BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi merupakan hal yang sangat menguntungkan bagi kehidupan masyarakat saat ini. Keuntungan yang paling dapat dirasakan adalah kemudahan untuk berkomunikasi dengan orang lain dimanapun dan kapanpun. Selain kemudahan dalam berkomunikasi, keuntungan lain yang dapat dirasakan adalah kemudahan dalam mengakses segala macam informasi dalam berbagai bentuk karena adanya berbagai macam media sosial yang dapat memfasilitasi hal tersebut. Kemudahan dalam mengakses informasi memang telah menjadi sebuah keharusan bagi kita yang hidup dimasyarakat yang terus menerus mengalami perubahan. Dilihat dari permukaan, kemudahan dalam mengakses informasi memang memiliki pengaruh yang positif. Jika kita teliti lebih dalam lagi ada sisi negatif yang harus kita ketahui. Kemudahan dalam mengakses informasi tidak hanya berarti kemudahan untuk mengakses informasi yang memang telah kita tentukan sendiri untuk dipublikasikan, namun juga informasi pribadi kita yang bersifat rahasia dan tidak untuk dipublikasikan.

Setiap orang memang memiliki kebebasan untuk membagikan informasi apapun yang ia miliki selama informasi yang dibagikan tersebut tidak dimaksudkan untuk merugikan suatu pihak. Saat ini dengan segala kemudahan dalam proses pengaksesannya, batas antara informasi publik dengan informasi pribadi menjadi tidak jelas. Akibatnya, masyarakat pun tidak

bisa membedakan informasi seperti apa yang layak dan tidak layak untuk dibagikan dan diakses oleh khalayak umum. Batas yang kabur antara informasi yang layak dan tidak layak untuk dibagikan dan diakses tersebut tentu saja memunculkan ketidaknyamanan bagi masyarakat dan ketidakamanan informasi pribadi milik yang bersangkutan. Kemudahan dalam pengaksesan informasi ini menimbulkan privasi seseorang menjadi terancam dan memunculkan kemungkinan penyalahgunaan informasi pribadi tersebut yang dapat merugikan kepentingan pemilik informasi yang bersangkutan.

Penyebarluasan atau pemublikasian data pribadi atau yang lebih sering kita kenal dengan istilah *doxing* adalah sisi negatif dari kemudahan penyebaran informasi yang sering kita lupakan dan bahkan sering kita lakukan. Tindakan *doxing* sendiri sudah ada sejak tahun 1990-an atau sejak kemunculan *World Wide Web* (www). Tindakan *doxing* yang dilakukan oleh para peretas ini sejak awal ditujukan untuk menyebarluaskan data pribadi seseorang yang bersifat sangat rahasia tanpa izin dari pemilik informasi tersebut guna kepentingan pihak tertentu. Seiring dengan perkembangannya, tindakan *doxing* ini semakin mudah dilakukan karena saat ini banyak pusat penyimpanan data pribadi yang berbasis *online*. Jika pusat penyimpanan data pribadi tersebut tidak memiliki proteksi yang kuat, maka orang-orang pun akan semakin mudah untuk meretas sistem yang dimiliki.

Di masa yang modern seperti sekarang ini, tindakan *doxing* terkesan semakin dilumrahkan, terutama data yang tersebar adalah milik seseorang yang terkenal, seperti politikus, selebriti, dan berbagai tokoh masyarakat lainnya.

Masyarakat salah mengartikan bahwa karena seseorang tersebut merupakan tokoh masyarakat sehingga semua data yang dimilikinya sudah sewajarnya untuk diketahui. Padahal, terdapat data yang bersifat rahasia dan didapatkan tanpa sepengetahuan dan izin dari tokoh masyarakat yang bersangkutan. Selain tokoh masyarakat, orang-orang biasa yang dibuat 'terkenal' oleh masyarakat karena tindakan atau perilaku orang tersebut pun juga sering menjadi korban *doxing*. Orang-orang biasa yang dibuat 'terkenal' tersebut umumnya adalah para terduga dan/atau pelaku tindakan pelecehan seksual.

Seperti yang telah disebutkan di atas, setiap orang memiliki kebebasan dalam mengakses dan membagikan data dalam bentuk apapun selama tidak merugikan pihak-pihak tertentu. Dengan beragam informasi yang tersebar itu, umumnya yang selalu menarik perhatian publik adalah pengakuan dari korban tindakan pelecehan seksual ataupun orang terdekatnya yang diunggah ke media sosial. Maraknya unggahan mengenai pengakuan para korban tindakan pelecehan seksual ataupun orang terdekatnya ke media sosial disebabkan oleh beragam faktor. Faktor-faktor yang paling sering dijadikan alasan unggahan tersebut adalah yang pertama, masih kurangnya penegakan hukum terhadap tindakan pelecehan seksual; yang kedua, di media sosial si pengunggah dapat bersembunyi dibalik anonimitas sehingga identitas si pengunggah tersebut tidak dapat diketahui dan data pribadi milik korban tidak bocor ke publik.

Dengan anonimitas tersebut, para korban maupun orang terdekatnya dapat membagikan pengakuannya tanpa perlu takut identitasnya tersebar dan malah berbalik disalahkan oleh publik. Dalam pengakuan-pengakuan yang

diunggah biasanya disertai oleh hasil tangkapan layar percakapan antara korban dengan pelaku ataupun video tindakan pelecehan seksual yang dilakukan oleh pelaku tersebut identitas si pelaku hampir tidak pernah ditutup-tutupi, kesan yang diberikan pun agar seluruh dunia tahu bahwa orang tersebut telah melakukan suatu tindakan yang tercela. Perlu dipahami bahwa tujuan dari pengakuan yang diunggah memang untuk memberikan perhatian kepada tindakan pelecehan seksual yang telah dilakukan oleh pelaku agar keadilan dapat ditegakkan. Efek dari tidak ditutupinya identitas si pelaku itu yang perlu menjadi perhatian.

Efek bagi pelaku yang paling umum terjadi adalah tersebarnya data pribadi miliknya tanpa sepengetahuan dan izin dari yang bersangkutan. Jika unggahan pengakuan tersebut tidak mendapatkan perhatian yang cukup besar dari publik, kemungkinan data pribadi yang tersebar pun tidak terlalu krusial seperti nama, tempat dan tanggal lahir, hingga domisili si pelaku. Jika unggahan tersebut mendapatkan perhatian yang besar dari publik, kemungkinan data yang krusial yang dapat bocor ke publik pun juga semakin besar. Bahkan dalam beberapa kasus, data yang tersebar dapat meliputi alamat, nomor telepon pribadi, hingga histori studi dan data yang menyangkut keluarga si pelaku.

Tindakan *doxing* yang dilakukan terhadap pelaku tindakan pelecehan seksual ini banyak dilakukan dan dibenarkan oleh masyarakat dengan alasan bahwa hal tersebut merupakan wujud sanksi yang layak dijatuhkan bagi pelaku tindakan pelecehan seksual. Masyarakat tidak sadar bahwa tindakan yang

mereka lakukan juga merupakan suatu tindakan pelanggaran hukum. Efek dari tindakan tersebut juga tidak main-main, yang dapat terjadi adalah terbunuhnya karakter dari si pelaku itu sendiri. Bahkan, yang lebih bahaya lagi jika efek yang terjadi bisa sampai menimbulkan kerugian fisik yang diderita oleh pelaku tersebut.

Berdasarkan uraian di atas, dapat kita simpulkan bahwa tindakan *doxing* merupakakan suatu bentuk vigilantisme atau main hakim sendiri, Hal ini tentu saja bertentangan dengan prinsip negara hukum yang dianut oleh negara Indonesia. Di dalam negara hukum segala tindakan harus didasarkan oleh peraturan perundang-undangan yang berlaku dengan tujuan untuk menciptakan ketertiban umum. Jika hal ini tidak dilaksanakan, maka yang akan terjadi adalah *chaos* atau kekacauan dalam masyarakat. Peraturan perundang-undangan di Indonesia sendiri telah mengatur mengenai tindakan *doxing* ini untuk mencegah dan/atau menghukum pelaku tindakan kejahatan tersebut. Adanya anonimitas di dunia maya membuat penegakkannya mengalami kendala yang sepertinya tidak kunjung menemukan solusinya.

B. Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, maka dapat dirumuskan masalah yaitu bagaimanakah penegakan hukum terhadap perbuatan *doxing* yang korbannya adalah pelaku tindak pidana pelecehan seksual?

C. Tujuan Penelitian

Untuk mengetahui dan memahami apakah penegakkan hukum privasi di Indonesia sudah sesuai dengan peraturan perundang-undangan yang berlaku.

D. Manfaat Penelitian

Penelitian ini dilakukan dengan tujuan untuk memberikan manfaat sebagai berikut:

1. Manfaat Teoritis

   Hasil daripada penelitian ini diharapkan dapat menambah bahan-bahan dalam hukum pidana khususnya dalam bidang hukum privasi dan juga untuk menambah pustaka bagi pihak-pihak yang ingin mengetahui, memahami, dan meneliti secara lebih mendalam mengenai hukum privasi.

2. Manfaat Praktis

   Hasil daripada penelitian ini diharapkan dapat menjadi masukkan maupun sarana pembelajaran bagi:

   a. Aparat penegak hukum yang terdiri dari pihak kepolisian, advokat, jaksa, dan hakim agar selalu setia menegakkan hukum dengan seadil-adilnya dan senantiasa menerapkan asas *equality before the law* dalam menjalankan kewajibannya sebagai penegak hukum.

   b. Pemerintah, baik pemerintah pusat maupun pemerintah daerah, agar senantiasa mengedukasi masyarakatnya tentang perkembangan, pemanfaatan, dan perlindungan data pribadi dalam penggunaan sistem informasi elektronik.

   c. Masyarakat agar senantiasa mengetahui perkembangan terbaru mengenai hukum perlindungan data pribadi dalam penggunaan sistem informasi elektronik sehingga mengetahui batasan-batasan pemanfaatan data pribadi tersebut.

E. Keaslian Penelitian

1. a. Judul Penelitian : Tinjauan Yuridis Perlindungan Data Pribadi Pada Media sosial

   b. Identitas

      1) Nama : Achmad Paku Braja Arga Amanda

      2) Fakultas : Hukum

      3) Universitas : Universitas Brawijaya Malang

      4) Tahun : 2013

   c. Rumusan Masalah : 1. Bagaimana tanggung jawab hukum media sosial Facebook dalam melindungi pengguna dari penyalahgunaan data pribadi?
      2. Bagaimana UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik beserta Peraturan Pelaksanaannya melindungi data pribadi pengguna media sosial *Facebook* dari penyalahgunaan data pribadi?

   d. Hasil Penelitian : Tanggung jawab hukum yang di berikan *Facebook* dalam melindungi data pribadi pengguna tertuang dalam *Statement of Rights and Responsibilities*. Dokumen hukum tersebut merupakan perjanjian antara *Facebook* dan pengguna terkait aktivitas di *Facebook*, dalam dokumen tersebut berisi hak dan kewajiban antara pengguna dan *Facebook* selaku penyelenggara sistem elektronik, serta pengaturan mengenai aktivitas pengguna dan penggunaan data

pengguna oleh *Facebook.* Pemerintah Republik Indonesia dalam Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur beberapa pasal terkait perlindungan data pribadi yang diatur dalam :

a. Pasal 15 mengenai hal-hal yang harus dilakukan oleh penyelenggara sistem elektronik.
b. Pasal 26 tentang pelarangan penggunaan informasi tanpa kehendak pemilik data dapat digugat atas dasar ganti kerugian.
c. Pasal 30 pelarangan pengaksesan secara ilegal diancam dengan pasal 46.
d. Pasal 32 tentang perlindungan data pribadi diancam dengan pasal 48.

Apabila terjadi penyalahgunaan data sesama pengguna yang merupakan Warga Negara Indonesia, maka akan diselesaikan dengan cara hukum Indonesia dan dilaksanakan di Pengadilan Indonesia. Berdasarkan Pasal 2 peraturan ini, maka mempunyai sifat ekstrateritorial yaitu dapat peraturan ini dapat dilaksanakan diluar batas negara Indonesia, apabila mempunyai akibat hukum dan kepentingan di Indonesia, maka apabila ada pengguna *Facebook* asing mempunyai masalah hukum di Indonesia, dapat dikenakan sesuai peraturan hukum di Indonesia.

Perbedaan antara penulisan hukum yang ditulis oleh Achmad Paku Braja Arga Amanda dengan penulisan hukum ini terletak pada objek dari perlindungan data pribadi tersebut. Dalam penulisan hukum

penulis tersebut dibahas mengenai *Facebook* sebagai suatu perusahaan yang bergerak dalam bidang media sosial yang bertanggungjawab atas data pribadi para pemilik akun media sosial *Facebook* dengan cara menjaga kerahasiaannya dan menjamin perlindungannya agar tidak tersebar dan disalahgunakan oleh pihak lainnya. Bentuk tanggungjawab itu sendiri diwujudkan dengan menerapkan *Privacy Policy* yang mengikuti ketentuan peraturan perundang-undangan yang berlaku dalam hal ini adalah *Statement of Rights and Responsibilities*; khusus di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik. Sedangkan dalam penulisan hukum ini lebih berfokus pada tanggungjawab pihak perusahaan pemilik media social seperti *Facebook* untuk selain menjaga kerahasiaan data pribadi milik para penggunanya juga menjaga unggahan para penggunanya tidak mengandung data pribadi baik milik sesama pengguna media social lainnya maupun diluar itu.

2. a. Judul Penelitian : *Mitigating The Effects of Doxing* (Mengurangi Efek *Doxing*)

   b. Identitas

      1) Nama : Ingrid N. Norris

      2) Fakultas : *Cybersecurity* (Keamanan Dunia Maya)

      3) Universitas : Utica College New York

      4) Tahun : 2012

c. Rumusan Masalah : 1. *How do hacktivists dox a targeted entity?* (Bagaimana *hacktivists* melakukan penyebaran data pribadi milik seseorang/badan?)

2. *What are the ramifications of doxing?* (Apa konsekuensi dari *doxing*?)

3. *What is the correlation between privacy and doxing?* (Apa korelasi antara privasi dan *doxing*?)

d. Hasil Penelitian : Dari penelitian yang dilakukan oleh Ingrid N. Norris disimpulkan bahwa *hacktivists* atau para pelaku *doxing* biasa menargetkan orang-orang atau organisasi publik yang bergerak disektor-sektor kehidupan yang kontroversial seperti politisi, anggota dan organisasi kepolisian, pemuka masyarakat, hingga selebriti. Para *hacktivist* memperoleh data pribadi targetnya melalui berbagai cara dan sarana, salah satunya yang paling mudah adalah melalui media sosial. Perolehan data pribadi tersebut dilakukan dengan menerobos sistem perlindungan yang dimiliki oleh berbagai situs media sosial, sistem informasi publik, dan situs layanan jasa publik, melakukan *phising*, hingga menerobos alamat IP milik jaringan nirkabel publik. Jika dilihat di permukaannya saja, tindakan *doxing* dilakukan dengan maksud untuk mengungkap identitas atau suatu informasi yang dirasa perlu diketahui oleh publik namun konsekuensinya cukup besar bagi para korbannya. Para korban tindakan *doxing* dapat mengalami kerugian psikis dan fisik

seperti dilecehkan, dikucilkan, hingga mendapatkan perlakuan yang dapat melukai dirinya. Para *hacktivists* biasanya tidak bertanggung jawab atas tindakan *doxing* yang dilakukan dan membiarkan data pribadi yang terungkap itu digunakan oleh masyarakat sesuai dengan keuntungan dan keinginan masing-masing. Dengan konsekuensi yang dapat diterima oleh para korbannya, tindakan *doxing* dan privasi memiliki keterikatan yang cukup kompleks dimana tindakan tersebut merupakan salah satu bentuk pelanggaran terhadap privasi yang merupakan hak dasar tiap subjek hukum yang harus dipenuhi. Tindakan *doxing* juga menjadi pengingat bagi kita bahwa keamanan data pribadi kita dapat sewaktu-waktu dibobol jika kita tidak teliti dan berhati-hati dalam menjaga kerahasiaan data pribadi tersebut.

Perbedaan dari penulisan hukum yang ditulis oleh Ingrid N. Norris dengan penulisan hukum ini terletak pada subjek dan objek dari tindakan *doxing* itu sendiri. Dalam penulisan hukum tersebut penulis berfokus pada para *hacktivist* atau orang-orang yang memiliki kemampuan untuk membobol sistem keamanan tertentu dan menyebarluaskan data-data pribadi targetnya yang sebagian besar adalah tokoh masyarakat dengan tujuan menurunkan reputasi para targetnya. Sedangkan dalam penulisan hukum ini penulis lebih berfokus pada penyebaran data pribadi yang dilakukan oleh orang awam kepada para pelaku tindak pidana pelecehan seksual dengan tujuan mengungkapkan identitas lengkap pelaku yang dapat berimbas pada keluarga maupun

orang-orang disekitar pelaku yang tidak memiliki kaitan dengan tindakan kriminal yang dilakukan.

3. a. Judul Penelitian : Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam *Cloud Computing System* Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik

b. Identitas

1) Nama : Radian Adi Nugraha

2) Fakultas : Hukum

3) Universitas : Universitas Indonesia

4) Tahun : 2012

c. Rumusan Masalah : 1. Bagaimana perbandingan pengaturan regulasi Perlindungan Data di Uni Eropa dan Malaysia dengan Undang-Undang Informasi dan Transaksi Elektronik?

2. Bagaimana Undang-Undang Informasi dan Transaksi Elektronik melindungi data pribadi dari pengguna Komputasi Awan di Indonesia?

3. Bagaimana tanggung jawab penyedia layanan komputasi awan terhadap perlindungan data pribadi pengguna layanan komputasi awan?

d. Hasil Penelitian : 1. Dari analisis perbandingan peraturan perundang-undangan yang mengatur mengenai perlindungan data

pribadi di Uni Eropa dan Malaysia yang telah penulis lakukan ditemukan bahwa perumusan perlindungan data pribadi dalam UU ITE masih belum komprehensif. *EU Directive 95/46/EC* yang berlaku di Uni Eropa mendefinisikan secara jelas dan rinci pengaturan pihak-pihak yang terkait, memiliki prinsip-prinsip perlindungan data yang komprehensif hingga membatasi perpindahan data pribadi ke negara-negara yang dianggap tidak memiliki regulasi perlindungan data pribadi yang sepadan. Sedangkan pengaturan perlindungan data pribadi yang komprehensif dalam Malaysia *Personal Data Protection Act* lebih banyak ditujukan pada perlindungan data pribadi dalam transaksi komersial. *Malaysia Personal Data Protection Act* memiliki prinsip-prinsip perlindungan data pribadi, hak-hak baru bagi setiap orang terkait data pribadinya, pemuatan sanksi pidana, hingga pembentukan lembaga penasihat, pengawas dan penegakan hukum yang terkait dengan perlindungan data ini. Apabila kita membandingkan dengan pengaturan perlindungan data pribadi dalam UU ITE maka hanya ditemukan 2 (dua) prinsip perlindungan data yang diterapkan dalam pasal 26 UU ITE yaitu *Notice* atau pemberitahuan dan *Consent* atau persetujuan.

2. Indonesia belum memiliki Undang-undang yang khusus membahas mengenai privasi dan perlindungan data pribadi. Tetapi perlindungan privasi dan data pribadi dapat ditemukan di beberapa

peraturan perundang-undangan. Khusus untuk perlindungan data pribadi yang secara spesifik berada di lingkup media elektronik terdapat dalam Pasal 26 Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Untuk dapat mengembangkan layanan komputasi awan yang menghormati privasi dan melindungi data pribadi pengguna layanan maka diperlukan regulasi yang lebih komprehensif.

3. Terkait dengan tanggung jawab penyedia layanan komputasi awan terhadap data maupun data pribadi pengguna layanannya, penulis melihat bahwa terdapat beberapa perbedaan kebijakan teknis yang diterapkan untuk melindungi data tersebut. Dalam hal ini penyedia layanan awan telah menerapkan prinsip tanggung jawab sebelum suatu kejadian (*ex-anteliability*). Kemudian penulis dapat menarik kesimpulan dari narasumber-narasumber dari beberapa penyedia layanan komputasi awan dimana penyedia layanan komputasi awan menghormati, melindungi dan tidak akan mengungkapkan data pribadi pengguna layanan komputasi awan tanpa adanya persetujuan dari pengguna layanan. Hal ini tentu selaras dengan maksud dan tujuan dari rumusan Pasal 26 UU ITE. Sedangkan apabila terjadi malfungsi dari sistem komputasi awan yang mengakibatkan tidak terpenuhinya layanan maksimal kepada pengguna layanan, maka berdasarkan *Service Contract Agreement* dan *Service Level Agreement* penyedia layanan komputasi awan (dalam hal ini Biznet

Networks) akan mengganti hingga 30 (tiga puluh) persen dari jumlah total tagihan dalam satu bulan. Di lain sisi apabila data pribadi pengguna layanan komputasi awan dicuri dan/atau dibobol oleh tindakan *hacking* dan/atau tindakan lain yang diluar kendali dari penyedia layanan maka penyedia layanan komputasi awan tidak bertanggungjawab atas kewajiban yang ditimbulkan dari gangguan tersebut dengan sebelumnya memberitahukan keadaan tersebut secepatnya kepada pelanggan.

Perbedaan penulisan hukum yang dilakukan oleh Radian Adi Nugraha dengan penulisan hukum ini terletak pada lingkup perlindungan data pribadi tersebut. Dalam penelitian tersebut perlindungan data pribadi lebih berfokus pada pengolahan, penyimpanan, dan pemanfaatan data pribadi para pengguna layanan *cloud computing system* yang merupakan tanggung jawab dari para penyedia jasa layanan tersebut. Sedangkan dalam penelitian ini, peneliti lebih berfokus pada penyebaran data pribadi yang dilakukan oleh para pengguna layanan media sosial.

F. Batasan Konsep

1. Perlindungan hukum adalah upaya yang dilakukan oleh pemerintah untuk menjamin perlindungan terhadap hak dan kewajiban tiap warganegaranya agar tidak terjadi penyalahgunaan dan tindakan sewenang-wenang. Untuk menjaga agar tidak kepentingan setiap orang terpenuhi maka pelaksanaannya pun harus dilakukan dengan ketentuan perundang-undangan yang berlaku. Penulis menggunakan batasan perlindungan

hukum sesuai dengan yang diatur dalam Pasal 1 ke. 2 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan Pasal 1 ke. 8 Undang-Undang Nomor 31 Tahun 2014 *juncto* Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban.

2. Data Pribadi adalah data tentang 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. Pengertian mengenai data pribadi tersebut dapat ditemukan dalam Pasal 1 ke. 1 Undang-Undang Nomor 27 Tahun 2022.

G. Metode Penelitian

1. Jenis Penelitian

   Penelitian ini dilakukan dengan penelitian hukum normatif. Penelitian hukum normatif merupakan penelitian yang dilakukan dengan cara mengkaji, meneliti, dan menelaah bahan pustaka dan data sekunder sebagai data utamanya. Oleh karena itu, penelitian hukum normatif juga disebut penelitian hukum kepustakaan, penelitian hukum teoritis/dogmatis.[1]

2. Sumber Data

   Bahan yang diteliti pada penelitian hukum normatif adalah bahan pustaka dan/atau data sekunder. Bahan pustaka merupakan bahan

[1]H. Ishaq, 2017, *Metode Penelitian Hukum Dan Penulisan Skripsi, Tesis, Serta Disertasi*, Penerbit Alfabeta, Bandung, hlm. 66.

yang berasal dari sumber primer dan sumber sekunder. Penulis akan menggunakan bahan yang berasal dari sumber primer sebagai berikut:

1) Kitab Undang-Undang Hukum Pidana
2) Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban yang telah diubah oleh Undang-Undang Nomor 31 Tahun 2014.
3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016.
4) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
5) Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.

Bahan hukum sekunder adalah bahan hukum yang tidak memiliki daya mengikat bagi subyek hukum, antara lain:

a. Pendapat hukum yang dipublikasikan dalam buku, jurnal, laporan hasil penelitian, surat kabar, majalah ilmiah.
b. Kamus hukum dan kamus non hukum.

3. Cara Pengumpulan Data

Dalam penelitian ini penulis memperoleh data sekunder dengan cara melakukan studi kepustakaan terhadap bahan hukum primer dan sekunder.

4. Analisis Data

Analisis data yang diperoleh akan dilakukan secara kualitatif, yakni analisis yang dilakukan dengan cara menguraikan data secara bermutu dalam bentuk kalimat yang teratur, runtun, logis, tidak tumpang tindih, dan efektif, sehingga memudahkan interpretasi data dan pemahaman hasil analisis. Cara ini memerlukan interpretasi atau pandangan penulis yang didasarkan pada konsep, teori, peraturan perundang-undangan, doktrin, prinsip hukum, dan pendapat para ahli.