BAB I

PENDAHULUAN

A. Latar Belakang

Globalisasi terbentuk karena adanya pengglobalan negara-negara dunia. Arus informasi menyebabkan tidak adanya batas ruang dan waktu untuk mengetahui segala sesuatu yang berada di luar negaranya. Batasan negara sudah tidak ada lagi karena adanya teknologi informasi yang semakin canggih.[1]

Informasi mempunyai peranan penting di dalam kehidupan manusia. Melalui kemajuan informasi, komunikasi, dan teknologi (*Information Communication Technology/ICT*) dapat mendorong perkembangan dan pertumbuhan ekonomi dunia.[2] Teknologi informasi dan komunikasi (TIK) telah mengubah prilaku masyarakat dan peradaban manusia secara global. Perkembangan teknologi informasi telah menyebabkan perubahan sosial yang secara signifikan berlangsung dengan cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[3]

---

[1] Abdul Wahid dan Mohammad Labib, 2010. *Kejahatan Mayantara (CyberCrime),* Refika Aditama, Bandung, hlm. 8. Lihat juga Hendra Halwani, 2002, *Ekonomi Internasional & Globalisasi Ekonomi*, Ghalia, Jakarta, hlm. 10.

[2] Istilah Teknologi Informasi dikenal pertama kali pada tahun 1989 saat dilakukannya merger Siemens dan Nixdorf. Lihat Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi,* Refika Aditama, Bandung, hlm. 131.

[3] Ahmad M. Ramli, 2004, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia,* Refika Aditama, Bandung, hlm. 1.

Berbagai penemuan di bidang teknologi informasi dan komunikasi saat ini memungkinkan orang menggunakan internet melalui komputer pribadi (*personal computer/PC*) atau media elektronik lainnya di manapun. Teknologi informasi dan komunikasi saat ini dimanfaatkan oleh pribadi (individu), korporasi, pemerintah dan kelompok-kelompok masyarakat untuk berbagai aktivitas, seperti pendidikan, kesehatan, bisnis, pemerintahan, komunikasi, hiburan dan lain-lain.[4]

Perkembangan komputer yang diikuti oleh perkembangan TIK[5] melahirkan jaringan komputer sebagai cikal bakal internet. Menurut Mueller, internet[6] merupakan komunikasi data global yang diwujudkan oleh interkoneksi jaringan telekomunikasi publik dan swasta dengan menggunakan *Internet Protocol* (IP), *Transmission Control Protocol* (TCP) dan protokol lain yang diperlukan guna mengimplementasikan *Internet Protocol* bekerja dalam skala global, seperti *Domain Name System* (DNS) dan paket protokol r*outing.*[7]

Sebagai alat komunikasi, melalui penggunaan arsitektur IP jaringan terbuka (*open network* IP), pengguna dapat melakukan pertukaran informasi melewati batas

[4] Sigid Suseno, 2012, *Yurisdiksi Tindak Pidana Siber*, Refika Aditama, Bandung, hlm. 1.

[5] Konvergensi TIK meliputi integrasi perangkat keras dan perangkat lunak teknologi informasi ke dalam sistem telekomunikasi, digitalisasi jaringan, dan peningkatan jaringan internet. Lihat Danrivanto Budhijanto, 2010, *Op cit.*, hlm. 5.

[6] *Internet is a collection of interconnected networks using the Internet Protocol which allows them to functionas a single, large virtual network* (internet adalah Kumpulan jaringan yang terhubung dengan menggunakan *Internet Protocol* yang memungkinkan menjadi jaringan virtual tunggal besar), Lihat International Telecommunication Union, 2005, *A Handbook on Internet Protocol* (IP)- *Based Network Related Topics and Issues,* hlm.3.

[7] Milton Mueller, John Mathiason, Hans Klein, "*The Internet and Global Governance: Principles and Norms for a New Regime,"* Global Governance Vol.13 No.2, 2007, hlm. 244

negara[8] sehingga mampu membuat interaksi antar individu di dalamnya dengan sebutan warganet atau *netizen* dalam suatu *global village*[9].

Interaksi dan komunikasi data secara global berakibat tidak hanya pada perkembangan teknologi, akan tetapi berdampak juga pada penyalahgunaan[10] terhadap data. Sehingga pada pertengahan tahun 2013, masyarakat internasional dikejutkan dengan pemberitaan adanya kegiatan pengumpulan data oleh *National Security Agency* (NSA) Amerika Serikat. Kasus ini bermula saat Edward Snowden, mantan kontraktor NSA mengungkapkan dokumen-dokumen rahasia milik NSA ke *The Washington Post* dan *The Guardian* pada tanggal 6 Juni 2013.[11]

Dokumen-dokumen tersebut berisi tentang program-program kerja NSA yang melakukan pengintaian terhadap tidak hanya warga negara Amerika Serikat, tetapi juga dilakukan secara luas terhadap negara-negara lainnya. Salah satu program NSA dalam tindakan pengintaian adalah program *Planning Tool for Resource Integration, Synchronization, and Management* (PRISM) yakni program pengumpulan data langsung dari server-server penyedia layanan internet yang berada di Amerika Serikat

---

[8] Wolfram Proksch, E.Schwiehoffer, 2001, "*Internet Governance and Territoriality Nationalisation of Cyberspace,"* 16 Bileta Annual Conference, Edinburg, hlm.5.

[9] Marshall McLuhan, *Predicts The Global Village,* https://www.livinginternet.com/i/ii_mcluhan.htm, dikunjungi pada tanggal 6 Juni 2024 jam 10.00 WIB.

[10] Penyalahgunaan data pribadi merupakan perbuatan yang memenuhi unsur-unsur perbuatan pidana seperti unsur tindak pidana pencurian dan unsur tindak pidana penipuan serta tindak pidana lainnya baik dari sisi unsur objektif maupun unsur subjektif. Dengan terpenuhinya unsur-unsur tersebut, maka sanksi administratif, sanksi perdata maupun sanksi pidana belum cukup untuk mengakomodir tindak pidana penyalahgunaan data pribadi yang senyatanya merupakan bentuk kejahatan yang sempurna. Lihat Sahat Maruli Tua Situmeang, "*Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber",* SASI, Vol. 27, No.1, 2021, hlm.39.

[11] Neil M. Richards, *The Dangers of Surveillance*, Harvard Law Review, http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf, dikunjungi pada tanggal 6 Juni 2024 jam 13.00 WIB.

seperti Google, Yahoo, Facebook, Twitter dan provider telekomunikasi lainnya. Neil M. Richards mengatakan bahwa: [12]

> *We know that governments have been buying and borrowing private-sector databases, and we recently learned that the National Security Agency (NSA) has been building a massive data and supercomputing center in Utah apparently with the goal of intercepting and storing much of the world's Internet communications for decryption and analysis.*

Seperti yang diketahui bahwa pemerintah telah membeli dan meminjam basis data sektor swasta, dan baru-baru ini mengetahui bahwa NSA telah membangun pusat data dan komputasi super besar di Utah yang tampaknya bertujuan untuk menyadap dan menyimpan sebagian besar komunikasi internet di dunia untuk didekripsi dan dianalisis.

Aktivitas tersebut sampai sekarang disinyalir masih berlangsung, hal tersebut sebagaimana yang dikemukan oleh Matt Binder dalam laporannya bahwa pada tahun 2019, Pemerintah Amerika Serikat telah meminta 163.000 data pengguna Google yang tersebar di seluruh dunia.[13] Pada perkembangannya, beberapa kasus lain terkait pengumpulan data oleh Negara terhadap data warga Negara lain juga ditemukan. Pada tahun 2014, Pemerintah China juga melakukan penyadapan terhadap informasi

[12] *Ibid.*

[13] Matt Binder, 2020, *US Government requests for google user data up 510 % since 2010, report says*, Mashable SE Asia, https://sea.mashable.com/tech/11104/us-government-requests-for-google-user-data-up-510-since-2010-report-says, dikunjungi pada tanggal 10 Maret 2024 jam 12.10 WIB.

sensitive dari 22, 1 juta Pegawai Pemerintah Amerika Serikat pada tahun 2014[14], melalui *platform* yang berbadan hukum China.

Kasus-kasus tersebut menunjukan bahwa telah terjadi pengumpulan data pribadi yang dilakukan oleh Negara melalui platfrom digital yang berbadan hukum di negaranya atas dasar keamanan nasional[15]. Pengumpulan data pribadi tersebut bukan hanya dilakukan terhadap warga negaranya melainkan turut pula menyasar pada warga Negara asing. Danrivanto mengatakan bahwa saat ini kita memasuki era "Kolonialisme Digital" dimana para penyedia platform aplikasi layanan virtual melakukan kegiatan pengumpulan data (*data collecting*), penelisikan data (*data crawling*), dan analisis perilaku interaksi data (*data behavior analyzing*) dari publik Indonesia. Data pribadi dari pengguna aplikasinya kemudian dimonetisasi menjadi keuntungan korporasi dan daya tarik bagi investor.[16] *Platform digital* pengumpul data pribadi tersebut, tidak dapat

[14] Patrick C.R. Terry, *"Don't Do as I Do"—The US Response to Russian and Chinese Cyber Espionage and Public International Law*, German Law Journal, Vol.19 No.03, 2019, hlm 1.

[15] Keamanan nasional adalah kebutuhan dasar bagi suatu bangsa untuk melindungi dan menjaga kepentingan nasional. Faktor utama yang menjadi dasar konsep keamanan nasional suatu bangsa adalah kebutuhan untuk memenuhi kepentingan nasional. Keamanan nasional memiliki tujuan untuk memelihara dan mempertahankan eksistensi negara selain dari tujuannya untuk menjaga dan melindungi negara.Konsep keamanan menekankan peran pemerintah dalam melindungi integritas teritorial negara dari ancaman yang datang dari luar maupun dari dalam negeri. Dalam hubungan internasional kontemporer, keamanan nasional yang diupayakan untuk melindungi kepentingan nasional tidak lagi hanya mencakup isu tradisional. Hal tersebut seperti yang diutarakan oleh pakar keamanan internasional, Barry Buzan bahwa, "Keamanan tidak hanya meliputi aspek militer dan aktor negara semata melainkan akan meliputi aspek-aspek non militer dan melibatkan pula aktivitas-aktivitas aktor nonnegara. Lihat Afifah Fidina Rosy, "*Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber",* Journal of Government Science (GovSci), Jurnal Ilmu Pemerintahan, Vol.1, No.2, 2020, hlm. 118-129.

[16] Danrivanto Budhijanto, 2023, *Hukum Pelindungan Data Pribadi di Indonesia*, Refika Aditama, Bandung, hlm. 70. Dalam ekosistem ekonomi digital, data pribadi tidak lagi dipandang sekadar sebagai informasi administratif, melainkan telah berkembang menjadi aset ekonomi strategis yang memiliki nilai komersial tinggi. Perusahaan teknologi, seperti penyedia media sosial, e-commerce, aplikasi keuangan digital, dan layanan berbasis platform lainnya, menjadikan data pengguna sebagai fondasi utama dalam pengambilan keputusan bisnis dan pengembangan layanan. Fenomena ini

menolak permintaan dari Pemerintah yang menjadi tempat perusahaannya berbadan hukum karena terikat dengan ketentuan keamanan nasional dari masing-masing Negara.

Di samping kasus-kasus pengumpulan data pribadi yang dilakukan oleh Negara, dalam praktiknya saat ini kebocoran data pribadi di ruang siber sangat sering terjadi. Indonesia merupakan salah satu Negara dengan kebocoran data pribadi tertinggi di dunia. Hasil kajian perusahaan keamanan siber asal Belanda, Surfshark, menunjukan pada rentang Januari 2020 – Januari 2024 Indonesia menduduki peringkat ke-8 di dunia sebagai negara dengan kebocoran data terbanyak dengan total 94,22 juta data pribadi yang telah dibobol.[17]

Indonesia kembali mengalami kasus kebocoran data pada Pusat Data Nasional Sementara (PDNS) 2 di Surabaya bulan Juni 2024, dari total 282 instansi setidaknya 210 instansi pemerintah baik pusat maupun daerah terkena dampak dari bocornya data di PDNS 2 tersebut.[18] PDNS merupakan fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan,

kemudian dikenal sebagai praktik monetisasi data pengguna, yaitu proses mengubah data menjadi sumber keuntungan ekonomi. Lihat juga Christina Bagenda, a*t.all*, *Legalitas Monetisasi Data Pengguna Oleh Perusahaan Teknologi: Analisis Perlindungan Konsumen Dan Hukum Perekonomian Nasional*, Jurnal Kolaboratif Sains, Vol.8, No.12, 2025, hlm. 8708

[17] Cindy Mutia Annur, 2022, *10 Negara dengan Kasus Kebocoran Data Terbanyak*, https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia dikunjungi pada tanggal 10 Maret 2024. Lihat juga Adi Ahdiyat, 2024, *Indonesia Masuk 10 Negara dengan Kebocoran Data Terbesar*, https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar, dikunjungi pada tanggal 10 Mei 2026.

[18] CNN Indonesia, *Fakta-fakta Kebocoran Data PDNS, Dalang hingga Jumlah Tebusan*, https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan, dikunjungi pada tanggal 15 Juli 2024

penyimpanan dan pengolahan data dan pemulihan data. PDNS saat ini masih dalam proses pembangunan.

PDNS ini memiliki fitur atau layanan seperti *Government Cloud Computing* (ekosistem PDN yang disediakan oleh Kominfo), integrasi dan konsolidasi pusat data Instansi Pemerintah Pusat dan Daerah (IPPD) ke PDN, penyediaan *platform proprietary* dan *Open Source Software* guna mendukung penyelenggaraan aplikasi umum atau khusus Sistem Pemerintahan Berbasis Elektronik (SPBE) serta penyediaan teknologi yang mendukung big data dan kecerdasan buatan (*Artificial Intelegence/AI*) bagi IPPD.[19]

Big data mengacu pada kumpulan data yang sangat besar dan kompleks yang tidak dapat dikelola dengan metode pengolahan data tradisional. Fenomena ini dipicu oleh pesatnya kemajuan teknologi informasi dan komunikasi, serta eksplosi data yang dihasilkan dari berbagai sumber seperti media sosial, transaksi online, dan sensor IoT (*Internet of Things*)[20]. Transformasi digital yang didorong oleh big data telah menjadi kekuatan utama yang mengubah cara organisasi beroperasi dan membuat keputusan[21].

Big data memiliki potensi untuk memberikan wawasan yang mendalam dan analitik yang berharga, tetapi juga menimbulkan tantangan signifikan dalam hal perlindungan data pribadi, keamanan, dan privasi. Pemerintah dan organisasi di seluruh

[19] Dirjen Aptika, *PDN/PDNS*, https://aptika.kominfo.go.id/informasi/layanan/pdn-pdns/, dikunjungi pada tanggal 15 Juli 2024, Pukul 12.50 WIB.

[20] Julia Pohle and Thorsten Thiel, "*Digital sovereignty."* Internet Policy Review, Vol. 9, No. 4,2020, hlm. 2.

[21] Shoshana Zuboff, 2019, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York hlm. 270

dunia harus menghadapi tantangan ini dengan kerangka hukum yang efektif dan inovatif untuk melindungi data pribadi sambil memanfaatkan potensi big data untuk pertumbuhan ekonomi dan kemajuan teknologi.[22]

Evolusi big data dapat ditelusuri melalui beberapa fase utama yang mencerminkan kemajuan teknologi dan perubahan dalam cara data dikumpulkan, disimpan, dan dianalisis.[23] Pada awal era digital, data dikumpulkan secara manual dan disimpan dalam format tradisional seperti database relasional. Dengan kemajuan teknologi, terutama dalam komputasi dan penyimpanan, volume data meningkat pesat. Kemajuan ini memungkinkan penyimpanan dan pemrosesan data dalam jumlah besar yang sebelumnya tidak mungkin dilakukan.[24]

Masuknya era *cloud computing* dan teknologi analitik canggih membawa perubahan besar dalam pengolahan big data. Teknologi seperti Hadoop dan Spark memungkinkan pengolahan data besar dengan cara yang lebih efisien dan skalabel. *Cloud computing* menyediakan fleksibilitas dan skala yang diperlukan untuk menyimpan dan memproses data dalam jumlah besar secara efektif.[25]

Perkembangan terbaru dalam big data melibatkan integrasi kecerdasan buatan dan pembelajaran mesin. Teknologi ini memungkinkan analisis data yang lebih

---

[22] Yogi Muhammad Rahman, Aflah Haora, et al, "*Personal Data Protection in The Era of Globalization (Indonesia Perspective),"* Tirtayasa Journal of International Law, Vol. 2 No. 1, 2023, hlm. 15-30.

[23] De Mauro, A., Greco, M., & Grimaldi, M, 2016, *What is Big Data? A Consensual Definition and a Review of Key Research Topics,* Proceedings of the 2016 19th International Conference on Enterprise Information Systems, hlm. 67-75.

[24] Hashem, I.A.T., et al, "*The Rise of Big Data on Cloud Computing: Review and Open Research Issues,"* Information Systems, Vol. 47, 2015, hlm. 98-115.

[25] Prosimo, 2024, *What Are The Benefits Of Cloud Computing?* https://prosimo.io/what-are-the-benefits-of-cloud-computing/ dikunjungi pada tanggal 15 Juni 2024 jam 10.00 WIB.

canggih dan prediktif, membantu organisasi untuk membuat keputusan berbasis data yang lebih baik dan lebih cepat.[26] Kecerdasan buatan juga memungkinkan otomatisasi analitik dan pengolahan data yang lebih efisien, memberikan wawasan yang lebih mendalam dan mendukung inovasi di berbagai sektor.[27]

Penggunaan big data juga menimbulkan berbagai isu penting seperti privasi, keamanan, dan etika. Data yang dikumpulkan dari berbagai sumber dapat mengandung informasi sensitif yang dapat disalahgunakan jika tidak diatur dengan baik.[28] Isu-isu ini memerlukan perhatian khusus dalam merancang regulasi dan kebijakan yang efektif untuk melindungi data pribadi sambil memanfaatkan potensi big data untuk kemajuan sosial dan ekonomi.[29]

Indonesia, sebagai negara dengan pertumbuhan digital yang pesat, menghadapi berbagai tantangan dalam pengaturan big data dan perlindungan data pribadi. Seiring dengan pesatnya perkembangan teknologi dan digitalisasi, Indonesia perlu menanggapi tantangan ini melalui regulasi yang efektif untuk melindungi data pribadi warganya serta mendukung pertumbuhan ekonomi digital.

Saat ini Indonesia mempunyai regulasi terkait data pribadi, yakni Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (selanjutnya disebut

[26] Chen, M., Mao, S., & Liu, Y, *"Big Data: A Survey,"* Mobile Networks and Applications, Vol. 19 No. 2, 2014, hlm. 171-209.

[27] Jordan, M.I., & Mitchell, T.M, *"Machine Learning: Trends, Perspectives, and Prospects,"* Science, Vol. 349 No. 6245, 2015, hlm. 255-260.

[28] Helen Nissenbaum, 2010, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, hlm. 17

[29] Daniel J. Solove, 2021, *Understanding Privacy*, Harvard University Press, London, hlm. 12

UU PDP) yang merupakan langkah penting dalam upaya Indonesia untuk mengatur perlindungan data pribadi[30].

UU PDP ini mengatur berbagai aspek, mulai dari hak subjek data pribadi, pemrosesan data pribadi, kewajiban pengendali dan prosesor data, transfer data pribadi sanksi, kelembagaan hingga kerjasama internasional. Adapun tujuan dari UU PDP yaitu pelindungan data pribadi untuk menjamin hak dan kebebasan individu dalam pengelolaan data pribadi Beberapa pasal penting dalam UU PDP yakni: Pasal 2 terkait yurisdiksi, sedangkan Pasal 3 dijelaskan mengenai prinsip-prinsip perlindungan data pribadi yang harus diikuti oleh pengendali data, termasuk prinsip pelindungan, kepastian hukum, kepentingan hukum, kemanfaatan, kehati-hatian, keseimbangan dan kerahasiaan. Selanjutnya dalam Pasal 5 sampai dengan Pasal 10 diatur hak-hak pemilik data, seperti hak untuk mengakses, memperbaiki, dan menghapus data pribadi mereka. Adapun terkait sanksi dapat ditemukan dalam Pasal 57 yang menetapkan sanksi administratif bagi pelanggaran ketentuan perlindungan data pribadi, dapat mencakup peringatan tertulis, penghentian sementara, penghapusan atau pemusnahan serta denda administratif. Terkait kelembagaan diatur dalam Pasal 58 sampai dengan Pasal 61, akan tetapi sampai saat ini Lembaga pengawas tersebut belum terbentuk.

Indonesia juga sudah memiliki Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) yang mengatur terkait kriminalisasi terhadap kejahatan

[30] Republik Indonesia, *"Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi"* Lembaran Negara R.I. Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820.

siber. Akan tetapi sampai saat ini belum ada pengaturan khusus terkait keamanan siber. Hal ini mengakibatkan adanya kekosongan hukum apabila kasus-kasus seperti kebocoran data, *ransomware* dan serangan siber lainnya terjadi lagi di kemudian hari.

Disamping kekosongan hukum, persoalan mendasar terletak pada belum adanya sistem hukum nasional yang terintegrasi dalam pengaturan big data dan keamanan siber. Regulasi yang ada masih tersebar dalam berbagai instrumen hukum sektoral seperti UU PDP, UU ITE, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) serta berbagai regulasi sektoral lain di bidang telekomunikasi, intelijen, administrasi pemerintahan, dan keamanan nasional.

Fragmentasi regulasi tersebut menimbulkan konflik norma yang menyebabkan ketidakpastian hukum dalam pengelolaan big data. Konflik norma tersebut tidak hanya bersifat teknis administratif, melainkan juga menyangkut benturan kepentingan antara perlindungan hak privasi warga negara, kepentingan ekonomi digital, dan kepentingan keamanan nasional. Dalam konteks tertentu, negara berupaya memperluas pengawasan digital demi keamanan nasional, namun pada saat yang sama harus menghormati hak konstitusional warga negara atas perlindungan data pribadi dan privasi.[31]

Konflik norma yang sangat krusial juga terlihat dalam pengaturan transfer data lintas negara (*cross-border data transfer*). Pasal 56 UU PDP mengatur bahwa transfer

[31] Daniel J. Solove, 2008, *Understanding Privacy*, Harvard University Press, Cambridge, hlm. 80

data pribadi ke luar wilayah Indonesia hanya dapat dilakukan apabila negara penerima memiliki tingkat perlindungan data yang setara atau lebih tinggi dibanding Indonesia.

Norma tersebut menunjukkan adanya prinsip *data sovereignty*[32] yang bertujuan menjaga kontrol negara terhadap data pribadi warga negara Indonesia. Akan tetapi, ketentuan tersebut bertentangan dengan Pasal 21 PP PSTE yang memberikan fleksibilitas lebih luas terhadap penyelenggara sistem elektronik untuk melakukan pemrosesan dan penyimpanan data di luar negeri sepanjang memenuhi prinsip efektivitas pengawasan.

Konflik norma ini sangat berbahaya karena menyangkut yurisdiksi hukum dan keamanan data nasional. Ketika data warga negara Indonesia disimpan di luar negeri menggunakan layanan *cloud computing* asing, maka negara kehilangan kontrol langsung terhadap data strategis nasional. Dalam situasi tertentu, data tersebut dapat diakses oleh pemerintah asing berdasarkan hukum domestik negara tempat server berada. Sebagai contoh, Amerika Serikat memiliki *Clarifying Lawful Overseas Use of Data Act* yang memungkinkan pemerintah Amerika meminta akses terhadap data yang dikelola perusahaan teknologi Amerika meskipun server berada di luar wilayah negaranya. Kondisi ini menunjukkan bahwa lemahnya pengaturan lokalisasi data (*data localization*) di Indonesia.

Konflik norma berikutnya terjadi dalam pembagian kewenangan kelembagaan keamanan siber nasional. Badan Siber dan Sandi Negara berdasarkan Peraturan

[32] Patrick Hummel, *et.all, Data sovereignty: A review,* Big Data & Society, Vol. 1, No.17, 2021, hlm. 1-16

Presiden Nomor 28 Tahun 2021 memiliki fungsi penyelenggaraan keamanan siber nasional. Akan tetapi, kewenangan pengawasan sistem elektronik juga dimiliki oleh Kementerian Komunikasi dan Digital berdasarkan UU ITE dan PP PSTE.

Selain itu, sektor jasa keuangan diawasi oleh Otoritas Jasa Keuangan, sedangkan pengawasan transaksi pembayaran digital berada di bawah kewenangan Bank Indonesia. Dalam konteks tertentu, Badan Intelijen Negara juga memiliki kewenangan pengumpulan intelijen siber berdasarkan UU Intelijen Negara.

Banyaknya lembaga yang memiliki otoritas di bidang keamanan siber menyebabkan terjadinya *overlapping authority*. Konflik tersebut terlihat dalam penanganan kasus kebocoran data nasional, di mana tidak terdapat kejelasan mengenai siapa yang bertanggung jawab melakukan investigasi utama, pemberian sanksi administratif, hingga mitigasi sistem keamanan.

Pelindungan big data dan data pribadi merupakan aspek krusial dalam keamanan siber. Di Indonesia, insiden pelanggaran data[33] dan serangan siber[34] telah meningkat dalam beberapa tahun terakhir, menyoroti kebutuhan mendesak untuk meningkatkan keamanan data. Pelindungan data pribadi memerlukan koordinasi antara berbagai lembaga pemerintah dan sektor swasta. Saat ini, terdapat tantangan dalam hal

[33] Pelanggaran data adalah setiap insiden keamanan di mana pihak yang tidak berwenang mengakses informasi sensitif atau rahasia, termasuk data pribadi (nomor Jaminan Sosial, nomor rekening bank, data layanan kesehatan) dan data perusahaan (catatan pelanggan, kekayaan intelektual, informasi keuangan) lihat Matthew Kosinski, *Apa itu pelanggaran data?*, https://www.ibm.com/id-id/think/topics/data-breach dikunjungi pada tanggal 10 Mei 2026 jam 09.00 WIB

[34] Serangan siber adalah upaya yang disengaja untuk mendapatkan akses tidak sah ke jaringan komputer, sistem komputer, atau perangkat digital. Tujuannya adalah untuk mencuri, mengekspos, mengubah, menonaktifkan atau menghancurkan data, aplikasi, atau aset lainnya. Lihat Tom Krantz dan Alexandra Jonker, *Apa yang dimaksud dengan serangan siber?* https://www.ibm.com/id-id/think/topics/cyber-attack#498277090 dikunjungi pada tanggal 10 Mei 2026 jam 09.00 WIB

koordinasi dan kolaborasi antara lembaga yang bertanggung jawab atas keamanan siber, perlindungan data, dan penegakan hukum[35].

Kedaulatan digital merujuk pada hak dan kemampuan suatu negara untuk mengatur, mengendalikan, dan melindungi data serta infrastruktur digital yang berada di dalam wilayahnya. Isu kedaulatan digital semakin penting seiring dengan meningkatnya peran teknologi informasi dalam kehidupan sehari-hari dan ekonomi global[36].

Kedaulatan digital mencakup hak negara untuk menetapkan kebijakan dan regulasi terkait data, informasi, dan infrastruktur digital di wilayahnya. Ini termasuk pengaturan penyimpanan data, perlindungan data pribadi, dan keamanan siberKedaulatan digital memastikan bahwa negara dapat melindungi data dan infrastruktur digital dari ancaman dan penyalahgunaan yang mungkin timbul dari luar negeri[37].

Banyak negara, termasuk Indonesia, menerapkan kebijakan data lokal yang mengharuskan data pribadi dan sensitif disimpan di dalam negeri. Kebijakan ini bertujuan untuk meningkatkan kontrol negara atas data dan melindungi data pribadi dari risiko pelanggaran yang mungkin terjadi di luar negeri.

[35] Badan Siber dan Sandi Negara, 2023. *Laporan Tahunan Badan Siber dan Sandi Negara*. Jakarta.

[36] Paul Timmers, 2024, *Sovereignty in the Digital Age*. In: Hannes Werthner, *et al. Introduction to Digital Humanism*. Springer, Cham, hlm. 586

[37] Sudarmadi, Damar Apri and Runturambi, Arthur Josias Simon, *"Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia,"* Jurnal Kajian Stratejik Ketahanan Nasional Vol. 2, No. 2, 2019, hlm. 163-179.

Kedaulatan digital juga mencakup kontrol atas infrastruktur digital, seperti pusat data dan jaringan komunikasi, yang merupakan bagian penting dari ekonomi digital suatu negara[38]. Pengaturan dan pengendalian infrastruktur ini penting untuk memastikan keamanan dan keberlanjutan sistem digital di negara tersebut.

Meskipun penting, mewujudkan kedaulatan digital menghadapi beberapa tantangan, termasuk:

a. Globalisasi dan Aliran Data Lintas Batas: Globalisasi dan integrasi ekonomi digital global seringkali bertentangan dengan kebijakan data lokal dan kontrol nasional atas data[39]. Perusahaan multinasional yang beroperasi di berbagai negara membutuhkan aliran data lintas batas untuk operasional dan analisis bisnis mereka. Pembatasan data lokal dapat menghambat efektivitas dan efisiensi operasional global, serta mempengaruhi investasi dan pertumbuhan ekonomi digital.
b. Isu Perdagangan dan Kebijakan Internasional: Kebijakan kedaulatan digital dapat berdampak pada hubungan perdagangan internasional dan perjanjian ekonomi. Beberapa negara mungkin mengalami tekanan dari mitra perdagangan atau organisasi internasional untuk mengurangi pembatasan data dan mengadopsi kebijakan yang lebih liberal mengenai aliran data lintas batas.[40]
c. Ketersediaan Teknologi dan Infrastruktur: Pengembangan dan pemeliharaan infrastruktur digital yang memadai merupakan tantangan utama bagi negara-negara berkembang. Ketersediaan teknologi, kapasitas

[38] Geoff Gordon, *Digital sovereignty, digital infrastructures, and quantum horizons*. AI & Soc, Vol. 39, 2024, hlm. 125–137

[39] Portal Kemlu, *"Konektivitas Asia-EU: Potensi Ekonomi Digital"*, hlm.4 https://kemlu.go.id/files/repositori/56594/12_Asia-EU%20Connectivity_%20Potensi%20Ekonomi%20Digital.pdf dikunjungi pada 24 Juni 2024.

[40]Mira Burri, Kholofelo Kugler, *Regulatory autonomy in digital trade agreements*, Journal of International Economic Law, Vol.27, No.3, 2024, hlm. 397–423.

infrastruktur, dan sumber daya manusia yang terampil sangat penting untuk mengimplementasikan kebijakan kedaulatan digital dengan efektif[41].

Kedaulatan digital sering kali terkait erat dengan perlindungan privasi, karena negara-negara berusaha untuk melindungi data pribadi warganya dari penyalahgunaan dan pelanggaran[42]. Beberapa aspek penting meliputi:

a. Pengaturan Perlindungan Data: Negara-negara mengembangkan undang-undang perlindungan data pribadi untuk memastikan bahwa data pribadi diproses dan dikelola dengan cara yang transparan dan adil[43]. UU PDP di Indonesia, misalnya, bertujuan untuk memberikan perlindungan yang lebih baik bagi data pribadi warga negara dan mengatur hak-hak individu terkait data mereka[44].
b. Kerjasama Internasional dalam Perlindungan Data: Kedaulatan digital juga melibatkan kerjasama internasional untuk memastikan bahwa standar perlindungan data konsisten dan dapat diterima secara global. Perjanjian internasional seperti *General Data Protection Regulation* (*GDPR*) di Uni Eropa berfungsi sebagai acuan untuk perlindungan data pribadi dan mempengaruhi kebijakan di negara-negara lain, sedangkan Konvensi

[41] Helia Pazhohan, "*Global Data Protection Standards: A Comparative Analysis of GDPR and Other International Privacy Laws*," Legal Studies Digital Age, Vol.2 No.3, 2023, 1-12.
[42] Soshanna Zuboff, *"The Age of Surveillance Capitalism Revisited: Implications for Privacy and Security,"* Journal of Privacy and Security Studies, Vol.15, No.1, 2022, hlm. 56-71.
[43] Usman Tariq, *at.all*, "*A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review*," Sensors, Vol.23 No.8, 2023 hlm. 4117.
[44] Danil Erlangga Mahameru, *at. all*, "*Implementasi Uu Perlindungan Data Pribadi Terhadap Keanmanan Informasi Identitas Di Indonesia*," Jurnal Esensi Hukum, Vol. 5, No. 2, 2024, Hlm.115-131.

Budapest di Uni Eropa serta Konvensi Hanoi 2024 di tingkat global bertujuan untuk mengatur kejahatan siber.

Keamanan siber merupakan aspek penting dalam kedaulatan digital, karena ancaman terhadap infrastruktur digital dan data pribadi dapat merusak kedaulatan suatu negara. Negara-negara menghadapi risiko ancaman siber seperti peretasan, serangan ransomware, dan pencurian data yang dapat merusak infrastruktur digital dan mengancam kedaulatan nasional[45]. Investasi dalam keamanan siber dan peningkatan kapabilitas untuk mendeteksi dan merespons ancaman siber sangat penting untuk melindungi kedaulatan digital.[46]

Keamanan siber sering memerlukan koordinasi internasional karena serangan siber dapat berasal dari luar negeri dan mempengaruhi banyak negara[47]. Kerjasama internasional dalam berbagi informasi ancaman dan strategi pertahanan merupakan langkah penting untuk menjaga keamanan siber global dan mendukung kedaulatan digital.

---

[45] BRM Yehizkia Y. Kristalia, dan Indra Wisnu Wibisono., *"Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital"*, Jurnal Ilmiah Multidisiplin, Vol. 3 No. 2, 2024, hlm. 83-93.

[46] Deteksi dan respons ancaman (Threat Detection and Response/TDR) memungkinkan organisasi untuk mengidentifikasi dan mengatasi ancaman siber secara proaktif, sehingga mengurangi risiko pelanggaran data dan gangguan operasional. Selain itu, deteksi dini memungkinkan penanganan cepat terhadap malware, ransomware, dan aktivitas jahat lainnya. Hal ini meminimalkan potensi kerusakan dan mencegah ancaman menyebar di seluruh jaringan. Selain itu, TDR mendukung kesinambungan bisnis dengan memastikan respons tepat waktu terhadap serangan siber, sekaligus membantu organisasi memenuhi persyaratan regulasi dan kepatuhan. Dengan cara ini, TDR memperkuat postur keamanan secara keseluruhan dan melindungi aplikasi, aset, dan data penting dari ancaman yang terus berkembang. Lihat Fortinet, *Threat Detection And Response (TDR): Mitigating Advanced Cyber Threats* https://www.fortinet.com/resources/cyberglossary/threat-detection-and-response dikunjungi pada 5 Mei 2026

[47] Diny Luthfah, *"Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia,"* Teras Law Jurnal, Vol.3, No.1, 2021, hlm.11-20.

Indonesia juga mengembangkan inisiatif keamanan siber seperti Badan Siber dan Sandi Negara (BSSN) untuk menangani ancaman siber dan melindungi infrastruktur digital[48]. Inisiatif ini mencakup penguatan kemampuan deteksi dan respons terhadap ancaman siber serta koordinasi dengan lembaga internasional untuk keamanan siber[49]. Akan tetapi BSSN sebagai lembaga yang diamanatkan untuk menjaga keamanan siber belum optimal dalam menjalankan penegakan kedaulatan digital. Hal ini terlihat dari lambatnya koordinasi serta semestinya BSSN memegang peranan kunci dalam proses investigasi kasus ini.[50]

Sementara itu belum terbentuknya Lembaga Pelindungan Data Pribadi mengakibatkan tidak terlaksananya perumusan kebijakan strategi, pengawasan terhadap kepatuhan, penegakan hukum administratif terhadap pelanggaran UU PDP dan kerja sama dengan Lembaga Pelindungan Data Pribadi dari negara lain.

Berkaitan dengan pola perilaku terutama membahas mengenai penegakan hukum. Berarti membahas mengenai kedaulatan negara, termasuk di dalamnya penegakan hukum nasional di wilayah negara. Kedaulatan merupakan suatu prasyarat

[48] Hidayat Chusnul Chotimah, *"Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara,"* Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, Vol. 10 No.2, 2019, hlm.113-128.

[49] Ali Shoker, *"Digital Sovereignty Strategies for Every Nation,"* ACIG, Vol.1, No.1, 2022, hlm.3.

[50] ELSAM, 2024, *Insiden Keamanan Siber dan Dugaan Kegagalan Pelindungan Data PDN Sementara, Harus Ditangani Secara Simultan dan Tuntas* https://www.elsam.or.id/siaran-pers/insiden-keamanan-siber-dan-dugaan-kegagalan-pelindungan-data-pdn-sementara--harus-ditangani-secara-simultan-dan-tuntas

hukum untuk adanya suatu negara sebagaimana tercantum dalam Konvensi Montevideo tahun 1933.[51]

Pada konsep hukum internasional unsur-unsur konstitutif yang harus dimiliki suatu masyarakat politik agar dapat diakui sebagai negara tidak cukup hanya dengan adanya tiga unsur konstitutif menurut konsep ilmu politik, tetapi harus ada kemampuan untuk mengadakan hubungan dengan negara-negara lain. Negara dalam perspektif hukum internasional harus memenuhi syarat-syarat tertentu sebagaimana dinyatakan dalam Pasal 1 Konvensi Montevideo 1933 tentang Hak-hak dan Kewajiban-kewajiban Negara.

Selanjutnya kedaulatan menunjukkan bahwa dalam suatu wilayah tertentu dilaksanakan yurisdiksi eksklusif suatu negara terhadap orang-orang dan harta benda yang terdapat didalamnya tanpa ada kedaulatan negara lain.[52] Konsep dasar dalam pelaksanaan kedaulatan suatu negara adalah adanya wilayah dengan batas-batas yang jelas. Mochtar Kusumaatmadja berpendapat bahwa kedaulatan adalah kekuasaan tertinggi yang dimiliki negara dimana ruang berlakunya kekuasaan tertinggi itu dibatasi oleh batas wilayah negara yang memiliki kekuasaan itu.[53]

Dalam pengaturan hukum internasional, setidaknya terdapat 3 (tiga) konvensi internasional berkenaan dengan kedaulatan suatu Negara. Ketiga konvensi tersebut adalah Konvensi Montevideo Tahun 1933, Konvensi Paris 1944 dan Konvensi Hukum

---

[51]Boer Mauna, 2010, *Hukum Internasional, Pengertian dan Fungsi dalam Era Dinamika Global*, P.T. Alumni, Bandung, hlm. 23.

[52]Huala Adolf, 1996, *Aspek-aspek negara dalam Hukum Internasional*, P.T. RajaGrafindo Persada, Jakarta, hlm. 99.

[53]*Ibid*

Laut 1982 (UNCLOS 1982). Kedaulatan sebuah Negara berdasarkan konvensi internasional tersebut meliputi kedaulatan di wilayah daratan, kedaulatan di wilayah udara, kedaulatan di wilayah laut dan kedaulatan di dasar laut dan tanah di bawahnya. Dalam konvensi tersebut, penegasan terhadap kedaulatan Negara hanya terbatas pada ruang fisik/nyata. Sedangkan, kedaulatan di ruang maya belum terdapat pengaturan berkenaan dengan kedaulatannya, terkhusus terhadap data yang melintasi batas Negara (*cross border data*).

Kedaulatan sangatlah penting bagi suatu Negara, Hakim Huber dalam kasus *Island of Palmas* menyatakan bahwa:[54]

> *"Sovereignty in relation to a portion of the surface of the globe is the legal condition necessary for the inclusion of such portion in the territory of any particular state".*

Kedaulatan menurut apa yang disampaikan oleh Hakim Huber bermakna bahwa terjadi keterkaitan yang erat antara Negara dengan wilayah yang dikuasainya, dan penguasaan atas wilayah tersebut yang menjadi kedaulatan suatu Negara. Pemaknaan tersebut, mengharuskan Negara memiliki kekuasaan efektif terhadap wilayahnya untuk dapat menerapkan kedaulatan di wilayah tersebut. Wilayah merupakan atribut yang sangat penting bagi eksistensi suatu Negara.[55] Di atas wilayahnya Negara memiliki

[54] Malcom N. Shaw, 2017, *International Law Eighth Edition*, Cambridge University Press, New York, hlm. 363. Lihat juga Daniel-Erasmus Khan, "*Max Huber as Arbitrator: The Palmas (Miangas) Case and Other Arbitrations,"* The European Journal of International Law, Vol. 18, No. 1, hlm.145-170

[55] Sefriani, 2018, *Hukum Internasional, Suatu Pengantar Edisi Kedua*, RajaGrafindo, Depok, hlm. 173.

hak-hak untuk melaksanakan kedaulatan atas orang, benda juga peristiwa atau perbuatan hukum yang terjadi di wilayahnya.[56] Wilayah merupakan atribut yang sangat penting bagi eksistensi suatu Negara. Di atas wilayahnya Negara memiliki hak-hak untuk melaksanakan kedaulatan atas orang, benda juga peristiwa atau perbuatan hukum yang terjadi di wilayahnya.

Lebih jauh, kedaulatan juga memberikan hak kepada Negara untuk menjalankan kewajibannya yakni melindungi seluruh entitas yang ada dalam penguasaannya khususnya terhadap warga Negaranya. Begitupun terhadap keamanan data pribadi milik warganegaranya, dimana Negara perlu menjamin keamanan data-data tersebut guna menjaga kepentingan nasional maupun kepentingan warga negaranya.

Ahmad M. Ramli menyatakan bahwa berdasarkan karakter khusus dalam konteks ruang siber, terdapat beberapa teori untuk menentukan yurisdiksi suatu Negara terkait pelaku pelanggaran di ruang siber, yakni:[57]

1. *The Theory of Uploader and the Downloader*. Berdasarkan teori ini, kegiatan *uploading* dan *downloading* yang dilakukan di ruang siber dapat menentukan wilayah fisik tergugat.
2. *Theory the Law of the Server*. Pendekatan ini memperlakukan server di mana *webpages* secara fisik berlokasi, yaitu di mana mereka dicatat sebagai data elektronik.
3. *The Theory of International Space*. Ruang siber dianggap sebagai f*ourth space*, yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.

[56] *Ibid.*
[57] Ahmad M. Ramli, 2010, *Op. cit.*, hlm. 22.

Ketiga teori tersebut menjadi pintu masuk dalam peletakan dasar kedaulatan Negara di ruang siber. Dari ketiga teori tersebut, dapat dilihat bahwa saat ini penafsiran kedaulatan Negara di ruang siber masih terpusat pada teori kedua yakni *teori the Law of the Server*, yakni Negara memiliki yurisdiksi pada aktivitas dunia maya dengan mengikuti dimana server atas data berada atau *platform digital* berbadan hukum. Hal ini pula yang memicu persoalan berkenaan dengan tanggung jawab Negara dalam melindungi data pribadi warga negara yang berada di Negara dimana *platform digital* berkedudukan hukum.

Pengaturan pengelolaan big data dalam ancaman terhadap keamanan siber di Indonesia masih belum optimal dikarenakan belum adanya payung hukum terkait kemanan siber itu sendiri, serta penegakan kedaulatan digital di Indonesia masih belum terkoordinasi dengan baik ketika dihadapkan dengan kasus-kasus terkait big data. Kondisi tersebut menyebabkan ketidakpastian hukum, lemahnya perlindungan big data, dan meningkatnya ancaman terhadap kedaulatan digital Indonesia.

Hukum bertujuan untuk menciptakan keseimbangan dalam hubungan antara anggota masyarakat. Tujuan hukum tersebut setidaknya diwujudkan dalam rasa keadilan, kepastian, dan kemanfaatan. Hukum juga harus mampu mengendalikan kegiatan masyarakat guna terciptanya ketertiban di tengah masyarakat. Dalam upaya memberikan pelindungan terhadap data pribadi dan big data dari tindakan sewenang-wenang baik yang dilakukan oleh Negara maupun individu lainnya, khususnya yang terjadi di ruang siber, hukum harus mampu memberikan pengaturan di dalamnya.

Pengaturan tersebut tentu harus berorientasi pada nilai-nilai keadilan dan kepastian dalam setiap pemanfaatan dunia siber khususnya bagi pelindungan data pribadi dan big data.

B. Rumusan Masalah

Berdasarkan uraian dalam latar belakang di atas dapat dikemukakan beberapa permasalahan sebagai berikut :

1. Bagaimana pengaturan hukum terkait pengelolaan big data dalam menghadapi ancaman keamanan siber?
2. Bagaimana penegakan kedaulatan digital terhadap ancaman keamanan siber di Indonesia?
3. Bagaimana model pengaturan hukum yang ideal untuk mengelola serta melindungi big data dari ancaman keamanan siber dalam menegakkan kedaulatan digital di Indonesia?

C. Tujuan Penelitian

Tujuan yang diharapkan dari penelitian dalam rangka penulisan disertasi ini adalah:

1. Untuk mengkaji pengaturan hukum terkait pengelolaan big data dalam menghadapi ancaman keamanan siber.
2. Untuk mengkaji dan menganalisis penegakan kedaulatan digital terhadap ancaman keamanan siber di Indonesia.

3. Untuk merumuskan konsep hukum mendatang tentang model pengaturan hukum yang ideal untuk melindungi big data dari ancaman keamanan siber dalam menegakkan kedaulatan digital di Indonesia.

D. Manfaat Penelitian

Adapun manfaat penelitian dalam penulisan disertasi ini adalah sebagai berikut:

1. Secara teoritis, penelitian ini diharapkan dapat merupakan sumbangan pemikiran dalam mengembangkan hakikat sebagai suatu ilmu, khususnya dalam kajian bidang hukum Internasional, *cyberlaw* dan kerjasama internasional. Penelitian ini diharapkan dapat memberikan gagasan yang baru bagi kalangan ilmuan akademisi dan praktisi dalam memahami big data dan penegakan hukum dalam kedaulatan digital.
2. Kegunaan Praktis

   Penelitian ini diharapkan dapat bermanfaat bagi kalangan praktisi baik para pembuat undang-undang (*legislator*), pemerintahan maupun para penegak hukum. Penelitian ini diharapkan dapat memberikan pemikiran baru bagi para pembuat undang-undang dan pembuat kebijakan agar dapat membuat suatu pedoman atau ketentuan yang dapat dijadikan dasar bertindak bagi praktisi hukum maupun para ahli hukum yang terkait dan yang khusus bagi pembuat undang-undang. Penelitian ini diharapkan dalam pelaksanaan penerapan hukum internasional dan hukum siber dapat lebih diamati guna mencapai sasaran yaitu pelaksanaan penegakan kedaulatan

digital sesuai dengan pengaturan terkait big data yang merupakan bentuk upaya penegakan hukum yang baik.

E. Keaslian Penelitian

Berdasarkan hasil penelusuran terhadap Disertasi dengan topik penelitian sejenis, Peneliti menemukan beberapa disertasi yang membahas topik penelitian sejenis, yakni:

1.) P.J. Blount, Rurgees, The State University of New Jersey. US. 2019 dengan judul *Reprogramming the World: Cyberspace and the Geography of Global.* Disertasi ini berfokus pada pemanfaatan *Cyberspace* yang berdampak pada kedaulatan territorial. Sedangkan dalam disertasi ini berfokus pada kedaulatan negara atas keamanan siber.

2.) RFC Ezenwajiaku, Brunel University London, 2017 dengan judul *Respect for The inviolability of state territory*. Disertasi ini berfokus pada interpretasi terbatas dari Pasal 2(4) Piagam PBB terkait ancaman dan penggunaan kekerasan. Bahwa serangan yang dimaksud dalam Pasal 2(4) adalah serangan yang dilakukan terhadap kedaulatan teritori suatu negara. Sehingga pertanyaan yang muncul adalah apakah Pasal 2(4) berlaku pula terhadap serangan di dunia maya. Disertasi ini berargumentasi bahwa pengabaian total terhadap makna luas dalam Pasal 2(4) adalah sebuah kesalahan mengingat konteks penyusunan Piagam PBB serta sejarah hukumnya. Oleh karena itu, merekomendasikan interpretasi yang luas terhadap Pasal 2(4) yang berbunyi, penghormatan terhadap tidak dapat diganggu gugatnya wilayah Negara.

3.) Annisa Hikmiyati, Universitas Indonesia 2006 dengan judul Penentuan *Locus Delicti* Dalam *Cyber Crime* Sebagai Usaha Pembaruan Hukum Pidana Nasional. Disertasi ini berfokus pada penentuan *locus delicti* berdasarkan ajaran *locus delicti* dalam tindak pidana *cyber crime* sifatnya kasuistis sehingga hukum pidana mampu mengatasi permasalahan *borderless* dari suatu tindak pidana. Sedangkan dalam disertasi ini mengkaji dari sudut pandang hukum internasional dan hukum siber.

4.) Sigid Suseno, Universitas Padjajaran, 2011 dengan judul Implikasi Yuridis Terhadap Tindak Pidana Siber Berdasarkan Peraturan Perundang-Undangan Indonesia Dihubungkan Dengan Konvensi Dewan Eropa 2001. Disertasi ini berfokus pada yurisdiksi terhadap tindak pidana siber berdasarkan peraturan perundang-undangan Indonesia memiliki implikasi berkaitan dengan wewenang negara untuk melakukan regulasi terhadap tindak pidana siber. Terhadap hukum pidana materiil adalah adanya perlindungan hukum dan keadilan terhadap masyarakat dengan adanya kriminalisasi perbuatan tertentu sebagai tindak pidana siber. Sedangkan dalam disertasi ini, penulis berfokus pada penegakan kedaulatan digital dalam ruang siber.

5.) Siti Yuniarti, Universitas Padjajaran, 2024 dengan judul: Pengaturan Hukum Siber Dalam Platform Digital Marketplace Guna Pembangunan Ekonomi Digital Indonesia. Disertasi ini berfokus bahwa dalam era *Privacy* 3.0 dan *Cyberlaw* 2.0 prinsip-prinsip hukum siber dalam pemrosesan data pribadi dan algoritma membutuhkan prinsip tambahan yang menempatkan Platform sebagai *fiduciary information* dengan atribut *a duty of confidentiality*, *a duty of care*, dan *duty of*

loyalty terutama dalam konteks distribusi data pada pihak lain dan penggunaan algoritma otomatis, termasuk AI. Legislasi hukum siber Indonesia menempatkan Platform *digital marketplace* tidak hanya sebagai *internet intermediary*, namun dilengkapi dengan ragam peran. Norma turunan dari prinsip kehati-hatian dalam UU PDP baru sebatas penilaian risiko,kewajiban dan tanggung jawab Pengendali Data Pribadi dan Prosesor Data Pribadi,namum belum mengakomodir atribut dari *fiduciary information*. Algoritma otomatis dalam UU PDP memerlukan peraturan pelaksana yang memetakan lingkup otomatisasi dan mengedepankan pendekatan ex-ante. Secara khusus,pendekatan AI masih menggunakan perspektif pelindungan data pribadi dimana memerlukan penelitian lanjutan. Sedangkan dalam disertasi ini mengkaji terkait pegelolaan big data dalam ancaman keamanan siber.

F. Kerangka Teoritis dan Konseptual

1. Kerangka Teoritis

Dalam menganalisis permasalahan-permasalahan yang telah dikemukakan di atas, penelitian ini akan mempergunakan teori-teori, yaitu : a) Teori Kedaulatan Negara, b) Teori Kepastian Hukum dan c) Teori Hak Atas Privasi

a. Teori Kedaulatan Negara

Kerangka pemikiran tentang atau butir-butir pendapat teoritis mengenai suatu permasalahan yang dapat dijadikan sebagai bahan pegangan teoritis.[58]

[58] Fred N. Kerlinger, *Asas-asas Penelitian Behavioral*, diterjemahkan Landung R. Simatupang, Yogyakarta, Gajah Mada University Press, 1996, hlm. 14.

Jika berbicara mengenai penegakan hukum berarti berbicara mengenai kedaulatan negara, termasuk di dalamnya penegakan hukum nasional di wilayah negara tersebut. Kedaulatan merupakan suatu prasyarat hukum untuk adanya suatu negara sebagaimana tercantum dalam Konvensi Montevideo tahun 1933.[59]

Konsep negara dapat ditinjau baik dari konsep ilmu politik maupun dari konsep hukum internasional. Dalam konsep ilmu politik unsur konstitutif dari negara adalah adanya penduduk, wilayah dan pemerintah. Demikian pula dalam doktrin klasik mengenai negara hanya mensyaratkan adanya tiga unsur yang harus dimiliki suatu masyarakat politik agar diterima sebagai negara, yaitu rakyat, daerah dan pemerintah.[60]

Dalam konsep hukum internasional unsur-unsur konstitutif yang harus dimiliki suatu masyarakat politik agar dapat diakui sebagai negara tidak cukup hanya dengan adanya tiga unsur konstitutif menurut konsep ilmu politik, tetapi harus ada kemampuan untuk mengadakan hubungan dengan negara-negara lain. Unsur-unsur negara dalam perspektif hukum internasional harus memenuhi syarat-syarat tertentu sebagaimana dinyatakan dalam Pasal 1 Konvensi Montevideo 1933 tentang Hak-hak dan Kewajiban-kewajiban Negara, yaitu:

1. Memiliki penduduk yang tetap (*a permanent population*)

[59] Boer Mauna, *Op. cit.*, hlm. 23.
[60] Yudha Bhakti Ardhiwisastra,1999, *Imunitas Kedaulatan Negara di Forum Pengadilan Asing*, Alumni, Bandung, hlm. 56.

2. Memiliki wilayah yang tertentu (*a definite territory*)
3. Memiliki pemerintahan (*a government*)
4. Memiliki kemampuan untuk melakukan hubungan-hubungan dengan negara lain (*a capacity to enter into relations with other states*).[61]

Rumusan unsur pertama sampai ketiga merupakan wujud kedaulatan internal, sedangkan unsur keempat dalam Konvensi Montevideo tersebut pada dasarnya merupakan kedaulatan eksternal sebagai unsur mutlak yang harus dimiliki suatu negara sebagaimana dikemukakan beberapa pakar hukum internasional. Rumusan tersebut juga dipandang lebih sesuai dengan kenyataan yaitu terdapat masyarakat politik tertentu meskipun tidak memiliki kedaulatan penuh tetapi memiliki kemampuan untuk mengadakan hubungan internasional sehingga dapat dianggap sebagai subyek hukum internasional. Menurut Briggs walaupun terdapat pandangan bahwa kedaulatan unsur esensial dari negara namun beberapa masyarakat politik tidak memiliki kemampuan untuk mengadakan hubungan internasional. Masyarakat politik atau negara tersebut dapat dianggap sebagai pribadi internasional atau sebagai negara dalam hukum internasional.[62]

Kedaulatan menunjukkan bahwa dalam suatu wilayah tertentu dilaksanakan yurisdiksi eksklusif suatu negara terhadap orang-orang dan harta

[61] J.G. Starke, 2004, *Pengantar Hukum Internasional*, (Terjemahan Bambang Iriana Djajaatmadja), Sinar Grafika, Jakarta, hlm. 127-128.

[62] S. Tasrip, 1987, *Hukum Internasional tentang Pengakuan dalam Teori dan Praktek*, Abardin, Jakarta, hlm. 12.

benda yang terdapat didalamnya tanpa ada kedaulatan negara lain.[63] Konsep dasar dalam pelaksanaan kedaulatan suatu negara adalah adanya wilayah dengan batas-batas yang jelas. Mochtar Kusumaatmadja berpendapat bahwa kedaulatan adalah kekuasaan tertinggi yang dimiliki negara dimana ruang berlakunya kekuasaan tertinggi itu dibatasi oleh batas wilayah negara yang memiliki kekuasaan itu.[64]

Evolusi konsep kedaulatan dipengaruhi oleh Prinsip *Responsibility to Protect* atau disingkat RtoP diciptakan sebagai akibat dari sejumlah kegagalan komunitas internasional untuk menghentikan pembunuhan massal di Yugoslavia, Bosnia dan Rwanda. RtoP adalah suatu prinsip yang berusaha menjamin agar komunitas internasional tidak akan gagal lagi untuk bertindak ketika pembunuhan massal dan kejahatan kemanusiaan lainnya terjadi.

Ide mengenai RtoP pada awalnya berkembang dari bidang kerja yang digeluti oleh Francis Deng – seorang mantan diplomat asal Sudan yang menjadi Perwakilan Khusus PBB untuk Masalah Pengungsi Internal (Internally Displaced Persons/IDPs) selama dekade 1990-an – dan juga sejumlah ahli lainnya yang berkecimpung dalam bidang yang sama. Deng dan para ahli lainnya itu berpendapat bahwa ide mengenai kedaulatan negara harus didasarkan bukan pada hak mutlak dari setiap negara untuk melakukan apa yang dikehendakinya tanpa ada campur tangan internasional, tetapi bahwa

[63]Huala Adolf, 1996, *Op. cit.*, hlm. 99.
[64]*Ibid*

kedaulatan negara harus diasaskan pada perlindungan terhadap rakyatnya yang tinggal di wilayah tersebut. Secara sederhana, kedaulatan negara harus dibangun di atas konsep "kedaulatan sebagai tanggung jawab (*sovereignty as responsibility*).[65]

b. Teori Kepastian Hukum

Kepastian merupakan ciri yang tidak dapat dipisahkan dari hukum, terutama untuk norma hukum tertulis. Hukum tanpa nilai kepastian akan kehilangan makna karena tidak dapat lagi digunakan sebagai pedoman perilaku bagi setiap orang.

Kepastian sendiri disebut sebagai salah satu tujuan dari hukum. Keteraturan masyarakat berkaitan erat dengan kepastian dalam hukum, karena keteraturan merupakan inti dari kepastian itu sendiri. Keteraturan menyebabkan orang dapat hidup secara berkepastian, sehingga dapat melakukan kegiatan-kegiatan yang diperlukan dalam kehidupan bermasyarakat.

Menurut Sudikno Mertokusumo, kepastian hukum adalah jaminan bahwa hukum dijalankan, bahwa yang berhak menurut hukum dapat memperoleh haknya dan bahwa putusan dapat dilaksanakan.[66]

---

[65] https://r2pasiapacific.org/files/331/R2P_basic_info_Bahasa.pdf hlm. 2, dikunjungi pada 25 Januari 2025 Pukul 14.25 WIB.

[66] Sudikno Mertokusumo, 2007, *Mengenal Hukum Suatu Pengantar*, Liberty, Yogyakarta, hlm. 160.

Kepastian hukum erat kaitannya dengan keadilan, namun hukum tidak identik dengan keadilan. Hukum bersifat umum, mengikat setiap orang, bersifat menyamaratakan. Keadilan bersifat subyektif, individualistis, dan tidak menyamaratakan. Kepastian hukum merupakan pelaksanaan hukum sesuai dengan bunyinya, sehingga masyarakat dapat memastikan bahwa hukum dilaksanakan. Penciptaan kepastian hukum dalam peraturan perundang-undangan, memerlukan persyaratan yang berkenaan dengan struktur internal dari norma hukum itu sendiri.[67]

Kepastian hukum mengehendaki adanya upaya pengaturan hukum dalam perundang-undangan, dibuat oleh pihak yang berwenang dan berwibawa, sehingga aturan-aturan itu memiliki aspek yuridis. Aspek ini nantinya dapat menjamin adanya kepastian, bahwa hukum berfungsi sebagai suatu peraturan yang harus ditaati.

Jan M. Otto berpendapat bahwa kepastian hukum disyaratkan menjadi beberapa hal sebagai berikut: 1) Kepastian hukum menyediakan aturan hukum yang jelas serta jernih, konsisten serta mudah diperoleh atau diakses. Aturan hukum tersebut haruslah diterbitkan oleh kekuasaan negara dan memiliki tiga sifat yaitu jelas, konsisten dan mudah diperoleh. 2) Beberapa instansi penguasa atau pemerintahan dapat menerapkan aturan hukum dengan cara yang konsisten serta dapat tunduk maupun taat kepadanya. 3) Mayoritas warga pada suatu

[67] Fernando M Manulang, 2007, *Hukum Dalam Kepastian*, Prakarsa, Bandung, hlm. 95.

negara memiliki prinsip untuk dapat menyetujui muatan yang ada pada muatan isi. Oleh karena itu, perilaku warga pun akan menyesuaikan terhadap peraturan yang telah diterbitkan oleh pemerintah. 4) Hakim peradilan memiliki sifat yang mandiri, artinya hakim tidak berpihak dalam menerapkan aturan hukum secara konsisten ketika hakim tersebut dapat menyelesaikan hukum. 5) Keputusan dari peradilan dapat secara konkrit dilaksanakan. Menurut Jan M. Otto kelima syarat dalam kepastian hukum tersebut menunjukan, bahwa kepastian hukum dapat dicapai, apabila substansi hukum sesuai dengan kebutuhan yang ada pada masyarakat.[68]

Dari uraian-uraian mengenai kepastian hukum di atas, maka kepastian dapat mengandung beberapa arti, yakni adanya kejelasan, tidak menimbulkan multitafsir, tidak menimbulkan kontradiktif, dan dapat dilaksanakan. Hukum harus berlaku tegas di dalam masyarakat, mengandung keterbukaan sehingga siapapun dapat memahami makna atas suatu ketentuan hukum. Hukum yang satu dengan yang lain tidak boleh kontradiktif sehingga tidak menjadi sumber keraguan. Kepastian hukum menjadi perangkat hukum suatu negara yang mengandung kejelasan, tidak menimbulkan multitafsir, tidak menimbulkan kontradiktif, serta dapat dilaksanakan, yang mampu menjamin hak dan kewajiban setiap warga negara sesuai dengan budaya masyarakat yang ada.

[68] Jan Michiel Otto, "*Rule of Law Promotion, Land Tenure and PovertyAlleviation: Questioning the Assumptions of Hernando de Soto*," Hague Journal of Rule of Law, Vol 1, No. 1, 2009 hlm.173–195.

c. Teori Hak Atas Privasi

Berdasarkan *Black's Law Dictionary*, *privacy* adalah *The condition or state of being free form public attention to intrusion into or interference with one's acts or decisions*.[69] Pengertian tersebut bermakna bahwa privasi merupakan kondisi atau keadaan bebas dari perhatian atau gangguan baik oleh tindakan seseorang maupun keputusan seseorang. Hak atas privasi secara sederhana didefinisikan oleh Westin sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan dengan orang lain.[70]

Pengaturan secara universal mengenai pelindungan terhadap hak atas privasi diatur oleh *Universal Declaration of Human Rights* (UDHR) tahun 1948. Di dalam Pasal 12 diatur bahwa:[71]

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."

Pelindungan terhadap hak atas privasi sebagaimana yang diatur dalam Pasal 12 UDHR memiliki makna bahwa tidak seorangpun boleh

[69] Bryan A Garner, 2009, *Black's Law Dictionary Ninth Edition*, Dallas, Texas: West Publishing, hlm. 1315.

[70] Wahyudi Djafar, *Memastikan Pelindungan Hak atas Privasi dalam Pertahanan Siber*, http://www.elsam.or.id/downloads/565962_Memastikan_pelindungan_hak_atas_privasi_dalam_pertahanan_siber-Wahyudi_Djafar.pdf, dikunjungi pada tanggal 2 April 2023 jam 13.00 WIB.

[71] Pasal 12 *Universal Declaration of Human Rights* (UDHR) 1948. Lihat juga Kendry Tan, Hari Sutra Disemadi, *Urgency of Electronic Wallet Regulation in Indonesia*, Nagari Law Review, Vol. 5, No.1, 2021, hlm. 1-14.

diganggu kehidupan pribadinya secara sewenang-wenang (tanpa dasar hukum) dan oleh karenanya setiap orang memiliki hak untuk mendapatkan pelindungan hukum terhadap gangguan tersebut. Pelindungan terhadap hak atas privasi menunjukan bahwa hak atas privasi merupakan hak yang penting untuk mendapatkan pelindungan. Adapun alasan hak atas privasi harus dilindungi yaitu:[72]

1. Dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu.
2. Seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*) sehingga privasi sangat diperlukan oleh seseorang.
3. Privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hak ini akan hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum.
4. Privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut.
5. Pelanggaran terhadap privasi menimbulkan kerugian yang sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya, sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapatkan kompensasi.

Di samping itu, pelindungan terhadap hak-hak pribadi atau hak privat akan meningkatkan nilai-nilai kemanusiaan; meningkatkan hubungan antara individu dan masyarakatnya; meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan; meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi

[72] Idris, dkk (ed), 2013, *Peran Hukum Dalam Pembangunan di Indonesia Kenyataan, Harapan, dan Tantangan*, Remaja Rosdakarya, Bandung, hlm. 293-294.

kekuasaan pemerintah.[73] Bloustein mengatakan bahwa hak atas privasi menunjukan esensi seseorang sebagai manusia termasuk di dalamnya martabat dan integritas individu serta kemandirian dan kemerdekaan seseorang.[74] Sehingga pelanggaran terhadap hak atas privasi juga akan menciderai martabat dan moral seseorang.

2. Kerangka Konseptual

Agar terdapat pemahaman yang sama terhadap berbagai istilah yang digunakan dalam penelitian ini, maka perlu diberikan batasan terhadap beberapa istilah berikut ini:

a. Ruang Siber (*Cyberspace*)

Pembahasan mengenai ruang sebagai dasar penerapan aturan hukum siber haruslah dapat didefinisikan sebagai acuan utama dalam penerapan aturan yang ada dalam Hukum Siber. Seperti kebanyakan peristilahan komputer, definisi dari ruang siber tidak memiliki definisi standar. Ruang siber biasanya digunakan untuk mendeskripsikan dunia virtual komputer. Sebagai contoh, sebuah objek dalam ruang siber biasanya menunjuk kepada sekumpulan data yang melayang disekitaran suatu jaringan komputer atau network. Dengan keuntungan dari internet, ruang siber sekarang lebih berkembang memasuki *global network* dari komputer.

[73] Danrivanto Budhijanto, 2010, *Op. cit.*, hlm. 4.
[74]Stanford Encyclopedia of Philosophy, Privacy, http://plato.stanford.edu/entries/privacy/, dikunjungi pada tanggal 2 April 2023 jam 08.00 WIB.

Penggunaan peristilahan ruang siber sekarang lebih sering dikaitkan dengan internet karena perkembangan teknologi. Kata *cyber* sendiri berasal dari kata *cybernetics*, merupakan suatu bidang ilmu perpaduan antara robotik, matematika, elektro, dan psikologi yang dikembangkan oleh Norbert Wiener di tahun 1948. Salah satu aplikasi dari *cybernetics* adalah di bidang pengendalian (robot) dari jarak jauh. Dalam hal ini tentunya yang diinginkan adalah sebuah kendali yang betul-betul sempurna (*perfect control*).[75]

Pengertian dari ruang siber tidak terbatas hanya pada dunia yang tercipta ketika terjadi hubungan melalui internet. Ruang siber dapat juga diartikan hubungan yang tercipta ketika seseorang menggunakan telepon, dimana mereka dapat saling berhubungan tanpa tatap muka langsung atau keberadaannya tidak bergantung pada batas-batas konvensional mengenai benda berwujud. Tingkat perkembangan ruang siber secara fundamental telah mengaburkan definsi lama tentang ruang fisik identitas dan komunitas.

Ruang siber menyebabkan hubungan komunikasi dan koordinasi yang terjadi sangat berbeda dengan kehidupan nyata. Dalam ruang siber, seseorang dapat melakukan hubungan dengan orang lain tanpa perlu bertemu langsung pada suatu tempat dan bahkan dalam ruang siber seseorang dapat berinteraksi dengan orang baru, berdiskusi, dan yang paling buruknya adalah merencanakan untuk melakukan suatu tindak pidana internasional.

[75] Dikdik M. Arief Mansur dan Elisatris Gultom, 2009, *Cyber Law; Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, hlm. 6

Hukum internasional mengenal 3 (tiga) wilayah hukum internasional (*international space*), yaitu Antartika, ruang angkasa, dan laut bebas. Untuk menganalisis status yurisdiksi dalam ruang siber, ruang siber harus diperlakukan sebagai wilayah ke-empat hukum internasional (*international space*).[76]

Teori ruang Internasional diawali dengan sebuah pemikiran awal pada nasionalitas dan bukan teritorialitas, konsep ini adalah basis dari yurisdiksi dalam ruang angkasa, Antartika, dan laut bebas. Kategori relevan lainnya dilihat dari pesawat, kapal, maupun bangunan yang dimiliki sebagai suatu *extended territoriality* dari suatu negara di ruang-ruang internasional tersebut.[77]

Penerapan teori ruang internasional untuk ruang siber dapat terhadang secara konsep dalam keadaan fisiknya. Pada dasarnya ketiga ruang internasional yang telah dikenal oleh masyarakat internasional merupakan ruang yang nyata secara fisik, yang berbeda dengan ruang siber. Tetapi secara kualitas internasional dan *sovereignless*, maka ruang siber dapat dikategorikan dalam ruang internasional, dengan konsekuensi perlu dibuatnya suatu peraturan internasional yang mengatur mengenai ruang siber sebagaimana ruang-ruang internasional lainnya, termasuk membentuk badan khusus bagi penyelenggaraan kegiatan dan pengawasan ruang siber sebagaimana yang diaplikasikan dalam ruang-ruang internasional lainnya.[78]

Keamanan siber (*cybersecurity*) adalah upaya untuk melindungi sistem komputer, jaringan, dan data dari serangan atau akses tidak sah yang bertujuan untuk

---

[76]*Ibid.*
[77]*Ibid.*
[78]*Ibid.*

mencuri, merusak, atau mengganggu informasi atau layanan digital. Konsep ini mencakup berbagai aspek teknologi, hukum, dan kebijakan, karena ancaman siber dapat berasal dari berbagai sumber, seperti hacker, malware, virus, dan bahkan negara asing[79]

Tiga elemen utama dalam keamanan siber adalah:

1. *Confidentiality* (Kerahasiaan): Memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Contohnya adalah penggunaan enkripsi dan kontrol akses untuk melindungi data sensitive.
2. *Integrity* (Integritas): Menjaga keakuratan dan keutuhan data selama proses penyimpanan, pengiriman, atau pemrosesan. Ini bertujuan agar data tidak dapat dimodifikasi tanpa izin.
3. *Availability* (Ketersediaan): Memastikan bahwa informasi dan sistem penting selalu tersedia bagi pengguna yang sah. Contohnya adalah melindungi sistem dari serangan DDoS yang bertujuan untuk mengganggu ketersediaan layanan.

Ancaman terhadap keamanan siber dapat bervariasi mulai dari kejahatan siber (*cybercrime*), spionase siber, hingga perang siber (*cyber warfare*). Hal ini menuntut penerapan kebijakan dan teknologi yang komprehensif, baik di sektor publik maupun swasta.

[79] Hanindita Basmatulhana, *Cyber security atau Keamanan Siber: Pengertian, Jenis, dan Ancamannya*, https://www.detik.com/edu/detikpedia/d-6262847/cyber-security-atau-keamanan-siber-pengertian-jenis-dan-ancamannya, dikunjungi pada tanggal 25 Mei 2024 jam 08.25 WIB.

b. Big Data

Big Data mengacu pada kumpulan data yang sangat besar dan kompleks yang tidak dapat dengan mudah dikelola, diproses, atau dianalisis menggunakan metode pemrosesan data tradisional. Kumpulan data ini dicirikan oleh volume yang besar, kecepatan tinggi (kecepatan data dihasilkan dan dikumpulkan), dan variasi yang luas (berbagai jenis dan format data).[80] Secara tradisional, big data berdasarkan tiga karakteristik: volume, kecepatan dan variasi yang juga dikenal sebagai "tiga V". Namun, dua V tambahan telah muncul selama beberapa tahun terakhir: kebenaran dan nilai.

Penambahan tersebut masuk akal karena saat ini, data telah menjadi modal. Pikirkan beberapa perusahaan teknologi terbesar di dunia. Banyak produk yang mereka tawarkan didasarkan pada data mereka, yang terus-menerus mereka analisis untuk menghasilkan lebih banyak efisiensi dan mengembangkan inisiatif baru. Keberhasilan bergantung pada kelima karakteristik tersebut.

Karakteristik pertama yaitu *Volume*. Dengan big data, data harus memproses data bervolume tinggi dengan kepadatan rendah dan tidak terstruktur. Ini bisa berupa data dengan nilai yang tidak diketahui, seperti umpan data X (dulu Twitter), aliran klik pada halaman web atau aplikasi seluler, atau peralatan yang menggunakan sensor. Bagi

[80] Michael Chen, *Apa itu Big Data?*, https://www.oracle.com/big-data/what-is-big-data/ dikunjungi pada tanggal 2 Oktober 2024 jam 17.15 WIB.

beberapa organisasi, ini mungkin berupa puluhan terabyte data. Bagi yang lain, mungkin ratusan petabyte.

Karakteristik kedua yaitu *Velocity* atau Kecepatan. Kecepatan adalah kecepatan cepat data diterima dan (mungkin) ditindaklanjuti. Biasanya, kecepatan tertinggi aliran data langsung ke memori dibandingkan dengan yang ditulis ke disk. Beberapa produk pintar yang mendukung internet beroperasi secara real time atau mendekati real time dan akan memerlukan evaluasi dan tindakan secara real time.

Karakteristik ketiga yaitu *Variety* atau Keragaman. Keragaman mengacu pada berbagai jenis data yang tersedia. Jenis data tradisional terstruktur dan sesuai dengan basis data relasional. Dengan munculnya big data, data hadir dalam jenis data tak terstruktur baru. Jenis data tak terstruktur dan semiterstruktur, seperti teks, audio, dan video, memerlukan praproses tambahan untuk memperoleh makna dan mendukung metadata.

Karakteristik keempat yaitu *Veracity* atau Kebenaran. Gagasan tentang kebenaran dalam data terkait dengan konsep fungsional lainnya, seperti kualitas data dan integritas data. Pada akhirnya, semua ini saling tumpang tindih dan mengarahkan organisasi ke repositori data yang memberikan data berkualitas tinggi, akurat, dan andal untuk mendukung wawasan dan keputusan.

Karakteristik kelima yaitu *Value* atau Nilai. Data memiliki nilai intrinsik dalam bisnis. Namun, data tidak berguna hingga nilai tersebut ditemukan. Karena big data menggabungkan wawasan yang luas dan mendalam, di suatu tempat dalam semua

informasi tersebut terdapat wawasan yang dapat menguntungkan organisasi Anda. Nilai ini dapat bersifat internal, seperti proses operasional yang mungkin dioptimalkan, atau eksternal, seperti saran profil pelanggan yang dapat memaksimalkan keterlibatan.

Big data memiliki potensi untuk merevolusi berbagai industri dan meningkatkan kehidupan dalam banyak cara. Namun, memanfaatkan kekuatannya membutuhkan mengatasi tantangan yang signifikan dan memastikan praktik data yang bertanggung jawab dan etis.

c. Penegakan Hukum

Penegakan hukum sebagaimana dirumuskan secara sederhana oleh Satjipto Rahardjo, merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan.[81] Keinginan-keinginan hukum yang dimaksudkan di sini yaitu yang merupakan pikiran-pikiran badan pembentuk undang-undang yang dirumuskan dalam peraturan-peraturan hukum itu. Perumusan pikiran pembuat hukum yang dituangkan dalam peraturan hukum, turut menentukan bagaimana penegakan hukum itu dijalankan.

Dengan demikian pada gilirannya, proses penegakan hukum itu memuncak pada pelaksanaannya oleh para pejabat penegak hukum itu sendiri. Dari keadaan ini, dengan nada ekstrim dapat dikatakan bahwa keberhasilan ataupun kegagalan para

[81] Satjipto Rahardjo, 1983, *Masalah Penegakan Hukum*, Sinar Baru, Bandung, hlm. 24

penegak hukum dalam melaksanakan tugasnya sebetulnya sudah dimulai sejak peraturan hukum yang harus dijalankan itu dibuat.[82]

Proses penegakan hukum, dalam pandangan Soerjono Soekanto[83], dipengaruhi oleh lima faktor. Pertama, faktor hukum atau peraturan perundang-undangan. Kedua, faktor aparat penegak hukumnya, yakni pihak-pihak yang terlibat dalam peroses pembuatan dan penerapan hukumnya, yang berkaitan dengan masalah mentalitas. Ketiga, faktor sarana atau fasilitas yang mendukung proses penegakan hukum. Keempat, faktor masyarakat, yakni lingkungan sosial di mana hukum tersebut berlaku atau diterapkan; berhubungan dengan kesadaran dan kepatuhan hukum yang merefleksi dalam perilaku masyarakat. Kelima, faktor kebudayaan, yakni hasil karya, cipta dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.

Sementara itu Satjipto Rahardjo, membedakan berbagai unsur yang berpengaruh dalam proses penegakan hukum berdasarkan derajat kedekatannya pada proses, yakni yang agak jauh dan yang agak dekat. Berdasarkan kriteria kedekatan tersebut, maka Satjipto Rahardjo membedakan tiga unsur utama yang terlibat dalam proses penegakan hukum.[84] Pertama, unsur pembuatan undang-undang yang meliputi lembaga legislatif. Kedua, unsur penegakan hukum yang meliputi polisi, jaksa dan hakim. Dan ketiga, unsur lingkungan yang meliputi pribadi warga negara dan sosial.

---

[82] *Ibid*

[83] Soerjono Soekanto, 1983, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Rajawali, Jakarta, hlm. 4-5.

[84] Satjipto Rahardjo, *Op.cit.*, hlm.24

d. Kedaulatan Digital

Sejarah lahirnya konsep dari kedaulatan digital dimulai pada Juli 2020, saat pemerintah Jerman mengumumkan niatnya untuk menetapkan kedaulatan digital sebagai bagian dari kebijakan digital Eropa. Istilah kedaulatan digital telah digunakan oleh pemerintah untuk menyampaikan gagasan bahwa negara harus menegaskan kembali otoritas pemerintah atas internet dan melindungi warga negara serta sektor bisnis dari berbagai tantangan terhadap penentuan nasib sendiri di ranah digital.[85]

Sejak awal, ranah digital tampaknya menjadi lingkungan yang hampir tidak tepat untuk pelaksanaan kedaulatan, karena tidak memiliki batasan sendiri dan melintasi ruang fisik lainnya, mengaburkan pengaruh batas geografis. Terlepas dari waktu sejak awal kemunculannya, pertanyaan tentang kedaulatan di dunia digital masih menjadi kontroversi.[86]

Pada tahun 2020, Muller menulis artikel *"Against Sovereignty in Cyberspace"*[87] membahas debat kedaulatan siber dikaitkan dengan penelitian Hubungan Internasional tentang kemunculan kedaulatan secara historis, yang menunjukkan bagaimana teknologi secara rutin mengubah dasar tatanan internasional

[85] Julia Pohle and Thorsten Thiel, *Op.cit.* hlm.2

[86] Margarita Robles-Carrillo, "*Sovereignty vs. Digital Sovereignty*." Journal of Digital Technologies and Law, Vol 1, No.3, 2023, hlm. 673–690.

[87] Milton. L. Mueller, "*Against Sovereignty in Cyberspace"*, International Studies Review, Vol. 22, No.4, 2020, hlm. 779–801.

dan menantang anggapan bahwa kedaulatan teritorial adalah prinsip organisasi internasional yang stabil dan seragam yang dapat diterapkan secara presumtif pada internet. Mueller juga menghubungkan debat konseptual tentang kedaulatan siber dengan perjuangan geopolitik dunia nyata atas tata kelola internet, menunjukkan bagaimana konsepsi kedaulatan yang berbeda melayani kepentingan kekuatan yang berbeda.

Sementara pada tahun 2021, K. J. Heller menerbitkan *"In Defense of Pure Sovereignty in Cyberspace"*[88]. Heller menegaskan bahwa kedaulatan negara dalam hukum internasional bukan sekadar prinsip abstrak, melainkan merupakan aturan hukum primer yang juga berlaku penuh di ruang siber. Penulis menunjukkan bahwa operasi siber berintensitas rendah, termasuk peretasan, infiltrasi sistem, dan spionase siber tanpa persetujuan negara target, tetap dapat dianggap sebagai pelanggaran kedaulatan meskipun tidak mencapai ambang penggunaan kekuatan bersenjata atau intervensi terlarang. Dengan menganalisis praktik negara, putusan pengadilan internasional, serta doktrin hukum internasional, artikel ini mendukung pendekatan *pure sovereignty* yang memandang setiap penetrasi non-konsensual terhadap infrastruktur digital negara lain sebagai tindakan melawan hukum internasional. Oleh karena itu, perkembangan ruang siber tidak menghapus eksistensi kedaulatan negara,

[88] Kevin Jon Heller, *In Defense of Pure Sovereignty in Cyberspace,* International Law Studies, No. 97, 2021, hlm. 1432–1499.

tetapi justru memperluas relevansi dan urgensi perlindungan kedaulatan dalam menghadapi ancaman serta operasi siber lintas batas negara.

Gagasan kedaulatan digital telah diperkenalkan dalam debat politik, kelembagaan, dan akademis di tingkat internasional, nasional, dan Eropa. Terlepas dari kuantitas dan kualitas kontribusi ilmiah tentang subjek ini, tidak ada konsensus tentang konsep ini, ruang lingkup dan maknanya, sifatnya, atau bahkan, khususnya, hubungannya dengan kedaulatan fisik. Sebenarnya, kedaulatan digital diklaim baik oleh Negara maupun oleh Uni Eropa, yang tidak memiliki atribut kedaulatan.

Kedaulatan digital tampaknya bukan hanya versi daring dari prinsip kedaulatan. Hubungan antara kedaulatan dan kedaulatan digital masih jauh dari tuntas. Namun demikian, ini adalah pertanyaan yang harus dijawab untuk memastikan apakah keduanya setara, saling melengkapi, otonom, atau merupakan konsep yang berbeda sebagai langkah awal yang diperlukan untuk pemahaman yang lebih baik tentang gagasan kedaulatan digital.[89]

Kedaulatan digital mencakup hak negara untuk menetapkan kebijakan dan regulasi terkait data, informasi, dan infrastruktur digital di wilayahnya. Ini termasuk pengaturan penyimpanan data, perlindungan data pribadi, dan keamanan siber[90].

[89] Julia Pohle and Thoersten Thiel, *Op.cit.* hlm.2

[90] Graham Greenleaf, *"Global Data Privacy Laws 2023: 162 National Laws & 20 Bills"*, Privacy Laws & Business International Report, Issue 181, 2023, hlm.1-32

Kedaulatan digital memastikan bahwa negara dapat melindungi data dan infrastruktur digital dari ancaman dan penyalahgunaan yang mungkin timbul dari luar negeri[91].

Hubungan antara kedaulatan dan kedaulatan digital jauh dari sederhana. Dari perspektif kontekstual, keduanya merupakan kategori otonom. Dalam konteks digital, tidak ada kesamaan antara negara-negara yang membela prinsip kedaulatan di dunia maya dan negara-negara yang mengadvokasi kedaulatan digital. Selain itu, ketika pihak pertama juga menuntut kedaulatan digital, baik motivasi maupun makna dari gagasan ini berbeda.

Sedangkan kedaulatan adalah prinsip umum dengan cakupan dan makna yang sama untuk semua Negara dan di mana pun, kedaulatan digital tidak memiliki pemahaman yang sama dalam semua kasus dan untuk semua Negara. Konteks yang berbeda di mana kedaulatan digital diterapkan mengubah baik konsep maupun fungsinya.

Dari sudut pandang konseptual, kedaulatan digital didefinisikan sebagai kekuasaan, kemampuan, otonomi, atau dari perspektif aksiologis. Meskipun tidak ada konsensus tentang konsep ini, dalam kebanyakan kasus, definisi kedaulatan digital tidak terkait dengan prinsip kedaulatan. Dari perspektif fungsional, tidak seperti prinsip kedaulatan, tidak ada konsensus tentang fungsi atau tujuan kedaulatan digital. Namun, seruan untuk kedaulatan digital baik dalam kasus Negara maupun Uni Eropa memiliki beberapa konsekuensi penting.

[91] Sudarmadi, Damar Apri and Runturambi, Arthur Josias Simon, *Op.cit*, hlm.165

Bagaimanapun, kedaulatan digital bukanlah sekadar versi daring dari kedaulatan tradisional, dan tidak menggantikan atau menyingkirkan prinsip kedaulatan. Karena berbeda dari kedaulatan fisik dari perspektif kontekstual, konseptual, dan fungsional, maka otonominya dapat dianggap sebagai kategori pengetahuan.

G. Metode Penelitian

Bagian subbab ini penulis akan menjelaskan *Pertama* mengenai *Research Paradigm, Kedua* mengenai *Research Philosophies* dilanjutkan dengan menguraikan proses penelitian dengan mengunakan metode penelitian pada disertasi ini. Penelitian ini berfokus pada aspek normatif mengenai pengelolaan big data dalam ancaman keamanan siber dan kajian terhadap penegakan kedaulatan digital di Indonesia. Deskripsi mengenai sifat dan tipe penelitian, pendekatan penelitian, teknik pengumpulan data dan analisis data dijelaskan pada bagian ini.

1. *Research Paradigm*

Research Paradigm merupakan pandangan dasar penulis dalam melakukan penelitian mengartikulasikan keyakinan mengenai sifat realitas dan apa yang dapat diketahui atas ontologi (seperangkat asumsi mengenai realitas), epistimologi (pengetahuan tentang realitas) dan metodologi (cara-cara tertentu untuk mengetahui

realitas tersebut).[92] Dalam menjawab rumusan masalah, penelitian ini juga menggunakan *research paradigm* sebagai pemandu dalam pelaksanaan penelitian sebagai berikut:

a. *Research Ontology*

Ontologi merupakan suatu asusmsi tentang realitas. Ontologi bersifat subjektif-objektif. Bentuk ungkapan subjektif-objektif, oleh seseoarang dilakukan dalam lingkup intersubjektif. Di dalam melakukan suatu penelitian, peneliti memiliki asumsi tentang realitas, bagaimana realitas itu ada dan apa yang dapat diketahui tentang realitas tersebut. Ontologi mengarahkan peneliti untuk melakukan penelitian terhadap realitas yang ada. Ontologi menentukan realitas yang akan dipelajari, dan apa dapat diketahui tentangnya. Terkait dengan pengaturan pengelolaan big data dalam ancaman terhadap keamanan siber dalam menegakkan kedaulatan digital di Indonesia.

b. *Research Epistemology*

Epistemologi mengacu pada cabang filsafat yang mempelajari sifat pengetahuan dan proses dimana pengetahuan diperoleh dan divalidasi. Realitas bersifat subjektif-objektif yang melibatkan epistimologi. Epistimologi mmeberikan tantangan perkembangan yang menarik bagi peneliti atau disebut subjektivitas kritis. Dalam perspektif epistemologi, pengetahuan dalam penelitian ini diperoleh melalui beberapa cara. Pertama, melalui penafsiran hukum, yaitu memahami norma-norma big data dan keamanan siber dalam hukum Internasional, regional dan nasional seperti *Universal*

[92] Neil Haigh and Andrew John Withell, "*The Place of Research Paradigms in SoTL Practice: An Inquiry",* Teaching and Learning Inquiry, Vol. 8, No. 2, 2020, hlm.17-31.

Declaration of Human Right, United Nations Convention against Cybercrime (Hanoi Convention), GDPR, Konvensi Budapest, UU PDP dan UU ITE. Kedua, melalui penyusunan konsep, yaitu mengembangkan model pengaturan yang ideal terhadap pengelolaan big data dalam ancaman terhadap keamanan siber, agar penegakan kedaulatan digital di Indonesia dapat diterapkan.

c. *Research Method*

Metodologi penelitian menentukan cara peneliti mempelajari secara sistematis tentang realitas objek penelitian. Penjelasan tentang research methods yang digunakan dalam penelitian ini akan dibahas pada bagian metodologi penelitian.

2. *Research Philosophies*

Research Philosophies di dalam penelitian ini menggunakan pendekatan konstruksionis. Sebagaimana realitas di dalam penelitian ini terdiri dari serangkaian kontruksi sosial yang bervariasi, sehingga dalam penelitian ini dapat mengadopsi sikap epistemologis yang politis dan menggunakan metodologi yang memungkinkan peneliti untuk mendekonstruksikan realitas.

3. Metode Penelitan

3.1 Jenis Penelitan

Dalam penulisan disertasi ini, jenis penelitian hukum yang digunakan adalah penelitian hukum yuridis normatif.[93] Penelitian metode yuridis normatif

[93] Sunaryati Hartono, 1994 *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20,* Alumni Bandung, hlm.125

digunakan untuk menelusuri dan menganalisis pengaturan pengelolaan big data baik yang bersumber dari Perjanjian Internasional, Kebiasaan Hukum Internasional, Prinsip-Prinsip Hukum Umum, Putusan Pengadilan dan peraturan perundang-undangan, dan kebijaksanaan-kebijaksanaan di bidang hukum. Dengan kata lain, penelitian normatif adalah penelitian terhadap kaidah dan asas hukum yang ada.

Penelitian yuridis normatif bertujuan untuk menemukan jawaban atas bagaimana pengaturan pengelolaan big data dalam ancaman terhadap keamanan siber serta bagaimana model terkait pengaturan hukum yang ideal dalam melindungi big data guna menegakkan kedaulatan digital di Indonesia.

Penelitian hukum normatif merupakan penelitian hukum yang menggunakan data sekunder dari kepustakaan. Pengunaan data sekunder untuk menghasilkan tinjauan kepustakaan. Tinjauan kepustakaan adalah metode ilmiah untuk mengidentifikasi, mengevaluasi dan menafsirkan semua literatur yang relevan dengan topik penelitian ini.

Penelitian ini juga menggunakan data primer berdasarkan wawancara. Metode wawancara dilakukan pada badan/Lembaga yang bertangggung jawab atas pengelolaan big data yang diamanatkan Undang-Undang (Kementrian Komunikasi dan Digital dan Peraturan Presiden yakni BSSN. Wawancara dilakukan dengan maksud untuk mengklarifikasi bahan-bahan hukum.

3.2 Pendekatan Penelitian

Dalam penelitian ini peneliti menggunakan beberapa pendekatan penelitian, yakni: pendekatan perundang-undangan (*Statute Approach*), pendekatan komparatif (*Comparative Approach*) dan pendekatan konseptual (*Conceptual Approach*). Pendekatan perundang-undangan dalam penelitian ini berarti menelusuri kemudian menganalisa seluruh peraturan perundangan-undangan yang terkait dengan permasalahan hukum yang dihadapi. Pendekatan ini digunakan untuk mengkaji peraturan hukum internasional, regional dan nasional yang mengatur big data dan keamanan siber, seperti: Konvensi Montevideo, UDHR, ICCPR, ITU regulation, Konvensi Hanoi, GDPR, Konvensi Budapest, APEC Privacy Framework, ASEAN Framework on Digital Data, serta peraturan nasional USA, China dan Indonesia.

Pendekatan komparatif dilakukan membandingkan peraturan hukum yang eksisting di Indonesia dengan peraturan hukum di negara lain. Pendekatan komparatif dilakukan untuk memperoleh persamaan dan perbedaan di antara peraturan hukum di Indonesia terkait pengelolaan big data dalam ancaman terhadap keamanan siber sebagai suatu kajian penegakan kedaulatan digital dalam upaya membuat konsep yang ideal dalam pengaturan pengelolaan big data. Adapun negara yang menjadi komparasi dalam pengaturan big data pada penelitian ini adalah Amerika Serikat dan China. Kemudian peneliti membandingkan juga terkait praktek penegakan kedaulatan digital, diantaranya: Amerika Serikat, China, Uni Eropa dan Rusia. Keseluruhan negara tersebut dipilih sebagai studi komparasi dikarenakan regulasi dan praktek yang baik dalam pengelolaan big data dalam

ancaman keamanan siber serta praktek penegakan kedaulatan digital yang baik. Pendekatan ini digunakan sebagai pisau analisis untuk menjawab rumusan masalah pertama terkait peraturan dan rumusan masalah kedua terkait penegakan kedaulatan digital.

Pendekatan konseptual dalam penelitian ini memberikan sudut pandang analisis penyelesaian permasalahan dalam penelitian hukum dilihat dari aspek konsep-konsep hukum yang melatarbelakanginya. Pendekatan ini digunakan untuk memahami konsep big data, keamanan siber dan penegakan hukum serta kedaulatan digital. Pendekatan ini digunakan untuk membuat model yang ideal terkait pengaturan pengelolaan big data dalam ancaman keamanan siber untuk mewujudkan penegakan kedaulatan digital.

3.3 Teknik Pengumpulan Data

Dengan penjabaran sebagai berikut :

a. Penelitian Kepustakaan (*Library Research*), yaitu mengkaji data sekunder yang terdiri dari:

(1) Bahan-bahan hukum primer berupa peraturan-peraturan perundang-undangan, antara lain:
   a) Undang-Undang Dasar 1945;
   b) Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana;
   c) Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi;
   d) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

e) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
f) *ITU Regulation 2007;*
g) *EU Convention on Cybercrime 2001*
h) *Konvensi Montevideo* 1933;
i) *EU Regulation General Data Protection Regulation;*
j) Resolusi Majelis Umum PBB A/Res/68/167 tentang Hak Atas Privasi di Era Digital 2013;
k) African Union Convention on Cyber Security and Personal Data Protection 2014;
l) APEC Privacy Framework 2015;
m) ASEAN Framework on Personal Data Protection 2016;
n) ASEAN Framework on Digital Data Governance 2018;
o) ASEAN Model Contractual Clauses for Cross Border Data Flows 2021;
p) California Consumer Privacy Act of 2018;
q) Clarifying Lawful Overseas Use of Data Act (CLOUD Act) 2018;
r) Convention on Cybercrime (Budapest Convention) 2001;
s) Cybersecurity Law of the People's Republic of China 2017;
t) Data Security Law of the People's Republic of China 2021;
u) Digital Personal Data Protection Act India 2023;
v) International Covenant on Civil and Political Rights (ICCPR) 1966;
w) Personal Information Protection Law of the People's Republic of China 2021;
x) Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence 2021;
y) United Nations Convention against Cybercrime (Hanoi Convention) 2024;
z) Naskah Akademik RUU Keamanan dan Ketahanan Siber dan kebiasaan suatu negara yang menjadi sumber hukum serta peraturan-peraturan

dibawah Undang-undang, baik itu Peraturan Pemerintah, Peraturan Presiden dan peraturan teknis lainnya di Tingkat Kementerian/Lembaga.

(2). Baha n-bahan hukum sekunder, yaitu bahan-bahan hukum yang memberikan petunjuk atau penjelasan terhadap bahan-bahan hukum primer yang berupa buku-buku yang ditulis para ahli, rancangan undang-undang, hasil penelitian terdahulu dan media massa yang isinya mempunyai relevansi dengan bahasan disertasi ini.

(3). Bahan-bahan hukum tersier, yaitu bahan-bahan lain yang ada relevansi dengan pokok permasalahan yang memberikan informasi tentang bahan-bahan hukum primer dan sekunder antara lain artikel, kamus, majalah dan koran.

b. Cara pengumpulan data

Cara pengumpulan data adalah dengan cara studi dokumen, yaitu dengan mengkaji, menguji serta menemukan peraturan perundang-undangan yang berlaku dan dikaitkan dengan teori-teori dalam ilmu hukum yang membahas pengelolaan big data, keamanan siber dan kedaulatan digital. Pengumpulan data sekunder seperti pada bab dua dengan menggunakan mesin pencari *science direct* (https://www.sciencedirect.com), *google scholar* (https://scholar.google.com). Sementara wawancara tidak dapat peneliti lakukan karena tidak adanya respon dari Kementerian Komunikasi dan Digital dengan alasan berubahnya nama Kementerian dari Kominfo ke Komdigi dan saat peneliti menyerahkan surat permohonan penelitian disampaikan secara lisan menunggu nomenklatur yang baru terkait dengan Direktorat Jenderal yang berwenang dalam memberikan klarifikasi atau informasi. Demikian juga ke Badan Siber Sandi Negara, hingga saat ini belum

ada info dan respon terkait kelanjutan surat permohonan penelitian yang peneliti sampaikan.

3.4 Analisis Data

Bahan penelitian berupa bahan-bahan hukum yang telah dikumpulkan tersebut selanjutnya diolah dan dianalisis secara kualitatif, yakni berwujud dengan kata-kata dan tidak berwujud dengan angka-angka. Data yang diperoleh kemudian disusun secara sistematis dan selanjutnya dianalisis secara kualitatif untuk memperoleh kejelasan dan menemukan pemecahan atas masalah yang diteliti. Adapun instrumen analisis yang digunakan adalah metode interpretasi (penafsiran) sebagaimana lazim yang digunakan dalam penelitian ilmu hukum, khususnya penelitian normatif, seperti metode penafsiran ektensif, gramatikal dan sistematis.[94]

[94] Yudha Bhakti Ardiwisastra, 2000, *Penafsiran dan Kontruksi Hukum,* Alumni Bandung, hlm. 9-10.