manusia mengembangkan potensi dirinya secara penuh sebagai manusia.[2]

Hak konstitusional yang termaktub dalam UUD NRI 1945 meliputi hak warga negara. Salah satunya yaitu hak atas perlindungan diri pribadi sebagaimana termaktub dalam Pasal 28F UUD NRI 1945, yang menyatakan:

> "*Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia"*.

Pasal 28G ayat (1), yang memuat ketentuan bahwa :

> *"Setiap orang berhak atas perlindungan pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya serta*

[2] Akub, M. S., & Ilyas, A. *Wawasan Due Process Of Law Dalam Sistem Peradilan Pidana*, (Yogyakarta: Rangkang Education, 2013), hal. 79.

berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Seiring dengan kemajuan teknologi khususnya penggunaan internet di era modern saat ini berkaitan dalam kehidupan sehari-hari. Sebagian besar masyarakat mengimplementasikan internet sebagai sarana dalam melakukan berbagai aktivitas dengan harapan dapat melakukan semua aktivitas tersebut secara efektif, akurat dan efisien. Perkembangan teknologi, informasi dan komunikasi memungkinkan terjadinya penyebaran informasi dan data secara cepat. Internet, yang awalnya hanya untuk menyebarkan informasi (satu arah), lalu menjadi pola yang lebih interaktif dan kemudian menjadi wahana transaksi.[3]

Di era digital ini, tidak hanya dipermudah dalam hal berkomunikasi, kita juga lebih mudah untuk memperoleh akses informasi. Lebih tepatnya, internet menjadi sumber informasi, alat komunikasi, dan media hiburan. Dengan memanfaatkan mesin pencari (*search engine*) seperti Google, netizen di seluruh dunia mempunyai akses internet yang mudah atas pusparagam informasi.[4]

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

---

[3] Edmon Makarim, *Kerangka Kebijakan Dan Reformasi Hukum Untuk Kelancaran Perdagangan Secara Elektronik (E-commerce) Di Indonesia*, Jurnal Hukum & Pembangunan, Februari 2016, https://doi.org/10.21143/jhp.vol44. No. 3.25, diakses tanggal 15 Maret 2022.

[4] Yasonna H. Laoly, *Birokrasi Digital,* (Jakarta: PT Pustaka Alvabet, September 2019), hal. 26.

untuk melindungi data pribadi. Hak privasi adalah hal-hal sensitif yang berkaitan dengan data pribadi atau identitas individu. Identitas tersebut antara lain Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Paspor, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), Nomor Rekening, Sidik jari, Ciri khas seseorang dan sebagainya.

Disamping itu, pentingnya aliran data lintas batas (*cross-border data flow*) menjadi salah satu alasan penting dalam pembentukan regulasi pelindungan data pribadi di Indonesia. Peningkatan Aliran Data Lintas Batas telah menyebabkan peningkatan signifikan dalam aliran data lintas batas negara, khususnya menyangkut aktivitas ekonomi digital. Dengan semakin maraknya data pribadi yang mengalir melewati batas negara, maka diperlukan kerangka hukum yang jelas untuk melindungi data tersebut yang diharapkan mampu memberikan jaminan keamanan dalam aktivitas ekonomi digital yang melibatkan pelaku usaha dari dalam maupun luar negeri, termasuk swasta, pemerintah, dan konsumen.

Dengan adanya Kerangka hukum yang jelas mengenai aliran data lintas batas dapat mendukung inovasi dan pengembangan ekosistem ekonomi digital juga dapat memberikan kemudahan terhadap transfer data, terutama dalam mendukung transformasi digital yang diinginkan pemerintah sebagai elemen kunci dalam memastikan adanya kepercayaan dan hubungan timbal balik antarnegara terkait pelindungan data pribadi. Indonesia dapat meningkatkan standar pengaturan pelindungan data pribadi ke taraf internasional, hal ini penting untuk memperkuat posisi Indonesia dalam tata kelola data global dan meningkatkan kepercayaan

internasional terhadap pengelolaan data di Indonesia serta mengantisipasi Potensi Pelanggaran dan Risiko Keamanan.

Adanya kebutuhan akan pentingnya regulasi Pelindungan Data Pribadi di Indonesia juga dapat sebagai antisipasi akan potensi pelanggaran seperti kebocoran dan penyalahgunaan data pribadi, serta kemungkinan adanya pengawasan asing. Pentingnnya pembentukan regulasi pelindungan data pribadi demi keamanan nasional dan harus menjadi pertimbangan dalam menyusun aturan terkait aliran data lintas batas. Dengan demikian, pentingnya *cross-border data flow* menjadi salah satu pertimbangan utama dalam pembentukan Undang-Undang Pelindungan Data Pribadi di Indonesia. Regulasi ini diharapkan dapat memberikan perlindungan yang memadai terhadap data pribadi warga negara, sekaligus mendukung perkembangan ekonomi digital dan hubungan internasional Indonesia di era globalisasi data.

Disamping itu, manfaat teknologi dan data informasi dalam era digital saat ini akan sangat terasa dalam bidang pendidikan, ekonomi, kesehatan dan lain-lain. Di zaman sekarang ini, saat dunia menghadapi pandemi Covid-19, rakyat dan bangsa Indonesia dalam berjuang melewati pandemi Covid-19 dan pemulihan ekonomi nasional menjadikan relevannya teknologi informasi. Dalam pidato Sidang MPR-RI tanggal 14 Agustus 2020, Presiden Joko Widodo menegaskan bahwa, "*Semua platform teknologi harus mendukung transformasi kemajuan bangsa. Peran media-digital yang saat ini sangat besar, harus diarahkan untuk membangun nilai-nilai kemanusiaan dan kebangsaan."* Hal ini tentu sejalan dengan Landasan filosofis pelindungan data pribadi itu sendiri yaitu Pancasila

khususnya Sila Kedua, "*Kemanusiaan yang adil dan beradab"* hal ini mengingat bahwa perlindungan yang dimaksud akan menciptakan keadilan dan membentuk peradaban manusia yang menghormati dan menghargai data pribadi.

Dunia internasional telah melihat urgensi pengaturan pelindungan data pribadi, baik secara nasional maupun regional. Saat ini, setidaknya terdapat 157 negara telah memiliki regulasi yang secara khusus mengatur tentang pelindungan data pribadi warga negaranya.[6] Di ASEAN sendiri, beberapa negara juga telah memiliki aturan khusus yang terkait dengann pelindungan data pribadi. Misalnya, Malaysia pada tahun 2010, Singapura pada tahun 2012, Filipina pada tahun 2012 dan Thailand pada tahun 2019. Pelindungan data pribadi di berbagai negara menekankan pada adanya pengaturan mengenai jangkauan keberlakuan yang ekstrateritorial, pembagian jenis data pribadi, prinsip-prinsip pelindungan data pribadi, hak Subjek Data pribadi, syarat sah pemrosesan data pribadi, otoritas lembaga pengawasan dan sanksi pelanggaran penggunaan data pribadi.[7]

Pengaturan perlindungan hukum atas penyalahgunaan data pribadi sebagai wujud dalam penanggulangan pelanggaran data pribadi dan upaya dalam menjamin kepastian hukum bagi masyarakat luas.[8] Salah satu penyebab adanya penyalahgunaan data pribadi dikarenakan kurangnya kesadaran masyarakat akan pentingnya menjaga dan memahami regulasi pelindungan data pribadi dalam

---

[6] Aly Apacible-Bernardo, Like Fischer, https://iapp.org/news/a/Identifying-global-privacy-laws-relevant-DPAs|IAPP, *Identifying global privacy laws, relevant DPAs*, diakses tanggal 17 September 2024

[7] Penjelasan Pemerintah Mengenai Rancangan Undang-Undang Tentang Pelindungan Data Pribadi, (Jakarta: tanggal 25 Februari 2020).

[8] https://fhukum.unpatti.ac.id/jurnal/sasi/article/view/394/285, *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber*, diakses tanggal 15 Maret 2024.

melakukan aktivitas sehari-hari. Sebagai contoh, saat mengunduh suatu *platform* aplikasi, biasanya terdapat adanya permintaan untuk mengisi data pribadi dengan meminta persetujuan kepada subjek data untuk dapat mengakses kontak, foto, dan lokasi tempat subjek data pribadi, dan tidak ada pilihan selain untuk menyetujui permintaan tersebut jika ingin mengakses *platform* aplikasi tersebut, yang tanpa disadari *platform* aplikasi tersebut bisa saja dapat menyalahgunakan dan mungkin mengakibatkan kerugian bagi subjek data tersebut. Contoh lainnya adalah sejumlah kasus aplikasi ojek *online* dimana terdapat penyalahgunaan data yang berujung pada kerugian bagi konsumen ojek *online*, ditambah lagi saat ini maraknya berbagai kasus Pinjaman *online* (Pinjol) dan Judi *online* (Judol).

Beberapa kasus penjualan data pribadi yang dijual-belikan melalui *dark website. Dark web atau dark website* adalah sarana atau bagian dari internet yang memungkinkan orang menyembunyikan identitas dan lokasi subjek data dari orang lain serta dari penegak hukum. Akibatnya, *dark web* dapat digunakan untuk menjual info pribadi yang didapatkan secara ilegal. Selain itu, dalam konteks ini, juga dikenal beberapa istilah kejahatan *cyber* sebagai bentuk penyalahgunaan data pribadi, antara lain :[9]

1. ***Hacking***

   Hacking adalah kegiatan menerobos program komputer milik orang lain, termasuk pada suatu website. Pelaku hacking ini biasa dikenal dengan

[9] Retia Kartika Dewi, Serafica Gischa *7 Jenis Kejahatan Dunia Maya atau Cyber Crime*, https://www.kompas.com/skola/read/2023/07/13/220000469/7-jenis-kejahatan-dunia-maya-atau-cyber-crime?page=all, diakses pada tanggal 15 Oktober 2024.

sebutan *Hacker,* yaitu orang yang memiliki keahlian pemrograman, dan senang mengamati sistem keamanannya.

2. ***Cracking***

   Cracking adalah aktivitas berupa percobaan penyusupan sistem komputer dengan meretas sistem keamanan komputer, jaringan, atau *software*-nya. Pelaku *cracking* alias *Cracker* mencuri dan memanipulasi data tersebut untuk tujuan ilegal atau kriminalitas.

3. ***Skimming***

   Skimming adalah sebuah tindak kejahatan di mana pelaku memasang sebuah alat di ATM atau EDC (*electronic data capture*). Alat ini terlihat seperti bagian dari mesin tersebut, padahal bukan.

4. ***Scamming***

   Scamming merupakan suatu tindakan kriminal yang berupa penipuan dengan menargetkan sejumlah uang atau barang-barang berharga dari korban dengan sejumlah cara, baik di dunia maya maupun nyata.

5. ***Doxing***

   Doxing atau *Doxxing* berasal dari kata "dox", singkatan dari dokumen, adalah sebuah tindakan berbasis internet untuk meneliti dan menyebarluaskan informasi pribadi secara publik (termasuk data pribadi) terhadap seseorang individu atau organisasi.

6. ***Carding***

   Carding adalah suatu bentuk penyalahgunaan di dunia maya (*cyber crime*) dengan cara berbelanja menggunakan nomor dan identitas kartu kredit orang

lain, yang diperoleh secara ilegal (melawan hak), biasanya dengan mencuri data-data dari internet. Kejahatan ini menargetkan data atau informasi sensitif dari kartu kredit target, terutama nomor kartu dan PIN.

7. ***Phishing***

   Kejahatan ini dilakukan dengan mencuri informasi atau data sensitif seseorang melalui pesan atau tautan (link) palsu yang terlihat kredibel. Pelaku menghubungi target seperti biasa dan mengaku berasal dari pihak atau instansi tertentu, kemudian mencuri data sensitif dari target tersebut.

8. ***Spoofing***

   Spoofing sebenarnya mirip seperti *phishing*, yakni pelaku mengaku sebagai pihak berwenang dan mencuri data pelanggan untuk tujuan ilegal. Perbedaannya, *spoofing* bisa mengirimkan virus atau *malware* berbahaya ke perangkat atau *website* target. Apabila *website* tersebut diakses oleh pengguna, besar kemungkinan virusnya bisa menyebar ke perangkat mereka.

9. ***Defacing***

   Defacing adalah kegiatan mengubah halaman suatu website, dengan tampilan yang tidak semestinya. Biasanya yang dilakukan hanyalah mengubah halaman index dari situs tersebut atau halaman yang memiliki celah keamanan.

10. **SIM Swap**

    SIM Swap adalah jenis kejahatan siber di mana penjahat mencuri nomor telepon milik korban dengan mengganti kartu SIM korban yang sah dengan kartu SIM milik penjahat. Setelah berhasil memasang kartu SIM tersebut,

penjahat dapat mengakses akun *online* yang menggunakan verifikasi dua faktor (2FA) melalui nomor telepon korban.

11. ***Spamming***

    Spamming adalah tindakan yang tidak terpuji, yaitu pengiriman e-mail yang isinya tidak dikehendaki oleh si penerima, bisa juga melalui kotak komentar atau buku tamu sebuah situs. Spam sering disebut jug sebagai *bulk emai*l atau *junk e-mail* alias "sampah", pengirim email spam disebut sebagai spammer. Biasanya berisi sebuah penawaran produk, jasa, atau undian berhadiah.

12. **Serangan *Malware***

    Malware adalah program, *software*, atau *file* yang bisa membahayakan keamanan komputer. Rata-rata kejahatan siber di atas memanfaatkan serangan *malware* untuk mencuri data korban serta melumpuhkan sistem komputernya.

13. ***Ransomware***

    Ransomware merupakan salah satu jenis serangan dengan menggunakan *malware*. Peretas akan mengunci serta mengenkripsi data-data penting korban. Pelaku biasanya akan meminta korban membayar tebusan uang agar data-data tersebut dapat terbuka dengan memberikan kunci dekripsi guna memulihkan akses data korban.

14. ***Cyberstalking***

    Cyberstalking adalah salah satu kejahatan dunia maya yang dilakukan melalui media sosial, email, pesan teks, atau *platform* komunikasi *online* lainnya

dengan tujuan mengintimidasi, menakut-nakuti, atau mempersekusi seseorang secara online.

15. ***Cyber Espionage***

    Jenis kejahatan siber ini berada di level tertinggi karena pelaku memanfaatkan sistem komputer untuk memata-matai target dari si Pelaku. Organisasi *hacker* biasanya melakukan *cyber espionage* karena alasan politis dan menargetkan orang penting yang memiliki data rahasia dalam sistem komputernya.

16. ***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.[10]

Dari beberapa penjelasan mengenai jenis kejahatan *cyber* tersebut di atas, tentunya merupakan bagian dari ancaman serius dalam bentuk kejahatan *cyber* yang tidak hanya membahayakan pada data pribadi individu, tetapi juga menciptakan bahaya bagi dampak sosial dan ekonomi yang luas, sehingga memerlukan perhatian serius dari berbagai pihak, termasuk legislator dan penegak hukum.

[10] Ida Bagus Rahmadi Supancana, Ida Bagus Ayodhya Dirgantara, *Mengawal Pelindungan Data Pribadi (Global, Regional dan Nasional*), (Bekasi: Bintang Kejora, 2024), hal.18.

Kekhawatiran tentang penyalahgunaan data pribadi juga tercermin ketika data pribadi disalahgunakan oleh perusahaan atau pihak tertentu semata-mata untuk keuntungan pribadi, sejauh menyangkut Subjek Data. Pertumbuhan pengguna internet tidak jauh dari realisasi masyarakat tentang teknologi, yang mana di era modern ini mendesak kemudahan sebagai faktor penyokong aktivitas lainnya, termasuk adanya bentuk-bentuk kriminalitas baru. Penyalahgunaan data pribadi termasuk perbuatan yang terdapat unsur-unsur tindak pidana, misalnya unsur pencurian dan unsur penipuan serta tindak pidana lainnya, baik ditinjau dari unsur objektif maupun subjektif.

Kasus kebocoran data pribadi di Indonesia telah menjadi sorotan publik dalam beberapa tahun terakhir. Menurut laporan lembaga keamanan siber, terdapat peningkatan signifikan dalam jumlah kebocoran data yang terjadi. Data yang bocor sering kali mencakup informasi sensitif seperti nama, alamat, nomor telepon, hingga nomor identitas. Kasus-kasus ini bukan hanya merugikan individu yang datanya bocor, tetapi juga dapat menimbulkan dampak negatif bagi reputasi dan kepercayaan terhadap institusi yang mengelola data tersebut.

Salah satu kasus yang begitu menyita perhatian publik adalah kebocoran data pengguna *platform e-commerce* yang mengakibatkan informasi pribadi jutaan pengguna tersebar di internet. Selain kerugian finansial bagi individu, kasus tersebut juga menimbulkan dampak sosial yang lebih luas, seperti peningkatan risiko penipuan dan kejahatan siber. Penipuan identitas adalah salah satu konsekuensi paling serius dari kebocoran data, di mana pelaku kejahatan

memanfaatkan informasi yang bocor untuk melakukan penipuan atau aktivitas ilegal lainnya.

Maraknya kasus kejahatan PDP dan implikasinya, sehingga sangat penting dibutuhkan adanya suatu formulasi sanksi pidana yang tegas dan komprehensif. Diharapkan dengan adanya sanksi pidana yang tegas dan komprehensif dapat memberikan efek jera bagi pelaku kejahatan PDP dan dapat meminimalisir kejahatan PDP dikemudian hari, selain itu dengan adanya pengaturan Sanksi pidana dalam UU PDP membuktikan dan menegaskan komitmen bangsa Indonesia dalam melindungi hak privasi warga negara di era digital.

Dengan adanya ancaman sanksi pidana bagi pelaku kejahatan PDP mendorong perusahaan dan individu untuk lebih serius dalam menjaga keamanan data pribadi sehingga menempatkan Indonesia sejajar dengan negara-negara lain yang telah memiliki regulasi PDP berstandar Internasional. Sanksi pidana dalam UU PDP menjadi instrumen penting dalam menjaga kedaulatan negara di ranah digital. Dengan demikian, formulasi sanksi pidana yang tegas dalam UU PDP menjadi langkah krusial untuk mengatasi maraknya kejahatan terhadap data pribadi dan melindungi hak-hak digital warga negara Indonesia.

Pelindungan Data Pribadi mulai dikenal pengaturannya dalam masyarakat Internasional melalui Mejelis Umum Perserikatan Bangsa-Bangsa (PBB) melalui Resolusi 68/167 tentang *The Right to Privacy in The Digital Age*, mengingatkan banyaknya praktik pengawasan (*surveillance*) dan intersepsi komunikasi yang dilakukan secara sewenang-wenang dan melawan hukum (*Unlawfull*), termasuk pengumpulan data pribadi secara sewenang-wenang yang merupakan suatu bentuk

pelanggaran terhadap Hak Privasi. Di Eropa sendiri negara yang pertama kali mengesahkan Undang-Undang Pelindungan data Pribadi adalah Jerman pada tahun 1970 yang kemudiaan diikuti oleh beberapa negara-negara Eropa lainnya.[11]

Pentingnya untuk melindungi data pribadi menggerakkan negara-negara di dunia untuk mengadakan pengaturan yang memberikan perlindungan terhadap data pribadi tersebut, antara lain dengan disahkannya :

1. *The Organization for Economic Co-Operation and Development Gudelines on The Protection of Privacy and Transborder Data Flows of Personal Data Files* oleh Majelis Umum PBB pada tahun 1980.
2. *The Council of Europe Convention for The Protection of Individuals With Regrad to Automatic Processing of Personal Data* pada tahun 1981.
3. EU *General Data Protection Regulation* (EU GDPR) 2018
4. *European Charter of Human Rights* (ECHR) pada tahun 2000 disaat dunia memasuki Abad Millenial ke-20.
5. *The European Union DP Directive* (Directive) diperkenalkan tahun 1995
6. Asia *Pacific Economic Cooperation Privacy Framework* pada tahun 2004.
7. ASEAN *Framework on Personal Data Protection* 2016.
8. ASEAN *Framework on Digital Data Governance* 2018,
9. ASEAN *Human Rights Declaration* (AHRD) pada tahun 2012 sebagai suatu bagian dari *Universal Declaration of Human Rights* yang sudah ada pada tahun 1948.

[11] Wahyudi Djafar and M. Jodi Santoso, *Perlindungan Data Pribadi*; *Konsep, Instrumen, Dan Prinsipnya* (Jakarta: Studi dan Advokasi Masyarakat (ELSAM), 2019)., hal.1.

10. Hak Privasi melalui pelindungan data pribadi juga telah diatur dalam Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945)
11. *American Convention on Human Rights* (ACHR) 1979 Konvensi Amerika tentang Perlindungan Hak Asasi Manusia
12. *Kairo Declaration of Islamic Human Rights*, 1990 Deklarasi Kairo tentang Hak Asasi Manusia Islam

Urgensi mengenai perlunya Undang-Undang Pelindungan Data Pribadi dapat dilihat sebagai bagian dari Hak Asasi Manusia yang diatur oleh Pasal 12 Deklarasi Universal Hak Asasi Manusia (UDHR), yang menjamin dasar hukum bagi negara-negara anggota terkait dengan kewajiban negara untuk melindungi dan menghormati hak asasi setiap warga negara.

Dalam Kovenan Internasional tentang Hak Sipil dan Politik atau yang secara global dikenal dengan *International Convention on Civil and Political Rights* ("**ICCPR**"). Konvensi ini ditetapkan dengan Resolusi 2200 A pada tanggal 16 Desember 1966 dan berlaku sejak tanggal 23 Maret 1976. Instrumen hukum internasional ini menawarkan perlindungan yang lebih eksplisit terhadap hak-hak pribadi manusia. Pasal 17 (1) ICCPR menyebutkan bahwa tidak seorang pun boleh ada gangguan sewenang-wenang atau tidak sah terhadap privasi, keluarga, rumah atau korespondensinya, atau serangan yang tidak sah terhadap kehormatan dan reputasinya; setiap orang berhak atas perlindungan hukum dari gangguan atau serangan. Konvensi ini menekankan bahwa tidak seorang pun boleh diperlakukan

secara sewenang-wenang atau melawan hukum dengan campur tangan dalam urusan pribadi, keluarga, rumah tangga atau surat-menyuratnya.

Perumusan aturan tentang Pelindungan Data Pribadi dapat dipahami karena adanya kebutuhan untuk melindungi hak individu didalam masyarakat sehubungan dengan pemrosesan Data Pribadi baik yang dilakukan secara elektronik dan non elektronik menggunakan perangkat olah data. Perlindungan yang memadai atas Data Pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan Data Pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak pribadinya. Dengan demikian, pengaturan mengenai Pelindungan data Pribadi akan menciptakan keseimbangan antara hak individu dan masyarakat yang diwakili kepentingannya oleh Negara.[12]

Hukum harus melindungi semua pihak berdasarkan status hukumnya karena setiap orang mempunyai kedudukan yang sama di hadapan hukum. Aparat penegak hukum memiliki kewajiban untuk menegakkan hukum. Dengan berfungsinya negara hukum, maka hukum secara tidak langsung akan memberikan perlindungan bagi setiap hubungan koeksistensi atau keadaan dalam hubungan masyarakat untuk saling menghormati, menghargai perbedaan dan menyelesaikan konflik tanpa kekerasan yang diatur oleh Undang-Undang. Sementara itu, menurut Lili Rasjidi dan I.B. Wyasa Putra, hukum dapat digunakan untuk menciptakan perlindungan yang tidak hanya adaptif dan fleksibel, tetapi juga prediktif dan antisipatif,[13] yaitu,

---

[12] Teguh Prasetyo, *Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat, (*

[13] Lili Rasjidi & I.B Wyasa Putra*, Hukum Sebagai Suatu Sistem*, (Bandung: Remaja Rosdakarya, 1993), hal. 118.

hukum merupakan suatu sistem yang dirancang untuk memberikan perlindungan yang tidak hanya mampu beradaptasi dan fleksibel terhadap perubahan, tetapi juga dapat memprediksi dan mengantisipasi permasalahan yang mungkin terjadi di masa depan.

Di Indonesia, sebelum disahkannya Undang-Undang No. 27 tahun 2022 tentang Pelindungan Data Pribadi, sebelumnya telah ada ketentuan Peraturan Perundang-undangan yang mengatur mengenai Pelindungan Data Pribadi dengan mengandalkan berbagai norma hukum yang tersebar di sejumlah Peraturan Perundang-undangan. Namun, regulasi yang ada saat itu masih bersifat fragmentaris atau parsial dan belum memberikan jaminan perlindungan yang komprehensif bagi data pribadi. Hal ini tentu menciptakan celah hukum yang dapat dimanfaatkan untuk penyalahgunaan data pribadi, baik oleh individu maupun oleh entitas bisnis.

Adapun Undang-Undang terkait dengan Pelindungan Data Pribadi yang telah ada sebelumnya, antara lain:

1. UU No 7 tahun 1992 sebagaimana diubah dengan UU No 10 tahun 1998 tentang Perbankan.
2. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
3. Undang- Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
4. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
5. Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

6. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang sebelumnya Perubahan Pertama melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik).
7. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
8. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.
9. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK).
10. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).
11. Peraturan Pemerintah Nomor 80 tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
12. Peraturan Presiden Nomor 26 Tahun 2009 sebagaimana telah beberapa kali diubah dengan Peraturan Presiden Nomor 112 Tahun 2013 tentang Perubahan Keempat atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional (Perpres KTP).
13. Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah.
14. Peraturan Menteri Komunikasi dan Informasi (Permenkominfo) Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik.

15. Peraturan Menteri Komunikasi dan Informasi (Permenkominfo) Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi
16. Peraturan Menteri Komunikasi dan Informasi (Permenkominfo) Nomor 5 Tahun 2020 sebagaimana diubah dengan Peraturan Menteri Komunikasi dan Informasi Nomor 10 Tahun 2021 tentang Penyelenggaraan Sistem Elektronik Sektor Privat.
17. Peraturan Menteri Komunikasi dan Informasi (Permenkominfo) Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi.
18. Peraturan Bank Indonesia (PBI) No 18 tahun 2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran.
19. Peraturan Otoritas Jasa Keuangan (POJK) No 1 tahun 2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan
20. Surat Edaran (SE) OJK No 14 tahun 2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen

Pergeseran pemanfaatan data dalam lingkungan yang sedang bertransisi menggunakan teknologi dan dengan maraknya kasus-kasus kebocoran data pribadi yang terjadi di Indonesia kemudian mendorong pemerintah untuk membuat regulasi tentang Pelindungan Data Pribadi yaitu Undang-Undang No. 27 tahun 2022 tentang Pelindungan Data Pribadi (selanjutnya disebut dengan UU PDP) yang telah disahkan oleh DPR RI pada tanggal 20 September 2022 dan diundangkan pada tanggal 17 Oktober 2022, yang diharapkan mampu menjadi payung hukum untuk

mengatur dan memberikan perlindungan, pengaturan, pengawasan dan pengenaan sanksi atas penyalahgunaan data pribadi sebagaimana diatur dalam UU PDP.

Dalam UU PDP, Data Pribadi didefinisikan sebagai orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Sedangkan definisi tentang pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstusional subjek data pribadi.

UU PDP merupakan perwujudan kehadiran negara dalam melaksanakan amanat konstitusi untuk memberikan pelindungan data pribadi bagi warga negara yang bertujuan untuk memberikan perlindungan yang lebih baik terhadap data pribadi individu serta memberikan sanksi kepada Pelaku Penyalahgunaan data pribadi baik yang dilakukan oleh individu atau Pengguna (user), oraganisasi maupun perusahaan (*private sector*) yang tidak mengelola data secara bertanggung jawab, tentunya dibawah pengawasan yang berwenang menurut UU PDP. Perusahaan selaku pengendali data dan prosesor data dalam hal ini, juga perlu meningkatkan transparansi kepada pengguna mengenai bagaimana data pribadidigunakan dan dilindungi. Edukasi publik tentang pentingnya keamanan data pribadi serta langkah-langkah yang dapat diambil untuk melindungi informasi pribadi juga sangat diperlukan.

Dengan berlakunya UU PDP, Indonesia telah menunjukkan komitmen untuk memberikan perlindungan yang lebih baik terhadap data pribadi. UU ini tidak hanya memberikan definisi yang jelas mengenai data pribadi, tetapi juga

menetapkan hak-hak subjek data, kewajiban pengendali data, serta mekanisme pengawasan dan penegakan hukum. Di dalam UU PDP, terdapat pengaturan mengenai sanksi bagi pelanggaran, baik sanksi administratif maupun sanksi pidana. Sanksi administratif dapat berupa denda administratif, sementara sanksi pidana mencakup hukuman penjara bagi pelanggar yang melakukan tindakan yang merugikan subjek data.

Pengenaan sanksi baik administratif, perdata dan pidana sangat berperan penting sebagai instrumen untuk mencegah dan menanggulangi kejahatan yang berkaitan dengan data pribadi. Khusus mengenai penerapan Sanksi Pidana yang diterapkan, seharusnya tidak hanya bersifat represif, tetapi juga preventif, untuk menciptakan efek jera bagi pelaku dan penanggulangan penyalahgunaan data pribadi. Namun, bagaimana penerapan formulasi sanksi pidana yang ideal dalam UU PDP di Indonesia masih menjadi perdebatan. Saat ini, ketentuan dalam UU PDP masih dianggap belum memadai dalam memberikan perlindungan yang optimal terhadap data pribadi masyarakat khususnya dalam merumuskan dan menerapkan sanksi pidana.

Jika dibandingkan dalam konteks global, banyak negara telah mengadopsi regulasi pelindungan data pribadi yang lebih ketat, serta merumuskan sanksi pidana yang jelas dan tegas. Sebagai salah satu contoh yaitu, Uni Eropa dengan *General Data Protection Regulation* (GDPR) telah menetapkan sanksi yang signifikan bagi para pelanggar, termasuk denda yang bisa mencapai hingga miliaran bagi pelaku penyalahgunaan data pribadi. Pendekatan ini menunjukkan bahwa sanksi pidana

yang ideal harus mampu memberikan efek jera dan kesadaran dalam menciptakan kepercayaan masyarakat terhadap sistem pelindungan data pribadi.

Salah satu tantangan utama dalam merumuskan sanksi pidana yang ideal adalah adanya ketidakjelasan definisi mengenai apa yang dimaksud dengan pelanggaran data pribadi, sehingga definisi yang tidak jelas dapat menyebabkan kesulitan dalam penegakan hukum dan pengenaan sanksi. Selain itu, terdapat perbedaan pandangan mengenai jenis-jenis pelanggaran yang harus dikenakan sanksi pidana. Sebagian pihak berargumen bahwa pelanggaran ringan seharusnya cukup dikenakan sanksi administratif, sementara pelanggaran berat harus dikenakan sanksi pidana yang lebih tegas. Hal ini menimbulkan dilema dalam menentukan sanksi yang tepat antara pencegahan dan penegakan hukum.

Di sisi lain, efektivitas sanksi pidana juga dipengaruhi oleh faktor-faktor eksternal, seperti tingkat kesadaran masyarakat akan pentingnya pelindungan data pribadi serta kemampuan penegak hukum dalam menegakkan regulasi yang ada. Kesadaran masyarakat yang rendah dapat menyebabkan banyak pelanggaran yang dilakukan tanpa merasa terancam, sementara kemampuan penegak hukum yang terbatas dalam hal sumber daya dan pelatihan juga dapat menghambat upaya penegakan hukum.

Dalam hukum pidana dikenal adanya asas legalitas yaitu asas yang fundamental. Asas legalitas dalam hukum pidana penting dalam menentukan dapat tidaknya suatu kaidah hukum pidana diterapkan pada suatu tindak pidana yang telah

dilakukan. Sehingga jika terjadi suatu tindak pidana apakah aturan yang ada dapat ditindak terhadap tindak pidana yang dilakukan.[20]

Asas legalitas merupakan asas yang dapat digambarkan sebagai landasan hukum pidana. Asas ini tersirat dalam Pasal 1 KUHP yang berbunyi sebagai berikut:

1). Tidak ada perbuatan yang dapat dipidana kecuali berdasarkan ketentuan pidana dalam Peraturan Perundang-undangan yang berlaku sebelum perbuatan itu dilakukan.

2). Jika hukum berubah setelah kejahatan dilakukan, aturan yang lebih ringan berlaku untuk terdakwa.

Dalam Pasal 2 KUHP yang menyatakan bahwa :

"*ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu tindak pidana di Indonesia*".

Pengaturan terkait hak privasi juga diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang terbaru yaitu melalui Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, dalam KUHP terbaru tersebut terdapat beberapa Pasal yang secara langsung maupun tidak langsung berkaitan dengan pelindungan data pribadi dan hak privasi individu. Meskipun Pasal-Pasal dalam KUHP terbaru tidak secara eksplisit menyebutkan "data pribadi" atau "hak privasi", namun dapat diinterpretasikan bahwa KUHP terbaru mempunyai hubungan dengan pelindungan data pribadi dan hak privasi. Adapun

[20] Mahrus Ali, *Dasar-Dasar Hukum Pidana*, (Jakarta: Sinar Grafika, 2012), hal. 59.

Pasal-Pasal KUHP terbaru yang juga masih memiliki keterkaitan dengan hak privasi maupun Pelindungan Data Pribadi, antara lain :

1. **Perlindungan terhadap Kerahasiaan**: Pasal 236 dan 237 dapat ditafsirkan melindungi data pribadi yang bersifat rahasia, terutama dalam konteks profesional atau pekerjaan.
   a. **Pasal 236**

      Pasal ini mengatur tentang larangan membuka rahasia. Seseorang yang karena jabatannya atau pekerjaannya wajib merahasiakan sesuatu, namun dengan sengaja membuka rahasia tersebut, dapat dipidana dengan pidana penjara paling lama 1 tahun atau denda paling banyak kategori II.
   b. **Pasal 237**

      Pasal ini berkaitan dengan pembukaan rahasia yang dilakukan karena kealpaan. Seseorang yang karena kelalaiannya menyebabkan rahasia yang wajib disimpannya karena jabatan atau pekerjaannya diketahui oleh umum, dapat dipidana dengan pidana penjara paling lama 3 bulan atau denda paling banyak kategori II.
2. **Perlindungan terhadap Ruang Pribadi**: Pasal 301 dan 302 dapat dianggap melindungi privasi fisik seseorang, yang secara tidak langsung juga melindungi data pribadi yang mungkin tersimpan dalam ruang pribadi tersebut.
   a. **Pasal 301**

      Pasal ini mengatur tentang larangan memasuki rumah, ruangan, atau pekarangan tertutup tanpa izin. Tindakan ini dapat dipidana dengan pidana penjara paling lama 1 tahun atau denda paling banyak kategori II.

b. Pasal 302

Pasal ini berkaitan dengan larangan memaksa masuk ke dalam rumah, ruangan, atau pekarangan tertutup yang dipakai orang lain dengan melawan hukum atau berada di situ tanpa izin. Pelaku dapat dipidana dengan pidana penjara paling lama 2 tahun atau denda paling banyak kategori III.

Berdasarkan Pasal-Pasal dalam KUHP terbaru sebagaimana tersebut di atas, dapat dilihat sebagai bagian dari kerangka hukum yang lebih luas dalam melindungi privasi dan data pribadi warga negara Indonesia. Dalam pengaturan tentang Pelindungan Data Pribadi di Indonesia telah lebih spesifik diatur dalam UU PDP yang merupakan landasan hukum utama, untuk pelindungan data pribadi di Indonesia. Dalam rangka mencapai tujuan tersebut, kolaborasi antara pemerintah, swasta, akademisi, dan masyarakat sipil sangatlah penting. Setiap pihak memiliki peran dan tanggung jawab dalam menciptakan ekosistem yang aman dan terlindungi keamanan data pribadi. Dengan demikian, formulasi sanksi pidana yang ideal bukan hanya menjadi tanggung jawab pemerintah, tetapi juga harus melibatkan partisipasi dari seluruh lapisan masyarakat.

Rekomendasi ini akan mencakup aspek-aspek yang perlu diperhatikan dalam penetapan sanksi pidana, seperti proporsional sanksi pidana dan administratif, penentuan jenis pelanggaran, dan mekanisme penegakan hukum yang lebih efektif. Hasil penelitian ini juga diharapkan dapat mendukung upaya peningkatan kesadaran masyarakat mengenai pentingnya pelindungan data pribadi sebagai bagian dari masyarakat yang semakin digital, dan individu perlu menyadari hak-

hak terkait dengan data pribadi serta konsekuensi hukum yang mungkin timbul akibat penyalahgunaan data pribadi. Oleh karena itu, upaya edukasi dan sosialisasi mengenai pelindungan data pribadi harus menjadi bagian integral dari regulasi yang ada.

Dengan adanya beberapa permasalahan tersebut di atas, maka pentingnya memberikan kepastian hukum dan keadilan bagi masyarakat dalam penegakan dan implementasi pelindungan data pribadi di Indonesia, sehingga hal tersebut menjadikan alasan bagi Peneliti untuk melakukan penelitian dalam penulisan disertasi ini, yang bertujuan untuk merumuskan sanksi pidana yang ideal dalam regulasi pelindungan data pribadi di Indonesia, yang diharapkan mampu memberikan rekomendasi yang dapat dijadikan acuan bagi legislator dan pembuat kebijakan dalam merumuskan regulasi pelindungan data pribadi yang lebih baik.

Dengan latar belakang yang telah dijelaskan di atas, penelitian ini tidak hanya akan memberikan kontribusi terhadap pengembangan regulasi pelindungan data pribadi di Indonesia, tetapi juga akan menjadi acuan bagi negara-negara lain yang menghadapi tantangan serupa. Oleh karena itu, penting untuk melakukan penelitian mendalam mengenai formulasi sanksi pidana yang ideal dalam regulasi pelindungan data pribadi, agar perlindungan terhadap data pribadi masyarakat dapat ditingkatkan dan kepercayaan publik terhadap sistem hukum dapat dipulihkan.

Berdasarkan fenomena di atas, maka peneliti menganalisis dan menulis disertasi hukum dengan judul **"FORMULASI SANKSI PIDANA YANG IDEAL DALAM REGULASI PELINDUNGAN DATA PRIBADI"**.

1.2 Rumusan Masalah

Dengan latar belakang yang peneliti uraikan di atas, rumusan masalahnya adalah sebagai berikut :

1. Bagaimana pengaturan pembentukan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia?
2. Bagaimana implementasi pengaturan sanksi pidana dalam Undang-Undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi?
3. Bagaimana formulasi sanksi pidana yang ideal dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi?

1.3 Tujuan Penelitian

Tujuan dalam penelitian disertasi ini, adalah sebagai berikut :

1. Untuk mengkaji dan merumuskan pengaturan pembentukan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia.
2. Untuk mengkaji dan menganalisis implementasi pengaturan sanksi pidana dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.
3. Untuk mengkaji dan menemukan formulasi sanksi pidana yang ideal dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

1.4 Keaslian Penelitian

Sengaja Peneliti mengambil judul *"Formulasi sanksi pidana yang ideal dalam regulasi pelindungan data pribadi"* karena keaslian atau originalitas

penelitian dalam menyusun disertasi ini belum ada suatu penelitian di Indonesia yang secara khusus mengkaji tentang aturan sanksi pidana dalam regulasi pelindungan data pribadi setelah disahkannya UU PDP, ada beberapa disertasi dan penulisan ilmiah yang telah membahas tentang Pelindungan Data Pribadi, namun pendekatan dan perumusan masalah tentu jauh berbeda, antara lain :

Pertama, Sinta Dewi, dengan jurnal hukum berjudul "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan *cloud computing* di Indonesia" penelitian ini dimaksudkan karena meningkatnya pemanfaatan teknologi internet tentu melahirkan tantangan baru dalam perlindungan atas privasi dan data pribadi, terutama dengan semakin meningkatnya praktik pengumpulan, pemanfaatan dan penyebaran data pribadi seseorang. Selain itu ketertinggalan instrumen dan regulasi menjadi salah satu pemicu lemahnya mekanisme proteksi terhadap privasi dan data pribadi khususnya dalam penggunaan teknologi *cloud computing*. *Cloud computing* adalah teknologi yang menggunakan internet dan server pusat yang jauh untuk menjaga atau mengelola data pengguna. *Cloud computing* membantu pengguna untuk menggunakan aplikasi tanpa melakukan instalasi sehingga file pribadi dapat diakses dimanapun dan kapanpun melalui akses internet. Oleh sebab itu, penelitian Sinta Dewi, bertujuan untuk menciptakan konsep pengaturan yang memadai dalam rangka memberikan perlindungan bagi pengguna jasa *cloud computing* di Indonesia.[37]

[37] Sinta Dewi, *Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan cloud computing di Indonesia*, Jurnal Yustisia Vol.5 No.1, 2016.

Kedua, Ariella Gitta Sari, Program Doktor Ilmu Hukum Universitas 17 Agustus 1945 (Untag) Surabaya, Januari 2024, dengan judul disertasi "Rekonstruksi Pengaturan Bentuk Kelembagaan Penyelenggara Pelindungan data Pribadi". Berdasarkan fenomena kerentanan pelindungan data pribadi karena kemajuan teknologi. Sementara Pasal 58 UU PDP, tidak mencantumkan secara eksplisit lembaga penyelenggara pelindungan data pribadi, sedangkan suatu lembaga yang independen diharapkan mampu memberikan perlindungan terhadap data pribadi, sebagai bagian dari Hak Asasi Manusia, akan tetapi substansi Pasal 58 tersebut tidak mencantumkan aspek atau nilai kepastian hukum pengaturan bentuk lembaga penyelenggara pelindungan data pribadi yang independen.Selain itu, untuk mengkaji dan menganalisis permasalahan tentang ratio legis pembentukan kelembagaan penyelenggara pelindungan data pribadi dalam Pasal 58 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta rekonstruksi pengaturan bentuk kelembagaan penyelenggara pelindungan data pribadi dalam Pasal 58 UU Pelindungan Data Pribadi.

1.5 Manfaat Penelitian

Penelitian ini diharapkan mampu memberikan manfaat secara teoritis dan praktis:

1.5.1 Manfaat Teoritis

Secara Teoritis, diharapkan bahwa penelitian ini dapat memberikan sumbangan pemikiran dan upaya mengembangkan ilmu pengetahuan hukum serta memberikan manfaat untuk mengembangkan ilmu hukum

menyangkut pelindungan data pribadi, khususnya terkait formulasi sanksi pidana yang ideal dalam Undang-Undang Pelindungan Data Pribadi.

1.5.2 Manfaat Praktis

Secara Praktis, hasil penelitian ini diharapkan mampu memberikan perlindungan hukum terhadap penggunaan data pribadi berdasarkan prinsip-prinsip Hak Asasi Manusia dengan memberikan manfaat dan jaminan kepastian hukum bagi masyarakat terhadap pelindungan data pribadi baik secara elektronik maupun non-elektronik. Disamping itu, hasil penelitian ini diharapkan berguna untuk mengevaluasi regulasi pelindungan data pribadi yang telah ada saat ini, sehingga dapat memberikan masukan bagi Pemerintah dan DPR RI dalam memberikan penjelasan secara jelas sehingga tidak menimbulkan penafsiran yang berbeda di kalangan masyarakat tentang tujuan pembentukan Undang-Undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi, serta memberikan masukan kepada Pemerintah dalam menyusun Peraturan Pelaksanaan-nya, khususnya terkait formulasi sanksi pidana yang ideal dalam regulasi Pelindungan Data Pribadi.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan peneliti adalah garis besar singkat materi yang terkandung, bab demi bab, dengan keterangan sebagai berikut:

Bab I : Pendahuluan

Dalam bab ini dimulai dengan pembahasan mengenai latar belakang dari permasalahan yang ada. Bagian ini akan mengidentifikasi permasalahan-permasalahan secara umum mengenai Pelindungan Data Pribadi, yang selanjutnya disusun pada rumusan masalah. Bab ini juga merumuskan tentang tujuan penelitian, keaslian penelitian dengan menguraikan novelty dari topik yang diangkat, manfaat penelitian yang terdiri dari manfaat teoritis dan manfaat praktis serta sistematika penulisan.

Bab II : Tinjauan Pustaka

Bab ini memberikan deskripsi yang terbagi menjadi landasan teori dan landasan konseptual yang dapat menghasilkan ide dan mendukung penelitian yang relevan dengan area yang diteliti. Landasan teori yang terdiri dari: Teori Tujuan Hukum oleh Gustav Radbruch, diharapkan mampu mendukung analisa rumusan masalah pertama. Selanjutnya, untuk menganalisa rumusan masalah kedua, peneliti menggunakan teori Perlindungan Hukum oleh Fitzgerald yang merujuk pada konsep yang dikemukakan oleh John William Salmond, dan untuk membahas rumusan masalah ketiga, peneliti menggunakan teori Hukum Progresif oleh Satjipto Rahardjo. Kemudian, dalam Landasan Konseptual yang terdiri dari: Bentuk dan Jenis Data Pribadi yang digunakan, konsep Pelindungan Data Pribadi (PDP), Konsep tentang Pidana dan Pemidanaan serta Penerapan Sanksi Pidana.

Bab III : Metodologi Penelitian

Bab ketiga yaitu bab yang memberikan penjelasan mengenai metodologi penelitian yang digunakan peneliti untuk menyelesaikan penelitian ini, yang terdiri dari Jenis Penelitian, Data Penelitian yang dijabarkan melalui Data Primer dan Data

Sekunder yang diperoleh melalui penelitian yuridis normatif, yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier, serta bahan non-hukum, dan pada akhirnya membahas tentang cara pengolahan dan analisis data serta pendekatan penelitian yang digunakan oleh peneliti.

Bab IV : Pembahasan dan Analisa

Bab keempat yaitu Pembahasan dan Analisa, yang merupakan bab terpenting dalam penelitian ini, peneliti merumuskan temuan dan analisis yang disusun mengenai 3 (tiga) rumusan masalah, yaitu: Pertama, bagaimana pengaturan mengenai Pelindungan Data Pribadi di Indonesia? Peneliti menjawab rumusan masalah pertama tersebut dengan mengkaji peraturan Perundangan-Undangan terkait dengan pelindungan data pribadi di Indonesia. Kedua, bagaimana implementasi pengaturan sanksi pidana dalam Undang-Undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi? Perlu Peneliti sampaikan bahwa mengingat UU PDP ini baru diundangkan pada bulan Oktober 2022 dan belum banyak ditemukan adanya penerapan sanksi pidana dalam UU PDP di Indonesia, sehingga Peneliti menggunakan perbandingan di beberapa negara antara lain Uni Eropa, Singapura, Thailand, dan Malaysia yang telah lebih dulu memiliki regulasi pelindungan data pribadi sebelum dibentuknya UU PDP di Indonesia, dan bagaimana negara-negara pembanding tersebut menjalankan dan menerapkan regulasi Pelindungan Data Pribadi khususnya mengenai penerapan sanksi Pidana yang berlaku negara tersebut sehingga penelitian ini diharapkan mampu memberikan gambaran sekaligus berkaca pada pengalaman dari beberapa negara tersebut tentang bagaimana penerapan sanksi pidana yang ideal dalam regulasi pelindungan data pribadi.

Ketiga, bagaimana formulasi sanksi pidana yang ideal dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi? Peneliti menjawab dengan melakukan analisis terhadap hasil kajian literatur, data-data yang ditemukan melalui verifikasi kajian empiris, serta dikaitkan dengan landasan teori.

Bab V : Penutup Kesimpulan dan Saran

Bab terakhir ini berisi kesimpulan yang merupakan jawaban dari ketiga permasalahan yang dianalisis pada bab keempat dan diakhiri dengan kesimpulan dan usulan atau saran dari peneliti sehubungan dengan penelitian ini.