BAB I

PENDAHULUAN

A. Latar Belakang

Setiap manusia memiliki bermacam-macam hak yang menunjang hidupnya dan tidak dapat diganggu gugat oleh siapapun dan berhak atas perlindungan hukum terhadap campur tangan atau serangan atas diri pribadi serta hak yang dimilikinya termasuk diantaranya data yang dimiliki. Pada dasarnya, privasi itu sendiri merupakan hak untuk mengontrol informasi pribadi seseorang dan kemampuan untuk menentukan dalam hal apa saja dan bagaimana informasi tersebut harus diperoleh dan dipergunakan.[1] Suatu data dapat diklasifikasikan sebagai data pribadi seseorang apabila data tersebut berhubungan dengan orang yang teridentifikasi atau dapat diidentifikasi, yaitu Subjek Data.[2] Tujuan utama dari adanya privasi adalah untuk memberikan hak bagi Subjek Data selaku pihak yang memiliki data pribadi tersebut agar dapat menentukan bagaimana dan kapan percakapan, pemikiran, atau perilaku mana yang dapat dipublikasikan.[3]

Adanya data pribadi erat kaitannya dengan tindakan-tindakan yang berkaitan dengan data pribadi. Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (selanjutnya disebut UU PDP) dan

[1]Edmon Makarim, *Pengantar Hukum Telematika Suatu Kompilasi Kajian*, PT Raja Grafindo Persada, Jakarta, 2005, hlm. 163.

[2]Council of Europe, *European Union Agency for Fundamental Rights, Handbook on European Data Protection Law*, Council of Europe, France, 2018, hlm. 86.

[3]Westin, A. F. Science, "Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy", *Columbia Law Review*, Vol. 66, No. 6, 1966, hlm. 1050.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP PSTE), mengatur mengenai tindakan-tindakan apa saja yang termasuk dalam pemrosesan data pribadi, hal itu meliputi pemerolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaharuan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan dan/ atau penghapusan atau pemusnahan.

Tindakan transfer data pribadi lintas batas merupakan salah satu bentuk kerjasama antara negara dan negara dimana dapat melihat adanya adopsi luas pendekatan konvergen terhadap privasi data untuk aliran data lintas batas yang tidak hanya dapat meningkatkan perlindungan privasi bagi individu, tetapi juga dapat meningkatkan aktivitas ekonomi berbasis data di seluruh wilayah.[4] Secara singkat, transfer data pribadi lintas batas merupakan proses berupa transfer data pribadi kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi di luar wilayah hukum Negara Republik Indonesia sebagaimana diatur dalam UU PDP.

Adanya pelaksanaan transfer data pribadi lintas batas bertujuan memungkinkan perusahaan untuk menawarkan produk yang sama sekali baru, adanya aliran informasi yang ditingkatkan dimungkinkan oleh tindakan transfer data pribadi lintas batas, memperluas dan memperdalam pasar dunia dan membuatnya semakin saling bergantung, dan kebijakan Telekomunikasi akan memiliki dampak yang akan meningkatkan perilaku perusahaan

[4]Lee-Makiyama Hosuk dan Lacey Simon, *Cross-Border Data Flows: The Impact of Data Localisation on IoT*, GSMA, 2021, hlm. 2.

multinasional dan karenanya perkembangan perdagangan dunia dan investasi asing.[5] Atas dampak yang dimiliki, membuat adanya tindakan transfer data pribadi lintas batas yang terjadi setiap saat. Hal ini dibuktikan dengan transfer data pribadi lintas batas yang menjadi sumber kehidupan ekonomi baru yang dianggap akan terus tumbuh hingga diperkirakan mencapai 65% PDB dunia pada akhir tahun 2022.[6] The International Data Corporation memperkirakan investasi dalam transformasi digital menjadi total USD 6,8 triliun dari tahun 2020 hingga 2023, setara dengan PDB gabungan Prancis dan Jerman.[7]

Pada akhir tahun 2021, *bandwidth* atau rentang frekuensi dalam yang digunakan untuk mentransmisikan sinyal lintas batas diperkirakan menjadi 400 kali lipat dari tahun 2005. Pada saat itu, lalu lintas Protokol Internet (IP) global, proksi untuk aliran data, diproyeksikan mencapai 150.700 gigabyte (GB) per detik, lebih dari 3 kali lebih banyak dari tiga tahun lalu.[8] Hal ini berkaitan dengan adanya peningkatan penggunaan internet melalui Survei Profil Internet Indonesia pada tahun 2022 yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia yang menyatakan bahwa jumlah penduduk terkoneksi internet mencapai 210.026.769 jiwa dari total populasi 272.682.600 jiwa penduduk Indonesia Tahun 2021. Yang mana, terdapat peningkatan persentase penetrasi internet di Indonesia dalam jangka waktu 2018-2022 (Q1) yaitu

---

[5]Chris Edwards, (et.al.), *Information Technology & The Law*, Palgrave Macmillan, London, 1990, hlm. 122.

[6]Deloitte, https://www2.deloitte.com/al/en/pages/legal/articles/gdpr.html, diakses pada 13 Desember 2022.

[7]Zurich Insurance Group, *Cross-border data flows Designing a global architecture for growth and innovation*, Zurich Insurance Group, 2022, hlm. 5.

[8]American Chamber of Commerce to the European Union, *The Transatlantic Digital Economy*, American Chamber of Commerce to the European Union, 2022, hlm. 54.

terdapat peningkatan sebesar 3,32% selama tahun 2021-2022 dari periode sebelumnya pada jangka waktu 2019-2020.[9]

Dengan adanya tindakan transfer data pribadi lintas batas bukan berarti akan selalu aman dan tanpa masalah. Terdapat kasus yang dikenal dengan *The Schrems Case*, dimana Maximillian Schrems yang telah menjadi pengguna Facebook sejak 2008 berdasarkan pengungkapan Edward Snowden pada tahun 2013 tentang praktik pengawasan yang digunakan oleh badan intelijen Amerika Serikat, Maximillian Schrems mengajukan keluhan kepada Komisaris Perlindungan Data Irlandia yang menuduh bahwa Facebook mentransfer datanya dari server Irlandia Facebook ke Amerika Serikat tanpa persetujuannya dan melanggar persyaratan Uni Eropa untuk memastikan perlindungan data yang setara. Badan Perlindungan Data Irlandia menolak klaim tersebut dan mengatakan bahwa *Privacy Shield* memberikan perlindungan yang cukup. Pengadilan Tinggi Irlandia kemudian mengkonsultasikan atas kasus tersebut dan Mahkamah Uni Eropa menerima evaluasinya. Namun, Mahkamah Uni Eropa membatalkan *Privacy Shield* dan Mahkamah Uni Eropa berpendapat bahwa sebelum menentukan kecukupan tersebut, Komisi Eropa seharusnya menegaskan bahwa hukum domestik negara ketiga yang dalam hal ini hukum domestik Amerika Serikat atau komitmen internasionalnya melindungi hak atas perlindungan data pribadi

[9]Asosiasi Penyelenggara Jasa Internet Indonesia, https://apjii.or.id/survei, diakses pada 20 Juli 2022.

yang seharusnya pada dasarnya setara.[10]

Kasus tersebut seolah memberikan fakta bahwa adanya tindakan transfer data pribadi lintas batas bukan tanpa hambatan. Salah satu permasalahannya adalah masalah yurisdiksi yang meliputi pilihan hukum yang berlaku dianggap cukup kompleks dalam aliran data pribadi lintas batas.[11] Hal ini dikarenakan setiap negara memiliki hukumnya sendiri yang merupakan hukum domestik atau bagian dari hukum domestik.[12] Selain itu, terdapat hambatan lainnya yaitu Peraturan penyimpanan lokal dan pemrosesan lokal yaitu persyaratan untuk menyimpan dan/atau memproses data pada server yang berlokasi di negara tertentu, Peraturan mengenai perlindungan data pribadi yang mengatur mengenai pengumpulan, penggunaan, dan transfer data pribadi, Keamanan siber yang meliputi kumpulan teknologi, proses, dan kontrol yang dirancang untuk melindungi sistem, jaringan, dan data dari eksploitasi yang tidak sah, hingga Pembatasan penggunaan Internet, penyensoran, dan pemblokiran terhadap transfer data.[13]

Berkaitan dengan adanya hambatan dalam pelaksanaan transfer data pribadi lintas batas tersebut, adanya kegiatan pengumpulan dan pemrosesan data pribadi dengan tujuan tanpa adanya persetujuan tentu berakibat pada

---

[10]Shakila Bu-Pasha, "Cross-Border Issues Under EU Data Protection Law With Regards To Personal Data Protection", *Information & Communications Technology Law*, Vol. 26, No. 3, 2017, hlm. 220.

[11]OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013, hlm. 9.

[12]OECD, "Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks", *OECD Digital Economy Papers No. 66*, OECD Publishing, Paris, 2000, hlm. 14.

[13]The OECD Digital Library, "Measuring the economic value of data and cross-border data flows", *OECD Digital Economy Papers*, No. 297, 2020, hlm. 28.

ketidaknyamanan Subjek Data, yang tentu melanggar hak atas privasi Subjek Data yang berarti bahwa setiap individu memiliki hak untuk memilih untuk berbagi atau tidak berbagi dengan orang lain informasi tentang dirinya, termasuk kehidupan pribadi, kebiasaan, tindakan, dan hubungan yang ia miliki.[14] Dengan adanya berbagai kasus terkait data pribadi, hal tersebut tentu melanggar hak privasi yang dimiliki Subjek Data yang memungkinkan individu untuk membatasi akses orang lain terhadap diri mereka sendiri dan informasi mereka.[15]

Menanggapi adanya kasus terkait transfer data pribadi lintas batas, berdampak pada kebijakan dan peraturan yang menangani aliran data lintas batas meningkat. Termasuk didalamnya mengenai diharuskannya memiliki perlindungan data pribadi yang setara guna mencegah adanya kasus pelanggaran data pribadi, karena saat terjadinya transfer data pribadi lintas batas tidak semua pihak memiliki kontrol atas data pribadi tersebut melainkan hanya bergantung pada negara penerima. Selain itu, terdapat berbagai alasan yang memotivasi negara-negara untuk mengatur aliran data lintas batas, mulai dari menjaga privasi individu dan data pribadi, perlindungan informasi yang dianggap sensitif hingga untuk mengembangkan kapasitas domestik di sektor yang intensif secara digital, sebagai bentuk kebijakan industri digital.[16]

Adanya kewajiban tingkat perlindungan yang sama atau yang memadai

---

[14]Dorothy J. Glancy, "The Invention of The Right to Privacy", *Arizona Law Review*, Vol. 21, No. 1, , 1979, hlm. 2.

[15]Adam Moore, "Defining privacy", *Journal of Social Philosophy*, Vol. 39, No. 3, 2008, hlm. 420.

[16]OECD, *Taking Stock Of Key Policies And Initiatives OECD Background Report For The G7 Digital And Technology Track*, OECD Publishing, Germany, 2022, hlm. 6.

bertujuan untuk meminimalisir adanya kegagalan dalam pemrosesan data pribadi. Menurut Pasal 37 *Data Protection Act* 2018 (selanjutnya disebut *Data Protection Act*) dikatakan bahwa data pribadi yang diproses untuk tujuan penegakan hukum apapun harus memadai, relevan, dan tidak berlebihan sehubungan dengan tujuan pemrosesannya, hal ini pun selaras dengan salah satu prinsip perlindungan data pribadi dalam *The EU General Data Protection Regulation (*selanjutnya disebut dengan EU GDPR) dan *The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy* (selanjutnya disebut *Madrid Resolution*). Perlindungan yang sama dalam hal ini merujuk pada istilah yang digunakan EU untuk menggambarkan negara, wilayah, sektor, atau organisasi internasional lain yang dianggapnya memberikan tingkat perlindungan data yang pada dasarnya setara dengan yang ada di dalam EU.[17] Maka, transfer data pribadi ke negara lain di luar Uni Eropa dapat terjadi ketika Komisi Eropa telah memutuskan bahwa negara tujuan data ketiga memberikan tingkat perlindungan data yang setara.[18]

Dalam *Recital* 104 EU GDPR dipertegas bahwa negara harus memberikan jaminan untuk memastikan perlindungan yang memadai, pada dasarnya setara dengan perlindungan di dalam UE, terutama ketika data pribadi diproses di satu atau lebih sektor tertentu. Secara khusus, negara ketiga harus memastikan mekanisme pengawasan dan kerjasama perlindungan data independen yang

[17]Information Commissioner's Office, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/, diakses pada 13 Desember 2022.

[18]Security, https://securiti.ai/blog/cross-borders-data-transfers-pipl/, diakses pada 13 Desember 2022.

efektif dengan otoritas perlindungan data negara anggota, dan harus memberikan subjek data hak yang efektif dan dapat ditegakkan serta upaya hukum administratif dan peradilan yang efektif.

Regulasi di Indonesia yang pertama kali berkaitan dengan tindakan transfer data pribadi lintas batas adalah PP PSTE terkait penyimpanan hingga pemrosesan data pribadi luar wilayah Indonesia dengan berkoordinasi dengan Menteri atau pejabat/lembaga yang diberi wewenang sebagaimana dijelaskan dalam PP PSTE. Kemudian, mengenai ketentuan dalam transfer data pribadi lintas batas harus memiliki tingkat perlindungan yang setara diatur dalam Pasal 56 Ayat 2 UU PDP yang menyatakan bahwa dalam melakukan transfer data pribadi, Pengendali Data Pribadi wajib memastikan negara tempat kedudukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima transfer Data Pribadi memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam UU PDP.

Dengan diaturnya mengenai kewajiban akan standar yang dianggap setara dan memadai antara negara pengirim dan negara penerima dalam proses transfer data pribadi lintas batas diharapkan pula kepatuhan mengenai standarisasi tersebut karena transfer data tetap menjadi masalah penting bagi pihak yang aktivitas bisnisnya melibatkan transfer data pribadi di negara non-UE ketiga. Mengingat beratnya sanksi jika terjadi pelanggaran aturan perlindungan data pribadi yang dapat mencapai €20 juta atau 4% dari omset global tahunan pihak tersebut.[19] Denda tersebut memiliki jumlah yang lebih

[19]Deloitte, *Op.cit.*

tinggi dibandingkan yang diatur dalam UU PDP yang mana sanksi paling tinggi ialah 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran dan diberikan oleh lembaga.

Hal ini selaras dengan tindakan atas pelanggaran bagi hukum kepercayaan atau *law of confidence* terkait kewajiban untuk menjaga kerahasiaan muncul ketika informasi rahasia diketahui oleh seseorang termasuk diantaranya otoritas publik seperti pada bidang kesehatan, keselamatan, dan lingkungan dalam keadaan yang tidak adil jika informasi tersebut diungkapkan kepada orang lain.[20] Namun, terjadi hal berupa pelanggaran atas data pribadi dan informasi tersebut telah digunakan untuk merugikan orang yang memilikinya, ganti rugi akan diberikan kepada orang yang bertanggung jawab.[21]

Dengan tidak setaranya tingkat perlindungan negara dalam kaitannya akan terjadinya transfer data pribadi lintas batas, maka akan meningkatkan tingkat probabilitas dari kegagalan data pribadi yang tentu melanggar hak pribadi seseorang. Berkaitan dengan transfer data pribadi lintas batas diperlukan adanya perjanjian ketika ingin melakukan transfer data pribadi lintas batas apabila tidak memenuhi standar setara dengan UU PDP, seperti halnya perjanjian antarnegara dalam lingkup ASEAN.[22] Dalam perjanjian tersebut harus ditegaskan pula bahwa data pribadi tidak boleh dialihkan ke suatu negara

[20]Health and Safety Executive, https://www.hse.gov.uk/enforce/enforcementguide/court/reporting-breach.htm#:~:text=Breach%20of%20confidence%20is%20the,3., diakses pada 13 Januari 2023.

[21]David I. Bainbridge, *Introduction to Computer Law*, Pitman Publishing, London, 1993, hlm. 55.

[22]Yusuf, https://aptika.kominfo.go.id/2020/08/transfer-data-antarnegara-bisa-dilakukan-jika-memiliki-aturan-setara-uu-pdp/, diakses pada 20 Juli 2022.

atau wilayah kecuali negara atau wilayah tersebut memastikan tingkat perlindungan yang memadai untuk hak dan kebebasan subjek data sehubungan dengan pemrosesan data pribadi.[23] Hingga saat ini, Komisi Eropa sejauh ini telah mengakui beberapa negara yang memiliki standar perlindungan yang memadai atau setara, antara lain Andorra, Argentina, Kanada, Kepulauan Faroe, Guernsey, Israel, Isle of Man, Jepang, Jersey, Selandia Baru, Republik Korea, Swiss, Inggris Raya di bawah EU GDPR dan LED, dan Uruguay.[24]

Jepang menjadi negara pertama di Asia Pasifik yang mendapatkan Keputusan Kecukupan atau *Adequacy Decision* oleh Komisi Eropa pada 23 Januari 2019. *Adequacy Decision* tersebut mengizinkan transfer data pribadi dari Wilayah Ekonomi Eropa yaitu 28 (dua puluh delapan) negara anggota Uni Eropa ditambah Norwegia, Liechtenstein, dan Islandia) ke Jepang. Komisi Perlindungan Informasi Pribadi Jepang atau *Japan's Personal Information Protection Commission* (selanjutnya disebut PPC) juga mengeluarkan pemberitahuan pada hari yang sama yang menunjukkan bahwa negara-negara anggota Wilayah Ekonomi Eropa ditambahkan ke *whitelist* atau daftar putih Jepang untuk transfer data pribadi lintas batas terkait Act on the Protection of Personal Information (selanjutnya disebut APPI).[25]

UU PDP sendiri di sahkan dengan tujuan sebagai bentuk kepastian hukum

---

[23]Ombudsman Cayman Island, https://ombudsman.ky/images/pdf/guide/60-eighth-data-protection-principle-international-transfers.pdf, diakses pada 17 November 2022.

[24]European Comission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, diakses pada 17 Maret 2023.

[25] Tim Hickman, Shino Asayama, https://www.whitecase.com/insight-alert/eu-japan-adequacy-decision-now-force, diakses pada 16 Maret 2023.

dan diproyeksikan antara lain untuk menjawab realitas ketiadaan standar dan kriteria perlindungan data pribadi.[26] Hal ini selaras dengan adanya asas kepastian hukum dalam Pasal 3 Huruf B UU PDP yang bertujuan agar setiap pemrosesan data pribadi dilakukan atas dasar landasan hukum perlindungan data pribadi dan pelaksanaan langkah-langkah pendukung untuk mendapatkan sanksi hukum di dalam dan di luar pengadilan.

Diharapkan dengan disahkannya UU PDP dapat lebih mengakomodir mengenai transfer data pribadi lintas batas lebih rinci agar PSE yang melakukan transfer data pribadi lintas batas tidak lagi seolah meraba-raba atau mengira-ngira bahwa sistem keamanan yang mereka miliki memadai dan setara dengan UU PDP dan Subjek Data dapat lebih merasa aman mengenai data yang akan diproses. Terlebih, diharapkan dengan disahkannya UU PDP dapat berkaca pada APPI yang telah mendapatkan *Adequacy Decision* dari EU GDPR sejak tahun 2019 sekaligus menjadi negara pertama di Asia Pasifik yang mendapatkan *Adequacy Decision.*

Berdasarkan penelusuran yang telah dilakukan, terdapat beberapa skripsi yang berkaitan dengan data pribadi yang menjadi acuan bagi Peneliti, diantaranya yaitu:

1. "Tanggung Jawab Hukum *Internet Intermediary* Terhadap Perlindungan Data Pribadi Berdasarkan Hukum Positif Di Indonesia Serta Peraturan Di *European Union*" oleh Antonia Regirma Chrisly F. dengan NPM

[26]Prof. Dr. Ahmad M Ramli, https://nasional.kompas.com/read/2022/09/25/13335721/tafsir-uuperlindungan-data-pribadi-yang-perlu-diketahui., diakses pada 16 Maret 2023.

110110170093.

2. "Pelindungan Data Pribadi Atas Kebocoran Data Pengguna Situs Platform Desain Grafis Dikaitkan Dengan *Virtual Jurisdiction* Berdasarkan Hukum Positif Di Indonesia" oleh Fani Yofrisa Ismar dengan NPM 110110170381.

Berdasarkan hal tersebut, Peneliti tertarik untuk membuat penelitian dalam bentuk tugas akhir dengan judul **"PELINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA DALAM TRANSFER DATA PRIBADI LINTAS BATAS *(TRANSBORDER PERSONAL DATA TRANSFER)* BERDASARKAN PRINSIP *ADEQUACY* DITINJAU DARI HUKUM POSITIF INDONESIA"**.

B. Identifikasi Masalah

1. Bagaimana proses pelaksanaan transfer data pribadi yang diatur di Indonesia dalam kaitannya dengan *Transborder Personal Data Transfer*?
2. Bagaimana Hukum Positif Indonesia dapat memberikan perlindungan transfer data pribadi warga negara Indonesia ke negara lain yang tidak memiliki tingkat perlindungan sama (*adequate*) dalam kaitannya dengan *Transborder Personal Data Transfer*?

C. Tujuan Penelitian

1. Penelitian ini untuk mengetahui bagaimana proses pelaksanaan *Transborder Personal Data Transfer* di Indonesia dalam kaitannya dengan dianggapnya telah memiliki standar perlindungan yang sama dengan negara penerima.

2. Penelitian ini untuk menganalisis bagaimana Hukum Positif Indonesia dapat memberikan perlindungan hukum atas transfer data pribadi warga negara Indonesia dalam kaitannya dengan pelaksanaan *Transborder Personal Data Transfer* dengan negara lain yang tidak memiliki perlindungan yang sama (*adequacy)*.

D. Kegunaan Penelitian

1. Kegunaan Penelitian Umum:

   Dikarenakan meningkatnya tindakan transfer data pribadi lintas batas yang dapat dilakukan setiap saat yang mana tindakan tersebut terjadi tidak hanya pada yurisdiksi di Indonesia melainkan melibatkan yurisdiksi di luar Indonesia dan dikarenakan melihat adanya kasus *The Schrems Case* dimana adanya kasus pelanggaran data pribadi atas tindakan transfer data pribadi lintas batas tanpa persetujuan Subjek Data. Berdasarkan hal tersebut penelitian ini dilakukan dengan harapan dapat menambah wawasan masyarakat, terutama dalam kaitan seberapa penting data pribadi yang dimiliki.

2. Kegunaan Penelitian Praktis:
   a. Penelitian ini diharapkan dapat mengetahui lebih lanjut mengenai bagaimana proses pelaksanaan *Transborder Personal Data Transfer* di Indonesia.
   b. Penelitian ini diharapkan dapat memberikan perlindungan pada Subjek Data berdasarkan Hukum Positif Indonesia dalam kaitannya terjadinya *Transborder Personal Data Transfer* ke negara lain yang

tidak memiliki tingkat perlindungan sama.

E. Kerangka Pemikiran

Dengan adanya tindakan terkait data pribadi harus dirancang, dilakukan, dilaporkan dan didokumentasikan dengan tingkat kualitas dan transparansi yang memadai dan setara. Kualitas data harus dipertimbangkan dengan cermat karena menggunakan data berkualitas buruk untuk pengambilan keputusan dapat membahayakan satu atau lebih individu atau kelompok individu. Kualitas data harus diperiksa tujuan dan perlindungannya untuk menghindari dampak buruk yang jika memungkinkan, termasuk munculnya pelanggaran atas data pribadi.[27] Pasal 88 *Data Protection Act* 2018 mengatur mengenai pemrosesan data pribadi yang harus diproses secara memadai dan setara:

> *"Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."*

Pasal tersebut memiliki makna yang selaras dengan Pasal 8 *Madrid Resolution* yang mana menyatakan bahwa pemrosesan data pribadi harus disesuaikan dengan pemrosesan yang memadai, relevan, dan sejalan dengan tujuan yang ditetapkan di bagian sebelumnya. Lebih lanjut, Pasal 8 Ayat 2 *Madrid Resolution* mengatur bahwa secara khusus, penanggung jawab harus melakukan upaya yang wajar untuk membatasi data pribadi yang diproses seminimal mungkin yang diperlukan. Kemudian Pasal 45 Ayat 1 EU GDPR mengatur lebih lanjut dengan adanya transfer data pribadi lintas batas antara

[27]United Nations Sustainable Development Group, *Data Privacy, Ethics And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda*, 2017, hlm. 6.

wilayah atau satu atau lebih sektor tertentu di negara ketiga atau organisasi internasional yang bersangkutan memastikan tingkat perlindungan yang memadai:

> *"A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection."*

Sehubungan dengan adanya kewajiban untuk memastikan tingkat perlindungan yang memadai atau setara dalam tindakan transfer data pribadi, terdapat persetujuan yang menjadi dasar dalam melakukan pemrosesan data pribadi sebagaimana diatur dalam Pasal 20 UU PDP. Persetujuan dianggap cukup jika persetujuan tersebut diberikan secara sukarela, diberitahukan, dan diberikan secara tertulis. Persetujuan yang memadai harus diperoleh sebelum pengumpulan data atau jika tujuan penggunaan ulang data berbeda dari tujuan awal diperolehnya persetujuan. Persetujuan harus diperoleh sebelum data dikumpulkan atau digunakan, dan individu harus dapat menarik persetujuan atau menolak penggunaan data mereka.[28]

Alan Westin dalam bukunya berjudul *Privacy and Freedom* mengatakan bahwa data pribadi berkaitan dengan hak atas privasi, dimana data yang dimiliki oleh manusia sangat erat kaitannya dengan hak atas privasi, karena privasi didefinisikan sebagai persetujuan untuk menentukan kapan, bagaimana, dan sejauh mana informasi tentang orang tersebut dapat dikomunikasikan kepada orang lain.[29] Privasi sendiri diartikan sebagai kemampuan individu

[28]*Ibid,* hlm. 8.
[29]Westin. A. F., *Privacy and Freedom*, H: Wolff, New York, 1967, hlm. 7.

untuk mengontrol kapan, sejauh mana, dan bagaimana informasi tentang diri pribadinya dapat dikomunikasikan kepada orang lain.[30] Adanya privasi tentu erat kaitannya dengan data pribadi, sebagaimana data pribadi merupakan hal yang terdapat dalam ruang lingkup privasi.

Warren dan Brandeis menyatakan bahwa perlu bagi sistem hukum untuk mengakui hak atas privasi karena, ketika informasi tentang kehidupan pribadi seseorang tersedia bagi orang lain, hal itu cenderung mempengaruhi dan bahkan melukai inti kepribadian seseorang, penilaiannya tentang dirinya sendiri.[31] Warren dan Brandeis memperdebatkan adanya hak privasi, yang mereka yakini telah dilindungi oleh pengadilan secara tidak langsung melalui bidang hukum lainnya, seperti pencemaran nama baik, properti, atau kontrak. Mereka berpendapat bahwa dalam kasus di mana privasi dipertaruhkan, keputusan akan lebih masuk akal jika hak privasi langsung diminta.[32] Tidak adanya hak umum untuk privasi telah dikritik tetapi kesulitan dalam mencapai keseimbangan antara kepentingan individu dan kebebasan berbicara harus diakui sehubungan dengan perkembangan atas teknologi komputer dan penyimpanan, manipulasi, dan pengambilan informasi tentang orang yang masih hidup, privasi dan perlindungan memiliki arti khusus, hal ini menjadi salah satu alasan dibentuknya *Data Protection Act* 1984 mengingat urgensi atas perlindungan atas privasi.[33]

---

[30]Ellison, N.B., (et.al), *Negotiating privacy concerns and social capital needs in a social media environment In Privacy Online*, Springer, Berlin, 2011, hlm. 19-32.

[31]Dorothy J. Glancy, *Op.cit.*, hlm. 2.

[32] Philosophy of Law, Warren and Brandeis on Privacy (pomona.edu) diakses pada 28 Juli 2023

[33]David I. Bainbridge, *Op.cit.*, hlm. 195

Definisi mengenai data pribadi diatur dalam Pasal 1 Ayat 1 Permen No. 20 Tahun 2016 yang menjelaskan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Selain Permen No. 20 Tahun 2016, UU PDP dan PP PSTE memiliki definisi serupa Pada Pasal 1 Ayat 1 yang menyatakan bahwa 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.

Dalam Penjelasan Umum PDP, dikatakan bahwa penggunaan teknologi informasi memudahkan data pribadi seseorang untuk dikumpulkan dan dipindahkan dari satu pihak ke pihak lain tanpa persetujuan dari Subjek Data, sehingga mengancam hak konstitusional Subjek Data. Nyatanya, perlindungan data pribadi termasuk dalam perlindungan hak asasi manusia, oleh karena itu pengawasan terhadap data pribadi merupakan wujud dari pengakuan dan perlindungan atas hak asasi manusia. Masalah perlindungan data pribadi muncul dari kekhawatiran adanya pelanggaran terhadap data pribadi yang mungkin dialami oleh individu dan/atau badan hukum yang dapat mengakibatkan kerugian materiil dan immateriil. Yang mana, dengan tidak adanya perlindungan atas privasi yang dimiliki oleh Subjek Data terutama dalam tindakan transfer data pribadi lintas batas dapat berakibat pada adanya pelanggaran data pribadi seperti pada kasus *The Schrems Case* yang dialami Maximillian Schrems dalam putusan Mahkamah Eropa tanggal 6 Oktober 2015

dalam Kasus C-362/14.[34]

Inisiasi untuk memberikan perlindungan atas privasi di Indonesia diatur pertama kali dalam Undang-Undang Dasar 1945 (selanjutnya disebut UUD 1945).[35] Terkait hak asasi manusia yang tercantum dalam UUD 1945, hal ini dapat merujuk pada Pasal 28F UUD 1945 yang menyatakan bahwa hak berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta hak mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia. Hak untuk memperoleh informasi tidak terbatas hanya kepada cara perolehan informasi melalui kontak secara langsung, melainkan dapat dilakukan dengan penggunaan *platform online* yang menggunakan internet maupun teknologi tertentu.

Sejalan dengan adanya hak asasi untuk memperoleh informasi, dalam Pasal 28G UUD 1945 mengatur bahwa:

> "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."

Dengan adanya ketentuan tersebut yang jika dikaitkan dengan Pasal 28F sebelumnya, dapat diartikan bahwa tiap orang berhak mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi asalkan tidak bertentangan dengan hak asasi manusia lainnya dan tidak diizinkan pula

[34]European Parliment, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0529_EN.html#def_1_2, diakses pada 15 Maret 2023.

[35]Sinta Dewi Rosadi, *Privacy on personal data from International Law, Regional and National Perspectives*, Refika Aditama, Jakarta, 2015, hlm. 8.

adanya penyerangan terhadap kehormatan, martabat, dan harta benda dalam hal apapun yang mengakibatkan orang tersebut merasa tidak aman dan merasa adanya ancaman ketakutan.

Pengaturan mengenai hak privasi diatur dalam Pasal 12 *Universal Declaration of Human Rights* (selanjutnya disebut UDHR), dikatakan bahwa tidak seorang pun boleh diganggu secara sewenang-wenang terhadap privasi, keluarga, rumah atau korespondensinya, atau serangan terhadap kehormatan dan reputasinya. Kehadiran dari Pasal 12 UDHR diperkuat dengan adanya Pasal 17 *International Covenant on Civil and Political Rights* (selanjutnya disebut ICCPR) yang mengandung pasal dengan definisi serupa dengan Pasal 12 UDHR.

Perlindungan diri pribadi dapat mengacu pada perlindungan atas data yang dimiliki, termasuk di dalamnya data yang dibuat, dikumpulkan, diakses, diproses, dan ditransfer dalam lingkup bisnis.[36] Tak hanya Indonesia, sejumlah negara juga mengakui perlindungan data sebagai hak konstitusional sebagai hak seseorang untuk mendapatkan perlindungan atas data yang dimilikinya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya.[37] Mengacu PP PSTE menjelaskan terkait definisi dari Data Pribadi, yaitu:

> *"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."*

[36]The 1st ASEAN Digital Senior Officials' Meeting (ADGSOM*), ASEAN Data Management Framework: Data Governance and Protection Throughout The Data Lifecycle*, 2021, hlm. 8.

[37]Sinta Dewi Rosadi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia", *Yustisia Jurnal Hukum*, Vol. 5, No. 1, 2016, hlm. 26.

Dalam regulasi internasional terdapat *The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (selanjutnya disebut *OECD Privacy Guidelines*) yang menjelaskan terkait definisi data pribadi dalam Pasal 1 Huruf B yang menyatakan bahwa data pribadi berarti informasi apa pun yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi oleh Subjek Data. Dapat diartikan bahwa data pribadi memiliki cakupan yang luas dan tidak hanya terbatas pada apa yang kita daftarkan pada PSE saja seperti nama lengkap ataupun nomor telpon saja. Melainkan, jauh lebih kompleks dibanding itu semua.

Berkaitan dengan apa yang diutarakan dalam *OECD Privacy Guidelines,* UU PDP dalam Pasal 4 mengatur bahwa data pribadi seseorang juga memiliki macam-macamnya, yang terbagi menjadi 2 yaitu Data Pribadi yang bersifat spesifik dan Data Pribadi yang bersifat umum. Data Pribadi bukan hadir tanpa kegunaan, dalam hal adanya pendaftaran serta pendataan dalam rangka penggunaan fitur yang dimiliki oleh PSE, maka akan dilakukannya pemrosesan data pribadi oleh PSE tersebut. Dalam Pasal 16 Ayat (1) UU PDP menjelaskan bahwa makna dari pemrosesan data pribadi meliputi tindakan pemerolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaharuan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, dan/atau penghapusan atau pemusnahan. Dalam Pasal 4 Ayat 23 EU GDPR, dijelaskan mengenaid definisi transfer data pribadi lintas batas, yaitu:

> "*(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a*

> *controller or processor in the Union where the controller or processor is established in more than one Member State; or*
> *(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*"

Transfer data pribadi lintas batas terutama ke negara ketiga hanya dapat terjadi jika tingkat perlindungan yang memadai dipastikan. Oleh karena itu, jika negara ketiga memiliki tingkat perlindungan memadai yang sama, transfer akan sah.[38] Negara-negara dengan undang-undang perlindungan data pribadi yang ketat khawatir bahwa jika transfer data pribadi lintas batas diizinkan masuk ke negara lain yang tidak memberikan tingkat perlindungan yang sama, tidak akan adanya perlindungan yang dianggap memadai dan ketat untuk melindungi data pribadi yang ada.[39]

Dengan adanya tindakan berupa pemrosesan data pribadi milik Subjek Data, diatur pula terkait prinsip-prinsip Pelindungan Data Pribadi sebagaimana diatur dalam Pasal 16 Ayat (2) UU PDP yaitu Pengumpulan data pribadi dilakukan secara terbatas dan khusus, sah menurut hukum dan transparan, serta pengolahan data pribadi harus dilakukan sesuai peruntukannya dengan tetap menjamin hak-hak Subjek Data secara akurat dan lengkap, tidak menyesatkan, dan dapat dipertanggungjawabkan.

Pemrosesan data pribadi tersebut harus sesuai dengan prinsip dalam UU PDP yang memiliki keamanan dari kemungkinan adanya akses yang tidak sah,

---

[38]Yves Poullet, (et.al), "Data Protection and Privacy in Global Networks: A European Approach*", 8 Elec. Data Interchange L.R.*, No. 147, 2001, hlm. 163.

[39]Beling, Craig T. "Transborder Data Flows: International Privacy Protection and the Free Flow of Information". *Boston College International and Comparative Law Review*, Vol. 6, No. 2, 1983, hlm. 593.

pengungkapan yang tidak sah, modifikasi yang tidak sah, penyalahgunaan, perusakan dan/atau kehilangan data pribadi. Dan setiap tindakan pemrosesan data pribadi harus memberitahukan tujuan dan kegiatan pemrosesan pada subjek data termasuk apabila terjadi kegagalan perlindungan data pribadi yang mana tujuan tersebut tidak boleh diluar atau bertentangan dari apa yang telah diinformasikan kepada Subjek Data sebelumnya. Serta adanya ketentuan bahwa data pribadi dapat dimusnahkan dan/atau dihapus setelah periode penyimpanan berakhir atau berdasarkan permintaan Subjek Data kecuali ditentukan lain oleh peraturan perundang-undangan dan pemrosesannya dilakukan dengan bertanggung jawab dan dapat dibuktikan dengan jelas. Hal ini dapat terlihat dari adanya sanksi yang akan dikenakan dalam UU PDP apabila melanggar prinsip pelindungan data pribadi mulai dari sanksi administratif hingga ketentuan pidana.

Kemudian dalam Pasal 26 EU GDPR menjelaskan terkait pentingnya prinsip-prinsip dalam perlindungan data pribadi yang tidak boleh berlaku untuk informasi anonim, yaitu informasi yang tidak terkait dengan orang perorangan yang teridentifikasi atau dapat diidentifikasi atau dengan data pribadi yang dibuat anonim sedemikian rupa sehingga subjek data tidak dapat atau tidak lagi dapat diidentifikasi. Hal ini dikarenakan dalam hal pemrosesan maupun perlindungan atas data pribadi yang dimiliki maka harus dapat merujuk kepada siapa data pribadi tersebut dimiliki.

Dalam Pasal 56 UU PDP menyatakan mengenai pihak-pihak yang terlibat dalam tindakan transfer data pribadi lintas batas, antara lain Pengendali Data

Pribadi yang merupakan pihak bertindak yang secara sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi, Prosesor Data Pribadi yang merupakan yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi, dan Subjek Data selaku pemilik data pribadi. Dan lebih lanjut, dalam Pasal 57 UU PDP dikenakan adanya pemberian sanksi bagi yang melanggar Pasal 56 UU PDP dan sanksi tersebut diberikan oleh lembaga, yaitu pihak yang melakukan penyelenggaraan Pelindungan Data Pribadi dan bertanggungjawab kepada presiden sebagaimana dalam Pasal 58 UU PDP.

Dalam pelaksanaanya transfer data pribadi lintas batas dapat dilakukan oleh siapapun dari berbagai media. Data tersebut biasanya akan disimpan atau diproses ulang di negara selain negara asal. Transfer data pribadi lintas batas umumnya dapat diklasifikasikan ke dalam empat jenis standar informasi yaitu pribadi, bisnis, teknis, dan organisasi. Jenis-jenis ini umumnya digunakan dalam empat konteks utama, yaitu informasi intra-perusahaan, informasi antar perusahaan, kebutuhan informasi pemerintah, dan pengejaran transnasional sumber daya informasi, yaitu penggunaan sumber daya informasi terhadap database jarak jauh.[40] Ketika terjadi transfer data pribadi antar antar dan intra perusahaan, perjanjian transfer data perusahaan atau aturan perusahaan yang mengikat sering digunakan sebagai instrumen hukum.[41] Dan untuk

[40]Chris Edwards, (et.al.), Op.cit, hlm. 121.

[41]Asosiasi Praktisi Pelindungan Data Pribadi, https://appdi.or.id/tantangan-pengiriman-data-pribadi-lintas-negara/, diakses pada 17 November 2022.

memfasilitasi perdagangan internasional, perlindungan yang memadai terkait dengan privasi pada data pribadi khususnya transfer data pribadi lintas batas merupakan prasyarat yang harus dipertimbangkan.[42]

Suatu data diklasifikasikan menjadi lima kategori atau status identifikasi data, yang meliputi data yang diidentifikasi yaitu data yang secara jelas dapat dikaitkan dengan orang tertentu karena informasi identitas pribadi dapat diamati dalam informasi tersebut, data pseudonim yaitu data yang semua pengenalnya diganti dengan alias yang penugasan aliasnya sedemikian rupa sehingga tidak dapat dibalik dengan upaya yang wajar dari siapa pun selain pihak yang melakukannya, data pseudonim yang tidak ditautkan yaitu data yang semua pengidentifikasinya dihapus atau diganti dengan alias yang fungsi penugasannya dihapus atau tidak dapat diubah, sehingga tautan tidak dapat dibuat kembali dengan upaya yang wajar dari siapa pun termasuk pihak yang melakukannya, data yang dianonimkan yaitu data yang tidak ditautkan dan atribut mana yang diubah sedemikian rupa sehingga ada tingkat kepercayaan yang wajar bahwa seseorang tidak dapat diidentifikasi, secara langsung atau tidak langsung, oleh data itu sendiri atau dalam kombinasi dengan data lain, dan data agrega yaitu data statistik yang tidak berisi entri tingkat individu dan digabungkan dari informasi tentang cukup banyak orang yang berbeda sehingga atribut tingkat individu tidak dapat diidentifikasi.[43]

Dalam kaitannya dengan transfer data pribadi lintas batas umumnya dapat

[42]Sinta Dewi Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia", *Brawijaya Law Journal*, Vol. 5, No. 2, 2018,hlm. 148-149.

[43]OECD, *Mapping Approaches To Data And Data Flows Report for the G20 Digital Economy Task Force*, OECD Library, Saudi Arabia, 2020, hlm. 13-14.

diklasifikasikan ke dalam empat jenis standar informasi pribadi, bisnis, teknis dan organisasi. Jenis-jenis ini umumnya digunakan dalam empat konteks utama informasi yaitu intra-perusahaan, informasi antar-perusahaan, kebutuhan informasi pemerintah, dan pengejaran transnasional sumber daya informasi, yaitu penggunaan database secara jarak jauh.[44]

Dengan adanya regulasi baik di Indonesia maupun regulasi internasional yang mengatur terkait pemrosesan data pribadi, diharapkan tidak adanya kasus kebocoran maupun kegagalan pemrosesan data pribadi, terutama mengenai adanya standar perlindungan yang setara bagi tiap negara yang akan melaksanakan transfer data pribadi lintas batas, dalam hal ini pemrosesan data pribadi tidak hanya dilakukan di wilayah Indonesia, melainkan dapat dilakukan di luar wilayah Indonesia sebagaimana Pasal 20 dan Pasal 21 PP PSTE yang menyatakan bahwa PSE baik dalam lingkup publik maupun lingkup privat dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di wilayah Indonesia dan/atau di luar wilayah Indonesia.

Dimana, transfer data pribadi lintas batas merujuk pada transmisi data atau informasi di atas batas-batas nasional.[45] Contoh dari adanya tindakan Transfer Data Pribadi Lintas Batas adalah transaksi yang menyertakan informasi yang dapat diidentifikasi secara pribadi, seperti riwayat kredit, catatan kriminal, catatan pekerjaan, riwayat medis, dan daftar nama. Informasi yang dapat

[44] Walden, I., Savage, N, Transborder Data Flows. In: Edwards, C., Savage, N., Walden, I. (eds) *Information Technology & The Law*, Palgrave Macmillan, London, 1990, hlm. 121

[45]Hardy, I.Trotter.," Transborder Data Flow: An Overview and Critique of Recent Concerns", *William & Mary Law School Scholarship Repository*, 1983, hlm. 19.

diidentifikasi secara pribadi tersebut kemudian muncul dalam aliran data komersial dan keuangan.[46] Dengan adanya manfaat yang dialami, maka kemudian timbul tantangan seperti pertanyaan mengenai yurisdiksi yaitu kemampuan pengadilan untuk melakukan penyelesaian sengketa yang didasarkan kehadiran fisik pihak terkait dalam forum hukum atau setidak-tidaknya perilaku pihak terkait yang terikat pada forum.[47] Namun, hal ini berbeda dengan penggunaan internet yang tidak peduli pada lokasi fisik dimana lokasi pengguna internet sulit untuk ditetapkan. Perlindungan hak pribadi dan arus informasi lintas batas merupakan hal yang dilematis, bagaimana satu pihak ingin mencapai kebebasan namun di pihak lain harus menjaga perlindungan hak pribadi terlebih informasi tersebut dapat menjangkau lintas batas negara.[48]

Dengan adanya tindakan transmisi yang merupakan termasuk dalam tindakan pemrosesan tersebut maka diperlukannya perlindungan data pribadi yang komprehensif dan setara terkait akan dilaksanakannya hingga selesai dilaksanakannya pengiriman data pribadi ke luar negeri serta kualifikasi dan syarat secara rinci terkait apa saja yang diperlukan dengan kaitannya akan dilaksanakannya pengiriman data pribadi tersebut.

F. Metode Penelitian

1. Metode Pendekatan

[46]Beling, Craig T, *Op.cit.*, hlm. 19.

[47]D. Burk, "Jurisdiction In A World Without Borders", *Virginia Journal Law & Technology*, 1 Va. J.L. & Tech. 3, 1997, hlm. 2.

[48]Nudirman Munir, *Pengantar Hukum Siber Indonesia*, PT Raja Grafindo Persada, Depok, 2017, hlm. 77.

Metode penelitian yang digunakan adalah yuridis komparatif, dengan membandingkan undang-undang suatu negara dengan undang-undang yang satu atau lebih dengan negara lain mengenai hal yang sama.[49] Melalui metode ini akan dilakukan perbandingan antara undang-undang negara Negara Indonesia dengan undang-undang Negara Jepang mengenai data pribadi dan *adequacy* melalui data-data yang didapatkan dari undang-undang serta peraturan dibawahnya, buku, jurnal, dan artikel yang didapatkan melalui internet.

2. Spesifikasi Penelitian

Pada penelitian ini menggunakan spesifikasi penelitian berupa Deskriptif-Analitis yang mana dirancang untuk memberikan gambaran serta analisis penerapan dalam peraturan berdasarkan ketentuan hukum yang berlaku. Demikian pula, dimaksudkan untuk memberikan gambaran yang realistis tentang suatu objek atau keadaan masalah sehingga dapat dianalisis dengan ditarik kesimpulan umum.[50] Pada penelitian ini akan menggambarkan mengenai bagaimana proses pelaksanaan *Transborder Personal Data Transfer* hingga bagaimana pertanggungjawaban terhadap Subjek Data dalam proses pelaksanaan *Transborder Personal Data Transfer.*

3. Tahapan Penelitian

Tahap penelitian yang akan Peneliti lakukan meliputi tahapan sebagai

[49]Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi*, Kencana Prenada Media Group, Jakarta, 2016, hlm. 93.

[50]Ashofa Burhan, *Metode Penelitian Hukum*, Rineka Cipta, Jakarta, 2013, hlm. 19.

berikut:

a. Studi Kepustakaan

1) Bahan Hukum Primer, yaitu peraturan perundang-undangan yang berlaku, di antaranya:

a) Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi;

b) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, Tanggal 1 Desember 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik;

c) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

d) The EU General Data Protection Regulation;

e) Act on the Protection of Personal Information.

2) Bahan Hukum Sekunder, adalah hukum yang memberikan penjelasan atas keterangan atau sebagai pendukung bahan hukum primer yang dapat berupa buku-buku, jurnal, ataupun majalah yang ditulis oleh para sarjana hukum, teori-teori, dan pendapat ahli, serta situs internet yang berhubungan dengan permasalahan tersebut dan semacamnya.

3) Bahan Hukum Tersier, adalah bahan hukum yang memberikan petunjuk dari bahan hukum primer dan bahan hukum sekunder. Dapat berupa kamus umum, kamus hukum, kamus besar bahasa

Indonesia dan kamus berbahasa Inggris.[51]

b. Studi Lapangan

Studi lapangan merupakan tahap penelitian dimana data yang diperoleh Peneliti didapatkan langsung dari sumber pertama di lapangan, baik dari responden maupun narasumber.[52] Studi lapangan ini dilakukan dengan melakukan wawancara dengan beberapa pihak yang dianggap ahli di bidang ini guna mengetahui mengenai hal-hal yang belum Peneliti ketahui maupun belum temukan jawabannya sehingga diharapkan bisa didapatkannya jawaban yang lebih luas dan lengkap.

4. Teknik Pengumpulan Data

a. Studi Kepustakaan

Studi kepustakaan merupakan jenis data sekunder dengan data yang diperoleh bukan langsung dari sumber pertama, tetapi dari data yang terekam dalam bentuk bahan hukum.[53]

b. Teknik Wawancara

Dalam melakukan pengumpulan data juga dilakukan dengan beberapa pihak yang berkaitan, antara lain:

1) Direktorat Jenderal Aplikasi Informatika;
2) Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI).

---

[51]Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Rajawali Press, Jakarta, 1990, hlm. 14-15.

[52]I Made Pasek Diantha, *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*, Kencana, Jakarta, 2016, hlm. 192.

[53]*Ibid.*

5. Teknik Analisis Data

Dalam penelitian ini menggunakan teknik analisis data dengan yuridis kualitatif, yang melakukan pengkajian hasil olah data yang tidak berbentuk angka serta lebih menekankan analisis hukumnya pada proses penyimpulan deduktif, berupa penarikan kesimpulan dari yang umum ke khusus dan penyimpulan induktif dengan menggunakan cara-cara berfikir formal dan argumentatif.[54]

[54]M. Syamsuddin, *Operasionalisasi Penelitian Hukum*, Grafindo Persada, Jakarta, 2007, hlm. 133.