

# BAB I

## PENDAHULUAN

### A. Latar Belakang

Perkembangan teknologi informasi dan media komunikasi di era revolusi industri 4.0 saat ini berkembang sangat pesat. Perkembangan ini mempengaruhi tatanan kehidupan masyarakat dan mendorong terjadinya perubahan pada sektor ekonomi, sosial, budaya, pertahanan, keamanan, dan penegakan hukum. Perubahan perilaku masyarakat yang biasanya dilakukan secara fisik sekarang lebih menitikberatkan kegiatan pada dunia digital.<sup>1</sup> Hal ini relevan dengan adanya peningkatan pengguna internet di Indonesia.

Pengguna internet di Indonesia tahun 2024 mencapai 221.563.479 jiwa atau sekitar 79,5% dari total populasi penduduk Indonesia berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia tahun 2024.<sup>2</sup> Situasi ini menggambarkan bahwa masyarakat lebih masif dalam pemanfaatan teknologi digital. Dengan adanya kondisi ini, transformasi digital tidak dapat dihindari.<sup>3</sup>

Dalam menyongsong percepatan transformasi digital diperlukan upaya-upaya terobosan yakni perluasan akses dan infrastruktur digital, percepatan integrasi Pusat Data Nasional, peningkatan SDM, dan aspek regulasi.<sup>4</sup> Percepatan transformasi digital ini dilakukan demi mewujudkan pelayanan publik yang terintegritas, Sistem Pemerintahan Berbasis Elektronik

---

<sup>1</sup> Kristophorus Hadiono dan Rina Candra Noor Santi, 2020, "Menyongsong Transformasi Digital", Proceeding SENDIU, hlm. 1.

<sup>2</sup> Komdigi, "Pengguna Internet Meningkat, Komdigi Galang Kolaborasi Tingkatkan Kualitas Layanan", [https://www.Komdigi.go.id/content/detail/54481/siaran-pers-no-80hmKomdigi012024-tentang-pengguna-internet-meningkat-Komdigi-galang-kolaborasi-tingkatkan-kualitas-layanan/0/siaran\\_pers](https://www.Komdigi.go.id/content/detail/54481/siaran-pers-no-80hmKomdigi012024-tentang-pengguna-internet-meningkat-Komdigi-galang-kolaborasi-tingkatkan-kualitas-layanan/0/siaran_pers), dikunjungi pada tanggal 4 Maret 2024 Jam 21.00.

<sup>3</sup> Resego Morakanyane, *Et. Al*, 2017, "Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature", BLED 2017 Proceedings. 21. hlm. 436.

<sup>4</sup> OJK Institute, "5 Langkah Percepatan Transformasi Digital", <https://www.ojk.go.id/ojk-institute/id/news/read/1220/5-langkah-percepatan-transformasi-digital>, dikunjungi pada tanggal 5 Maret 2024 Jam 14.00.

(SPBE) dan Satu Data Indonesia yang terpadu. Merujuk pada ketentuan Pasal 1 angka (1) dan (2) Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2023 Tentang Percepatan Transformasi Digital Dan Keterpaduan Layanan Digital Nasional, Sistem Pemerintahan Berbasis Elektronik adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan. Sedangkan Satu Data Indonesia adalah suatu kebijakan tata kelola data pemerintah.

Selain itu transformasi digital juga perlu dilakukan pada aspek regulasi untuk memastikan adanya supremasi hukum terhadap perlindungan data khususnya Pelindungan Data Pribadi terkait keamanan siber/*cybersecurity*. *Cybersecurity* menurut ISO (*International Organization for Standardization*), tepatnya ISO/IEC 27032:2023 adalah suatu tindakan melindungi manusia, masyarakat, organisasi, dan negara dari resiko ancaman dunia maya.<sup>5</sup> Hal ini tentu relevan karena mengingat perkembangan teknologi informasi dan komunikasi tidak hanya memberikan manfaat, tetapi juga membawa resiko adanya ancaman keamanan siber. Ancaman keamanan siber/*cybersecurity* salah satunya terkait keamanan data. Keamanan data juga perlu ditingkatkan karena mengingat semakin banyaknya kasus-kasus pelanggaran data.

Setiap warga negara berhak mendapatkan perlindungan terhadap keamanan data pribadi yang dimiliki. Sebagaimana diatur dalam Pasal 28G ayat (1) UUD NRI Tahun 1945 bahwasanya setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan

---

<sup>5</sup> Article 3.6 of ISO/IEC 27032:2023 – Cybersecurity-Guidelines for Internet security, <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en>, dikunjungi pada tanggal 22 Maret 2024 Jam 11.36.

dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu merupakan hak asasi. Selain diatur dalam konstitusi negara, Indonesia harus melindungi privasi dan data pribadi setiap warga negara sebagaimana mengakui bahwasanya hak asasi manusia merupakan hak dasar yang melekat pada diri manusia yang harus dilindungi, dihormati, dan dipertahankan. Hal ini tidak terlepas dari adanya pengesahan *International Covenant On Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik). Perlindungan yang diberikan tidak hanya dalam konteks hubungan langsung, tetapi juga perlindungan atas hal-hal yang melekat pada diri setiap warga negara seperti data pribadi atau informasi pribadi.<sup>6</sup>

Perlindungan terhadap data pribadi merupakan suatu perlindungan hak asasi manusia. Oleh karena itu pengaturan mengenai Pelindungan Data Pribadi ini merupakan manifestasi dari pengakuan dan perlindungan negara atas hak dasar manusia. Pengaturan mengenai Pelindungan Data Pribadi di Indonesia sebenarnya sudah ada, namun pengaturan tersebut hanya bersifat parsial dan sektoral. Beberapa peraturan perundang-undangan yang mengatur mengenai Pelindungan Data Pribadi dan/atau *cyber law* diantaranya UU Nomor 10 Tahun 1998 Tentang Perbankan, UU Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, UU Nomor 39 Tahun 1999 Tentang HAM, UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan lain sebagainya.

Ketentuan-ketentuan diatas memiliki defenisi, ruang lingkup, dan mekanisme perlindungan data yang berbeda. Ketidakselarasan regulasi ini tentu berdampak pada ketidakpastian hukum dalam Pelindungan Data Pribadi

---

<sup>6</sup> Galung Pratama Subakti, 2023, "Pengaturan Pelindungan Data Pribadi Dalam General Data Protection Regulation Dan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi", Skripsi Universitas Andalas, Padang, hlm. 5.

di Indonesia. Hal inilah yang melatarbelakangi pemerintah untuk membentuk suatu regulasi khusus yang mengatur mengenai Pelindungan Data Pribadi. Sehingga lahirlah Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi untuk melindungi dan menjamin hak dasar warga negara, menjamin masyarakat mendapatkan pelayanan dari Korporasi, Badan Publik, dan Pemerintah serta mendorong pertumbuhan ekonomi digital.

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi merupakan ketentuan khusus atau dikenal istilah *Lex Specialis* yang mengatur tentang jaminan atas perlindungan dan keamanan data pribadi. Sedangkan ketentuan umum atau *Lex Generalis* diatur didalam Kitab Undang-Undang Hukum Perdata. Kitab Undang-Undang Hukum Perdata mengatur bahwa data pribadi merupakan hak milik seseorang atau hak yang melekat pada seseorang sehingga perlu untuk mendapatkan jaminan perlindungan hukum. Sehingga apabila terjadi pelanggaran data pribadi seperti pencurian ataupun peretasan data maka perbuatan tersebut adalah suatu perbuatan melawan hukum yang dapat dimintakan pertanggungjawabannya.

Berdasarkan data dari Kementerian Komunikasi dan Informasi yang nomenklaturnya telah mengalami perubahan menjadi Kementerian Komunikasi dan Digital (Komdigi), sebagaimana diatur dalam Peraturan Presiden Nomor 140 Tahun 2024 tentang Organisasi Kementerian Negara, yang untuk selanjutnya disebut Komdigi, sangat banyak kasus pelanggaran data pribadi di Indonesia. Terdapat 94 kasus pencurian data di dalam negeri sejak tahun 2019 – Juni 2023. Kasus pencurian data tersebut terdiri dari 62 kasus terkait dengan penyelenggara sistem elektronik (PSE) privat atau swasta

dan 32 kasus yang menyangkut PSE pemerintah.<sup>7</sup> Kasus pelanggaran data pribadi yang baru-baru ini terjadi adalah peretasan Pusat Data Nasional (PDN).

PDN mengalami gangguan sejak hari Kamis 20 Juni 2024 lalu. Kepala Badan Siber dan Sandi Negara (BSSN) Republik Indonesia masa itu Hinsa Siburian mengonfirmasi bahwa insiden ini disebabkan oleh serangan siber yang bersumber dari file *Ransomware* bernama *Brain Cipher*. *Ransomware* ini merupakan *Ransomware* jenis terbaru berjenis *Ransomware Lockbit 3.0*. Hinsa Siburian menginformasikan bahwa dari insiden tersebut, BSSN menemukan adanya upaya menonaktifkan fitur keamanan *Windows Defender* mulai tanggal 17 Juni 2024 pada pukul 23.15 WIB. Kemudian aktivitas *malicious* mulai terjadi pada tanggal 20 Juni 2024 pada pukul 00.54 WIB, diantaranya melakukan instalasi file *malicious* dan menonaktifkan sistem yang sedang berjalan. Dihari yang sama pukul 00.55 WIB, *Windows Defender* tidak dapat beroperasi.<sup>8</sup>

*Ransomware* ini merupakan *malware* (perangkat lunak jahat) yang mengenkripsi data. Sehingga korban tidak dapat mengakses data tersebut.<sup>9</sup> Akibatnya berbagai instansi pemerintah mengalami gangguan dalam pelayanan publik. Kementerian Komunikasi dan Digital menginformasikan 210 instansi pemerintah turut terdampak. Tak terkecuali yang terdampak adalah layanan keimigrasian. Gangguan sistem pada PDN menghambat seluruh layanan keimigrasian seperti layanan paspor, visa, izin tinggal, dan

---

<sup>7</sup> Kontan.co.id, “Komdigi Catat 94 Kasus Kebocoran Data Pribadi Sejak 2019 hingga Juni 2023”, <https://nasional.kontan.co.id/news/Komdigi-catat-94-kasus-kebocoran-data-pribadi-sejak-2019-hingga-juni-2023>, dikunjungi pada tanggal 2 April 2024 Jam 05.33.

<sup>8</sup> Komdigi. “BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware”, <https://www.komdigi.go.id/content/detail/57321/bssn-identifikasi-pusat-data-nasional-sembentara-diserang-ransomware/0/berita>, dikunjungi pada tanggal 8 Agustus 2024 Jam 04.31.

<sup>9</sup> Kompas.com, “Siapa itu Brain Chiper, Operator Serangan “Ransomware” PDN?”, <https://www.kompas.id/baca/investigasi/2024/07/03/siapa-itu-brain-cipher-operator-serangan-ransomware-pdn>, dikunjungi pada tanggal 9 Agustus 2024 Jam 20.00.

perlintasan. Tentu hal ini merugikan banyak pihak. Akibat gangguan tersebut, dilakukanlah layanan secara manual.<sup>10</sup>

Adapun luas kebocoran data akibat serangan *Ransomware* dari 210 instansi yang terdampak belum ada angka pasti mengenai jumlah *record* data yang terenkripsi atau bocor. Namun, indikasinya adalah: data terkunci, tidak bisa diakses, dan dalam risiko bocor meski belum dikonfirmasi secara publik. Peretas tersebut menuntut tebusan (\$8 juta) untuk mendekripsi dan mengembalikan akses. Jika tidak dibayar, mereka biasanya mengancam menyebarkan atau menghapus data korban. Pada kasus ini pemerintah menolak membayar tebusan sebesar US\$ 8 juta (sekitar Rp 131 miliar). Belum ada laporan resmi bahwa data tersebut telah dicuri atau dijual. hal yang dikhawatirkan adalah data tersebut telah bocor di *dark web*.<sup>11</sup>

Berdasarkan Ketentuan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi mengatur mengenai pertanggungjawaban hukum terhadap pelanggaran pemrosesan data pribadi. adanya kebocoran ataupun peretasan data pribadi merupakan suatu pelanggaran dalam pemrosesan data pribadi. Pelindungan Data Pribadi dalam hal pemrosesan data haruslah dilakukan dengan bertanggung jawab dan dapat dibuktikan dengan jelas sehingga memberikan aspek kepastian hukum sebagaimana diamanatkan pada Pasal 16 ayat (2) huruf h UU Pelindungan Data Pribadi.<sup>12</sup> Pemerintah

---

<sup>10</sup> CNN Indonesia, “Deret Layanan Terdampak Peretasan Pusat Data Nasional”, <https://www.cnnindonesia.com/nasional/20240628202216-12-1115511/deret-layanan-terdampak-peretasan-pusat-data-nasional>, dikunjungi pada tanggal 9 Agustus 2024 Jam 20.10.

<sup>11</sup> Reuters.com, “Presiden Indonesia perintahkan audit pusat data pascaserangan siber”, [https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/?utm\\_source=chatgpt.com](https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/?utm_source=chatgpt.com) dikunjungi pada tanggal 15 Agustus 2025 Jam 02.36.

<sup>12</sup> Zulian Claudia dan Ariawan Gunadi, 2023, “Vicarious Liability in Personal Data Protection”, Rechtsidee, Vol. 11, No. 2, hlm.7.

memiliki kewajiban hukum untuk menyampaikan pemberitahuan kepada publik apabila terjadi kegagalan dalam perlindungan data seperti halnya peretasan Pusat Data Nasional. Kewajiban ini secara eksplisit tertuang dalam Pasal 46 ayat (3) UU PDP, yang menyatakan bahwa dalam situasi tertentu, Pengendali Data Pribadi harus memberikan informasi kepada masyarakat terkait insiden pelanggaran keamanan data. Adapun penjelasan atas frasa “dalam hal tertentu” mengacu pada kondisi di mana kegagalan tersebut berdampak langsung pada terganggunya pelayanan publik atau menimbulkan konsekuensi serius bagi kepentingan masyarakat luas. Dalam konteks insiden peretasan yang menyebabkan lumpuhnya Pusat Data Nasional, kondisi ini sangat relevan, mengingat gangguan yang terjadi telah menghambat berbagai sektor pelayanan publik yang bersifat esensial.<sup>13</sup>

Pemerintah dalam hal ini Kementerian Komunikasi dan Digital (Komdigi) menjalankan tugas dan fungsinya sebagaimana diatur dalam Peraturan Presiden Nomor 174 Tahun 2024 Tentang Kementerian Komunikasi dan Digital Pasal 6 yang menegaskan bahwa kewenangan perumusan, penetapan, dan pelaksanaan kebijakan di bidang infrastruktur digital, teknologi pemerintah digital, ekosistem digital, pengawasan ruang digital, perlindungan data pribadi, dan komunikasi publik dan media. Dalam rangka tersebut, Komdigi sebagai Penyelenggara Sistem Elektronik dan pengendali data pribadi bertanggung jawab atas pemrosesan data pribadi. Tanggung jawab tersebut meliputi kegagalan perlindungan Pusat Data Nasional, dimana kewajiban

---

<sup>13</sup> Husein Muhammad Iqbal, dkk, 2025, “Bentuk Pertanggungjawaban Pemerintah Terhadap Lumpuhnya Pusat Data Nasional Berdasarkan Hukum Administrasi Negara”, Vol. 3, No. 2, hlm. 80-81.

hukum pemerintah adalah menunjukkan pertanggungjawabannya secara hukum.

Upaya yang dilakukan pemerintah pasca Peretasan Pusat Data Nasional tersebut adalah melakukan upaya pemulihan teknis dan normalisasi layanan publik yang terdampak. Pemulihan tersebut mencakup : Proses pemulihan layanan melalui *backup server* dari *Cold site* Batam sebagaimana dimuat dalam Surat Nomor B-698/DJAI/AI.01.01/03/2024 tanggal 21 Juni 2024; Melakukan koordinasi dengan Instansi Pemerintah Instansi Pemerintah Pusat dan Daerah (IPPD) dalam rangka pemulihan layanan IPPD yang terdampak (Surat Plt. Direktur LAIP Nomor B-738/DJAI.3/AI.01.01/06/2024 tanggal 28 Juni 2024); Mengkoordinasikan progress recovery Layanan PDNs, dengan menyampaikan strategi recovery jangka pendek, menengah, dan panjang (Surat Direktur LAIP Nomor: B-876/DJAI.3/ AI.01.01/07/2024 tanggal 12 Juli 2024); pengaturan *backup* data dan layanan kementerian/lembaga/ pemerintah daerah sebagai bentuk upaya menjaga keberlangsungan layanan sebagaimana dimuat dalam Surat Nomor B-876/DJAI.3/AI.01.01/07/2024 tanggal 16 Juli 2024.<sup>14</sup>

Meskipun pemerintah telah melaksanakan sejumlah langkah teknis untuk memulihkan layanan akibat insiden peretasan Pusat Data Nasional, namun hal tersebut belum menyentuh bentuk pertanggungjawaban atau sanksi tegas agar kejadian peretasan bisa dicegah dan/atau meminimalisir kejadian.

Dalam perspektif hukum, peretasan PDN dapat dipandang sebagai perbuatan

---

<sup>14</sup> Kemkondigi, 2024, Sejumlah Layanan Publik Yang Terganggu Serangan Ransomware Kembali Normal Juli 2024, [https://www.instagram.com/p/C865-rEyrHZ/?utm\\_source=ig\\_embed&ig\\_rid=58b8a9f3-5f96-4733-8d5a-53b42774791&img\\_index=3](https://www.instagram.com/p/C865-rEyrHZ/?utm_source=ig_embed&ig_rid=58b8a9f3-5f96-4733-8d5a-53b42774791&img_index=3), dikunjungi pada tanggal 2 April 2024 Jam 06.00.

melawan hukum (*onrechtmatige daad*) sebagaimana diatur dalam Pasal 1365 KUH Perdata. Unsur-unsur *onrechtmatige daad* yakni adanya perbuatan melawan hukum, kesalahan, kerugian, dan hubungan kausalitas. hal ini dapat dianalisis bukan hanya pada pelaku peretasan (hacker) yang dengan sengaja menyerang sistem elektronik negara, tetapi juga pada pemerintah sebagai pengelola PDN yang lalai memenuhi kewajibannya untuk melindungi data pribadi. Hal ini sejalan dengan Pasal 12 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang memberi hak bagi subjek data untuk menuntut ganti rugi apabila terjadi pelanggaran dalam pemrosesan data pribadi. Dengan demikian, kelalaian pemerintah dapat menimbulkan tanggung jawab perdata, karena kegagalan perlindungan data secara langsung menimbulkan kerugian bagi masyarakat sebagai pemilik data.

Secara doktrinal, memang terdapat perdebatan apakah kelalaian pemerintah dalam kasus ini digolongkan ke dalam *onrechtmatige overheidsdaad* (perbuatan melawan hukum oleh penguasa) yang merupakan ranah hukum administrasi negara. Akan tetapi, dalam konteks pelanggaran data pribadi, fokus utama korban adalah pemulihan hak dan ganti rugi, yang secara konseptual lebih dekat dengan rezim *onrechtmatige daad* dalam hukum perdata. Oleh karena itu, kajian terhadap pertanggungjawaban perdata pemerintah menjadi relevan, karena pemerintah dalam kapasitasnya sebagai pengendali data bukan hanya badan publik, tetapi juga subjek hukum keperdataan yang harus tunduk pada prinsip Pelindungan Data Pribadi. Dengan demikian, kasus peretasan PDN membuka ruang untuk analisis mengenai sejauh mana pemerintah dapat dimintai pertanggungjawaban perdata atas kebocoran data pribadi.

Kendati demikian, penerapan norma pasal 12 UU PDP mengenai ganti rugi tersebut dalam praktik masih menghadapi berbagai kendala. Salah satu hambatan utama adalah adanya celah hukum yang menyebabkan lemahnya penerapan sanksi terhadap instansi pemerintah sebagai pelaku pelanggaran, meskipun ketentuan ganti rugi ini telah diatur secara normatif dalam UU PDP, implementasinya masih terhambat karena kekosongan hukum tentang ganti rugi seperti apa yang dapat diterapkan apakah dalam bentuk ganti rugi materil, atau immateriil, atau keduanya. Penafsiran bentuk ganti kerugian ini juga belum dapat ditafsirkan karena belum terbentuknya lembaga independen yang memiliki otoritas dalam menjatuhkan sanksi administratif maupun menyelesaikan sengketa perdata terkait pelanggaran data pribadi. Ketiadaan lembaga ini menciptakan kekosongan hukum yang berisiko memperburuk ketidakadilan bagi individu yang datanya telah disalahgunakan serta menghambat pemajuan prinsip *accountability* dalam tata kelola data publik.

Oleh karena itu, perlu diketahui bagaimana kewajiban pemerintah sebagai pengendali data pribadi pada kasus peretasan PDN tersebut dan pertanggungjawabannya secara perdata terhadap peretasan Pusat Data Nasional yang diatur oleh Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data. Berdasarkan uraian latar belakang di atas, penulis tertarik untuk mengkaji dan membahas mengenai **“PERTANGGUNGJAWABAN PERDATA TERHADAP PERETASAN PUSAT DATA NASIONAL DITINJAU DARI PERSPEKTIF UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI”**.

## **B. Rumusan Masalah**

Sebagaimana gambaran permasalahan diatas, penulis tertarik untuk merumuskan dan mengidentifikasi masalah-masalah sebagai berikut :

1. Bagaimana Kewajiban Pemerintah Terhadap Peretasan Pusat Data Nasional Ditinjau dari Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi?
2. Bagaimana Pertanggungjawaban Perdata Terhadap Peretasan Pusat Data Nasional Ditinjau dari Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi?

## **C. Tujuan Penelitian**

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Untuk mengetahui dan menganalisis bagaimana kewajiban pemerintah terhadap peretasan Pusat Data Nasional ditinjau dari perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi
2. Untuk mengetahui dan menganalisis bagaimana pertanggungjawaban perdata terhadap peretasan Pusat Data Nasional ditinjau dari perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

## **D. Manfaat Penelitian**

Berdasarkan tujuan penelitian, penelitian ini diharapkan dapat memberikan manfaat bagi penulis maupun para pembaca, baik secara langsung maupun tidak langsung. Adapun manfaat tersebut diuraikan sebagai berikut:

1. Manfaat Teoritis
  - a. Untuk menambah ilmu pengetahuan dan wawasan serta melatih kemampuan penulis dalam penulisan karya ilmiah khususnya mengenai hukum perdata, yang diharapkan dapat menjadi referensi bagi sesama

mahasiswa, dosen, dan/atau masyarakat yang tertarik dengan permasalahan yang dikaji.

- b. Untuk memberikan sumbangan pemikiran terhadap ilmu pengetahuan dari penelitian ini terkhusus mengenai bentuk pertanggungjawaban perdata terhadap peretasan Pusat Data Nasional ditinjau dari perspektif UU No 27 Tahun 2022.

## 2. Secara Praktis

- a. Diharapkan dapat memberikan sumbangan pemikiran mengenai pemecahan masalah terhadap perlindungan hukum terkait data pribadi yang diberikan kepada subjek data pribadi.
- b. Diharapkan agar hasil penelitian ini dapat menjadi pertimbangan dan dapat digunakan bagi semua pihak baik bagi pemerintah, masyarakat umum maupun para pihak yang bekerja di bidang hukum.

## E. Metode Penelitian

Penelitian merupakan penyaluran hasrat keingintahuan manusia terhadap suatu ilmu pengetahuan. Seseorang menyadari bahwa sebab dan akibat dari setiap gejala yang muncul dapat diketahui penjelasannya secara ilmiah. Selain itu, suatu penelitian adalah bersikap obyektif, karena hasil penelitian diperoleh dengan metode ilmiah sehingga dapat diketahui kebenaran akan penelitian tersebut.<sup>15</sup>

Adapun metode penelitian yang digunakan adalah sebagai berikut :

### 1. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum yuridis normatif. Penelitian ini mendasarkan analisisnya pada peraturan

---

<sup>15</sup> Bambang Sunggono, 2013, *Metode Penelitian Hukum*, Raja Grafindo Persada, Jakarta , hlm. 32.

perundang-undangan, analisis teori, dan permasalahan hukum yang terjadi. Penelitian hukum normatif adalah penelitian hukum yang mempelajari ilmu hukum, yang dianggap sebagai norma dan aturan yang berlaku dalam masyarakat dan menjadi acuan bagi setiap perilaku individu.<sup>16</sup> Penelitian dilakukan dengan cara meneliti dokumen-dokumen dan/atau bahan kepustakaan yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.<sup>17</sup>

## 2. Pendekatan Penelitian

Terdapat 5 (lima) pendekatan dalam penelitian hukum sebagaimana dinyatakan oleh Peter Mahmud Marzuki, yaitu pendekatan Undang-Undang (*statute approach*), pendekatan konseptual (*conceptual approach*), pendekatan perbandingan (*comparative approach*), pendekatan kasus (*case approach*), dan pendekatan historis (*historical approach*).<sup>18</sup> Adapun pendekatan yang digunakan pada penelitian ini adalah pendekatan undang-undang dan pendekatan kasus. Pendekatan dilakukan dengan mengkaji dan menganalisis semua regulasi yang berkenaan dengan topik penelitian yaitu mengenai pertanggungjawaban perdata terhadap pelanggaran data pribadi dan dikaitkan dengan kasus peretasan Pusat Data Nasional.

## 3. Sifat penelitian

Penelitian berikut bersifat deskriptif. Menurut Sugiyono, penelitian deskriptif adalah metode deskriptif yang digunakan untuk memberikan

---

<sup>16</sup> Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, hlm. 52-54.

<sup>17</sup> H. Abdurrahman Soejono, 2003, *Metode Penelitian Hukum*, Rineka Cipta, Jakarta hlm. 56.

<sup>18</sup> Peter Mahmud Marzuki, 2011, *Penelitian Hukum*, cetakan ke-11, Kencana, Jakarta, hlm. 93-95.

gambaran suatu hasil dari penelitian tetapi tidak digunakan untuk membuat kesimpulan yang lebih luas.<sup>19</sup>

#### 4. Sumber Data

Sumber data dalam suatu penelitian terdiri dari 2 macam, yaitu data primer dan data sekunder. Data primer adalah data yang diperoleh langsung oleh peneliti dari sumbernya. Data ini diperoleh oleh peneliti melalui wawancara, pengamatan, observasi, dan lain sebagainya. Data primer ini diolah sendiri oleh peneliti. Sedangkan data sekunder adalah data yang diperoleh secara tidak langsung oleh peneliti dari sumbernya. Misalnya buku-buku, karya ilmiah, peraturan perundang-undangan, dan sebagainya.<sup>20</sup> Adapun jenis sumber data yang digunakan pada penelitian ini adalah data sekunder.

Sumber data sekunder dapat diperinci menjadi 3 macam, yaitu sebagai berikut :<sup>21</sup>

##### a. Bahan hukum primer

Yaitu bahan-bahan hukum yang memiliki kekuatan mengikat secara hukum atau yuridis. Dalam penelitian ini bahan hukum primer yang digunakan adalah Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, peraturan perundang-undangan yang berkenaan dengan Pelindungan Data Pribadi, transaksi elektronik, penyelenggaraan sistem dan transaksi elektronik, dan sebagainya.

##### b. Bahan hukum sekunder

---

<sup>19</sup> Suketi dan Galang Taufani, 2018, *Metode Penelitian Hukum (Filsafat, Teori dan Praktik)*, Raja Grafindo Persada, Depok, hlm. 182.

<sup>20</sup> *Ibid.*, hlm. 214.

<sup>21</sup> *Ibid.*, hlm. 216.

Yaitu bahan-bahan yang berkaitan dengan bahan hukum primer yang dapat membantu menganalisis bahan hukum primer tersebut. Bahan hukum sekunder dapat berupa buku-buku, karya ilmiah para sarjana, pendapat para ahli, jurnal, dan sebagainya.

c. Bahan hukum tersier

Yaitu bahan-bahan yang melengkapi bahan hukum primer dan bahan hukum sekunder, misalnya Kamus Hukum, bibliografi, dan indeks.

5. Metode Pengumpulan Data

Alat pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan. Studi kepustakaan/dokumen adalah alat pengumpulan data yang tidak diteliti secara langsung terhadap subjek penelitian. Pengumpulan data dalam studi kepustakaan/dokumen adalah kegiatan memeriksa, menganalisis, dan mengkaji data-data sekunder. Data sekunder yang dapat diteliti meliputi data sekunder yang bersifat pribadi dan data sekunder yang bersifat publik seperti data resmi dari pemerintahan, data-data yang dipublikasikan diantaranya Undang-Undang Dasar NRI Tahun 1945, Undang-Undang, Peraturan Pemerintah, Peraturan Presiden, dan sebagainya.<sup>22</sup>

6. Analisis Data

Analisis data bergantung pada jenis metode penelitian yang dilakukan. Dikarenakan metode penelitian yang peneliti gunakan adalah penelitian normatif, maka analisis data yang digunakan juga menerapkan analisis

---

<sup>22</sup> *Ibid.*, hlm. 216-217.

normatif. Kemudian data-data berupa peraturan perundang-undangan tersebut dianalisis secara induktif kualitatif.<sup>23</sup>



---

<sup>23</sup> Beni Ahmad Saebani, 2008, *Metode Penelitian Hukum*, Pustaka Setia, Bandung, hlm. 93.