

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi dewasa ini telah banyak membawa dampak dalam kehidupan manusia, baik dampak positif maupun dampak negatif. Dampak positif dari perkembangan teknologi informasi dan komunikasi ini misalnya, mempermudah manusia untuk dapat saling terhubung kapanpun dan dimanapun antara satu manusia dengan sama lainnya tanpa mengenal batas waktu dan wilayah. Adapun dampak negatif dari perkembangan teknologi dan komunikasi ini misalnya, juga memperluas cakupan kejahatan yang semula hanya dapat dilakukan secara konvensional, kini dapat dilakukan secara siber.

Dengan semakin berkembangnya teknologi informasi dan komunikasi, banyak sektor di dalam kehidupan manusia yang dipermudah dengan memanfaatkan sistem teknologi informasi dan komunikasi, sebut saja sektor perdagangan melalui sistem perdagangan elektronik (*electronic commerce*), sektor pendidikan melalui sistem pendidikan elektronik (*electronic education*), sektor pemerintahan melalui sistem pemerintahan elektronik (*electronic government*), sektor kesehatan melalui sistem kesehatan elektronik (*electronic health*), sektor olahraga /permainan melalui sistem olahraga elektronik (*electronic sport*), maupun sektor-sektor kehidupan manusia lainnya yang dapat dipermudah melalui adanya perkembangan sistem teknologi informasi dan komunikasi.

Namun, pemanfaatan teknologi informasi dan komunikasi dalam berbagai sektor kehidupan manusia tersebut tentunya membawa resiko tersendiri, khususnya bagi data pribadi seseorang. Hal ini karena, pemanfaatan teknologi informasi dan komunikasi mengakibatkan data pribadi seseorang sangatlah mudah untuk dikumpulkan, dipindahkan serta disebarluaskan dari satu pihak kepada pihak lainnya tanpa sepengetahuan pemilik data pribadi, yang mana hal ini tentunya mengancam hak atas privasi pemilik data pribadi tersebut, bahkan data pribadi seseorang tersebut sangat rentan untuk disalahgunakan, baik disalahgunakan di dalam sistem elektronik itu sendiri maupun pada sistem nonelektronik, yang mana tentunya sangat berbahaya dan merugikan bagi pemilik data pribadi.

Definisi Data Pribadi dapat ditemukan dalam beberapa Peraturan Perundang-Undangan berikut. Pertama, berdasarkan ketentuan Pasal 1 angka 22 Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU 23/2006 jo. UU 24/2013), yang menyatakan “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya”.

Kedua, berdasarkan ketentuan Pasal 1 angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), bahwa “Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri

atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik”.

Ketiga, Definisi tentang Data Pribadi juga termuat dalam Pasal 1 Angka 1 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo 20/2016), yang menyatakan “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya”.

Adapun data pribadi itu di klasifikasi menjadi 2 (dua) jenis¹. Pertama, Data Pribadi yang sifatnya umum, yaitu nama lengkap, jenis kelamin, agama/kepercayaan yang dianut, kewarganegaraan, serta data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Kedua, yaitu data pribadi yang sifatnya spesifik, antara lain data dan informasi kesehatan, data genetika, data biometrik, orientasi seksual, pandangan politik, data anak, catatan kejahatan, data keuangan pribadi, serta data spesifik lainnya yang sesuai dengan peraturan perundang-undangan yang berlaku. Bahkan, identitas seperti nomor ponsel, alamat rumah, termasuk keterangan yang benar dan nyata yang melekat dan dapat diidentifikasi pada masing-masing individu, termasuk sebagai data pribadi². Lebih lanjut, *Southeast Asia Freedom of Expression Network*

¹ Kementerian Komunikasi dan Informatika Republik Indonesia, 2020, “*Bersama Lindungi Data Pribadi di Platform Digital*”, Artikel Dalam Jaringan 31 Juli, (Diakses 24 Agustus 2022), tautan : <https://m.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel>.

² Erizka Permatasari, 2021, “*Hukumnya Menyalahgunakan Data Pribadi untuk Emergency Contact Pinjol*”, Artikel Dalam Jaringan 28 Juli, (Diakses 24 Agustus 2022), tautan : <https://www.hukumonline.com/klinik/a/hukumnya-menyalahgunakan-data-pribadi-untuk-iemergency-contact-i-pinjol-lt610129a817b6c>.

(SAFEnet) menjelaskan bahwa, data pribadi atau dikenal juga sebagai PII (*Personally Identifiable Information*), ialah suatu ataupun sekelompok hal dan/atau informasi yang dapat digunakan guna mengidentifikasi, melacak, ataupun merujuk kepada individu tertentu secara spesifik³. SAFEnet juga mengklasifikasikan jenis-jenis data pribadi, pada tabel sebagai berikut⁴.

Tabel 1 : Jenis-Jenis Data Pribadi

TIPE DATA PRIBADI	JENIS DATA PRIBADI
Nama	Nama Lengkap, Nama Semasa Kecil, Nama Ibu, Alias
Nomor Identitas Pribadi	Nomor Induk Kependudukan (NIK), Nomor Pokok Wajib Pajak (NPWP), Surat Izin Mengemudi (SIM), Nomor Paspor, Plat Nomor Kendaraan, Nomor Kartu Anggota Rumah Sakit, Rekening Bank, Nomor Kartu Debit/Kredit
Alamat Pribadi	Alamat Rumah (Fisik), Alamat Surat Elektronik (<i>E-Mail</i>)
Nomor Kontak Personal	Ponsel Pribadi, Telepon Rumah
Karakteristik Personal	Gambar Fotografik (Utamanya atas wajah atau bagian lain yang menunjukkan karakteristik yang

³ Ellen Kusuma dan Nenden Sekar Arum, 2019, *Memahami dan Menyikapi Kekerasan Berbasis Gender Online*, SAFEnet, Bali, h. 11.

⁴ *Ibid*, h. 12.

	dapat dikaitkan pada seseorang), Sidik Jari, Tulisan Tangan
Data Biometrik	Pindai/Scan retina, Tanda Suara (<i>Voice Signature</i>), Sidik Jari, Geometri Wajah
Informasi Atas Properti Pribadi	Nomor Kendaraan, Akta Tanah dan Bangunan
Informasi Aset Teknologi	Alamat <i>Internet Protocol (IP address)</i> atau alamat <i>Media Access Control (MAC Address)</i> yang secara konsisten terhubung pada satu individu tertentu
Lainnya	Tanggal dan Tempat Lahir, Nomor Telepon Bisnis, Alamat Surat Elektronik (<i>E-Mail</i>) atau Surat Menyurat untuk keperluan Bisnis, Ras, Agama, Indikator Geografis, serta informasi terkait Pekerjaan, Kesehatan, Edukasi, atau Finansial.

Sumber : SAFEnet

Selain jenis dan tipe data pribadi sebagaimana dipaparkan diatas, data pribadi juga termasuk data-data perseorangan sebagaimana diatur dalam Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, khususnya pada Angka 12 Pasal 58 ayat (2), yang menyatakan : “Data perseorangan meliputi:

- a. nomor KK (Kartu Keluarga);
- b. NIK (Nomor Induk Kependudukan);

- c. nama lengkap;
- d. jenis kelamin;
- e. tempat lahir;
- f. tanggal/bulan/tahun lahir;
- g. golongan darah;
- h. agama/kepercayaan;
- i. status perkawinan;
- j. status hubungan dalam keluarga;
- k. cacat fisik dan/atau mental;
- l. pendidikan terakhir;
- m. jenis pekerjaan;
- n. NIK ibu kandung;
- o. nama ibu kandung;
- p. NIK ayah;
- q. nama ayah;
- r. alamat sebelumnya;
- s. alamat sekarang;
- t. kepemilikan akta kelahiran/surat kenal lahir;
- u. nomor akta kelahiran/nomor surat kenal lahir;
- v. kepemilikan akta perkawinan/buku nikah;
- w. nomor akta perkawinan/buku nikah;
- x. tanggal perkawinan;
- y. kepemilikan akta perceraian;

- z. nomor akta perceraian/surat cerai;
- aa. tanggal perceraian;
- bb. sidik jari;
- cc. iris mata;
- dd. tanda tangan; dan
- ee. elemen data lainnya yang merupakan aib seseorang”.

Permasalahan yang kerap muncul terkait data pribadi ini ialah kebocoran data pribadi, dimana seperti yang sudah dipaparkan sebelumnya, bahwa data pribadi yang bocor/tidak terlindungi dengan baik, mengancam hak atas privasi pemilik data pribadi, bahkan data pribadi tersebut sangat rentan untuk disalahgunakan, baik disalahgunakan di dalam sistem elektronik itu sendiri maupun pada sistem non-elektronik, yang mana tentunya sangat berbahaya dan merugikan bagi pemilik data pribadi. Masalah kebocoran data pribadi belakangan marak terjadi di Indonesia. Dilansir dari Tempo⁵, setidaknya ada 6 (enam) kasus kebocoran data pribadi yang menjadi perbincangan hangat di tengah masyarakat, yaitu kebocoran data pribadi di Sistem Kesehatan Elektronik milik Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan) yang terjadi pada Mei 2021, kebocoran data pribadi di Sistem Keuangan Elektronik yakni Cermati pada akhir tahun 2020, kebocoran data pribadi di Sistem Perdagangan Elektronik Lazada pada akhir tahun 2020, kebocoran data pribadi Sistem Keuangan/Perbankan yakni Bank Rakyat Indonesia (BRI) *Life* pada Juli

⁵ Caesar Akbar, 2021, “6 Kasus Kebocoran Data Pribadi di Indonesia”, Artikel Berita Dalam Jaringan, (Diakses 25 Agustus 2022), tautan : <https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>.

2021, kebocoran data pribadi di Sistem Perdagangan Elektronik yakni Tokopedia pada Mei 2020, serta kebocoran data pribadi di Sistem Elektronik milik Penyelenggaran Pemilihan Umum yakni Komisi Pemilihan Umum Republik Indonesia (KPU RI) pada Mei 2020.

Hingga awal Penelitian Skripsi ini dilaksanakan, ada beberapa kasus kebocoran data pribadi yang tengah hangat diperbincangkan masyarakat, yaitu kasus kebocoran data pribadi pelanggan penyedia jasa layanan Internet milik Badan Usaha Milik Negara (BUMN) yaitu PT. Telkom Indonesia, khususnya pada anak usahanya yakni IndiHome pada 21 Agustus 2022, dimana data-data yang mengalami kebocoran tersebut dijual melalui forum *breached.to*.⁶ Serta, kasus terbaru yang paling banyak jadi sorotan masyarakat pada September 2022, yaitu peretasan yang dilakukan oleh peretas dengan nama samaran “*Bjorka*”, yang menyebarkan data pribadi tokoh-tokoh penyelenggara negara seperti data pribadi Ketua Dewan Perwakilan Rakyat Republik Indonesia Puan Maharani, data pribadi Menteri Koordinator Maritim dan Investasi Republik Indonesia Luhut Binsar Pandjaitan, bahkan data pribadi Menteri Komunikasi dan Informatika Republik Indonesia Johnny Gerard Plate⁷.

Perlu diketahui bahwa, lembaga/perusahaan yang mengalami kebocoran data pribadi tersebut memberikan layanannya ke seluruh wilayah Republik

⁶ Intan Rakhmayanti Dewi, 2022, “*Data Indihome Bocor dari Browsing History, Ini kata Telkom*”, Artikel Berita Dalam Jaringan, (Diakses 13 September 2022), tautan : <https://www.cnbcindonesia.com/tech/20220822171913-37-365689/data-indihome-bocor-dari-browsing-history-ini-kata-telkom>.

⁷ CNN Indonesia, 2022, “*Serangan Bjorka ke Puan hingga Luhut Masuk Kategori Doxing, Apa Itu?*”, Artikel Berita Dalam Jaringan, (Diakses 13 September 2022), tautan : <https://www.cnnindonesia.com/teknologi/20220912141823-192-846671/serangan-bjorka-ke-puan-hingga-luhut-masuk-kategori-doxing-apa-itu>.

Indonesia, termasuk di Kota Pontianak, yang artinya data pribadi masyarakat Kota Pontianak juga mengalami kebocoran, sehingga rawan untuk disalahgunakan. Lebih lanjut, masyarakat, tak terkecuali masyarakat di Kota Pontianak pastinya pernah menerima pesan baik dari layanan pesan singkat (*short message service*) maupun melalui layanan obrolan (*chat*) dari nomor ponsel yang tidak dikenal yang entah darimana menemukan nomor ponsel masyarakat, yang isinya menawarkan layanan-layanan ilegal seperti judi daring (*online*), menawarkan hadiah tertentu dengan syarat tertentu, memberikan tautan (*link*) penipuan, dan lain-lain yang tentunya mengganggu privasi masyarakat dan rawan menimbulkan kerugian bagi masyarakat apabila masyarakat tidak berhati-hati dan/atau tidak memiliki pengetahuan yang cukup dalam menjaga keamanan data pribadinya.

Bahwasannya, yang menjadi alasan utama Peneliti mengambil topik data pribadi untuk diangkat ke dalam Penelitian Hukum (Skripsi) ialah, pada September 2021 lalu, ada kasus penyebarluasan data pribadi di Kota Pontianak. Adapun data-data pribadi tersebut disebarluaskan melalui *Short Message Service* (SMS) dan *WhatsApp* kepada kontak-kontak yang ada di ponsel pemilik data pribadi, yang mana Peneliti menjadi salah satu kontak yang menerima data pribadi yang disebarluaskan tersebut. Hal tersebut yang membuat Peneliti tertarik untuk menelusuri bagaimana perlindungan data pribadi dilaksanakan, khususnya di Kota Pontianak.

Adapun bentuk-bentuk penyalahgunaan data pribadi yang bocor, setidaknya sebagai berikut⁸.

1. Data pribadi yang bocor bisa dimanfaatkan untuk membobol rekening keuangan seseorang. Data pribadi yang bocor tersebut dimanfaatkan untuk melakukan proses verifikasi layanan keuangan, sehingga layanan keuangan pemilik data pribadi yang bocor dapat diakses oleh pembobol dan dapat menimbulkan kerugian materil bagi pemilik data pribadi yang bocor tersebut.
2. Penyalahgunaan data pribadi seseorang untuk melakukan pinjaman daring/*online* (pinjol). Adapun peminjaman uang ini dilakukan orang lain yang berpura-pura sebagai pemilik data pribadi yang sebenarnya. Pemilik data pribadi (korban) bahkan tidak mengetahui soal pinjaman tersebut, yang mana Pemilik data pribadi yang sebenarnya malah menjadi pihak yang diteror untuk pengembalian uang dan bunga atas pinjaman yang tidak dilakukannya.
3. Data pribadi yang bocor bisa digunakan oleh pihak yang tidak bertanggungjawab untuk memetakan profil pemilik data pribadi, misalnya untuk keperluan politik tertentu ataupun iklan di media sosial.
4. Data pribadi yang bocor bisa digunakan oleh pihak yang tidak bertanggungjawab untuk meretas akun sosial media pemilik data pribadi, sehingga akun media sosial tersebut berpotensi untuk disalahgunakan bahkan dapat dijadikan sebagai media untuk menipu orang lain ataupun bentuk kejahatan lainnya.

⁸ Adyaksa Vidi, 2021, “4 Risiko Kebocoran Data Pribadi dan Cara Mengantisipasinya dengan Mudah”, Artikel Berita Dalam Jaringan. (Diakses 26 Agustus 2022), tautan : <https://www.liputan6.com/cek-fakta/read/4645011/4-risiko-kebocoran-data-pribadi-dan-cara-mengantisipasinya-dengan-mudah>.

Selain bentuk-bentuk penyalahgunaan data pribadi sebagaimana dipaparkan diatas, sebenarnya masih banyak lagi bentuk penyalahgunaan data pribadi yang tentunya melanggar hak atas privasi maupun keamanan pemilik data pribadi, salah satunya ialah *doxing*. *Doxing* ialah tindakan mempublikasikan/menyebarkan data pribadi milik orang lain ke dalam jaringan (internet) tanpa izin, yang mana dapat berupa foto, nomor ponsel, alamat rumah maupun data pribadi lainnya⁹, yang tujuannya untuk pemaksaan kehendak, memperlakukan secara daring (*online*), pemerasan, bahkan untuk main hakim sendiri maupun tujuan lainnya yang mengganggu hak atas privasi serta keamanan bagi pemilik data pribadi yang data pribadinya dipublikasikan/disebarluaskan tanpa izin¹⁰.

Dalam rangka memberikan perlindungan terhadap data pribadi dan/atau mengisi kekosongan hukum terkait belum adanya pengaturan terhadap perlindungan data pribadi, yang mana sebelumnya secara yuridis belum diatur secara tegas dalam Peraturan Perundang-Undangan, Pemerintah melalui Kementerian Komunikasi dan Informatika Republik Indonesia sebenarnya sudah menerbitkan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

⁹ Abu Hasan Banimal, Damar Juniarto dan Ika Ningtyas, 2020, *Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia*, SAFE-net, Bali, h. 1.

¹⁰ Alvana Noor Fariza, 2021, “Kenali apa Itu Doxing Serta Tips Mencegah Kejahatan Siber”, Artikel Dalam Jaringan. (Diakses 1 September 2022), tautan : <https://www.sekawanmedia.co.id/blog/apa-itu-doxing/>.

Diharapkan, dengan adanya Peraturan Hukum tersebut, dapat memberikan kepastian terhadap perlindungan data pribadi yang sebelumnya belum ada regulasinya. Cakupan dari perlindungan data pribadi ini diatur pada Pasal 2 ayat (1) Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, yang menyatakan “Perlindungan Data Pribadi dalam Sistem Elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi”.

Namun, meskipun Peraturan Hukum ini sudah diundangkan dan dilaksanakan, nyatanya perlindungan terhadap data pribadi di Indonesia secara umum, dan di Kota Pontianak secara khusus, masih belum berjalan dengan optimal sebagaimana contoh kasus yang telah dipaparkan sebelumnya.

Berdasarkan pemaparan latar belakang permasalahan diatas, maka Peneliti merasa tertarik untuk memberikan perhatian lebih terhadap permasalahan tersebut, dengan mengangkatnya menjadi suatu Penelitian Hukum (Skripsi) dengan Judul **“PELAKSANAAN PERLINDUNGAN DATA PRIBADI DALAM SISTEM ELEKTRONIK BERDASARKAN KETENTUAN PASAL 2 AYAT (1) PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA NOMOR 20 TAHUN 2016 TENTANG PERLINDUNGAN DATA PRIBADI DALAM SISTEM ELEKTRONIK (STUDI DI KOTA PONTIANAK)”**.

B. Rumusan Masalah

Rumusan masalah dalam suatu penelitian menjadi bagian yang sangat penting, termasuk bagi penelitian hukum. Hal ini karena, setiap penelitian pasti bermula dari timbulnya permasalahan, dalam hal ini tentunya permasalahan hukum. Rumusan masalah dalam penelitian hukum ialah awal permulaan dan menjadi satu-satunya alasan mengapa suatu penelitian hukum harus dilaksanakan¹¹. Artinya bahwa, rumusan masalah ialah suatu hal yang belum di ketahui jawabannya dan sesuatu yang masih mengandung berbagai pertanyaan sehingga memancing niat peneliti untuk mencari informasi dan data yang akurat dan untuk menemukan jawaban atas permasalahan, dalam hal ini permasalahan hukum tersebut.

Oleh sebab itu, berdasarkan latar belakang masalah yang dipaparkan sebelumnya beserta penjelasan diatas, maka penelitian ini dilaksanakan atas dasar rumusan masalah berikut. “Mengapa data pribadi dalam sistem elektronik di Kota Pontianak belum sepenuhnya mendapatkan perlindungan berdasarkan ketentuan Pasal 2 Ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik ?”.

C. Tujuan Penelitian

Suatu penelitian (*research*), tak terkecuali penelitian hukum (*legal research*), tentunya memiliki tujuan yang hendak dicapai. Tujuan penelitian ini menggambarkan arah dan/atau guna menegaskan dengan jelas mengenai apa

¹¹ Bachtiar, 2018, *Metode Penelitian Hukum*, UNPAM PRESS, Tangerang, h. 115.

yang hendak dicapai dan/atau dituju dengan diadakannya suatu penelitian¹². Untuk mahasiswa/i jurusan ilmu hukum, tujuan penelitian hukum ialah bermaksud untuk menemukan jawaban atas pertanyaan yang diajukan dalam rumusan masalah pada suatu penelitian hukum. Karenanya, pada setiap kegiatan penelitian hukum, tujuan penelitian hukum ialah untuk menjelaskan maksud dari kegiatan penelitian hukum yang dilakukan tersebut¹³.

Oleh sebab itu, berdasarkan rumusan masalah yang dipaparkan sebelumnya beserta penjelasan diatas, maka penelitian ini dilaksanakan guna mencapai tujuan berikut.

1. Mendapatkan informasi serta menganalisa pelaksanaan perlindungan data pribadi di Kota Pontianak, khususnya berdasarkan ketentuan Pasal 2 Ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
2. Mengetahui faktor-faktor yang mempengaruhi pelaksanaan perlindungan data pribadi di Kota Pontianak beserta penyebab data pribadi di Kota Pontianak belum sepenuhnya mendapatkan perlindungan, khususnya berdasarkan ketentuan Pasal 2 Ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
3. Mengetahui upaya yang dapat dilakukan guna memberikan perlindungan terhadap data pribadi, agar pelaksanaan perlindungan data pribadi, khususnya di Kota Pontianak, dapat berjalan dengan lebih baik dan optimal.

¹² M. Syamsudin, 2007, *Operasionalisasi Penelitian Hukum*, RajaGrafindo Persada, Jakarta, h. 84.

¹³ *Ibid*, h. 121.

D. Manfaat Penelitian

Peneliti berharap dengan diadakannya penelitian hukum ini, dapat memberikan manfaat, baik manfaat teoritis maupun manfaat praktis, sebagai berikut.

1. Manfaat secara teoritis (bagi pengembangan ilmu pengetahuan), diharapkan penelitian hukum ini dapat menjadi referensi bagi penelitian yang sejenis dan/atau penelitian dalam ruang lingkup yang hampir sama, dalam hal ini terkait data pribadi yang pada era digital saat ini, menjadi isu yang sangat penting. Hal ini mengingat perkembangan teknologi informasi dan komunikasi yang begitu cepat menuntut ilmu hukum juga harus mampu mengikuti perkembangan tersebut, supaya ilmu hukum tetap relevan di setiap masanya dan mampu menyelesaikan permasalahan hukum yang terjadi di dalam kehidupan masyarakat, dalam hal ini permasalahan hukum yang timbul akibat perkembangan teknologi informasi dan komunikasi, khususnya berkenaan dengan permasalahan hukum yang muncul terkait data pribadi.
2. Manfaat praktis (pemecahan terhadap suatu masalah yang terjadi), diharapkan penelitian hukum ini dapat memberikan solusi dan/atau sebagai alternatif penyelesaian masalah hukum yang terjadi, dalam hal ini permasalahan terkait data pribadi dalam sistem elektronik di Kota Pontianak yang masih belum sepenuhnya mendapatkan perlindungan dengan baik dan optimal, terutama berdasarkan Pasal 2 Ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

E. Kerangka Pemikiran

1. Tinjauan Pustaka

Mendefinisikan hukum menjadi sesuatu yang baku sangatlah sulit, hal ini terbukti karena sejak dahulu hingga saat ini, para ahli di bidang hukum, belum mencapai suatu kesepakatan tentang definisi baku mengenai hukum itu sendiri. Namun yang pasti, hukum itu dibuat dalam rangka memenuhi kepentingan masyarakat, yakni guna terpenuhinya rasa keadilan, keamanan, kedamaian, keseimbangan dan kesejahteraan di dalam kehidupan masyarakat¹⁴.

Secara umum di Indonesia, kajian ilmu hukum dibagi menjadi 3 (tiga) bagian, yakni hukum tata negara, hukum pidana serta hukum perdata, yang pada hakikatnya sama-sama guna memenuhi kepentingan masyarakat itu tadi. Secara khusus berbicara mengenai hukum tata negara, objek kajiannya diantaranya meliputi ilmu pengetahuan dan teknologi serta informasi dan telematika¹⁵.

Artinya bahwa, perlindungan data pribadi dalam sistem elektronik, masuk kedalam ruang lingkup kajian dari hukum tata negara, terutama dalam rangka memenuhi kepentingan masyarakat atas rasa keamanan dan hak atas privasi pada masa berkembang pesatnya kemajuan teknologi informasi dan komunikasi (era digital) saat ini.

¹⁴ Subiharta, *Moralitas Hukum Dalam Hukum Praksis Sebagai Suatu Keutamaan (Legal Morality In Practical Law As A Virtue)*, Jurnal Hukum dan Peradilan, Vol. 4, No. 3 (November 2015), h. 387.

¹⁵ Jimly Asshiddiqie, 2006, *Pengantar Ilmu Hukum Tata Negara*, Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi Republik Indonesia, Jakarta, h. 86-87.

Pemenuhan kepentingan masyarakat atas rasa keamanan dan hak atas privasi di era digital ini, merupakan pemenuhan atas hak asasi manusia. Hal ini karena, perlindungan terhadap data pribadi sebagai pemenuhan kepentingan masyarakat atas rasa keamanan dan hak atas privasi di era digital, merupakan perwujudan pengakuan dan perlindungan atas hak-hak dasar manusia, sebagaimana tertuang di dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Setelah Amandemen), khususnya Pasal 28G ayat (1) yang menyatakan “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Berbicara mengenai pemenuhan rasa keamanan, khususnya keamanan digital di era perkembangan teknologi informasi dan komunikasi saat ini, dapat dipahami sebagai berikut. Bahwasannya, keamanan digital dapat dipahami sebagai suatu proses guna memastikan penggunaan layanan-layanan digital, baik secara dalam jaringan (*daring/online*) maupun secara luar jaringan (*luring/offline*), dapat dilakukan secara aman dan nyaman, yang mana tidak terbatas untuk mengamankan data-data umum yang kita miliki, melainkan juga melindungi data pribadi yang sifatnya rahasia¹⁶. Konsep keamanan digital ini juga pada hakikatnya untuk memberikan rasa aman dan perlindungan dari segala bentuk kejahatan, baik kejahatan dalam jaringan

¹⁶ Gilang Jiwana Adikara *et.al.*, 2021, *Aman Bermedia Digital*, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia, Jakarta, h. 3-4.

(*daring/online*) maupun kejahatan di luar jaringan (*luring/offline*), yang saat ini dikenal sebagai kejahatan siber.

Kemajuan teknologi informasi dan komunikasi yang saat ini kita rasakan, dikarenakan semakin pesatnya perkembangan alat, perangkat, serta sarana dan prasarana telekomunikasi yang memungkinkan arus informasi dan komunikasi mencakup seluruh dunia tanpa mengenal batas waktu dan tempat. Definisi telekomunikasi secara yuridis ialah sebagaimana ketentuan Pasal 1 angka 1 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, menyatakan “Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari hasil informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya”.

Jaringan internet sebagai salah satu sistem dalam telekomunikasi, tak bisa dipungkiri merupakan sistem yang paling berpengaruh dalam arus kemajuan teknologi informasi dan komunikasi yang saat ini kita rasakan. Sederhananya, internet (dalam bahasa Inggris : *Interconnection-networking*) ialah suatu sistem global pada jaringan komputer yang saling menghubungkan antara satu sama lain di seluruh penjuru dunia dengan menggunakan standar *Internet Protocol Suite*¹⁷. Hadirnya internet telah membangun pengetahuan, bahwa ada dunia yang memungkinkan terjadinya interaksi yang tanpa batas. Adapun dunia di dalam internet yang memungkinkan interaksi tanpa batas tersebut, disebut dengan dunia maya (*cyberspace*).

¹⁷ Alcianno Ghobadi Gani, *Sejarah Dan Perkembangan Internet Di Indonesia*, Jurnal Mitra Manajemen, Vol. 5, No. 2 (2013), h. 68.

Membahas perlindungan data pribadi dalam sistem elektronik, khususnya dari sudut pandang ilmu hukum, tentunya tidak dapat dilepaskan dari teori-teori hukum itu sendiri. Menurut Prof. Mr. Roeslan Saleh, teori hukum adalah salah satu cabang dari ilmu pengetahuan hukum yang mempelajari berbagai aspek, baik teoritis maupun praktis dari hukum positif tertentu secara tersendiri dan pada keseluruhannya secara interdisipliner, yang tujuannya ialah guna memperoleh penjelasan dan pengetahuan yang lebih baik, lebih jelas, serta lebih mendasar mengenai hukum positif yang bersangkutan¹⁸.

Menurut sudut pandang Peneliti, terdapat 3 (tiga) teori hukum yang sangat tepat dalam membahas dan mengulas topik perlindungan data pribadi dalam sistem elektronik, guna menemukan penjelasan dan pengetahuan yang lebih baik, lebih jelas, serta lebih mendasar mengenai perlindungan data pribadi dalam sistem elektronik. Teori hukum tersebut ialah teori perlindungan hukum, teori hukum responsif, dan teori kewenangan.

Teori perlindungan hukum adalah perkembangan dari konsep perlindungan dan pengakuan terhadap hak asasi manusia (HAM) yang tumbuh dan berkembang pada abad ke-19 (sembilan belas). Arah dari konsep tentang perlindungan dan pengakuan terhadap hak asasi manusia ini ialah dengan adanya pembatasan dan peletakan kewajiban kepada pemerintah dan

¹⁸ Muchyar Yara, *Teori Hukum: (Suatu Tinjauan Singkat tentang Posisi, Sejarah Perkembangan dan Ruang Lingkupnya)*, Jurnal Hukum dan Pembangunan, Vol. 28, No. 1-3 (Januari-Juni 1998), h. 3.

masyarakat¹⁹. Perlindungan hukum dibagi menjadi 2 (dua) jenis, yaitu perlindungan hukum preventif (berorientasi pada pencegahan terhadap potensi pelanggaran hukum) dan represif (berorientasi pada penindakan terhadap pelanggaran hukum). Dengan kata lain, perlindungan hukum preventif memiliki tujuan untuk mencegah terjadinya konflik/sengketa, sedangkan perlindungan hukum represif yaitu perlindungan hukum yang bertujuan bertujuan untuk menyelesaikan sengketa²⁰.

Selanjutnya, teori hukum responsif, yaitu teori atau model yang dikemukakan oleh Nonet-Selznick²¹. Teori hukum responsif sudah menjadi perhatian yang sangat serius dalam teori hukum modern, paradigma dalam teori hukum responsif ini ialah untuk membuat hukum lebih responsif terhadap kebutuhan sosial di masyarakat serta untuk memperhitungkan secara lebih cerdas dan lebih lengkap tentang fakta sosial yang menjadi landasan dan tujuan terhadap penerapan serta pelaksanaan hukum²².

Terakhir, teori kewenangan. Istilah kewenangan atau wewenang sering disamakan dengan istilah dalam bahasa Belanda, yakni “*bevoegdheid*” yang berarti berkuasa atau wewenang. Kewenangan merupakan bagian yang sangat penting dalam Hukum Administrasi Negara, karena pemerintah baru dapat menjalankan fungsinya atas dasar wewenang yang dimilikinya²³.

¹⁹ Luthvi Febryka Nola, *Upaya Pelindungan Hukum Secara Terpadu Bagi Tenaga Kerja Indonesia (TKI)*, Jurnal Negara Hukum, Vol. 7, No. 1 (Juni 2016), h. 39-40.

²⁰ *Ibid.*

²¹ Sulaiman, *Hukum Responsif: Hukum Sebagai Institusi Sosial Melayani Kebutuhan Sosial Dalam Masa Transisi (Responsive Law: Law as a Social Institutions to Service of Social Need in Transition)*, Jurnal Hukum Samudera Keadilan, Vol. 9, No. 2 (Agustus 2016), h. 2.

²² *Ibid.*, h. 2-3.

²³ Yusri Munaf, 2016, *Hukum Administrasi Negara*, Marpoyan Tujuh Publishing, Pekanbaru, h. 52.

2. Kerangka Konsep

Perlindungan data pribadi dalam sistem elektronik, di Republik Indonesia secara umum, dan di Kota Pontianak secara khusus, masih belum berjalan dengan optimal sebagaimana telah digambarkan pada latar belakang masalah, meskipun sebenarnya payung hukum dalam perlindungan data pribadi dalam sistem elektronik sudah ada, yaitu Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo 20/2016).

Selain itu juga tersebar di beberapa peraturan perundang-undangan lainnya, meskipun tidak spesifik ataupun tidak secara keseluruhan membahas tentang perlindungan data pribadi, sebagaimana sudah dipaparkan sebelumnya, seperti terdapat pada Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU 36/1999), Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Adminduk), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019).

Oleh karena itu, dalam rangka memberikan dasar hukum yang lebih kuat, efektif dan komprehensif terkait Perlindungan Data Pribadi, Pemerintah dan Dewan Perwakilan Rakyat melalui rapat paripurna yang diselenggarakan pada 20 September 2022 lalu, telah mengesahkan Rancangan Undang-Undang Pelindungan Data Pribadi menjadi Undang-Undang. Undang-Undang Pelindungan Data Pribadi tersebut disahkan oleh Presiden Republik Indonesia, Joko Widodo dan Diundangkan oleh Menteri Sekretaris Negara Republik Indonesia, Pratikno, pada 17 Oktober 2022, dengan nomor dan/atau nama Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

Oleh karenanya, menarik untuk ditunggu dan diamati bersama, apakah UU PDP ini mampu menjawab persoalan Perlindungan Data Pribadi yang masih belum berjalan dengan optimal, baik di Indonesia secara umum, dan di Kota Pontianak secara khusus. UU PDP, jika dibandingkan dengan UU ITE, PP 71/2019 dan/atau Permenkominfo 20/2016 memiliki kelebihan tersendiri dari segi regulasi dalam upaya memberikan Perlindungan terhadap Data Pribadi. Kelebihan tersebut diantaranya, sebagai berikut.

Pertama, UU PDP mengatur secara tegas subjek hukum yang terikat dalam Pelindungan Data Pribadi, sebagaimana diatur pada Pasal 2, yang intinya mengikat Setiap Orang, Badan Publik, dan Organisasi Internasional, baik di Indonesia maupun Luar Negeri, khususnya yang melakukan perbuatan hukum terkait data pribadi di Indonesia, yang mana hal ini tidak termuat dalam UU ITE, PP 71/2019 dan/atau Permenkominfo 20/2016. Hal

ini menjadi penting, mengingat bahwa pelaku kejahatan terhadap data pribadi, tidak hanya setiap orang dan/atau badan publik di Indonesia, namun juga bisa dari setiap orang dan/atau badan publik serta organisasi internasional di Luar Negeri.

Kedua, pada UU PDP, dipaparkan jenis-jenis data pribadi, sebagaimana diatur pada Pasal 4, yang mana jenis-jenis data pribadi ini tidak termuat dalam UU ITE, PP 71/2019 dan/atau Permenkominfo 20/2016. Hal ini menjadi penting, mengingat bahwa jika jenis data pribadi tidak diatur dengan jelas, dapat menimbulkan kerancuan dalam pelaksanaan perlindungan data pribadi, karena tidak jelasnya data-data apa saja yang diklasifikasikan sebagai data pribadi, sehingga bisa menyebabkan tidak terlindunginya suatu data pribadi karena tidak diklasifikasikan sebagai data pribadi.

Ketiga, UU PDP, mengatur Lembaga yang secara khusus memiliki wewenang terkait Pelindungan Data Pribadi di Indonesia, sebagaimana diatur pada BAB IX Kelembagaan, Pasal 58 – Pasal 61, yang mana hal ini juga tidak termuat dalam UU ITE, PP 71/2019 dan/atau Permenkominfo 20/2016. Hal ini menjadi sangat penting, karena selama ini, belum pernah ditegaskan secara jelas, Lembaga Negara mana yang berwenang dalam melaksanakan Perlindungan Data Pribadi, sehingga dalam prakteknya, Kementerian Komunikasi dan Informatika yang selama ini melaksanakan Perlindungan Data Pribadi, yang nyatanya belum efektif karena perlu Lembaga tersendiri yang tugas pokok dan fungsinya berfokus pada Perlindungan Data Pribadi.

Berdasarkan pemaparan-pemaparan tersebut, menurut Peneliti, dalam upaya untuk memberikan Perlindungan terhadap Data Pribadi, khususnya dari segi hukum, diperlukan adanya kesadaran dan keseriusan bersama semua pihak menyangkut Perlindungan Data Pribadi sebagai Perlindungan terhadap Hak Asasi Manusia, melalui pelaksanaan yang optimal dari semua Peraturan Perundang-Undangan yang berkaitan dengan Perlindungan Data Pribadi, khususnya UU PDP serta Permenkominfo 20/2016.

Selain itu, Peraturan Pelaksana/Turunan dari UU PDP khususnya, haruslah memuat hal-hal yang diperintahkan dan/atau memuat hal-hal yang memang belum/tidak dimuat dalam UU PDP, guna menutup celah-celah Pelanggaran dan/atau Penyalahgunaan terhadap Data Pribadi. Misalnya, dengan memperkuat fungsi pengawasan dan/atau penindakan oleh Pemerintah dalam rangka Perlindungan Data Pribadi, memperkuat peran Pemerintah dalam rangka memberikan edukasi kepada masyarakat terkait Perlindungan Data Pribadi, memperkuat keamanan siber dalam rangka Perlindungan Data Pribadi, serta melibatkan/memperkuat Peran Pemerintah Daerah dalam rangka Perlindungan Data Pribadi.

Hal-hal tersebut menjadi suatu rangkaian/kerangka konsep yang Peneliti ajukan kepada semua pihak yang terlibat dalam upaya Perlindungan Data Pribadi, guna memberikan Perlindungan terhadap Data Pribadi secara optimal, baik di Indonesia secara umum, dan Kota Pontianak secara khusus.

F. Metode Penelitian

1. Objek dan Lokasi Penelitian

Penelitian ini difokuskan terhadap data pribadi yang bersifat umum sebagai objek penelitiannya. Data pribadi yang bersifat umum tersebut, yaitu nama lengkap, jenis kelamin, agama/kepercayaan yang dianut, kewarganegaraan, serta data pribadi yang dikombinasikan untuk mengidentifikasi seseorang (data perseorangan yang bersifat umum yang merupakan data kependudukan, termasuk nomor ponsel/telepon serta alamat surat elektronik (*e-mail*) pribadi seseorang).

Penelitian terhadap data pribadi yang bersifat umum ini, dilaksanakan di Kota Pontianak, Provinsi Kalimantan Barat, dengan sasaran perolehan data penelitian yang berasal dari Pemerintah Kota Pontianak, khususnya Dinas-dinas terkait, yakni Dinas Komunikasi dan Informatika serta Dinas Kependudukan dan Pencatatan Sipil. Selain itu, sasaran perolehan data penelitian juga termasuk yang berasal dari Masyarakat Kota Pontianak, baik Masyarakat Kota Pontianak yang pernah menjadi korban penyebaran data pribadi serta masyarakat Kota Pontianak secara umum, guna memperoleh gambaran pelaksanaan perlindungan data pribadi di Kota Pontianak.

2. Jenis Penelitian

Secara umum, penelitian hukum dibagi dalam 2 (dua) jenis, yaitu penelitian hukum normatif dan penelitian hukum empiris. Adapun dalam penelitian ini, Peneliti menegaskan bahwa, jenis penelitian yang digunakan

ialah penelitian hukum empiris. Bahwasannya, penelitian hukum empiris atau penelitian hukum yuridis empiris merupakan jenis metodologi penelitian hukum yang dilakukan dengan cara mengkaji keadaan sebenarnya yang terjadi ditengah-tengah kehidupan masyarakat, yakni dengan mencari fakta-fakta yang berkaitan dengan permasalahan dalam suatu penelitian²⁴. Dalam penelitian ini, pendekatan penelitian hukum empiris digunakan untuk menemukan akar permasalahan dari segi empirik di tengah-tengah kehidupan masyarakat Kota Pontianak terkait dengan belum terlindunginya data pribadi dalam sistem elektronik.

3. Sifat Penelitian

Menurut sifatnya, secara umum penelitian hukum empiris dibedakan menjadi 3 (tiga), yaitu penelitian hukum yang sifatnya eksploratif, penelitian hukum yang sifatnya deskriptif, serta penelitian hukum yang sifatnya eksplanatoris. Dalam penelitian ini, Peneliti menegaskan bahwa, penelitian hukum yang dilakukan bersifat eksploratif. Penelitian hukum yang bersifat eksploratif ini dilakukan terhadap pengetahuan yang masih baru, yang mana data-data, teori-teori serta informasi tentang ketentuan atau norma-norma terkait topik/tema yang diangkat tersebut masih belum ada, ataupun jikalau ada, masih relatif sedikit dan terbatas. Konsekuensi logis dari belum adanya atau sedikit dan terbatasnya data-data, teori-teori, informasi serta norma-

²⁴ Kornelius Benuf dan Muhamad Azhar, *Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer*, Jurnal Gema Keadilan, Vol. 7, No. 1, (Juni 2020), h. 24.

norma terkait topik/tema yang diangkat dalam penelitian hukum tersebut ialah tidak diperlukan hipotesis (jawaban sementara) dalam suatu penelitian hukum yang dilakukan. Topik terkait perlindungan data pribadi merupakan pengetahuan yang bisa dibilang masih baru, terutama di Indonesia, sehingga ketersediaan data-data, teori-teori, informasi serta norma-norma terkait masih sangat sedikit dan terbatas. Hal ini karena, seperti yang telah dijelaskan sebelumnya pada latar belakang masalah, kemajuan teknologi informasi dan komunikasi di era digital saat ini, membawa resiko tersendiri bagi pelaksanaan perlindungan data pribadi.

4. Jenis dan Sumber Data

Dalam penelitian hukum empiris, terdapat 2 (dua) jenis data, yaitu Data Primer dan Data Sekunder, dengan sumber data sebagai berikut.

a. Data Primer

Data Primer adalah data yang dikumpulkan Peneliti dari penelitian yang dilakukan di lapangan, yakni suatu data yang didapatkan langsung dari sumber pertama di lapangan, baik yang berasal dari responden dan/atau berasal dari informan, yang berkaitan dengan pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak.

b. Data Sekunder

Data Sekunder adalah data yang dikumpulkan Peneliti dari penelitian kepustakaan, yakni suatu data yang tidak diperoleh secara

langsung dari sumber pertamanya, dengan kata lain bersumber dari data-data yang sudah terdokumenkan dalam bentuk bahan-bahan hukum, baik berupa bahan hukum primer serta bahan hukum sekunder, yang berkaitan dengan pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak.

5. Teknik Pengumpulan Data

Dalam penelitian hukum empiris, dikenal teknik-teknik guna pengumpulan data, yakni Studi Dokumen, Wawancara, Observasi, dan Penyebaran Angket/Kuisisioner. Namun, dalam penelitian hukum empiris ini, Peneliti menggunakan teknik-teknik, sebagai berikut.

a. Teknik Studi Dokumen (Kepustakaan)

Teknik Studi Dokumen (Kepustakaan) ini dilakukan terhadap bahan-bahan hukum yang relevan dengan topik permasalahan penelitian hukum yang diteliti, dalam hal ini terkait dengan pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak.

b. Teknik Wawancara (*Interview*)

Teknik Wawancara (*Interview*) ini merupakan salah satu teknik yang paling lazim dan sering digunakan pada penelitian hukum empiris. Dalam kegiatan penelitian hukum empiris, wawancara dilakukan terhadap narasumber yang relevan dan/atau kompeten serta pertanyaannya dirancang untuk memperoleh jawaban-jawaban yang

relevan dengan topik permasalahan penelitian hukum yang diteliti, dalam hal ini terkait dengan pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak.

c. Teknik Pengamatan (Observasi)

Teknik Pengamatan (Observasi) dapat dibedakan menjadi 2 (Dua), yaitu Teknik Pengamatan Langsung dan Teknik Pengamatan Tidak Langsung. Dalam penelitian hukum yang dilakukan ini, Peneliti menggunakan Teknik Pengamatan Langsung, dimana Peneliti melakukan pengamatan secara langsung dan tanpa alat terhadap gejala-gejala subjek yang diteliti, dalam hal ini guna mengidentifikasi pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak.

6. Populasi dan Sampel

Populasi dapat dimaknai sebagai keseluruhan ataupun himpunan objek dengan ciri yang sama. Adapun populasi dapat berupa himpunan orang, benda (hidup atau mati), kasus-kasus, kejadian, waktu, ataupun tempat, dengan sifat atau ciri yang sama²⁵. Sedangkan sampel ialah himpunan bagian atau sebagian dari populasi. Pada suatu penelitian, tak terkecuali penelitian hukum, umumnya observasi tidak dilakukan terhadap populasi, namun dilakukan terhadap sampel²⁶.

²⁵ Bambang Sunggono, 2011, *Metode Penelitian Hukum*, PT RajaGrafindo Persada, Jakarta, h. 118.

²⁶ *Ibid*, h. 119.

Pada penelitian hukum ini, Peneliti menentukan Populasi dan Sampel, sebagai berikut.

a. Populasi

Populasi pada penelitian hukum ini, terdiri dari :

1. Pemerintah Kota Pontianak;
2. Masyarakat Kota Pontianak.

b. Sampel

Sampel pada penelitian hukum ini, terdiri dari :

1. Kepala Dinas Komunikasi dan Informatika Kota Pontianak;
2. Kepala Dinas Kependudukan dan Pencatatan Sipil Kota Pontianak;
3. 1 Orang Masyarakat Korban Penyebaran Data Pribadi di Kota Pontianak;
4. 30 Orang Masyarakat Kota Pontianak Secara Umum.

7. Analisis Data

Pada penelitian hukum empiris, terdapat 2 (dua) model analisis data, yaitu Analisis Data Kualitatif dan Analisis Data Kuantitatif. Dalam penelitian hukum yang dilakukan ini, Peneliti menggunakan model Analisis Data Kualitatif. Model Analisis Data Kualitatif ini diterapkan pada suatu penelitian hukum yang bersifat Eksploratif dan Deskriptif. Telah ditegaskan sebelumnya, bahwa penelitian hukum yang dilakukan ini (pelaksanaan perlindungan data pribadi dalam sistem elektronik, khususnya di Kota Pontianak) bersifat Eksploratif, sehingga relevan dengan model Analisis Data Kualitatif.

Pada model Analisis Data Kualitatif ini pula, data yang dikumpulkan ialah data natural yang terdiri atas kata-kata dan kalimat (datanya sukar diukur dengan angka), sampel lebih bersifat Non-Probabilitas, serta pengumpulan data primer menggunakan pedoman wawancara dan/atau pengamatan (observasi).

