BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Sejak awal abad ke -21, perkembangan teknologi yang pesat telah menjadi pendorong utama dari perubahan dalam berbagai aspek kehidupan manusia, terutama mengubah cara kita berkomunikasi dan bekerja. Perkembangan teknologi memperluas akses masyarakat pada dunia, terutama dengan menggunakan internet. Penggunaan internet di Indonesia terus meningkat dari tahun ke tahun dengan meluasnya akses dan penerapan teknologi digital di berbagai bidang. Berdasarkan data yang dikeluarkan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022, jumlah pengguna Internet di Indonesia mencapai sekitar 210 juta jiwa atau sekitar 78,4% dari total penduduk Indonesia yang mencapai 267,7 juta orang.[1] Umumnya, pengguna internet di Indonesia melakukan beragam kegiatan melalui internet, mulai dari keperluan bisnis, pendidikan, hiburan, dan komunikasi di media sosial. Namun, di balik kemanfaatannya, perkembangan teknologi juga membawa tantangan baru, termasuk dalam isu privasi data dan keamanan siber yang kompleks.

Keamanan siber telah menjadi perhatian yang semakin penting bagi seluruh perusahaan dan lembaga pemerintahan Indonesia. Penggunaan internet yang

[1] Rian Dwi Hapsari dan Kuncoro Galih Pambayun, 2023, "*Ancaman Cybercrime di Indonesia Sebuah Tinjauan Pustaka Sistematis"*, Jurnal Konstituen Vol. 1, No. 1, 2023, hlm. 2.

semakin luas telah menyebabkan peningkatan serangan siber. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa jumlah kasus serangan siber di Indonesia mencapai 100 juta hingga April 2022.[2] Kekhawatiran terhadap serangan ini mendorong pemerintah dan penyelenggara sistem elektronik untuk meningkatkan perlindungan sistem dan manajemen serangan siber, terutama memastikan keamanan data.[3] Pelanggaran data dapat mengakibatkan rusaknya reputasi perusahaan, tuntutan hukum yang berisiko tinggi, dampak bisnis yang signifikan, pencurian kekayaan intelektual, dan kerentanan keamanan nasional, sehingga peningkatan keamanan siber menjadi sebuah urgensi.[4]

Pada tahun 2015, International Telecommunication Union (ITU) meluncurkan Global Cybersecurity Index (GCI) yang bertujuan untuk mengukur komitmen 193 negara anggota ITU terhadap keamanan siber untuk mengidentifikasi perbaikan dan mendorong negara-negara tersebut untuk mengambil tindakan dengan meningkatkan kesadaran akan keadaan keamanan siber.[5] Indeks komitmen keamanan siber negara anggota dipetakan dalam 5 pilar, yaitu tindakan hukum (*legal measures*), langkah teknis (*technical measures*), langkah organisasi (*organizational measures*), langkah pengembangan kapasitas (*capacity development*), dan langkah kerja sama (*cooperation measures*).[6] Pada tahun 2020, GCI memuat Indonesia pada

[2] Muhammad Subhan Abdullah, Ines Heidiani Ikasari, 2023, *"Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi dan Upaya Pencegahan",* JRIIN: Jurnal Riset Informatika dan Inovasi, Vol. 1, No. 1, 2023, hlm. 96.

[3] Ibid.

[4] Jeff Koseff, *Cybersecurity Law 2nd edition*, USA, John Wiley & Sons, Inc., Hoboken..

[5] Danrivanto Budhijanto, 2023, *Hukum Perlindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*, PT Refika Aditama, Bandung, hlm. 58.

[6] International Telecommunication Union, *Global Cybersecurity Index (GCI) 2020*.

peringkat ke-24 dari 194 negara dengan skor 94.88.[7] Menurut data pembanding lain, yaitu dari National Cyber Security Index (NCSI), Indonesia berada di peringkat ke-6 Asia Tenggara dan peringkat ke-83 dari 160 negara.[8] NCSI menilai Indonesia memiliki skor 38.96 dari 100 dalam hal keamanan siber.

Salah satu isu keamanan siber yang menjadi pembahasan adalah isu privasi dan perlindungan data pribadi. Secara umum, data pribadi adalah segala informasi yang dapat digunakan untuk mengidentifikasi seseorang secara langsung maupun tidak langsung. Jerry Kang menyatakan bahwa data pribadi menjelaskan suatu informasi yang berkaitan erat dengan seseorang yang akan membedakan karakteristik masing-masing individu.[9] Data pribadi mencakup informasi penting seperti nama, NIK, alamat, data genetis, dan lain-lainnya. Seiring dengan pesatnya perkembangan teknologi dan informasi, data pribadi menjadi sesuatu yang esensial karena menjadi bagian dari privasi.

Berdasarkan Teori Privasi Modern yang dikembangkan oleh Alan Westin, dalam bukunya yang berjudul *Privacy and Freedom*, ia menyatakan bahwa privasi adalah hak individu, kelompok, atau organisasi untuk menentukan apakah data tentang dirinya dikomunikasikan kepada pihak lain atau tidak.[10]

Westin menjelaskan empat fungsi privasi, yaitu:

1. *Personal autonomy* (otonomi pribadi) adalah keinginan individu untuk tidak dimanipulasi, didominasi, atau diekspos oleh orang lain.

[7] Ibid., hlm. 25.
[8] https://ncsi.ega.ee/, dikunjungi pada 3 Oktober 2024 pukul 08.20.
[9] Dhoni Martien, 2023, *Perlindungan Hukum Data Pribadi*, Mitra Ilmu, Makassar, hlm. 52.
[10] Ibid., hlm. 32.

2. *Emotional release* (pelepasan emosional) menggambarkan waktu istirahat dari tuntutan sosial, seperti tuntutan peran.
3. *Self-evaluation* (evaluasi diri) mempertimbangkan pengalaman-pengalaman yang telah diproses.
4. *Limited and protected communication* (komunikasi yang terbatas dan terlindungi) menetapkan batas-batas antar pribadi, sementara komunikasi yang terlindungi bertukar informasi dengan orang yang terpercaya.[11]

Selain itu, Westin juga mengemukakan "*Four Privacy States*" yang terdiri atas:

1. *Solitude:* Informasi tidak dibagikan kepada orang lain. Hal ini serupa dengan "hak untuk menyendiri." Dalam aspek digital, adanya sebuah teknologi yang menyediakan kontrol akses untuk menjaga kerahasiaan informasi.
2. *Intimacy*: Keintiman mengacu pada informasi yang dibagikan hanya dengan manusia tertentu. Dalam aspek digital, sebuah teknologi menyediakan pilihan untuk berbagi informasi hanya dengan orang tertentu, misalnya sebuah unggahan tertentu hanya dapat dibagikan dengan teman di jaringan sosial.
3. *Anonymity*: Anonimitas berarti informasi tidak dapat dihubungkan dengan individu. Dalam aspek digital, sebuah teknologi menawarkan kemungkinan untuk menyimpan atau mengirimkan data yang

[11] Nina Gerber, et.al, 2023, *"Human Factors in Privacy Research"*, Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-28643-8.

dianonimkan, misalnya dalam pemilihan secara daring, identitas pemilih tidak dapat diungkapkan.

4. *Reserve:* Kerahasiaan menggambarkan bahwa pengungkapan informasi kepada orang lain dibatasi.[12]

Privasi atas data pribadi merupakan pengakuan dan perlindungan hak asasi manusia yang dilindungi oleh hukum internasional, regional, dan nasional, sehingga data pribadi setiap individu wajib dilindungi. Perlindungan data pribadi merupakan salah satu hak asasi manusia yang termasuk dalam perlindungan hukum. Satjipto Rahardjo mengatakan, perlindungan hukum diberikan melalui perlindungan hak asasi manusia (HAM) yang merugikan pihak lain, yang menjamin masyarakat dapat menikmati manfaat dari seluruh hak yang diakui undang-undang.[13] Dasar hukum yang berkaitan dengan pentingnya perlindungan data pribadi di Indonesia terdapat dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang berbunyi:

> "Setiap orang berhak perlindungan data pribadi, keluarga, kehormatan, dan harta benda di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Peraturan tentang perlindungan data pribadi dimuat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang disahkan pada 20 September 2022 dan mulai berlaku pada Oktober 2024.

Perkembangan teknologi yang semakin pesat telah memperluas akses masyarakat terutama pada aspek penggunaan data dalam dunia maya. Hal ini

[12] Ibid.
[13] Satjipto Rahardjo, 2014, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, hlm. 53.

memunculkan potensi kejahatan siber yang menargetkan data pribadi sebagai objek perbuatan jahat.

Salah satu kejahatan siber yang berkaitan erat dengan data pribadi dan marak terjadi di dunia maya adalah tindakan penyebaran data pribadi atau dikenal dengan sebutan *doxing*. *Doxing* diambil dari kata *dox* (singkatan dari dokumen) dan *dropping* (menjatuhkan) yang didefinisikan sebagai kejahatan yang mengumpulkan data pribadi seseorang untuk dipublikasikan atau disebarluaskan secara daring (*online*) tanpa seizin pemilik data yang diperuntukkan sebagai ancaman dan intimidasi.[14] Dalam kamus Oxford, *doxing* diartikan sebagai pencarian dan publikasi informasi pribadi atau identitas orang tertentu di internet dan seringkali didasarkan atas niat jahat. Perbuatan *doxing* berupa merilis data pribadi suatu individu bertujuan untuk merusak kredibilitas, reputasi, dan/atau karakter individu tersebut.[15] Tindakan *doxing* dapat dilakukan oleh siapa saja, baik berhubungan erat dengan korban *doxing* maupun tidak.

Salah satu kasus *doxing* yang cukup geger terjadi di Indonesia adalah kasus *doxing* yang dilakukan oleh Bjorka. Pada tahun 2022 lalu, Bjorka membeberkan sejumlah data pribadi milik pejabat publik.[16] Selain itu, Bjorka juga membocorkan data pelanggan IndiHome, data pelanggan PLN, data internal Jasa Marga, data SIM Card, data KPU, dan sebagainya. Kasus serupa juga terjadi pada Denny Siregar. Pada tahun 2020, data pribadi Denny Siregar

[14] Artanti Tertia Mukti dan Mochammad Tanzil Multazam, 2023, *"Doxing Patterns Using Social Engineering in Cyberspace: Pola-Pola Doxing Menggunakan Social Engineering di Dunia Maya"*, hlm. 2.

[15] David M. Douglas, 2016, *"Doxing: A Conceptual Analysis",* Ethics Inf Technol, hlm. 205.

[16] CNN Indonesia, *"Sepekan Petualangan Bjorka: Doxing Hingga Muncul Tersangka",* https://www.cnnindonesia.com, dikunjungi pada 26 September 2024 pukul 13.17.

disebar oleh akun Twitter dengan *username* @opposite6891.[17] Akun tersebut kemudian diketahui dimiliki oleh Febriansyah Puji Handoko. Pelaku mengaku motifnya membeberkan data pribadi Denny adalah karena pelaku kesal dengan unggahan Denny di Twitter. Berdasarkan laporan, pelaku adalah seorang karyawan *outsourcing* Telkomsel di Rungkut Surabaya, sehingga pelaku memiliki akses terhadap data pribadi pelanggan. Pelaku secara tidak sah mengakses data pelanggan atas nama Denny Siregar tanpa otorisasi. Data pribadi Denny Siregar yang disebar oleh pelaku meliputi nama lengkap, alamat, Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga, *International Mobile Equipment Identity* (IMEI), hingga jenis perangkat. Atas perbuatannya, pelaku dijerat Pasal 46 atau Pasal 48 UU ITE, Pasal 50 Undang-Undang Nomor 26 Tahun 1999 tentang Telekomunikasi, Pasal 363 KUHP atau Pasal 95 Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan. Pelaku dijatuhkan hukuman pidana penjara 8 bulan dan pidana denda sebesar 2 juta rupiah.

Doxing dapat menimbulkan berbagai dampak merugikan, antara lain korban dapat mengalami pelecehan, intimidasi, pencurian indetitas, hingga ancaman fisik.[18] Komnas HAM menilai bahwa tindakan *doxing* merupakan suatu bentuk pelanggaran HAM digital yang harus diberantas karena mengancam kemanan warga negara Indonesia.

[17] Amir Baihaqi, *"Pembobol Data Pribadi Denny Siregar Divonis 8 Bulan Penjara"*, https://www.news.detik.com, dikunjungi pada 26 September 2024 pukul 13.06.

[18] Muhammad Kamarulzaman Satria, Hudi Yusuf, 2024, *"Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi"*, JICN: Jurnal Intelek dan Cendikiawan Nusantara, Vol. 1, No. 2, hlm. 2444.

Sebagai negara yang baru mengesahkan undang-undang mengenai perlindungan data pribadi, tindakan *doxing* diatur dalam Undang-Undang Pelindungan Data Pribadi sebagaimana yang dinyatakan dalam Pasal 65 ayat (2):

> "Setiap Orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya."

Sebelum disahkannya Undang-Undang Pelindungan Data Pribadi, regulasi tentang perlindungan data pribadi dan pelanggaran privasi telah dimuat dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Namun, implementasi dan penegakan hukum terhadap kasus pelanggaran data pribadi, khususnya *doxing*, masih menghadapi berbagai kendala dan belum ditangani secara memadai.[19]

Indonesia merupakan negara kelima di Asia Tenggara yang memiliki aturan perlindungan data pribadi setelah Singapura, Malaysia, Thailand, dan Filipina.[20] Di Singapura, peraturan perlindungan data pribadi dikenal dengan nama *Personal Data Protection Act 2012* (PDPA Singapura). Peraturan perundang-undangan tersebut memuat larangan mengumpulkan dan

[19] Teguh Cahya Yudiana, Sinta Dewi Rosadi, Enni Soerjati Priowirjanto, 2022, *"The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia"*, PADJADJARAN Journal of Law, Vol. 9, No. 1, hlm. 29.

[20] BBC Indonesia, *"DPR Sahkan UU Perlindungan Data Pribadi"*, https://www.bbc.com, dikunjungi pada 26 September 2024, pukul 13.30.

mengungkapkan data pribadi milik orang lain. Selain itu, Singapura telah mengklasifikasikan *doxing* secara khusus sebagai pelanggaran dalam *The Protection from Harassment Act* (POHA).

Singapura dikenal memiliki penegakan hukum yang kuat dan efektif dalam hal regulasi data pribadi, yaitu dengan didirikannya Personal Data Protection Commission Singapore (PDPC) sebagai otoritas utama yang bertugas mengawasi dan menegakkan perlindungan data pribadi sesuai PDPA. Singapura memiliki sistem yang lebih matang dalam hal penegakan hukum dan perlindungan data pribadi, yang menjadikan negara ini sebagai model dalam hal regulasi dan penanganan kasus kejahatan siber di Asia.

Peraturan mengenai perlindungan data pribadi dan pencegahan kejahatan di setiap negara bergantung pada sistem hukum yang dianut. Sudikno Mertokusumo berpendapat bahwa sistem hukum adalah suatu kesatuan yang terdiri dari unsur-unsur yang saling berinteraksi untuk mencapai tujuan bersama.[21] Implementasi sistem hukum dalam suatu negara dipengaruhi oleh sub sistem yang terdiri atas substansi hukum, struktur hukum, dan budaya hukum.[22] Sistem hukum baik yang berbasis *civil law, common law*, maupun sistem hukum campuran, memiliki pendekatan yang beragam dalam menindak ancaman digital. Hal ini menciptakan kebutuhan mendesak untuk memahami perbandingan hukum di berbagai yurisdiksi untuk mengidentifikasi praktik terbaik yang dapat diadaptasi dan diterapkan. Indonesia sendiri menganut sistem hukum *civil law* dan Singapura menganut sistem hukum *common law*.

[21] Misbahul Huda, 2020, *Perbandingan Sistem Hukum*, CV Cendekia Press, Bandung, hlm. 9
[22] Ibid, hlm. 1

Perbandingan hukum memberikan kerangka untuk mengetahui dan menganalisis peraturan terkait perlindungan data pribadi, khususnya dalam penanganan kejahatan siber, termasuk tindakan *doxing*. Isu *doxing* tidak hanya relevan dalam konteks nasional, tetapi juga menyangkut hubungan antar negara di era globalisasi. Harmonisasi peraturan perlindungan data pribadi antar negara di kawasan ASEAN menjadi semakin penting untuk menjamin keamanan privasi di seluruh kawasan. Keberagaman dalam regulasi dapat menciptakan tantangan dalam penegakan hukum, terutama pada kasus kejahatan siber lintas batas yang memerlukan kerja sama internasional.

Indonesia merupakan negara yang baru mengundangkan regulasi tentang perlindungan data pribadi. Dengan membandingkan peraturan di Indonesia dengan negara lain, kita dapat memahami bagaimana kedua negara dengan sistem hukum yang berbeda bersinergi dalam melindungi data pribadi dan memerangi kejahatan siber yang berkaitan dengan data pribadi khususnya *doxing*, serta untuk mempelajari pengalaman negara lain dalam rangka meningkatkan kerangka hukum domestik untuk menciptakan ekosistem digital yang aman dan berkeadilan.

Berdasarkan latar belakang di atas, penulis ingin mengkaji lebih jauh mengenai penelitian tentang "PERBANDINGAN REGULASI PERLINDUNGAN DATA PRIBADI TERKAIT DENGAN TINDAK PIDANA PENYEBARAN DATA PRIBADI (*DOXING*) ANTARA INDONESIA DAN SINGAPURA".

Dalam penelitian ini, penulis memilih negara Singapura sebagai bahan perbandingan karena Singapura adalah salah satu negara yang dikategorikan

sebagai negara dengan keamanan siber yang baik di Asia Tenggara. Dalam GCI 2020, Singapura mendapatkan skor 98,52 pada peringkat global dalam hal keamanan siber.[23] Singapura juga memiliki Cyber Security Agency (CSA) sebagai badan pemerintah yang didedikasikan untuk mengawasi dan mengembangkan strategi nasional dalam keamanan siber. Berdasarkan NCSI 2021, Singapura juga mendapatkan skor tertinggi dalam beberapa indikator, yaitu pendidikan dan pengembangan profesional, perlindungan layanan esensial, analisis ancaman siber, manajemen krisis siber, dan perlindungan data pribadi.[24]

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, adapun permasalahan yang akan dijabarkan dalam penelitian ini adalah sebagai berikut:

1. Bagaimanakah perbandingan regulasi perlindungan data pribadi antara Indonesia dan Singapura?
2. Bagaimanakah perbandingan regulasi tindak pidana penyebaran data pribadi (*doxing*) antara Indonesia dan Singapura?

C. Tujuan Penelitian

Tujuan yang diharapkan dari penelitian ini adalah:

1. Untuk mengetahui dan menganalisis persamaan dan perbedaan regulasi perlindungan data pribadi antara Indonesia dan Singapura.

[23] International Telecommunication Union, *Op.Cit.*
[24] Lucas Romero, 2023, *"National Cyber Security Index of Singapore 2021"*, https://www.statista.com, dikunjungi pada 2 Oktober 2024 pukul 13.59.

2. Untuk mengetahui dan menganalisis persamaan dan perbedaan regulasi tindak penyebaran data pribadi (*doxing*) antara Indonesia dan Singapura.
3. Untuk mengetahui dan menganalisis kelayakan peraturan perlindungan data pribadi di Indonesia.

D. Manfaat Penelitian

Terdapat dua manfaat yang ingin didapatkan penulis dari diadakannya penelitian ini, yaitu sebagai berikut:

1. Manfaat Teoritis

   Hasil dari penelitian ini diharapkan dapat bermanfaat bagi pengembangan ilmu pengetahuan di bidang ilmu hukum secara umum. Hasil penelitian ini diharapkan dapat menambah referensi di dunia kepustakaan untuk dapat digunakan dalam penelitian, khususnya pada perbandingan ketentuan hukum pidana dalam perlindungan data pribadi dan mengenai kejahatan *doxing*.

2. Manfaat Praktis

   Hasil dari penelitian ini diharapkan dapat bermanfaat bagi pembuat kebijakan di Indonesia dalam perbaikan dan pengembangan regulasi perlindungan data pribadi, serta dalam penegakan hukumnya. Hasil dari penelitian ini diharapkan sebagai referensi untuk evaluasi kebijakan digital nasional yang lebih luas, terutama terhadap keamanan dan privasi dalam dunia maya.

E. Metode Penelitian

1. Pendekatan Masalah

Penelitian hukum adalah sebuah kegiatan yang didasarkan pada metode, sistematika, dan pemikiran tertentu yang bertujuan untuk mempelajari satu atau lebih fenomena hukum tertentu dengan cara menganalisisnya.[25] Menurut Soetandyo Wignyosoebroto, penelitian hukum adalah segala usaha untuk mencari dan menemukan jawaban yang benar dan/atau jawaban yang tidak pernah salah mengenai suatu permasalahan.[26] Soerjono Soekanto berpendapat bahwa jenis penelitian hukum dapat dibedakan menjadi hukum normatif dan hukum empiris.[27] Pada penelitian ini, Penulis menggunakan pendekatan yuridis normatif. Pendekatan yuridis normatif merupakan suatu pendekatan yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder.[28] Penelitian menggunakan pendekatan yuridis normatif mencakup penelitian terhadap asas-asas hukum, penelitian terhadap sistematik hukum, penelitian terhadap taraf sinkronisasi vertikal dan horizontal, perbandingan hukum, dan sejarah hukum. Penulis juga menggunakan pendekatan undang-undang dalam penelitian ini. Pendekatan hukum ini dilakukan dengan cara mengkaji dan menganalisis peraturan dan undang-undang yang relevan dengan permasalahan atau kajian hukum yang akan dibahas.[29]

[25] Soerjono Soekanto, 1986, *Pengantar Penelitian Hukum*, UI Press, Jakarta, hlm. 43.
[26] Zainuddin Ali, 2009, *Metode Penelitian Hukum*, Sinar Grafika, Jakarta, hlm. 18.
[27] Ibid., hlm. 12.
[28] Soerjono Soekanto dan Sri Mamudji, 2014, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, PT Raja Grafindo Persada, Jakarta, hlm. 13-14.
[29] Muhaimin, 2020, *Metode Penelitian Hukum*, Mataram University Press, Mataram, hlm. 56.

2. Sumber dan Jenis Data

Berdasarkan sumbernya, jenis data dapat dibedakan menjadi dua, yaitu jenis data yang diperoleh dari masyarakat dan data yang diperoleh dari bahan pustaka.[30] Data primer adalah data yang diperoleh dari masyarakat. Data sekunder adalah data yang diperoleh dari bahan pustaka. Pada penelitian ini, Penulis menggunakan data sekunder. Data sekunder adalah data yang diperoleh dari bahan literatur seperti buku, dokumen resmi, hasil penelitian berwujud laporan, dan sebagainya.[31] Data sekunder dilakukan dengan cara mengutip dan menelusuri peraturan perundang-undangan, artikel ilmiah, kamus hukum, dan teori-teori ahli hukum. Data sekunder yang digunakan oleh Penulis pada penelitian kali ini terdiri dari:

a. Bahan hukum primer

Bahan hukum primer adalah bahan hukum yang mengikat.[32] Bahan hukum primer yang digunakan oleh penulis dalam penelitian kali ini meliputi:

1) Undang-Undang Dasar Negara Republik Indonesia 1945;
2) Undang-Undang Nomor 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana (KUHP);
3) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
4) *Personal Data Protection Act 2012 Singapore*;
5) *The Protection from Harassment Act*;

[30] Soerjono Soekanto, Ibid., hlm. 11.
[31] Ibid., hlm. 12.
[32] Soerjono Soekanto dan Sri Mamudji, *Op.Cit.*

6) Konvensi internasional atau peraturan perundang-undangan lain yang berkaitan dengan penelitian.

b. Bahan hukum sekunder

Bahan hukum sekunder adalah bahan hukum yang memberikan penjelasan mengenai isi dari bahan hukum primer, yaitu bahan pendukung yang terdiri dari dari buku-buku, literatur-literatur hukum, doktrin ahli hukum, keputusan yang berisi hasil penelitian, dan hal lain yang berkaitan dengan objek penelitian.[33]

c. Bahan hukum tersier

Bahan hukum tersier adalah bahan pendukung terhadap bahan hukum primer dan sekunder.[34] Bahan hukum tersier dapat ditemukan dalam buku literatur, skripsi, pendapat para ahli, artikel dari internet, hasil penelitian, dan sebagainya yang dapat mendukung penelitian.

3. Metode Pengumpulan Data

a. Studi Pustaka

Studi pustaka adalah metode pengumpulan data pustaka yang diperoleh dari berbagai sumber yang relevan dengan topik penelitian yang diteliti oleh Penulis, seperti buku, literatur, karya ilmiah, internet, media cetak, serta peraturan perundang-undangan yang berkaitan dengan penelitian.

[33] Ibid.
[34] Ibid.

b. Studi Perbandingan

Studi perbandingan digunakan dalam penelitian untuk menganalisis kesamaan dan perbedaan di antara dua atau lebih subjek yang berkaitan. Pendekatan ini bertujuan untuk memperoleh pemahaman yang lebih mendalam, mengidentifikasi pola atau prinsip universal, dan mengevaluasi praktik terbaik dalam suatu bidang. Dalam konteks hukum, studi perbandingan sangat bermanfaat untuk memahami bagaimana sistem hukum yang berbeda menangani isu-isu tertentu, khususnya dalam hal perlindungan data pribadi dan kejahatan *doxing*.

F. Metode Pengolahan & Analisis Data

Untuk mendapatkan analisis data yang sesuai dengan permasalahan yang diteliti, perlu dilakukan metode pengumpulan data. Proses pengumpulan dan pengolahan data tersebut mencakup tahap-tahap berikut:

a. Seleksi data, yaitu proses pemeriksaan kembali untuk mengetahui kelengkapan data yang telah diperoleh dari hasil penelitian.
b. Klasifikasi data, yaitu proses pengelompokkan data yang telah dikumpulkan berdasarkan kategori-kategori yang telah ditentukan guna memperoleh data yang tepat untuk analisis lebih lanjut.
c. Penyusunan data, yaitu proses mengorganisasi dan menyusun data yang saling berkaitan menjadi satu kesatuan yang utuh dan terpadu pada bagian pembahasan, sehingga memudahkan dalam interpretasi data.

Pendekatan yang diterapkan oleh Penulis dalam penelitian ini adalah pendekatan kualitatif. Pendekatan kualitatif merupakan suatu proses penelitian yang menghasilkan data dalam bentuk deskriptif.[35]

[35] Ibid., hlm. 32.