PENERAPAN PRINSIP YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

SKRIPSI

Oleh:

MOHAMMAD FADEL ROIHAN BA'ABUD

18410656

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

2022

PENERAPAN PRINSIP YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

SKRIPSI

Diajukan untuk Memenuhi Sebagian Persyaratan Guna Memperoleh

Gelar Sarjana (Strata-1) pada Fakultas Hukum

Universitas Islam Indonesia

Yogyakarta

Oleh:

MOHAMMAD FADEL ROIHAN BA'ABUD

No. Mahasiswa: 18410656

PROGRAM STUDI HUKUM PROGRAM SARJANA

FAKULTAS HUKUM

UNIVERSTAS ISLAM INDONESIA

YOGYAKARTA

2022

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENERAPAN YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

Telah diperiksa dan disetujui Dosen Pembimbing Tugas Akhir untuk diajukan ke depan TIM Penguji dalam Ujian Tugas Akhir / Pendadaran pada tanggal 28 Agustus 2023

Yogyakarta, 24 Juli 2023
Dosen Pembmbing Tugas Akhir,

Dodik Setiawan Nur Heriyanto, S.H., M.H., LL.M., Ph.D.

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENERAPAN YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

Telah Dipertahankan di Hadapan Tim Penguji dalam
Ujian Tugas Akhir / Pendadaran
pada tanggal dan Dinyatakan LULUS

Yogyakarta, 28 Agustus 2023

Tim Penguji			Tanda Tangan
1. Ketua	:	Dodik Setiawan Nur Heriyanto, S.H., M.H., LL.M., Ph.D.	.....
2. Anggota	:	Sefriani, Prof. Dr., S.H., M.Hum.	.....
3. Anggota	:	Nandang Sutrisno, S.H., LL.M., M.Hum., Ph.D.	.....

Mengetahui:
Universitas Islam Indonesia
Fakultas Hukum
Dekan,

Prof. Dr. Budi Agus Riswandi, S.H., M.H.
NIK. 014100109

SURAT PERNYATAAN ORISINALITAS

KARYA TULIS ILMIAH BERUPA TUGAS AKHIR
MAHASISWA FAKULTAS HUKUM UNIVERSITAS ISLAM INDONESIA

Bismillahirrahmanirrahim

Saya yang bertanda tangan di bawah ini:

Nama : **Mohammad Fadel Roihan Ba'abud**

NIM : **18410656**

Adalah benar-benar mahasiswa Fakultas Hukum Universitas Islam Indonesia Yogyakarta yang telah melakukan penulisan Karya Tulis Ilmiah Tugas Akhir berupa Skripsi dengan judul:

PENERAPAN PRINSIP YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

Sehubungan dengan hal tersebut, dengan ini saya menyatakan bahwa:

1. karya ilmiah ini adalah benar hasil karya saya mandiri yang dalam penyusunannya tunduk pada kaidah, etika dan norma penulisan sebuah karya tulis ilmiah sesuai dengan ketentuan yang berlaku;
2. saya menjamin hasil karya ini adalah orisinil dan bebas dari plagiasi;
3. meskipun secara prinsipil hak miliki atas karya tulis ilmiah ini ada pada saya, namun demi kepentingan-kepentingan yang bersifat akademik dan pengembangannya, saya memberikan kewenangan kepada Perpustakaan Fakultas Hukum Universitas Islam Indonesia untuk menggunakan karya tulis ilmia ini.

Selanjutnya, berkaitan dengan hal di atas, khususnya pada persyaratan butir 1 dan 2, saya sanggup menerima sanksi baik administratif, akademik maupun pidana jika saya terbukti secara kuat dan meyakinkan telah melakukan perbuatan yang menyimpang dari pernyataan tersebut, saya juga akan bersikap kooperatif untuk

hadir, menjawab, membuktikan dan melakukan pembelaan terhadap hak saya serta menandatangani Berita Acara terkait yang menjadi hak dan kewajiban saya di depan pihak berwenang apabila dalam penelitian ini terdapat tanda-tanda maupun terbukti terdapat plagiasi oleh Pihak Fakultas Hukum Universitas Islam Indonesia. Demikian surat pernyataan ini dibuat sebenar-benarnya tanpa paksaan dan secara sadar oleh penulis untuk dipergunakan sebagaimana mestinya.

Yogyakarta, 20 Juli 2023

Yang Bersangkutan

(Mohammad Fadel Roihan Ba'abud)

NIM 18410656

CURRICULUM VITAE

1.	Nama Lengkap	:	Mohammad Fadel Roihan Ba'abud
2.	Tempat Lahir	:	Ciamis
3.	Tanggal Lahir	:	30 Juli 2000
4.	Jenis Kelamin	:	Laki-Laki
5.	Golongan Darah	:	O
6.	Alamat Asal	:	Jl. Ir. H. Juanda No. 185, RT.03/RW.06, Kel. Ciamis, Kec. Ciamis, Kab. Ciamis, Jawa Barat.
7.	Identitas Orang Tua	:	
	a. Nama Ayah	:	Alwi Achmad
	Pekerjaan Ayah	:	Wiraswasta
	b. Nama Ibu	:	Nevie Alifah Assegaf
	Pekerjaan Ibu	:	Notaris
	Alamat Orang Tua	:	Jl. Ir. H. Juanda No. 185, RT.03/RW.06, Kel. Ciamis, Kec. Ciamis, Kab. Ciamis, Jawa Barat.
8.	Riwayat Pendidikan		
	a. TK	:	TK Aisyiyah Bustanul Athfal
	b. SD	:	SD Negeri 3 Ciamis
	c. SMP	:	SMP Negeri 1 Ciamis
	d. SMA	:	SMA Negeri 1 Ciamis
9.	Pengalaman Organisasi	:	
	a. *Organizing Committee* Divisi Wali Jama'ah Pekan Raya dan Silaturahmi Perkenalan (PERADILAN) Tahun 2020.		
	b. Koordinator Bidang Pendidikan Organisasi Mahasiswa Daerah Keluarga Persatuan Mahasiswa Galuh-Rahayu Yogyakarta.		

c. Sekretaris Unit Dakwah dan Pengabdian Masyarakat Himpunan Mahasiswa Islam Komisariat Fakultas Hukum UII Periode 2020-2021.

d. Sekretaris Umum Himpunan Mahasiswa Islam Komisariat Fakultas Hukum UII Periode 2021-2022.

e. Sekretaris Bidang Kajian Strategis dan Studi Peradaban Himpunan Mahasiswa Islam Cabang Yogyakarta Periode 2023-2024.

10. Prestasi :

a. Awardee program Indonesia International Student Mobility Awards Batch 2021

b. Pembawa Acara Indonesian Day Event di University of Warsaw, Polandia 2021

11. Pengalaman Kerja :

a. Magang di Kantor Notaris/PPAT Nevie Alifah Assegaf S.H., M.H. selama 2 bulan terhitung sejak 16 Januari – 6 Februari

12. Pengalaman Pendidikan dan Pelatihan

a. Karya Latihan Tulis dan Hukum (Kartikum) Ke- 36 Lembaga Konsultasi dan Bantuan Hukum (LKBH) Fakultas Hukum Universitas Islam Indonesia dengan predikat Jaksa Penuntut Umum Terbaik dalam Sidang Peradilan Semu.

13. Hobi :

a. Berdialog/diskusi, berbicara bahasa asing, membaca dan menulis.

Yogyakarta, 20 Juli 2023

Yang Bersangkutan

Mohammad Fadel Roihan Ba'abud

MOTTO

هَلْ جَزَآءُ ٱلْإِحْسَٰنِ إِلَّا ٱلْإِحْسَٰنُ

Tidak ada balasan kebaikan (kecuali) kebaikan pula.
(Q.S Ar-Rahman Ayat 60)

Perjuangan merupakan peningkatan kualitas iman yang membentuk jati diri seorang muslim. Kegagalan dalam perjuangan bukanlah titik kehinaan dalam keimanan seseorang. Dan keberhasilan bukanlah titik kemuliaan keimanan.
(Khittah Perjuangan)

HALAMAN PERSEMBAHAN

Dengan menyebut nama Allah yang Maha Pengasih lagi Maha Penyayang, dan dengan mengingat bahwa sesungguhnya seluruh shalatku, perjuanganku, hidupku dan matiku hanyalah untuk Allah SWT, tugas akhir ini dengan segala kerendahan hati saya persembahkan kepada:

1. Kedua orang tua penulis, yang membesarkan dan merawat penulis tanpa lelah, tanpa keluh, dan penuh cinta. Semoga sedikit capaian ini menimbulkan rasa bangga di hati kalian.
2. Adik saya tercinta, sebagai saksi hidup diri penulis yang membersamai 20 tahun dari kehidupan penulis, semoga tulisan ini dapat membangkitkan semangat dalam perjuanganmu, dik.
3. Keluarga Himpunan Mahasiswa Islam Fakultas Hukum Yogyakarta, sebagai wadah pola fikir dan gerak diri penulis sebagai mahasiswa Islam. Tetap satu dalam tujuan, dan menyatu dalam gerakan kawan-kawan seperjuanganku.
4. Seluruh Civitas Academica Universitas Islam Indonesia dan terkhusus Fakultas Hukum Universitas Islam Indonesia.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji dan syukur, patut kita persembahkan kepada Allah SWT, Dzat pencipta seluruh alam, yang tidak mengenal awal dan akhir, yang dari Dia-lah, kita lahir dan kepada Dia pula kita akan kembali. Shalawat serta salam juga terus kita sampaikan kepada nabi Muhammad SAW, patron dari sebaik-baiknya patron bagi manusia, yang dari perjuangan beliau kita bisa merasakan kenikmatan dan kehidmatan hidup sebagai manusia yang beradab dan berakal dalam garis keselamatan.

Telah sampai penulis pada akhir dari perjuangan menempuh studi selama kurang lebih 5 tahun lamanya, dalam menggapai strata sarjana di bidang hukum dengan tugas akhir yang berjudul "Penerapan Prinsip Yurisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Siber yang Dilakukan Secara Lintas Batas Negara", atas izin dari Allah SWT dan sebagai amanat untuk bermanfaat kepada sesama manusia. Meskipun dengan segala kekurangan dan kekhilafan dalam karya ini, semoga tulisan ini dapat bermanfaat bagi kita semua.

Tentu saja, tahap ini bukanlah menjadi akhir dari perjuangan, melainkan sebuah babak baru dalam kehidupan. Pengalaman perantauan juga melukiskan kesan dalam coretan hidup penulis yang mustahil untuk dilupakan. Maka dari itu, dalam kesempatan ini dengan penuh ketulusan hati penulis ucapkan terimakasih kepada kedua orang tua penulis, Nevie Alifah Assegaf dan Alwi Achmad Ba'abud yang membanting tulang dan mengorbankan segalanya. Selanjutnya juga kepada adik dari penulis, Zainab Fahira Nurfitria Ba'abud dalam segala suka dan duka yang

telah dibagi dalam kehidupan penulis. Teman-teman terdekat penulis, Muhammad Mahendra Adi dan Tikno boys, Muhammad Fariel Nabawi, Ahmad Haikal Nasution, Rofi Zaidan Mubarok, Aditya Akbar Lubis, Ahmad Qodri Barmawi, yang mendampingi pengalaman perkuliahan selama ini. Juga kepada dosen pembimbing saya, pak Dodik Setiawan yang juga mengurusi penulis ketika mengikuti studi IISMA, semoga jasa bapak selama ini menjadi ibadah yang diridhoi oleh Allah. Tak lupa juga kawan-kawan dalam Himpunan Mahasiswa Islam yang menjadi tempat berkembang penulis dalam masa perkuliahan ini. *Specjalne dzięki dla* Paulina Szcodrowska, *Zmieniłaś mnie w sposób, którego nie potrafię opisać, and for my good friends I met during my 4 months in Warsaw, Qiya, Samy, Raihan, Tio, Kerim Hakim, Jacek, Wanda, and also many others that I can't mention.* Tentu juga kepada seluruh teman-teman lainnya yang tidak bisa saya sebutkan satu per satu, namun ketahui bahwa rasa syukur selalu terucap untuk semua orang yang penulis kenal. Semoga kita bertemu di lain waktu, dalam keadaan yang baik dan lebih baik dari saat ini.

Untuk menutup kalam ini, penulis memohon maaf atas segala kekhilafan yang diperbuat dalam kesadaran maupun ketidaksengajaan, karena kesempurnaan hanyalah milik Allah, dan penulis seagai hambanya tidaklah luput dari kesalahan. Semoga tulisan ini bisa bermanfaat dan cita-cita dari tulisan ini bisa dilanjutkan dalam estafet keilmuan. *Dan sebaik-baiknya manusia adalah yang paling bermanfaat bagi manusia lainnya*.

Billahitaufik Wal Hidayah

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

DAFTAR ISI

ABSTRAK

Kejahatan tindak pidana siber merupakan realita yang terjadi seiring berkembangnya era digitalisasi. Salah satunya merupakan pencurian terhadap data pribadi yang merupakan tindak pidana siber yang paling umum dilakukan. Dalam momentum berlakunya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi yang berlaku secara ekstrateritorial diperlukan pendalaman terhadap bagaimana sebenarnya penerapan dari yurisdiksi terhadap pelaku pencurian data pribadi berbasis siber yang dilakukan secara lintas batas negara. Dari keresahan tersebut penulis melakukan penelitan normatif yang dilakukan melalui pendekatan statuta/perundang-undangan, konseptual serta perbandingan/komparatif dengan UU No. 27 Tahun 2022 sebagai pisau analisis perundang-undangan yang dimiliki Indonesia terhadap berbagai kerangka hukum dan konvensi yang dimiliki hukum Internasional terkait penegakan terhadap tindak pidana siber pencurian data pribadi yang dilakukan secara lintas batas negara. Dari hasil penelitian didapatkan bahwa hukum domestik yang bersifat ekstrateritorial bukan merupakan jawaban yang mutlak terhadap keberhasilan dari penerapan yurisdiksi ekstrateritorial. Secara garis besar dibutuhkan sebuah kerangka hukum internasional yang menyokong kooperasi internasional berkelanjutan untuk secara efektif menerapkan yurisdiksi ekstrateritorial terhadap pelaku pencurian data pribadi secara lintas batas negara.

Kata Kunci: digitalisasi, kejahatan lintas batas negara, perlindungan data pribadi, tindak pidana siber, yurisdiksi ekstrateritorial.

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi telah berkembang secara pesat, dimulai dengan berubahnya peradaban manusia yang melakukan semua hal secara manual, hingga digitalisasi dan "internetisasi" aktivitas manusia dengan konsep *Internet of Things (IoT)*. *IoT* merupakan sebuah konsep yang memperluas fungsi dari konektivitas internet yang tersambung secara terus menerus.[1] Dalam kehidupan yang sudah terdigitalisasi dan "internetisasi", data/informasi menjadi objek vital dalam kelangsungan suatu sistem. Sejatinya, dalam masyarakat modern banyak yang tidak menyadari bahwa sifat praktis yang dihasilkan dari konsep ini merupakan transaksi elektronik antara developer dengan data/informasi, sebagai perluasan fungsi dari konektivitas internet tersebut. Perkembangan ini juga berimplikasi kepada globalisasi digital, dimana batas antar negara semakin memudar dan menghasilkan *cross-border data flows* yang semakin meningkat.[2]

Dalam era ini data/informasi merupakan komoditas yang paling utama. Informasi menjadi komoditas dikarenakan bisa "diperjualbelikan" untuk mendapat

[1] Yoyon Efendi. "*Internet of Things (IoT) "Sistem Pengendalian Lampu Menggunakan Raspberry PI Berbasis Mobile*." Jurnal Ilmiah Ilmu Komputer, Vol. 4 No. 1 April 2018, Hlm. 19

[2] Susan Lund, James Manyika, James Bughin. 2016. *Harvard Business Review.* 14 Maret. Diakses pada: September 23 2022. Url: https://hbr.org/2016/03/globalization-is-becoming-more-about-data-and-less-about-stuff.

keuntungan baik secara langsung maupun tidak langsung dari penggunaan informasi/data tersebut. Sebagai komoditas, informasi merupakan perbatasan baru (*new frontier)* dalam konsep transaksi komersil, mulai dari menciptakan subjek komersial baru yang sukar untuk diketahui nilainya, hingga perlunya pembahasan yang mendalam terkait hak-hak dan kewajiban terhadap informasi sebagai komoditas komersial ini.[3] Sebagaimana pendapat dari Takumi Kimura yang mendefinisikan *Society 5.0* sebagai "*human-centered society that balances economic advancement with the resolution of social problem that highly integrates cyberspace and physical space.*" Yakni sebuah masyarakat bercorak manusia-sentris yang menyeimbangkan perkembangan ekonomi dengan penyelesaian masalah sosial melalui integrasi tingkat tinggi antara ruang siber dengan ruang fisik.[4] Integrasi antara data ini digunakan melalui skema *big data* dan *Internet of Things*, serta fasilitasi kecerdasan artifisial (A.I) dengan pelayanan manusia sebagai tujuan akhir dari sistem ini.

Namun, dia juga menyatakan bahwa digitalisasi ini menimbulkan kerentanan dari sistem baru ini terhadap serangan siber. Contoh paling umum adalah dalam ranah finansial, khususnya perbankan dengan sistem online banking yang menjadi salah satu target utama dalam serangan siber. Nigeria dan Kenya menjadi salah satu negara yang memiliki dampak negatif terbesar dari serangan ini, dengan kerugian

[3] Raymond T. Nimmer & Patricia Ann Krauthaus, *Information as a Commodity: New Imperatives of Commercial Law*, Vol.55 *Law and Contemporary Problems*, 1992. Hal. 103

[4] Takumi Kimura, Analis siber di NRI SecureTechnologies,Ltd. Dalam sebuah artikel yang diakses di https://www.nri.com/en/journal/2020/0825

mencapai $649 juta dan $210 juta per tahunnya.[5] Salah satu faktor kerentanan ini adalah tidak kuatnya regulasi mengenai tindak pidana siber dan secara khusus terkait perlindungan data untuk mempersiapkan digitalisasi yang sedang berlangsung.

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi mengambil *General Data Protection Regulation* Uni Eropa sebagai salah satu referensi dasar hukum privasi dari standar pembentukan regulasi perlindungan data pribadi[6]. Implementasi dari hal ini bisa kita bandingkan dari ruang lingkup subjek yang diberlakukan hukum ini, dimana pemerintah Indonesia telah secara berani menegaskan dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memberlakukan pengaturan nasional terkait data pribadi secara dengan menerapkan asas nasionalitas pasif sebagaimana termaktub dalam Pasal 2 ayat (1) butir b yang menyatakan bahwa Undang-Undang Pelindungan Data Pribadi ini berlaku untuk setiap orang, badan hukum ataupun organisasi internasional baik didalam maupun diluar wilayah hukum Indonesia selama perbuatan tersebut memiliki akibat hukum di wilayah hukum NKRI atau berdampak bagi subjek data pribadi WNI yang berada di luar wilayah hukum NKRI.

[5] Farah Hanan Muhamad, dkk., *Awareness on Financial Cybercrime among Youth: Experience, Exposure and Effect.* Society 5.0 2021 Proceedings, Vol. II, 2021. Hal. 298.
[6] Presentasi Dr. Edmon Makarim, S. Kom., S.H., LL.M. dalam Penelitian Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT) dalam RDPU RUU PDP. Diakses melalui: https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf

Namun, penegakan terkait dengan hal ini tentu sulit apabila direalisasikan hanya dengan sebuah hukum nasional tanpa mengkorelasikan dengan hukum internasional. Cita- cita dari pelaksanaan hukum yang mengikat terhadap siapapun selama berdampak bagi Indonesia dan subjek hukum Indonesia tetap jauh untuk direalisasikan, dengan kurangnya media instrumen hukum yang menyokong hal tersebut. Baru-baru ini, Republik Indonesia dikejutkan oleh berita terkait bocornya data registrasi SIM (*Subscriber Identity Module)* Card sebanyak 1.304.401.300 atau yang terkandung dalam file sebesar 87 GB (*GigaByte)* berisi Nomor Induk Kependudukan (NIK), nomor telepon, operator seluler yang digunakan dan juga tanggal penggunaan.[7] Data ini kemudian diperjualbelikan oleh sebuah akun bernama "Bjorka" di situs/forum "breached.co". Sampai saat ini pihak pemerintah masih belum bisa menangkap pelaku beralias Bjorka ini, dan salah satu faktor yang menjadi kesulitan dari penegakan terhadap kejahatan dalam bidang siber merupakan sulitnya melakukan pelacakan terhadap pelaku dari tindak pidana siber tersebut, terlebih mengingat anonimitas yang menjadi sifat dari kemajuan teknologi dan informasi ditambah dengan keahlian yang mumpuni dalam bidang tersebut tentu akan menambah taraf kesulitan dari penindakan tindak pidana siber. Selain kasus ini juga berdiri sederet kasus-kasus lain yang tidak menemukan kejelasan terkait penegakan hukum terhadap pelaku yang bertanggung jawab, seperti kasus

[7] Arrijal Rachman, dalam tulisan berita Tempo.co berjudul "*1,3 Miliar Data Sim Card Bocor, Kominfo: Baru 15-20 Persen yang Cocok"* 5 September 2022. Diakses melalui: https://bisnis.tempo.co/read/1630609/13-miliar-data-sim-card-bocor-kominfo-baru-15-20-persen-yang-cocok#:~:text=Senin%2C%205%20September%202022%2014%3A48%20WIB&text=Dari%20hasil%20penelusuran%20sementara%20dengan,data%20SIM%20Card%20yang%20bocor.

bocornya data BPJS pada tahun 2021, serta peretasan terhadap BSI yang diakui dilakukan oleh sindikat *cybercrime* Rusia bernama Lockbit yang tidak memiliki kelanjutan apapun dalam hal penegakan hukum.[8]

Kesulitan-kesulitan dalam penindakan terhadap tindak pidana siber tentu juga akan berkaitan dengan permasalahan terkait dengan terkikisnya klasifikasi wilayah beserta yurisdiksi teritorialnya. Sesuai dengan kalimat Debra L. Shinder, "*cybercrime cases, more than most others, often involve complex jurisdictional issues that can present both legal and practical obstacle to prosecution.*[9] Kesulitan terhadap penindakan *cybercrime* dalam ranah yurisdiksi sangat dipengaruhi dengan model dari tindak pidana siber itu sendiri yakni *bordeless* (tanpa batas) dan *anonymous* (tidak dikenal). Potensi dari pelaku kejahatan siber dapat berada dimana saja selama terdapat jaringan internet menjadikan dunia secara global sebagai wadah dari pelaku kejahatan siber, dan anonimitas dari pelaku itu sendiri dimana pelaku biasanya tidak bisa dikenali atau dilacak dengan metode konvensional untuk menemukan jejak dari kejahatan siber.

Sebagai konsekuensinya, hal tersebut menjadikan prinsip yurisdiksi konvensional dimana negara hanya memiliki kewenangan mutlak untuk memberlakukan hukumnya secara limitatif didalam daerah teritorinya sendiri

[8] Jayant Chakravarti, *LockBit Leaks 1.5 TB of Data Stolen from Indonesia's BSI Bank*. Bank Info Security, pada tanggal 18 Mei 2023. Diakses pada tanggal 19 Juli 2023 melalui: https://www.bankinfosecurity.com/lockbit-leaks-15tb-data-stolen-from-indonesias-bsi-bank-a-22110

[9]Sigid Suseno, *Cybercrime, Pengaturan dan Penegakan Hukumnya di Indonesia dan Amerika Serikat*, Jurnal Ilmu Hukum Padjajaran Jilid XXXIII, 2009, Hal. 41-42.

menjadi kuno dan tidak relevan, sebagaimana pernyataan Gercke dalam jurnalnya, "*It is difficult to base cooperation in cybercrime base in principles of traditional mutual legal assistance. The formal requirements and the time needed to collaborate with foreign law-enforcement agencies often hinder investigations".*[10] Adalah sulit untuk melandasi kooperasi untuk tindak pidana siber berdasarkan prinsip tradisional *mutual legal assistance.*[11]

Persyaratan formal dan waktu yang dibutuhkan untuk bekerjasama dengan agensi penindakan hukum asing seringkali menghambat jalannya proses investigasi. Sebagai contoh data yang vital untuk pelacakan kepada pelaku kejahatan seringkali dihapus atau disembunyikan dalam kurun waktu yang tidak lama setelah kejadian dilakukan, menyebabkan koordinasi antar institusi penegakan hukum negara-negara sebagai syarat prosedural menjadi tambahan waktu bagi pelaku untuk menyembunyikan jejaknya[12]. Mengingat pelbagai permasalahan diatas, maka penulis berniat untuk menulis penelitian ini yang berfokus kepada baik pengaturan dari tindak pidana siber pencurian data pribadi yang dilakukan secara lintas batas negara baik secara nasional dan internasional, maupun penerapan dari prinsip yurisdiksi ekstrateritorial sebagai jawaban bagi penegakan pelaku tindak

[10] Gercke, *The Slow Wake of a Global Approach Against Cybercrime,* Computer Law Review International 2006, Hal. 142.

[11] *Mutual Legal Assistance* adalah sebuah bentuk perjanjian antar negara yang memberikan dasar hukum bagi negara untuk meminta dan/atau memberikan bantuan yang berkaitan dengan masalah pidana transnasional dalam hal berkenaan terhadap proses penyidikan, penuntutan dan pemeriksaan agar pelaku dapat dikenakan hukum nasional dari negara yang meminta bantuan tersebut. Penjelasan lebih lanjut lihat Pasal 2 dan 3 UU No. 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.

[12] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges, and Legal Response.* International Telecommunications Union, 2012. Hal. 77.

pidana siber yang berkaitan dengan pencurian data pribadi dalam lingkup lintas batas negara.

B. Rumusan Masalah

1. Bagaimana pengaturan terkait dengan tindak pidana siber/*cybercrime* pencurian data pribadi yang dilakukan secara lintas batas negara menurut hukum Indonesia dan hukum Internasional?
2. Bagaimanakah implementasi dari prinsip yurisdiksi ekstrateritorial terhadap pelaku tindak pidana siber/*cybercrime* pencurian data pribadi yang dilakukan secara lintas batas negara?

C. Tujuan

Sejalan dengan rumusan masalah di atas, maka tujuan dari penelitian hukum ini adalah sebagai berikut:

1. Untuk mengkaji regulasi yang dimiliki terkait dengan tindak pidana siber/*cybercrime* pencurian data pribadi baik menurut hukum Indonesia serta hukum yang berlaku di lingkup Internasional.
2. Untuk mengkaji terkait prinsip yurisdiksi ekstrateritorial dan korelasinya terhadap penegakan pelaku tindak pidana siber/*cybercrime* pencurian data pribadi yang dilakukan secara transnasional.

D. Orisinalitas Penelitian

Skripsi berjudul "Penerapan Prinsip Yurisdiksi Ekstrateritorial terhadap Pelaku Tindak Pidana Pencurian Data Pribadi yang Dilakukan Secara Lintas Batas Negara" adalah skripsi yang ditulis berdasarkan penelitian yang dilakukan oleh penulis, dan bukan hasil tindakan plagiasi atau merupakan karya dari orang lain. Adapun perbedaan yang menjadi titik pembeda dari penelitian ini dibandingkan dengan penelitian terdahulu adalah fokus penelitian terhadap implementasi dari sifat yurisdiksi ekstrateritorial dalam UU No. 27 Tahun 2022 terhadap kasus pencurian data pribadi yang dilakukan secara lintas batas negara, disamping perbandingan UU No. 27 Tahun 2022 dengan berbagai instrumen hukum lain dalam bidang pelindungan data pribadi. Dibawah merupakan penelitian-penelitian yang mempunyai pembahasan yang serupa dan juga analisa terhadap faktor pembedanya sebagai pembuktian terhadap orisinalitas dari karya ini:

No.	Peneliti, Judul Penelitian, Jenis Penelitian/Publikasi, dan Tahun	Rumusan Masalah Penelitian	Deksripsi Perbedaan dengan Penelitian yang Dilakukan oleh Peneliti
1.	Rio Dwiky Perwira, Eddy O.S Hiariej, Penerapan Prinsip Yurisdiksi Ekstrateritorial Pada Cybergambling Sebagai	1. Bagaimana penerapan dari prinsip yurisdiksi ekstrateritorial yang diatur dalam pasal 2 UU ITE terhadap kejahatan	Dalam penelitian tersebut para penulis fokus terhadap kejahatan transnasional berupa *cybergambling*, dan menganalisis dengan UU

	Kejahatan Transnasional di Indonesia, Skripsi, 2019.	transnasional *cybergambling?* 2. Apa modus operandi dari kejahatan *cybergambling transnasional*?	ITE sebagai dasar hukumnya, sementara dalam penelitian ini penulis membahas terkait penerapan prinsip ektrateritorial terhadap pencurian data pribadi transnasional dengan menganalisis dengan payung hukum yang luas, baik dari hukum nasional, khususnya UU No. 27 Tahun 2022 tentang perlindungan data pribadi, konvensi-konvensi internasional, dan juga perjanjian bilateral.
2.	Qarib Triadi Kharisma, Implementasi Yurisdiksi Ekstrateritorial dalam Penanggulangan *Cybercrime* berdasarkan Hukum Internasional dan	Bagaimana penerapan prinsip ekstrateritorial menurut UU ITE Pasal 2 apabila ditinjau dari prinsip yurisdiksi negara.	Meskipun terdapat persamaan pada penelitian ini, yakni membahas terkait penerapan prinsip yurisdiksi ektrateritorialitas apabila di sandingkan dengan kedaulatan negara, namun

	Pengaturannya di Indonesia, Skripsi, 2015.		fokus dalam skripsi tersebut merupakan penerapan dari Pasal 2 UU ITE sebagai dasar hukum, sementara yang akan dibahas didalam skripsi ini akan lebih luas dengan menggunakan payung hukum utama perlindungan data pribadi Indonesia yakni UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta membahas pengaturan dalam hal terkait dalam perspektif internasional, yang akhirnya akan dikorelasikan.
3.	Okti Putri Andini, Tinjauan Yuridis Tindak Pidana Cyber Terrorism Dalam Perspektif Kejahatan Transnasional	1. Bagaimana pengaturan tindak pidana *cyber terrorism* ditinjau dari perspektif kejahatan transnasional terorganisir?	Dalam penelitian tersebut, terdapat kesamaan dalam pengkajian pengaturan mengenai sebuah tindak pidana transnasional, namun

	Terorganisir, Skripsi, 2020.	2. Bagaimanakah modus operandi tindak pidana *cyber terrorism*?	memang fokus pembahasan dalam skripsi tersebut ialah *cyber terrorism*, sementara penulis dalam skripsi ini membahas tentang *cybercrime* dalam bentuk pencurian data pribadi dan penanggulangannya.
4.	Mirsa Astuti, *Yurisdiksi Ekstrateritorial Sebagai Alat untuk Memerangi Parawisata Seks Anak,* Jurnal, 2018.	1. Bagaimana memberikan perlindungan bagi anak dari parawisata seks anak? 2. Bagaimana Yurisdiksi Ekstrateritorial dalam memerangi seks anak?	Kedua tulisan ini memiliki familiaritas dalam membahas penerapan dari prinsip yurisdiksi ekstrateritorial dalam suatu kasus transnasional, namun perbedaan dalam penelitian ini adalah objek pembahasan yakni ranah tindak pidana siber, sehingga memiliki irisan hukum siber dan membandingkan penerapannya dengan prinsip tersebut.

5.	Evi Retno Wulan, *Urgensi Asas Subyek Teritorial Pada Pemberantasan Kejahatan Siber*, Jurnal, 2019.	1. Apakah perlu asas subyek territorial diatur dan ditambahkan secara tegas dalam Pasal 2 UU No. 11 Tahun 2008?	Penerapan terhadap asas subyek territorial yang dijelaskan pada jurnal tersebut memiliki similaritas dengan asas yurisdiksi ekstrateritorial, dimana pemberlakuan hukum Indonesia untuk aktivitas apapun yang menimbulkan akibat hukum kepada subjek hukum Indonesia. Namun, yang menjadi pembeda adalah pembahasan dalam jurnal tersebut merupakan urgensi ditambahkannya penegasan prinsip asas territorial subyektif dalam UU ITE, sedangan skripsi ini membahas terkait penerapan dari prinsip yurisdiksi ekstrateritorial dalam sebuah tindak pidana

			siber pencurian data pribadi yang juga berdasarkan analisis perundang-undangan yang lebih relevan, yakni UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.
6.	A. Cery Kurnia, *Penerapan Prinsip Yurisdiksi Universal terhadap Penegakan Hukum dalam Tindak Pidana Siber (Cybercrime) di Indonesia,* Tesis.	1. Bagaimana penerapan prinsip yurisdiksi universal dalam penegakan hukum tentang tindak pidana siber di Indonesia? 2. Bagaimana bentuk Kerjasama internasional terkait dalam penegakan hukum tentang tindak pidana siber yang didasari prinsip yurisdiksi universal	Tesis tersebut meneliti terkait dengan implementasi dari prinsip yurisdiksi universal, dan penerapannya ditinjau dari hukum positif yang menerapkan Kerjasama internasional dalam penindakan terhadap pelaku tindak pidana siber, yang menjadi sumber perbedaan adalah prinsip yang dikaji merupakan prinsip yurisdiksi universal, sedangkan penelitian ini menelaah penggunaan yurisdiksi

			ekstrateritorial. Patut disebutkan bahwa dalam kesimpulan tesis tersebut penulis menyebutkan bahwa prinsip yang lebih patut untuk digunakan adalah yurisdiksi ekstrateritorial, karena prinsip yurisdiksi universal digunakan untuk kejahatan internasional yang termaktub dalam Statuta Roma 1998.

Dari analisis yang sudah digambarkan dalam tinjauan orisinalitas diatas dapat dilihat perbedaan antara penelitian-penelitian terdahulu dengan pembahasan yang serupa yakni terkait dengan penindakan terhadap *cybercrime* dan pengkajian prinsip yurisdiksi yang digunakan terhadap penindakan *cybercrime*, terdapat berbagai faktor pembeda yang bisa menjamin orisinalitas dari penelitian ini. Faktor pembeda tersebut terdapat baik pada subjek dan objek penelitian, yakni implementasi sifat ekstrateritorialitas UU No. 27 Tahun 2022 sebagai subjek penelitian, metode perbandingan antara berbagai instrumen hukum yang mengatur pelindungan data pribadi di Indonesia serta dalam ranah internasional, yang disertai

analisis terhadap bentuk-bentuk kekurangan yang terkandung dalam UU No. 27 Tahun 2022.

E. Definisi Operasional

Dalam penulisan penelitian hukum ini terdapat beberapa istilah yang akan penulis sertakan dengan pengertian-pengertian yang bersumber dari beberapa referensi, termasuk pada peraturan perundang-undangan. Adapun pengertian dari istilah-istilah yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Data Pribadi

   Undang-Undang No. 27 Tahun 2022 tentang perlindungan data pribadi mendefinisikan data pribadi sebagai "data tentang orang perseorangan yang teridetifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

2. Yurisdiksi Ekstrateritorial

   Memiliki pengertian yakni kemampuan/kecakapan suatu negara untuk melakukan atau melaksanakan kedaulatannya/kewenangannya di luar wilayahnya. Yurisdiksi ini juga dapat diartikan sebagai kepanjangan secara semu (*quasi extension)* dari yurisdiksi sesuatu negara di wilayah yurisdiksi negara lain[13].

3. Tindak Pidana Siber/*Cybercrime*

[13] Sumaryo Suryokusumo, *Yurisdiksi Negara vs. Yurisdiksi Ekstrateritorial*, dalam jurnal Hukum Internasional Vol. 2 Nomor 4 Juli 2005.

Untuk mendefinisikan *cybercrime* atau tindak pidana siber dalam konteks yang relevan dalam penelitian ini, maka penulis membedakan antara *computer related crime* dan *cyber crime*. Secara luas, *cybercrime* diartikan sebagai "segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[14]". Namun, dalam konteks penelitian ini, lebih tepat untuk mendefinisikan *cybercrime* sebagaimana dikatakan oleh Nazura Abdul Manaf[15], dimana *computer crime* dapat dikatakan sebagai kejahatan yang menggunakan computer sebagai alat dan menggunakan kontak langsung dari pelaku kepada korban, contohnya adalah dalam sebuah jaringan *Local Area Network* (LAN), sementara *cybercrime* dilakukan secara virtual melalui internet secara online. Artinya kejahatan tersebut tidak terbatas pada sebuah jaringan dan dapat dilakukan dimana saja.

4. Pencurian Data

Pencurian data dapat didefinisikan sebagai "*the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information[16]".* Yakni sebuah aktifitas pencurian terhadap informasi yang tersimpan dalam computer dari korban yang tidak mengetahui dengan maksud untuk membuka

[14] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Jakarta: PT. Refika Aditama, 2005. Hal. 40.
[15] Agus Raharjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya, 2002. Hal. 227.
[16] "Data Theft Definition", dalam portal *Cybercrime.org.za* diakses dari: https://cybercrime.org.za/data-theft/

informasi privat atau memperoleh informasi yang dirahasiakan. Dapat diartikan pula sebagai aktivitas memperoleh data pribadi secara melawan hukum. Data pribadi yang dimaksud disini adalah data pribadi sebagaimana dijelaskan menurut Pasal 2 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

5. Kejahatan Transnasional/Lintas Batas Negara

Kata transnasional dipadukan dari dua kata dasar yakni trans dan nasional. Trans dapat diartikan sebagai melintas, melalui, melintang, dan menembus, sementara nasional disini adalah batas wilayah kenegaraan. Dipadukan, kata kejahatan transnasional artinya adalah kejahatan yang bersifat melintasi batas-batas suatu negara, dengan kata lain suatu peristiwa yang dalam perencanaan, pelaksanaan, dan/atau dampaknya melintasi batas-batas wilayah yurisdiksi satu negara.[17]

F. Metode Penelitian

1. Jenis Penelitian

Penelitian yang dilakukan adalah penelitian normatif, dimana penulis mengkaji norma-norma, asas-asas, dan juga aturan-aturan hukum yang berlaku/positif.

2. Pendekatan Penelitian

[17] Baca lebih lanjut dalam: David O. Friedrichs. *Transnational Crime and Global Criminology: Definitional, Typological, and Contextual Conundrums.* Social Justice, Vol. 34. No. 2 (108), Beyond Transnational Crime, 2007. Hal 4-18.

Dalam penelitian ini, peneliti menggunakan tiga (tiga) macam metode pendekatan yaitu pendekatan perundang-undangan (*statute approach)*, pendekatan konseptual (*conceptual approach*) dan pendekatan perbandingan (*comparative approach)*. Secara spesifik dalam menjawab rumusan masalah pertama didalam skripsi ini yakni menganalisa pengaturan terkait tindak pidana siber pencurian data pribadi yang dilakukan secara lintas batas negara akan digunakan pendekatan perundang-undangan dan perbandingan yakni peraturan terkait tindak pidana siber dalam ranah domestic dan internasional. Sementara dalam menjawab rumusan masalah kedua akan difokuskan dengan pendekatan konseptual dan komparasi terhadap pengaturan domestic yang telah dianalisa pada rumusan masalah pertama.

3. Bahan Hukum Penelitian

Bahan hukum penelitian ini diambil dari bahan hukum primer, sekunder dan tersier:

a. Bahan Hukum Primer, merupakan sumber hukum yang mengikat yang terdiri dari hierarki peraturan perundang-undangan beserta peraturan teknis lainnya.
b. Bahan Hukum Sekunder, yaitu sumber hukum yang tidak mengikat tetapi menjelaskan bahan hukum primer yang merupakan hasil pikiran para pakar atau ahli yang mempelajari bidang tertentu. Bahan hukum ini didapatkan dalam berbagai jurnal hukum, artikel, dan juga pendapat-pendapat pakar mengenai masalah yang terkait.

c. Bahan Hukum Tersier, yaitu bahan penunjang hukum yang memberikan bimbingan dan pemahaman terhadap bahan hukum primer dan sekunder, seperti: Kamus hukum, kamus Bahasa Indonesia dan kamus Bahasa Inggris.

4. Teknik Pengumpulan Bahan Hukum

Penelitian ini mengumpulkan data menggunakan teknik metode penelitian studi kepustakaan (*library research*) yang terdiri dari perundang-undangan buku-buku, jurnal ilmiah, hasil wawancara/pernyataan resmi otoritas atau pakar terkait, media massa dan sumber internet serta referensi lain yang relevan dengan pembahasan.

5. Teknik Analisis Bahan Hukum

Karya tulis ilmiah ini menggunakan teknik analisis data berupa analisis isi (*content analisis*). Analisis ini dilakukan dengan mengolah bahan-bahan hukum yang telah dikumpulkan secara sistematis untuk menghasilkan kesimpulan yang dapat menjawab rumusan masalah. Sedangkan penyajian pembahasan menggunakan teknik deskriptif analitis untuk menjabarkan masalah dan solusi atas masalah tersebut.

G. Kerangka Skripsi

Untuk mempermudah dalam pendeskripsian analisis dalam penelitian ini, maka sistematika yang akan digunakan sebagai berikut:

1. Bab I: Bab ini merupakan pendahuluan sebagai pengantar sebelum memasuki pembahasan yang terdiri dari Latar Belakang, Rumusan

Masalah, Tujuan Penelitian, Orisinalitas Penelitian, Tinjauan Pustaka, Definisi Operasional, Metode Penelitian dan Sistematika Penulisan;

2. Bab II: Bab ini membahas terkait tinjauan umum mengenai hal yang akan menjadi pokok pembahasan dalam penelitian ini yaitu tentang prinsip yurisdiksi dan yurisdiksi ektrateritorialitas, tinjauan terhadap data pribadi, serta tinjauan umum terhadap *cybercrime* sebagai kejahatan transnasional dimana didalamnya terdapat penjabaran pencurian data pribadi sebagai bentuk *cybercrime,* serta tinjauan umum mengenai kejahatan transnasional dan tindak pidana siber sebagai kejahatan transnasional.
3. Bab III: Bab ini merupakan pembahasan dari hasil penelitian yang akan diuraikan secara sistematis dan objektif. Hasil pembahasan yang akan diuraikan adalah mengenai pengaturan yang ada dalam kancah internasional terhadap kejahatan transnasional *cybercrime* dalam tipologi pencurian data pribadi, dan juga analisis mengenai penerapan prinsip yurisdiksi ekstrateritorial terhadap kasus kejahatan tersebut.
4. Bab IV: Bab ini merupakan Penutup yang akan berisikan kesimpulan dan saran dari peneliti mengenai seluruh rangkaian yang ada dalam penelitian ini.

BAB II

TINJAUAN UMUM TENTANG PRINSIP YURISDIKSI, DATA PRIBADI, *CYBERCRIME* DAN KEJAHATAN TRANSNASIONAL

A. Prinsip Yurisdiksi

1. Istilah dan Pengertian Yurisdiksi

Yurisdiksi diambil dari Bahasa inggris yakni *Jurisdiction.* Kata tersebut sendiri berasal dari Bahasa Latin "*Jurisdictio"* yang merupakan gabungan dari dua suku kata. *Juris,* dimaknai sebagai kepunyaan/hak menurut hukum, dan *dictio,* yang berarti tulisan, ucapan, firman, sabda. Sebagaimana dijelaskan secara sekilas pada bab I, yurisdiksi merupakan sebuah konsekuensi yang timbul dari pengakuan terhadap kedaulatan suatu entitas negara, dimana suatu entitas politik selayaknya sebuah negara harus memiliki kedaulatan baik internal maupun eksternal. Kedaulatan secara eksternal dapat dipahami sebagai memiliki kedudukan yang sama (*equal stance)* dengan negara lain sesuai dengan prinsip persamaan kedaulatan yang kita kenal sekarang[18]. Konsekuensi dari persamaan kedudukan tersebut adalah negara memiliki beberapa status seperti:

a. Sebuah yurisdiksi atas wilayahnya dan warganya yang mendiaminya;

[18] Jawahir Thontowi, Pranoto Iskandar, *Hukum Internasional Kontemporer,* PT. Refika Aditama, Bandung 2016, Hal. 152.

b. Kewajiban bagi negara-negara lain untuk tidak mencampuri urusan atau persoalan yang terjadi di wilayah negara lain;

c. Timbulnya kewajiban-kewajiban yang dihasilkan dari kebiasaan-kebiasaan internasional dan perjanjian internasional yang didasari oleh kehendak dari negara itu sendiri[19].

Yurisdiksi dalam definisi sebagai sebuah terma dapat diartikan sebagai "*Authority of the state to affect legal interest. International law defines the jurisdiction of a state may exercise over persons or property with connections that a beyond that state's own territory"*. Yurisdiksi merupakan kompetensi bagi sebuah negara untuk memiliki kekuatan memberlakukan hukumnya kepada warga atau properti yang terdapat dalam wilayah teritori negara tersebut. Konsep yurisdiksi berkaitan erat dengan konsep kedaulatan suatu negara, dimana yurisdiksi merupakan sebuah refleksi dari kedaulatan suatu negara. Negara yang tidak memiliki yurisdiksi atas wilayahnya sendiri tidak memiliki hak untuk disebut sebagai negara yang berdaulat.

Apabila kita melihat dari sejarah terhadap awal mulanya konsep yurisdiksi modern, kedaulatan bagi negara yang kita kenal sekarang berawal dari sebuah kondisi kaos yang berlangsung secara terus menerus *(a constant state of chaos)*, dimana kerajaan-kerajaan dengan pengaruh gereja yang kuat pada masa pra-westphalia mengalami suatu kondisi yang disebut

[19] Ian Brownlie, *Principles of Public International Law*, Oxford: Clarendon Press, 1990, Hal. 227.

keseimbangan kekuasaan/*balance of power*, yakni kompetisi antar negara untuk mencapai supremasi kekuasaan secara internasional dan juga untuk mencegah bertambahnya kekuasaan dari negara lain. Panggung pertarungan kekuasaan ini sering dianalisa pada sejarah di benua Eropa sebagai aktor utama dalam aktivitas subjek internasional di masa pra-westphalia. Dominasi ini dilakukan dengan praktik kolonialisme dan imperialisme, serta usaha monopoli perdagangan. Sekumpulan entitas kenegaraan dengan kekuatan yang dominan ini tidak memiliki pemenang utama sebagai pemegang kekuasaan di Eropa, dikarenakan kekuatan yang relatif sama.

Puncak dari situasi *balance of power* ini ditandai dengan perang 30 tahun yang terjadi pada abad ke 15, yang mana perang tersebut sebenarnya merupakan kelanjutan dari perang-perang sebelumnya yang sudah berlangsung selama dua abad kebelakang, dengan bermotifkan perang suci (*holy war)* dan juga ekspansi territorial masing-masing aktor, menghasilkan situasi imbang (*stalemate*) diantara para kerajaan dan negara ini yang sudah menghabiskan sumber daya negaranya dalam perang tersebut[20]. Alhasil, para kerajaan ini menghentikan perang dan membuat sebuah kesepakatan damai yang dikenal dengan perjanjian Westphalia, yang dinamakan berdasarkan tempat diadakannya perjanjian tersebut yakni wilayah Westphalia, sebuah wilayah di Jerman pada tahun 1648.[21]

[20] Ahmad Abdi Amsir, *Perjanjian Westphalia dan Momentum Pendirian Negara Modern,* dalam Jurnal Sulesana Vol. 15 No. 1 (2021)

[21] *Ibid.*

Hasil dari perjanjian tersebut memberikan dampak yang substansial bagi kelanjutan corak politik internasional. Perjanjian tersebut memberikan pengakuan kedaulatan bagi wilayah dari pangeran-pangeran kerajaan dengan teritori yang ditentukan. Mereka memiliki kebebasan/kedaulatan mutlak atas wilayah teritorinya itu yang kita kenal sebagai yurisdiksi. Sistem internasional yang diterapkan pasca perjanjian Westphalia adalah sistem anarki, dimana tidak adanya suatu kekuasaan yang mengatur negara, sebagai konsep persamaan kedaulatan *(equal sovereignty)*. Richard Falk menyatakan dalam esai yang dia buat pada tahun 1969 berjudul "*The Interplay of Westphalia and Charter Conceptions of the International Legal Order"* tentang dampak perjanjian Westphalia yang dia sebut sebagai konsepsi Westphalia tentang sebuah sistem internasional yang didasari oleh kedaulatan, teritorialitas, dan non-intervensi, yang pada akhirnya terwujudkan dalam UN *Charter* dan menjadi sebuah sistem internasional kontemporer.[22]

2. Prinsip-Prinsip Yurisdiksi

Sebagaimana dijelaskan bahwa yurisdiksi merupakan refleksi dari kedaulatan negara, John O'Brien menjelaskan beberapa lingkup dari yurisdiksi dalam jenisnya yakni:[23]

[22] Sebastian Schmidt, *To Order the Minds of Scholars: The Discourse of the Peace of Westphalia in International Relations Literature,* International Studies Quarterly Vol. 55 No. 3 (September 2011) Hal. 601-623

[23] Sefriani, *Hukum Internasional: Suatu Pengantar*, Edisi ke-2, Cet. 6. Jakarta: Rajawali Press, 2016. Hal. 221. Lihat lebih lanjut dalam buku John O'Brien, *International Law,* Cavendish Publishing Limited, Great Britain, 200. Hal. 227.

a. *Legislative/Prescriptive Jurisdiction*

Yurisdiksi legislatif merujuk kepada kewenangan yang dimiliki sebuah negara untuk membuat hukum yang mengikat kepada para subjek dari negara tersebut;

b. *Executive/Enforcement Jurisdiction*

Yurisdiksi eksekutif merujuk kepada kewenangan yang dimiliki sebuah negara untuk melakukan tindakan yang memaksakan ketetuan hukum nasionalnya;

c. *Judicial Jurisdiction*

Yurisdiksi yudisial merujuk kepada kekuasaan dari pengadilan negara untuk mengadili dan memberikan putusan hukum.

Ketiga lingkup dari yurisdiksi ini memiliki pengaruh yang erat kaitannya dengan kewenangan sebuah negara terhadap orang, harta benda, perbuatan, dan peristiwa hukum. Terdapat beberapa perbedaan diantara para pakar terhadap pelaksanaan dari definisi ketiga lingkup yurisdiksi tersebut, sebagai contoh adalah pendapat Akehurst yang menekankan perbedaan antara lingkup yurisdiksi eksekutif dan yudisial. Menurutnya, *enforcement jurisdiction* adalah kekuatan untuk melakukan intervensi secara fisik/langsung yang dilakukan oleh kekuatan eksekutif, dalam hal ini pemerintah, sementara yurisdiksi judicial atau *judicial enforcement* adalah kewenangan dari pengadilan untuk memutus suatu peristiwa hukum.

Berbeda dengan Akehurst, Martin Dixon dan Tien Saefullah menggabungkan keduanya dalam klasifikasi *enforcement jurisdiction* dan

lebih menekankan perbedaan atau penggunaan dari lingkup *jurisdiction to prescribe* dan *jurisdiction to enforce.*[24] Sama halnya seperti pendapat beberapa pakar yang menyatakan bahwa *jurisdiction to prescribe* adalah kewenangan tidak terbatas suatu negara untuk meregulasi aktivitas, dan tindakan-tindakan yang dapat mengatur orang dan situasi, dimana kewenangan ini tidak terbatas pada lokasi orang itu berada, sementara *jurisdiction to enforce* adalah kemampuan negara untuk memberlakukan hukum-hukumnya, melalui kekuatan eksekutif dan yudisial.[25]

Dapat disimpulkan bahwa meskipun secara teori negara memiliki kekuasaan untuk membuat suatu hukum yang tidak terlimitasi oleh batasan-batasan teritorial, kemampuan untuk memberlakukan hukum tersebut terbatas hanya di wilayah teritorialnya saja[26], meskipun dalam beberapa kondisi dan situasi negara dapat memperpanjang yurisdiksinya dalam teritori negara lain. Pada tahun 1998, DJ Harris mengklasifikasikan prinsip-prinsip yurisdiksi yang digunakan secara umum oleh dunia internasional, yakni:[27]

a. Prinsip Teritorial, adalah sebuah prinsip yang menyatakan bahwa yurisdiksi ditentukan dari tempat terjadinya sebuah pelanggaran atau tindakan. Prinsip ini adalah prinsip yang paling sering digunakan mengingat kemudahan penentuan dari yurisdiksinya

[24] *Ibid.*

[25] Rothwell, Donald R., Stuart Kaye, Afshin Akhtarkhavari, dan Ruth Davis. *International Law: Cases and Materials with Australian Perspectives*. Cambridge: Cambridge University Press, 2010. Hal. 294

[26] Sefriani, *Op Cit*, Hal. 223.

[27] DJ Harris, *Cases and Materials on International Law,* Edisi ke-5, London: Sweet & Maxwell, 1998. Hal. 264-265.

dan tidak melanggar status kedaulatan dari negara-negara yang menyebabkan popularitas dari prinsip ini.[28] Yurisdiksi territorial dapat diklasifikasikan lebih lanjut menjadi dua tipe yakni territorial subjektif dan objektif. Prinsip teritorial subjektif merupakan sebuah prinsip yang menyatakan bahwa negara memiliki yurisdiksi terhadap seseorang yang menimbulkan kejahatan yang dimulai dari wilayahnya, tetapi diakhiri atau menimbulkan kerugian di negara lain. Sementara prinsip territorial objektif menyatakan bahwa negara memiliki yurisdiksi terhadap seseorang yang melakukan kejahatan yang menimbulkan kerugian di wilayahnya meskipun perbuatan tersebut dimulai dari negara lain.[29] Implementasi dari prinsip yurisdiksi territorial terhadap ruang dan tindak pidana siber merupakan dilemma yang masih dihadapi oleh masyarakat internasional hingga saat ini. Selain dari keengganan politik dalam menyerahkan yurisdiksinya kepada negara lain terhadap suatu peristiwa yang terjadi di dalam wilayah teritorinya, juga permasalahan kapabilitas dari suatu negara dalam menangani kasus tindak pidana siber yang melibatkan negara tersebut. Yurisdiksi territorial, sebagai basis yurisdiksi yang paling sedikit menimbulkan permasalahan, tidak diterima sebagai solusi yang

[28] Sefriani, *Op Cit.* Hal. 225.
[29] Sefriani, *Op Cit.* Hal. 227

memadai bagi penyelesaian isu kontemporer dimana salah satunya merupakan tindak pidana siber.[30]

b. Prinsip Nasionalitas, adalah sebuah prinsip yang menyatakan yurisdiksi ditentukan dari kewarganegaraan seseorang yang terlibat dalam suatu kejahatan. Prinsip Nasionalitas dapat diklasifikasikan menjadi nasionalitas aktif dan pasif, dimana nasionalitas aktif menetapkan yurisdiksi terhadap nasionalitas seseorang terlepas dari lokasi dia berada, dan nasionalitas pasif memberikan yurisdiksi kepada negara terhadap warga negaranya yang menjadi korban kejahatan yang dilakukan oleh orang asing di luar negeri;[31]

c. Prinsip Proteksi/Perlindungan, adalah sebuah prinsip yang menyatakan yurisdiksi ditentukan berdasarkan kepentingan nasional yang dirugikan oleh pelanggaran atau tindakan yang terjadi, menurut Kenneth S. Gallant, prinsip protektif memberikan kemampuan kepada negara untuk menindak warga negara asing yang bertindak diluar batas teritorinya terhadap kejahatan tertentu, pada umumnya kejahatan-kejahatan yang dapat ditindak berdasarkan prinsip ini adalah spionase, ancaman

[30] Dan E. Stigell, *International Law and The Limitations on The Exercise of Extraterritorial Jurisdiction in U.S Domestic Law.* 35 Hasting International and Comparative Law Review No. 323, 2012. Hal. 332.

[31] *Ibid.* Hal. 227-228.

terhadap pertahanan dan keamanan negara, atau ancaman terhadap keuangan negara, seperti pemalsuan uang;[32]

d. Prinsip Universal, dimana yurisdiksi ditentukan berdasarkan kriteria yang diklasifikasikan sebagai ancaman bagi umat manusia. *Institut de Droit International* mengeluarkan resolusi pada tahun 2005 tentang yurisdiksi universal yang menyatakan, "*Universal jurisdiction in criminal matters, as an additional ground of jurisdiction, means the competence of a state to prosecute alleged offenders and to punish them if convicted, irrespective of the place of commission of the crime and regardless of any link of active or passive nationality, or other grounds of justification recognized by international law"*.[33]

Dapat dimaknai bahwa prinsip yurisdiksi universal memberikan kompetensi bagi negara untuk mengambil tindakan dalam bentuk penegakan terhadap suatu kasus kriminal, untuk mengadili dan menghukum pelaku apabila terbukti bersalah, terlepas dari tempat kejadian dilakukan dan dari hubungan baik akitf ataupun pasif dari nasionalitas, atau dari justifikasi lain yang diakui oleh hukum internasional;

---

[32] Kenneth S. Gallant, *International Criminal Jurisdiction: Whose Law Must We Obey?* New York: Oxford University Press, 2022.

[33] Institut de Droit International, *Resolution on Universal criminal jurisdiction with regard to the crime of genocide, crime against humanity and war crimes.* Krakow Session, 2005. Didalam resolusi tersebut dijelaskan pula kejahatan yang menimbulkan yurisdiksi universal. Diakses dari: https://www.idi-iil.org/app/uploads/2017/06/2005_kra_03_en.pdf

3. Prinsip Yurisdiksi Ekstrateritorial

Dalam perkembangannya, prinsip yurisdiksi beradaptasi untuk memudahkan negara-negara dalam menanggapi permasalahan yang terjadi dalam dunia global. Contohnya saja adalah *transnational organized crime* atau kejahatan antar negara yang terorganisir dimana secara jelas sifat dari prinsip-prinsip yurisdiksi dapat menghambat penegakan dari kejahatan tersebut. Sebagaimana yang Mann katakan, permasalahan dari kehidupan modern menimbulkan keengganan untuk melokasisasi sebuah fakta, kejadian atau peristiwa yang menyebabkan penyelesaian yang didasar fokus berdasar kepada koneksi territorial tidak akan menghasilkan sebuah penyelesaian yang mencukupi kebutuhan dari negara.[34] Alhasil, konsep yurisdiksi ekstrateritorial menjadi metode penyelesaian terhadap masalah tersebut. Kata ekstrateritorial sendiri dapat diartikan sebagai sesuatu yang berada diluar batas wilayah teritorinya.[35]Apabila didefinisikan sebagai sebuah terminologi maka definisi dari yurisdiksi ini adalah "*extraterritorial jurisdiction is the situation when a state extends its legal power beyond its territorial boundaries"* yakni sebuah situasi dimana sebuah negara melebarkan kekuatan yuridisnya diluar batas teritori dari negara itu sendiri.[36]

---

[34] Mann, *The Doctrine of Jurisdiction in International Law*. Recueil des Cours de l'Académie de Droit International (RCADI), Vol. 111 No.9, 1964. Hal. 36-37.

[35] Black's Law Dictionary 929, *Extraterritorial*. (Edisi ke-9 2009)

[36] National Action Plans on Business and Human Rights, sebuah artikel tentang *Extraterritorial Jurisdiction*. Diakses dari: https://globalnaps.org/issue/extraterritorial-jurisdiction/#:~:text=Extraterritorial%20jurisdiction%20is%20the%20situation,power%20beyond%20its%20territorial%20boundaries.

Pemberlakuan dari yurisdiksi ekstrateritorial sendiri banyak memiliki limitasi dalam penggunaannya, karena penggunaan dari prinsip ini menyalahi prinsip yurisdiksi tradisional khususnya yurisdiksi territorial, dikarenakan tidak adanya hubungan langsung atau *direct and immediate link* antara mulainya tindakan dan hasil akhir dari kejahatan tersebut.[37] Beberapa limitasi yang dibutuhkan sebagai penerapan dari yurisdiksi ekstrateritorial adalah prinsip *comity*/rasa hormat dan *rule of reasonableness*/kelayakan.[38] Serta adanya kondisi dual kriminalitas (*double criminality)* yakni sebuah kondisi dimana menurut hukum kejahatan tersebut dapat ditindak berdasarkan hukum normatif dari negara lain menjadi fondasi bagi negara untuk memberlakukan yurisdiksinya di luar batas wilayah teritorinya. Dalam penerapan yurisdiksi ekstrateritorial yang didasari dengan doktrin hukum dual kriminalitas tersebut, terdapat beberapa teori dasar yurisdiksi dengan korelasinya terhadap kondisi dual kriminalitas, yakni:

1. Prinsip personalitas aktif, menyatakan bahwa negara hanya memiliki yurisdiksi terhadap warga negaranya yang melakukan kejahatan diluar negaranya. Prinsip ini didasarkan pada dua rasionalisasi yaitu negara harus memiliki kewenangan untuk memonitori kelakuan dari warganya bahkan di luar negeri, dan negara juga harus menyadari atas keperluan

[37] Sefriani, *Op Cit.* Hal. 235
[38] Dan E. Stigell, *Op Cit.* Hal. 335.

solidaritas internasional untuk menindaklanjuti sebuah kejahatan pada negara tempat kejahatan tersebut dilakukan[39].

2. Prinsip personalitas pasif, dimana negara memiliki yurisdiksi terhadap warga negaranya atas sebuah kejahatan yang dilakukan di luar dari negara tersebut. Penerapan teori ini kurang disukai oleh masyarakat internasional dibandingkan teori personalitas aktif, dan penerapan dari prinsip ini marak dilakukan di negara-negara Eropa yang dalam penerapan yurisdiksi legislatifnya tidak mengedepankan kedaulatan negaranya sebagai fokus penegakan. Contoh dari negara-negara yang menerapkan prinsip ini adalah Prancis dan Belgia. Negara yang menerapkan prinsip ini awamnya menggunakan dual kriminalitas sebagai kondisi atas yurisdiksi personalitas pasif.[40]

3. Prinsip *Protection*/Perlindungan, dimana pemberlakuan dari prinsip ini tidak memerlukan adanya kondisi dual kriminalitas dikarenakan urgensi mendesak yang menimbulkan adanya digunakan prinsip ini. Urgensi tersebut adalah adanya kejahatan dari luar teritori sebuah negara yang menimbulkan gangguan/ancaman terhadap keamanan dan kepentingan dari negara tersebut. Namun ancaman dari luar tersebut pada prakteknya dapat diperluas lagi menjadi kepentingan ekonomi dari suatu negara, terlepas dari apakah tindakan tersebut merupakan sebuah delik pidana di negara *locus delicti*.[41]

---

[39] Christine van den Wyngaert, *Double Criminality as a Requirement to Jurisdiction. Nordisk Tidsskrift for Kriminalvidenskab*, Vol. *76* No. 5, 1989. Hal. 46.

[40] *Ibid.* Hal. 47

[41] *Ibid.*

4. Prinsip *Universality/*Universal, dimana dalam penerapan prinsip ini tidak jelas apakah harus terdapat kondisi dual kriminalitas sebagai limitasi penerapan yurisdiksinya. Dapat dikatakan bahwa karena menyangkut terkait dengan masalah yang dianggap universal dalam lokasinya, maka kondisi dual kriminalitas tidak dibutuhkan dalam yurisdiksi penegakannya.[42]Salah satu karakteristik penting dari hal apa yang menjadi yurisdiksi dari prinsip universal adalah tentang kejahatan yang disepakati oleh negara-negara sebagai *international crime*. [43]

5. Prinsip Representasi, yang disebut juga sebagai yurisdiksi turunan atau yurisdiksi cabang (*derived jurisdiction or subsidiary jurisdiction*) merupakan sebuah prinsip yang menyatakan bahwa yurisdiksi dalam hal ekstrateritorial terjadi ketika terdapat sebuah tindakan pidana di suatu negara yang dilakukan oleh seorang yang bukan warga negaranya, dimana terdapat permohonan ekstradisi atas warga negara tersebut yang ditolak oleh negara *locus delicti* terjadi. Sebagai contoh apabila A seorang warga negara B melakukan kejahatan di negara C, lalu setelah kejadian tersebut B meminta permohonan ekstradisi kepada negara C namun ditolak oleh negara C, maka negara C mendapatkan yurisdiksi atas A dari penolakan ekstradisi tersebut. Berdasarkan pada prinsip ini, negara C pada dasarnya menjadi representasi

[42] *Ibid. Hal. 48.*

[43] Tien Saefullah, *Hubungan antara Yurisdiksi Universal dengan Kewajiban Negara berdasarkan Prinsip Aut Dedere Aut Judicare Dalam Tindak Pidana Penerbangan dan Implementasinya di Indonesia.* Jurnal Hukum Internasional UNPAD. Vol. 1 No. 1 Tahun 2002, Hal. 44-45.

dari negara B dalam mengadili terhadap tindakan yang dilakukan oleh A.[44] Prinsip ini sering digunakan dalam negara anggota konvensi-konvensi uni eropa terkait dengan penegakan kejahatan transnasional sebagai kompensasi dari penolakan terhadap permohonan ekstradisi.[45]

B. Data Pribadi

1. Pengertian Data Pribadi

Berdasarkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat teridentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik, sementara Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat Data Pribadi. Pengertian menurut UU ini sangat identik dengan pengertian data pribadi berdasarkan peraturan Uni Eropa, yang berbunyi "*Personal data mean any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier…*[46]"

Indonesia memang mengambil *General Data Protection Regulation* Uni Eropa sebagai patokan bagi regulasi data pribadi, sebagaimana presentasi

[44] *Ibid.* Hal. *49-50.*

[45] Lihat: *Convention for the Suppression of Terrorism, European Convention on the Transfer of Criminal Proceedings, European Convention on the International Validity of Criminal Judgments.*

[46] *Article 4, Definitions – Regulation (EU) 2016/679 (General Data Protection Regulation)*

Prof. Edmon Makarim dalam Rapat Dengar Pendapat perancangan UU PDP. Maka dari itu bisa kita komparasikan jenis-jenis data pribadi yang dimiliki oleh *GDPR* terkandung dalam muatan UU Pelindungan Data Pribadi. Sebelum terciptanya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, ketiadaan pengaturan yang mengatur secara spesifik terkait dengan data pribadi dan pelindungan yang diberikan secara hukum kepada data pribadi menimbulkan permasalahan secara sosio-yuridis.

Pengaturan data pribadi diperlukan karena mengatur tentang prosedur dari pengumpulan, penggunaan, pengungkapan, pengiriman serta keamanan dari data pribadi dan penting dalam hubungan sosio-politik dimana adanya dua kepentingan yang secara vis-à-vis bertentangan, dimana dalam satu sisi masyarakat yang membutuhkan pelindungan terhadap privasi dari data pribadinya dan juga dalam sisi lainnya pemerintah dan pelaku usaha yang membutuhkan data dari masyarakat luas untuk diproses dan digunakan untuk keperluan yang wajar dan tidak melawan hukum.[47] Regulasi ini juga menjadi payung hukum utama dalam seluruh kumpulan peraturan mengenai data pribadi yang tersebar dalam berbagai regulasi, alhasil diprediksi dapat meningkatkan efektifitas dan ketertiban dalam masalah pelindungan terhadap data pribadi.

2. Hak Privasi terhadap Data Pribadi

[47] Erlina Maria, Mery Christin Putri, *Loc.cit.*

Dalam kehidupan dimana nilai-nilai dalam dimensi maya dan realita menjadi sebuah kesatuan, data pribadi menjadi salah satu komoditas yang menjanjikan banyak keuntungan dari kemudahan yang disediakan oleh proses penggunaannya. Namun dalam kemudahan yang disajikan terdapat ancaman yang tersirat, baik terhadap kebebasan individu dan juga kemungkinan manipulasi data serta penjualan informasi pribadi. Sejatinya, hak privasi terhadap data pribadi berawal dari hak untuk menghormati kehidupan pribadi atau disebut dengan *the right to private life*, yakni konsep yang mengatur interaksi kehidupan pribadi manusia dengan manusia lain sebagai mahkluk sosial. Dengan kata lain, pemilik dari hak perlindungan data pribadi adalah perseorangan atau individu.[48]

Berbagai percobaan untuk mendefinisikan privasi telah banyak dilakukan oleh pakar, dengan perspektif yang berbeda-beda dimana Westin dan Flaherty mengemukakan bahwa privasi adalah sebuah klaim, hak, dan otoritas bagi seseorang (individu) untuk menentukan informasi apa mengenai seseorang tersebut yang bisa dikomunikasikan kepada orang lain.[49] Privasi juga didefinisikan sebagai kontrol seorang individu atas:

a. Informasi tentang dirinya;

[48] *European Union Agency for Fundamental Rights and Council of Europe,* Supra No. 5. Hal. 37.

[49]Alan Westin, *Privacy and Freedom*. New York: Atheneum Press. 1967, dan David Flaherty, *Privacy in Colonial New England*. Charlottesville: University of Virginia Press. 1972. Dikutip dari Jurnal Ferdinand Schoeman, *Privacy: Philosophical Dimensions.* American Philosophical Quarterly Vol. 21, No. 3, 1984. Hal. 199.

b. Kedalaman pengetahuan (*intimacy)* tentang identitas personal atau;

c. Siapa yang memiliki akses langsung terhadap dirinya (control terhadap akses pengetahuan yang menyangkut dirinya).[50]

Dan terakhir, sebagian mendefinisikan privasi sebagai kondisi atau situasi dimana terdapat akses yang terbatas terhadap seorang individu[51], sebagaimana yang Ernest Van Den Haag konsepkan dalam tulisannya bahwa, "Privasi adalah akses ekslusif seseorang (atau sebuah badan hukum) ke ranah yang merupakan miliknya sendiri". Akses ekslusif ini memberikan hak untuk mengecualikan orang lain dari: menonton, memanfaatkan, menyerang (dalam konteks menganggu atau memasuki dengan cara yang memengaruhi) wilayah milik pribadinya.[52]

Sebagai hak dasar dari manusia, privasi mendasari nilai-nilai lain seperti kebebasan berpendapat dan kebebasan berserikat dan/berkumpul, kebebasan beragama, dan hak-hak sipil lainnya, menjadikan hak privasi sebagai hak fundamental dalam sebuah peradaban bercorak demokratis. Hal ini juga berdampak dalam perkembangan dari konsep pelindungan data pribadi, dimana terjadi pergeseran dari penggunaan hukum untuk melindungi hak-hak individu. Hukum yang awalnya hanya melindungi seseorang

[50]Charles Fred, *Privacy.* Yale Law Journal No. 77, 1968. Hal. 475-93. Dikutip dari Jurnal Ferdinand Schoeman, Ibid.

[51]David O'Brien, *Privacy, Law, and Public Policy.* New York: Praeger Special Studies. 1979 dan Ruth Gavison, *Privacy and the Limits of the Law.* Yale Law Journal No. 89. 1980. Hal. 421-71. Dikutip dari Jurnal Ferdinand Schoeman, *Ibid.*

[52]Daniel J. Solove, *Conceptualizing Privacy,* California Law Review, Vol. 90 No. 4, 1975. Hal. 295-314.

terhadap gangguan yang terjadi secara fisik (*vi et armis*) tidak lagi memadai kehidupan peradaban masyarakat semi-digital. Pengakuan atas hak spiritual manusia, perasaan dan kecerdasan individu yang merupakan perluasan dari hukum pada akhirnya juga memperluas pengakuan hukum terhadap kepemilikan individu terhadap benda yang tidak berwujud, seperti halnya 'data' akhirnya dikenal sebagai salah satu bentuk dari kepemilikan seseorang.[53]

Regulasi Pelindungan Data Pribadi Uni Eropa atau yang awamnya disebut dengan *GDPR* merupakan salah satu pengaturan yang diakui oleh masyarakat internasional sebagai draft peraturan pelindungan data pribadi yang paling komprehensif dan kompleks memiliki beberapa prinsip-prinsip dalam penggunaan terhadap data pribadi sebagai pengejawantahan dari bentuk penyeimbang antara sisi pelindungan dan juga penggunaan dari data pribadi. Prinsip-prinsip tersebut antara lain:[54]

a. *Lawfulness, fairness and transparency,* Pemrosesan data pribadi harus dilakukan secara hukum, adil dan transparan terhadap pemilik dari data pribadi tersebut;
b. *Purpose limitation,* dimana data pribadi dikumpulkan untuk sebuah alasan yang spesifik, eksplisit dan dapat dibenarkan secara

[53] Samuel D. Warren dan Louis Brandeis, The Rights to Privacy. Harvard Law Review Vol. IV No. 5. 15 Desember 1890. Hal. 193-220.

[54] Bab II Pasal 5 Ayat 1 Huruf (a) sampai (f) Regulation (EU) 2016/679 of the European Parliament on the Protection of Natural Persons with Regard to The Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation)

hukum serta tidak diproses dengan cara-cara yang melawan hukum.

c. *Data Minimisation*, dimana data pribadi dipergunakan sesuai dengan ukuran yang wajar dan terbatas sebagaimana terkait dengan alasan data tersebut diproses.

d. *Accuracy*, data pribadi harus akurat atau sesuai dengan kenyataan, dan dalam hal-hal yang diperlukan selalu diperbarui, dan prosesor data pribadi harus mengambil langkah-langkah untuk mencegah kekeliruan dalam data pribadi tersebut, termasuk penghapusan terhadap data pribadi yang harus dilakukan tanpa jarak (*without delay).*

e. *Storage Limitation*, data pribadi hanya disimpan dalam jangka waktu sesuai dengan kebutuhan/alasan data pribadi tersebut digunakan, dan tidak melebihi jangka waktu tersebut untuk menjamin kebebasan dan hak dari pemilik data pribadi.

f. *Integrity and Confidentiality*, data pribadi diproses dengan cara-cara yang dapat menjaga keamanan dan keutuhan dari data pribadi tersebut, serta mendapatkan perlindungan terhadap penggunaan yang illegal atau melawan hukum dari data pribadi tersebut, perlindungan dari kehilangan yang disebabkan oleh kelalaian, kerusakan, menggunakan langkah-langkah yang memadai serta prosedur yang terstruktur dan sistematis.

C. *Cybercrime*/Tindak Pidana Siber

1. Pengertian *Cybercrime*

Dalam mengartikan *cybercrime,* terdapat perbedaan dalam memilih antara penggunaan terminologi *cybercrime* sebagai kejahatan computer, kejahatan terkait computer (*computer related crime)*, dan kejahatan dengan komputer (*crime by computer*). Yang diperlukan dalam menganalisa kejahatan *cybercrime* adalah penggunan teknologi dalam pelaksanaan kejahatan tersebut. Terma *cybercrime* sendiri diakui dan digunakan oleh UN, serta dalam konvensi Eropa tentang *cybercrime*. Didalam beragam terma terkait dengan tindak pidana siber, terdapat sebuah kesepakatan umum tentang makna dari penyebutan dari kejahatan siber, yakni kejahatan tersebut tergantung secara siber (*cyber-dependent)*, dan dapat dilakukan karena siber (*cyber-enabled)*.

Kejahatan yang tergantung secara siber adalah kejahatan-kejahatan yang hanya bisa dilakukan menggunakan computer, jaringan computer, atau teknologi informasi (*information communication technology/*ICT*)*. Umumnya, tipe ini digunakan dalam kejahatan-kejahatan dimana teknologi adalah alat utama dalam kejahatan, dimana tanpa adanya peralatan siber kejahatan ini tidak bisa terjadi. Contohnya kejahatan peretasan, *malware* dan DoS/serangan *Denial of Service*. Sementara kejahatan yang dapat dimungkinkan karena siber adalah pada umumnya berasal dari kejahatan-kejahatan tradisional yang aktifitas dari kejahatan tersebut ditingkatkan jangkauan atau skalanya dengan bantuan komputer, jaringan komputer, atau

teknologi informasi lainnya[55]. Kategori ketiga yakni kejahatan yang didukung oleh komputer, adalah kejahatan-kejahatan dimana computer digunakan sebagai alat yang secara tidak langsung berkaitan dengan kejahatan tersebut namun dapat membuahkan bukti dari kejahatan tersebut. Contohnya alamat yang ditemukan didalam komputer pribadi seorang tersangka pembunuhan.[56]

Apabila ditelusuri secara definisi terminologi, istilah *cybercrime* merujuk kepada sebuah kejahatan yang terjadi dalam ranah *cyberspace*. Terma *cyberspace* atau ruang siber ini dirujuk dalam sebuah novel fantasi yang ditulis oleh William Gibson yang berjudul *Neuromancer* pada tahun 1984,[57] yang menggambarkan sebuah halusinasi bersama yang dialami setiap harinya oleh milyaran dari operator resmi seperti sebuah film matrix dimana terdapat sebuah realita kenyataan fana yang tidak bisa dibedakan dengan realita kehidupan sebenarnya. Sebuah ruang siber ini diisi dengan populasi yang awamyna disebut dengan masyarakat maya atau *cyber community*, dengan aktivitasnya yang bersifat *virtual*/*intangible* (tidak kasat mata). [58] Sebuah kejahatan yang terjadi dalam realita inilah yang disebut sebagai kejahatan siber atau *cybercrime*.

Dalam hukum internasional, regulasi yang dijadikan sebagai sumber hukum internasional terhadap *cybercrime* hanya bisa ditemukan dalam *the*

[55] Jonathan Clough, *Principles of Cybercrime.* Cambridge University Press, 2015. Hal. 11.
[56] *Ibid.*
[57] Joanna Buick dan Zoran Jevtic, *Mengenal Cyberspace for Beginners.* Penerjemah Zulfahmi Andri. Bandung: Penerbit Mizan, 1997. Halaman 4-9.
[58] Burhan Bungin, *Pornomedia: Konstruksi Sosial Telematika dan Perayaan Seks di Media Massa*. Jakarta: Prenada Media, 2003. Hal. 34.

Council of Europe Convention on Cybercrime.[59] Konvensi ini, meskipun sebuah inisiasi yang tercipta secara regional, memang ditujukan untuk digunakan secara global oleh masyarakat internasional.[60] Salah satu preseden yang diterapkan oleh konvensi ini adalah mengenai contoh atau *role model* regulasi mengatur tindakan yang berkaitan dengan pidana siber. Salah satu dampak dari konvensi ini adalah berkembangnya regulasi terkait pidana siber atau elemen terkait secara global, dimana Indonesia merupakan satu contoh dengan diundangkannya UU Informasi dan Transaksi Elektronik yang menjadi pembuka pengaturan terkait masalah tindakan dalam ranah elektronik pada tahun 2008 silam.[61]

2. Unsur-Unsur *Cybercrime*

Menurut *routine activity theory* yang dikembangkan oleh L. Cohen dan M. Felson,[62] tiga unsur yang mengakibatkan dalam terjadinya suatu tindak kejahatan yang terencana adalah adanya pelaku yang termotivasi untuk melakukan kejahatan, adanya target yang sesuai, dan ketiadaan pengawasan (*supply of motivated offenders, the availability of suitable opportunities, and absence of capable guardians)*. Teori klasik terkait kriminologi ini dapat dikembangkan dalam evolusi dari tindak pidana dalam hal ini tindak pidana

[59] Widodo, *Memerangi Cybercrime: Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi.* CV. Aswaja Pressindo: Sleman, Yogyakarta, 2013. Hal. 5

[60] Council of Europe, *Project on Cybercrime: Final Report*, dalam laporan bernomor ECD/567(2009)1, Council of Europe, 15 Juli 2009. Hal. 5. Diakses melalui: https://rm.coe.int/16802fa0b7

[61] *Ibid.* Hal. 3.

[62] L. Cohen dan M. Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach*, dalam Jurnal American Sociology Review No. 44, 1979. Hal. 588-589.

siber yang terjadi bukan secara fisik. Namun, dalam pengembangannya, perlu kita telaah beberapa perbedaan mendasar dalam *cybercrime* dan tindak pidana klasik yang menjadi tantangan dalam pencegahan dan penegakan terhadap *cybercrime.* Perbedaan ini dapat kita urai menjadi beberapa unsur yakni:

a. Skala

Faktor skala menjadi salah satu pemeran vital dalam perbedaan *cybercrime* dengan kejahatan pada umumnya. Dengan estimasi angka sebanyak 4.9 milliar orang mengakses internet setiap harinya, menjadikan angka tersebut juga sebagai pelaku ataupun korban potensial (*potential offenders and victims)*[63]. Hal ini juga berlaku sebagai *force multiplier* atau tenaga penguat bagi skala dari tindak pidana, memungkinkan terjadinya suatu tindak pidana dalam sebuah skala yang tidak mungkin dilakukan dalam kondisi luar jaringan[64]. Perkembangan dari kejahatan siber yang bersifat tanpa batas/*borderless* dan kompleks juga dipengaruhi faktor globalisasi yang menempatkan teknologi informatika sebagai modal utama dalam pencapaian target/tujuan. Alhasil, kompleksitas pencapaian ekonomi secara *vis a vis* mempengaruhi juga kompleksitas kejahatan yang berbasis teknologi global.[65]

---

[63] International Telecommunications Union, *Measuring digital development: ICT facts and figures 2021,* dalam publikasi serikat telekomunikasi internasional, 2021. Diakses dari: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

[64] Jonathan Clough, Op Cit, Hal. 6

[65] Al. Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika,* Yogyakarta: Penerbit Atma Jaya, Cet. Ke-5, 2014. Hal. 23.

b. Aksesibilitas

Kemudahan dalam akses menjadikan teknologi menjadi salah satu prospek dan tantangan utama dalam pencegahan dan penegakan dari *cybercrime*. Kebanyakan dari tindak *cybercrime* hanya membutuhkan 3 alat sebagai modal, perangkat keras (*hardware)*, perangkat lunak (*software)*, dan akses internet.[66]Terlebih lagi dalam perihal kejahatan dalam dunia maya, keahlian menjadi modal paling utama selain dari spesifikasi dari perangkat yang digunakan.

Aksesibilitas terhadap informasi juga menjadi hal lain yang menjadi tantangan pemberantasan *cybercrime*, dimana informasi atau pengetahuan terkait dengan teknik-teknik *hacking* dan perihal lain dapat dengan mudah didapatkan dalam website, dan juga dalam forum-forum di internet dimana seseorang dapat menemukan "mentor" dan komunitas sepemikirannya. Menggunakan perangkat pencarian (*search engine)*, pelaku dapat mengumpulkan informasi terkait dengan targetnya yang tersedia secara publik tanpa menggunakan keahlian sekalipun.[67]

c. Anonimitas

Anonimitas secara Bahasa dapat diartikan 'tanpa nama'. Berasal dari Bahasa Yunani, terma ini biasa digunakan untuk mengutarakan

[66] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* International Telecommunications Union, 2012. Hal. 76.

[67] *Ibid.* Hal. 75-76

suatu kondisi dimana seseorang berlaku tidak atas nama, atau tidak diketahui apapun terkait dengan dirinya.[68] Anonimitas dapat diklasifikasikan menjadi dua jenis, yakni anonimitas sejati (*True Anonimity)* dan anonimitas semu (*Pseudo-Anonymity),* dimana keduanya merupakan konsep anonimitas yang memiliki perbedaan mendasar dalam bentuk ekspresi, dan perbedaan dalam bentuk perlindungan secara sosio-politis serta pembatasan yuridis.

Anonimitas sejati sebagaimana dimaksud adalah bentuk anonimitas dimana pelacakan terhadap komunikasi bentuk ini adalah mustahil. Identitas asli dari seseorang yang bertindak dalam bentuk anonimitas ini tidak bisa secara pasti diungkapkan dan hanya bisa terungkap berdasar kehendak dari pelaku atau secara insidental.[69] Anonimitas bentuk ini rentan menimbulkan penyalahgunaan karena pengguna komunikasi dengan anonimitas model ini tidak dapat dipertanggungjawabkan atas tindakan yang diperbuat. Sementara, model anonimitas semu (*Pseudo-Anonymity)* adalah bentuk anonimitas yang dapat dilacak. Dimana meskipun pengguna komunikasi model anonim semu ini dapat terlihat sama seperti model anonimitas sejati dikarenakan bentuk pelacakan yang membutuhkan upaya menggunakan teknologi dan *digital forensic*, namun tetap

[68] Kathleen A. Wallace, *Anonymity.* Journal of Ethics and Information Technology Vol. 1, 1999.

[69] George du Pont, *The Criminalization of True Anonymity in Cyberspace.* Michigan Telecommunication and Technology Law Review, Vol. 7 No. 191, Hal. 192.

dimungkinkan untuk mengungkap identitas dari pengguna tersebut. Model anonimitas ini dapat menimbulkan hasil positif dalam bentuk sosio-politis, dimana masyarakat dapat mengekspresikan opini mereka tanpa ketakutan atas represi struktural, namun juga memiliki bentuk pertanggungjawaban atas tindakannya apabila melanggar kriteria tertentu. Situasi terburuk adalah ketika pemerintah melanggar kepercayaan masyarakat atas bentuk model ini, dimana memaksa masyarakat untuk beralih kepada model anonimitas sejati.[70]

Terlebih seiring berkembangnya teknologi dan kemampuan manusia dalam bidang IT, pelaku dapat secara sengaja menyembunyikan identitas onlinenya dengan penggunaan *proxy server*, alamat IP (*internet protocol*), serta penggunaan identitas elektronik palsu. Pelacakan terhadap jejak digital juga dapat dipersulit dengan menggunakan perangkat lunak yang dapat menyembunyikan atau bahkan menghapus jejak-jejak digital. Anonimitas juga berarti bahwa pertukaran komunikasi dan informasi dapat terjadi di berbagai yurisdiksi sebelum mencapai tujuan, mengakibatkan pelacakan terhadap asal komunikasi sangat sulit dan menguras waktu. Pelaku *cybercrime* juga dapat menempatkan data ke dalam yurisdiksi negara

[70] Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*. Springer, Studies in Computational Intelligence Vol. 593. Hal. 98.

yang memiliki pengaturan dan pengawasan yang tidak ketat terkait dengan data dan anonimitas[71].

d. Portabilitas dan Transferabilitas

Menjadi fungsi pokok dari teknologi digital adalah untuk menyimpan sejumlah besar data dalam ruang yang sangat kecil, dan untuk dapat mereplikasi data tersebut secara identik dalam waktu yang sangat cepat apabila dibandingkan dengan proses tradisional. Belum lagi perkembangan dari teknologi itu sendiri yang berkembang pesat, pada masa lampau gawai yang dibutuhkan tidak praktis dan ukurannya relatif besar. Perangkat prosesor dan penyimpanan data yang dulu bisa memakan ruangan-ruangan kini dapat kita masukan kedalam saku celana kita. Perekaman suara, gambar, video, dapat dilakukan oleh siapapun yang memiliki *smartphone,* dan juga dapat diunggah kedalam net pada hitungan detik.

e. Jangkauan Global

Aturan tentang kejahatan pada dasarnya dibuat dengan restriksi wilayah, sebagai konsekuensi dari konsep yurisdiksi dan kedaulatan negara. Namun, tentu kejahatan siber menantang paradigma tersebut dengan interkoneksitas global yang dialami mengakibatkan yurisdiksi hanyalah satu perlindungan lagi bagi pelaku *cybercrime*. Menurut data UN, dari setengah negara yang melapor terkait aktivitas *cybercrime*

[71] Jonathan Clough, *Op Cit.* Hal. 7-8.

mengatakan bahwa antara 50-100 % dari aktivitas *cybercrime* melibatkan elemen transnasional.[72] Hal ini membuat sulitnya dari penegakan yang efektif dan termasuk tantangan untuk harmonisasi hukum secara global.

f. Ketiadaan Pengawasan

Faktor ini merupakan sebuah tantangan yang tertuju kepada pencegahan dan penegakan dari *cybercrime*. Pidana siber membuahkan penegakan hukum dengan permasalahan dan juga cara kerja yang baru, seperti teknik-teknik forensik siber yang dibutuhkan untuk mengektraksi, menganalisis, memvalidasi sebuah jejak digital yang akan digunakan dalam persidangan. Pengawasan sebagai sarana pencegahan juga memiliki permasalahannya sendiri, bahkan selain dari fakta jumlah *potential offender*, konsep dari jaringan dalam telekomunikasi modern membuat pengawasan terhadap pola-pola komunikasi dan transfer informasi yang mencurigakan sulit dilakukan.[73] Contohnya adalah infrastruktur jaringan digital hampir dikuasai oleh swasta, artinya penegak hukum harus melewati beberapa prosedur dari berbagai instansi. Komunikasi juga umumnya melewati berbagai yurisdiksi, alhasil membutuhkan kooperasi transnasional. Bahkan meskipun semua itu bisa dilalui, pertanyaan terakhir adalah

[72] United Nation Office on Drugs Crime, *Comprehensive Study on Cybercrime*, 2013. Hal. 55

[73] Jonathan Clough, *Op Cit.* Hal. 8-9

apakah pelaku dari tindak pidana siber yang dimisalkan berada di yurisdiksi negara lain tersebut bisa diekstradisi untuk menjalani hukuman. Sementara di ranah regulasi, terdapat empat modal untuk pencegahan *cybercrime* menurut Lessig yakni hukum, arsitektur (diartikan sebagai perancangan struktur kelembagaan), norma sosial, dan pasar.[74]

3. Bentuk-Bentuk Umum *Cybercrime*

Konsepsi tentang perbuatan apa saja yang dikategorikan sebagai *cybercrime* merupakan pembahasan yang sampai sekarang terjadi, namun pada umumnya kita mengkategorikan sebuah perbuatan menjadi *cybercrime* dengan dua tolak ukur, yakni *computer as a tool* atau *computer as a target* (komputer sebagai alat atau sebagai target).[75] Dalam konteks komputer sebagai alat, artinya penggunaan komputer atau lebih relevan apabila kita sebut sebagai alat IT dalam penggunaannya untuk melakukan suatu kejahatan seperti penipuan, pemalsuan, dan juga keterlibatannya dalam perencanaan suatu kejahatan. Sedangkan dalam konteks komputer sebagai target, artinya penargetan komputer dan/atau alat IT sebagai objek dari sebuah kejahatan seperti sabotase, pencurian, dan pengubahan terkait data-data didalamnya.[76] Sejak tahun 1980 dimana mulai munculnya kejahatan-kejahatan komputer,

---

[74] L. Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999. Hal. 85-99

[75] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara.* CV. Aswaja Pressindo: Sleman, Yogyakarta, 2013. Hal. 7. Lebih lanjut lihat: Joshua Dressler, *Encyclopedia of Crime & Justice*, Vol. 4, 2002.

[76] *Ibid.*

para ahli mencoba untuk mengklasifikasikan beberapa bentuk dalam kejahatan komputer secara umum, yang bisa diuraikan menjadi bentuk-bentuk seperti:

a. *Joycomputing;*
b. *Hacking;*
c. *Trojan Horse*;
d. *Data Leakage;*
e. *Data diddling;*
f. Penyia-nyiaan data komputer.

Adapun *European Convention on Cybercrime* mengklasifikasikan bentuk-bentuk dari kejahatan siber yang didefinisikan sebagai bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi berbasis komputer dan jaringan kedalam empat bagian, yakni: [77]

a. Kejahatan terhadap kerahasiaan, integritas dan ketersediaan dari data komputer dan sistem (*Offences against confidentiality*, *integrity and availability of computer data and systems).*
b. Kejahatan terkait komputer (*computer related offences)*, adalah jenis kejahatan yang sejatinya merupakan kejahatan-kejahatan konvensional yang pada umumnya dilakukan dengan media sebuah sistem komputer.

[77] Council Of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001.

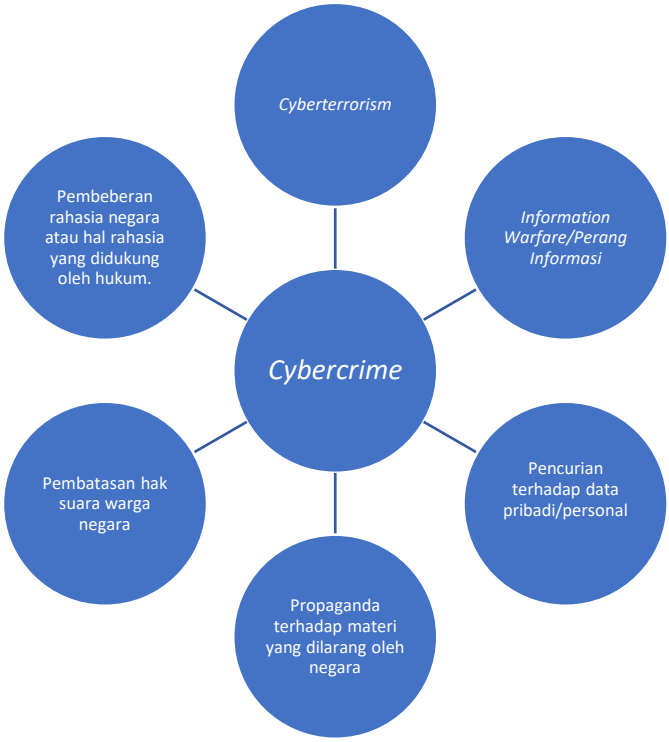
c. Kejahatan terkait konten (*content related offences)*, merupakan kejahatan yang dilakukan terhadap penyebaran konten-konten yang dianggap melanggar, seperti contohnya adalah penyebaran konten dari pornografi anak.

d. Kejahatan terkait pelanggaran hak cipta dan hak terkait (*offences related to infringements of copyright and related rights)*, merupakan kejahatan yang melanggar hak cipta dari pemilik dari sebuah produk baik (namun tidak terbatas pada) literatur, fotografi, musik, *audio visual*, dan produk lain yang memiliki hak kekayaan intelektual. Tujuan dari adanya pasal ini adalah sebagai perlindungan bagi pemilik hak kekayaan intelektual terhadap pelanggaran haknya karena internet merupakan salah satu tempat dimana terdapat pelanggaran yang signifikan dalam bentuk pelanggaran hak kekayaan intelektual.[78]

[78] *Ibid.* Nomor 107-117.

4. Pencurian Data Pribadi sebagai Bentuk *Cybercrime*

Secara garis besar, *cybercrime* sebagai tipologi dapat digolongkan dalam grafik dibawah ini:[79]



Gambar 1.0: Grafik Pembagian Tipologi *Cybercrime*

Dalam grafik diatas dapat kita klasifikasikan secara jelas perbuatan siber yang terjadi dalam bentuk-bentuk yang sudah didefinisikan sebelumnya, yakni kejahatan terhadap kerahasiaan, integritas dan ketersediaan dari sistem komputer dan data, juga dalam bentuk kejahatan terkait komputer atau *computer related offence* dan bentuk-bentuk lainnya. Klasifikasi paling utama dari pencurian data pribadi sebagai tindak pidana siber dapat ditelusuri dari kejahatan terhadap akses dari komputer atau *access offences*, yang

[79] Roman V. Veresha, *Preventive Measures Against Computer Related Crimes: Approaching an Individual.* Jurnal Informatologia, Vol. 51 No. 3-4, 2018. Hal. 193.

didefinisikan sebagai '*intentional and and without right access to the whole or part of a computer system'.* Tindakan secara disengaja dan tanpa hak untuk mengakses keseluruhan atau bagian dari sebuah sistem computer, dengan maksud untuk memperoleh data dari computer, atau jaringan terkait yang terhubung dengan jaringan computer lainnya.[80]Menurut Widodo akses ilegal/tidak sah merupakan jalan masuk bagi mayoritas dari perbuatan *cybercrime*, menjadikan akses ilegal sebagai titik penting dalam preventasi tindak pidana siber.[81]

Implementasi paling umum dari akses ilegal adalah penyalahgunaan data personal/pribadi yang dapat kita temui dalam tindakan pencurian data pribadi. Dalam konteks umumnya, pencurian data pribadi sering dikaitkan dengan *identity theft* atau pencurian identitas. Dari segi bahasa, istilah ini dapat menimbulkan beberapa kontradiksi dimana kata 'pencurian' pada umumnya merujuk kepada tindakan menguasai tanpa hak dari seorang pelaku yang menghilangkan hak pemiliknya untuk menguasai sebuah propertinya, namun dalam konteks ini properti yang dicuri tidak hilang secara *in concreto*, melainkan digunakan oleh orang lain tanpa persetujuan dari pemilik asli data/informasi pribadi tersebut[82]. Alhasil, pencurian identitas ini dapat disimpulkan sebagai tindakan melawan hukum dimana identitas dari

[80] Jonathan Clough, *Op. Cit.* Hal. 56.
[81] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Op. Cit. Hal. 70.
[82] Bert-Jaap Koops & Ronald Leenes, *ID Theft, ID Fraud and/or ID Related Crime. Definitions Matter.* Jurnal Datenschutz und Datensicherheit Vol. 9. Hal. 553-556.

seseorang digunakan sebagai target atau menjadi alat sebuah kejahatan tanpa sepengetahuan dan/atau persetujuan dari pemiliknya.[83]

Pada tahap regulasi, negara-negara memiliki perbedaan dalam mengakomodasi instrumen yuridis terkait dengan pencurian dan penyalahgunaan data. Britania Raya contohnya, menolak klausa memperoleh akses secara ilegal terhadap computer dengan alasan bahwa klausa tersebut terlalu menfokuskan terhadap keadaan fisik dari computer, dan tidak inklusif terhadap perbuatan yang merugikan data yang terkandung dalam jaringan computer terkhusus apabila tindakan yang dilakukan tidak memerlukan akses langsung terhadap computer.[84]Alhasil, frasa yang digunakan adalah menyebabkan computer untuk melakukan fungsi apapun secara disengaja dan tanpa hak/ilegal, dimana tentu frasa ini dapat diartikan secara luas dan bersifat non limitatif, ibaratnya perbuatan menyalakan computer secara ilegal saja dapat dikenakan delik tersebut.[85]

Sebagai perbandingan, Kanada menerapkan instrumen yuridis yang lebih limitatif dengan beberapa kondisi persyaratan (*preliminary condition*). Contohnya adalah klausa yang menjadi delik atas akses illegal yakni '*obtains, directly or indirectly, any computer service or uses or causes to be used, directly or indirectly, a computer system with intent to commit a specified offence.*' Memperoleh, secara langsung ataupun tidak langsung, layanan

[83] *Ibid.*

[84] Law Commission (UK), *Computer Misuse.* 1989, Pasal 3.22-3.25. Dikutip dari Jonathan Clough, *Op. Cit.* Hal. 72.

[85] Law Commission (UK), *Ibid.* Pasal. 3.19. Dikutip dari Jonathan Clough, *Ibid.*

computer atau menggunakan atau menyebabkan untuk digunaknnya sebuah system computer dengan tujuan melakukan sebuah pidana, baik secara langsung ataupun tidak langsung.[86]Limitasi yang paling besar adalah dari persyaratan memperoleh sesuatu hal secara melawan hukum, artinya kejahatan tersebut harus telah dilakukan, terlepas dari berhasil atau tidaknya upaya kejahatan tersebut. Hal ini sesuai dengan hukum nasional negara Kanada terkait dengan kejahatan terhadap properti, seperti telah dibahas dalam teori terkait data, sering digunakan oleh negara-negara sebagai ekstensifikasi dan mergerisasi antara komoditas 'data'.

Yang dapat kita simpulkan adalah pada umumnya terdapat dua metode untuk menanggulangi ranah kejahatan siber. Pertama adalah regulasi-regulasi dari negara terkait dengan pencurian data yang merupakan ranah kejahatan kontemporer dilakukan dengan mengaplikasikan modifikasi terkait dengan norma hukum tradisionalnya, seperti dengan mengakui hak data sebagai hak properti seseorang, memperluas definisi pencurian dalam konteks siber, yang bisa kita lihat dalam kasus negara Kanada. Atau model kedua adalah seperti yang dilakukan oleh Britania Raya, dengan membentuk pengaturan yuridis baru terkait dengan regulasi terkait kejahatan siber, yang dilakukan sangat spesifik sehingga tidak tersisa celah kekosongan dalam hukum tersebut.

5. Kejahatan Transnasional

a. Definisi dan Pengertian

[86] *Canada Criminal Code, Section 342.1 (1)(a)(c).* Dikutip dari Jonathan Clough, *Ibid.* Hal. 73.

Isu terhadap pemaknaan dari pengertian kejahatan transnasional menjadi sebuah titik yang penting dalam mengukuhkan sebuah *legal framework* terhadap elemen-elemen dari kejahatan transnasional. Kata trans sendiri yang diartikan sebagai 'di atau ke sisi yang lain, disebrang, melebihi/melintasi', dalam ilmu bahasa ditetapkan sebagai sebuah *prefix,* sebuah imbuan yang terdapat pada awal kata yang merubah makna dari kata tersebut. Dengan diimbuhkan pada kata nasional, yang merujuk kepada negara secara keseluruhan,[87] merubah makna dari nasional menjadi sesuatu hal yang bersifat melintasi batas kenegaraan.[88] Dari definisi tersebut, kejahatan transnasional bisa diartikan sebagai kejahatan yang bersifat melintasi batas-batas kenegaraan, yang disebabkan makin berkembangnya hubungan antar negara dalam aspek ekonomi/perdagangan, juga sistem teknologi informasi yang menjadi faktor utama dari globalisasi.[89]

Pada tahap awal, kejahatan transnasional sering digunakan sebagai bentuk klasifikasi kejahatan konvensional yang terjadi secara lintas negara, melalui sebuah wadah organisasi kejahatan yang rapih dan bergerak cepat di dan ke berbagai negara, sehingga disebut sebagai *transnational organized crimes* atau kejahatan transnasional

[87] Henry Campbell Black, *Black's Law Dictionary*, 4th Ed, National.
[88] https://www.merriam-webster.com/dictionary/transnational
[89] Romli Atmasasmita, *Dampak Ratifikasi Konvevnsi Tranasnational Organized Crime (TOC),* Jakarta: Penerbitan Badan Pembinaan Hukum Nasional Departemen Kehakiman dan Hak Asasi Manusia RI, 2004. Hal. 1

tergorganisasi/terorganisir (*TOC*).[90] Kegiatan dari kejahatan transnasional terorganisasi meliputi semua kegiatan bisnis/*profit oriented* yang terjadi secara internasional dengan artian kegiatan tersebut melibatkan lebih dari satu negara dalam aktivitasnya.[91] Bentuk-bentuk dari kejahatan transnasional terorganisir yang bersifat 'tradisional'[92] ini meliputi kekerasan, pemerasan, korupsi, juga penyelundupan baik senjata api, manusia, narkotika dan obat berbahaya.[93] Tentu contoh-contoh ini merupakan sebuah daftar kecil dari kegiatan lain yang menjadi klasifikasi dari kejahatan transnasional terorganisir.

b. Pengaturan/Regulasi tentang Kejahatan Transnasional

Legal Framework dari kejahatan transnasional dapat kita temui dalam Konvensi PBB menentang Kejahatan Transnasional Terorganisir (*United Nations Convention against Transnational Organized Crime*) sebagaimana dibahas pada bab sebelumnya. Dalam penetapan konvensi ini, masyarakat internasional mengakui berkembangnya bentuk kejahatan transnasional baik secara skala, lingkup dan juga

[90] *Ibid.* Hal. 2

[91] United Nation Office on Drugs and Office (UNODC), *Transnational Organized Crime-The Globalized Illegal Economy.* Flier/Facts Sheet UNODC, diakses dari: https://www.unodc.org/documents/toc/factsheets/TOC12_fs_general_EN_HIRES.pdf

[92] Frasa 'tradisional' disini diambil dari pendahuluan sebuah paper yang ditulis oleh: Allan Castle, *Transnational Organized Crime and Security.* Institute of International Relations the University of British Columbia, Working Paper No. 19. Tahun 1997 Hal. 1. Tradisional disini mengungkapkan pemikiran penulis terhadap berkembangnya kejahatan konvensional terorganisir berskala nasional yang berkembang menjadi transnasional.

[93] Romli Atmasasmita, *Op. Cit.* Hal. 2.

tingkatannya sehingga diperlukan adanya pembahasan yang berlanjut sebagai penanggulangan dari kejahatan ini. Konvensi ini memberikan kualifikasi terhadap kejahatan yang bisa dikategorikan sebagai *transnational crime* yaitu:

1) Dilakukan di satu negara, namun persiapan, perencanaan dan pengarahan atau pengendalian terhadap aksi tersebut berada di negara lain;
2) Dilakukan di satu negara namun melibatkan grup kriminal yang melakukan kegiatan kejahatan di lebih dari satu negara secara terorganisir; atau
3) Dilakukan di satu negara namun memiliki dampak yang substansial di negara lain[94].

c. *Cybercrime sebagai Kejahatan Transnasional*

Interpol menyatakan bahwa *cybercrime* adalah salah satu dari kejahatan transnasional yang paling berkembang yang dihadapi oleh negara anggota dari interpol. Perkembangan yang pesat dalam bidang Informasi dan Teknologi khususnya internet dan teknologi komputer, dalam satu sisi membuahkan peningkatan ekonomi dan sosial. Namun di sisi lainnya, kebergantungan negara dan masyarakat terhadap internet dan teknologi komputer juga menghasilkan resiko dan

[94] *Article 3, Scope of Application. Paragraph 2,*

kerentanan terhadap aktivitas kejahatan yang menggunakan metode *cybercrime*.[95]

Meskipun apakah *cybercrime* dapat dikatakan sebagai bentuk dari kejahatan terorganisir merupakan sebuah perdebatan, dikarenakan sifat natural dari *cybercrime* itu sendiri pada dasarnya tidak membutuhkan sekelompok orang untuk melaksanakan kejahatan, namun sifat transnasional yang dimiliki oleh *cybercrime* tidak dapat dipungkiri lagi secara global. Widodo menyebutkan beberapa karakteristik dari kejahatan *cybercrime* yakni:[96]

1) Bersifat lintas negara,
2) Bukan hanya menggunakan computer konvensional (melainkan sudah menggunakan gawai yang tidak terikat dengan tempat misalnya *handphone*, laptop, tablet, dan lainnya),
3) Ada yang dapat digolongkan *white-collar criminal* dan ada yang bukan *white-collar criminal*,
4) Bukan merupakan kejahatan terorganisasi,
5) Dapat merupakan kejahatan korporasi dan bukan kejahatan korporasi.

[95] INTERPOL, *Global Action Plan Strategy Summary.* 2017. Diakses dari: https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf

[96] Widodo, *Kebijakan Kriminal terhadap Kejahatan yang Berhubungan dengan Komputer di Indonesia*, Disertasi, Pascasarjana Universitas Brawijaya. Hal. 467.

Meskipun Widodo menyebutkan bahwa *cybercrime* secara murni bukan merupakan kejahatan terorganisasi, namun potensi dari kegiatan kejahatan siber yang terorganisir bukanlah sebuah hal yang baru. McCusky berpendapat bahwa konseptualisasi terkait dengan sebuah sindikat atau penjahat siber yang terorganisir merupakan perdebatan antara perspektif logika dan pragmatisme. Dalam satu sisi, logika mengatakan bahwa sindikat kriminal tradisional akan menggunakan dunia digital sebagai wadah bagi melakukan aktivitasnya, sementara dalam sudut pandang pragmatisme timbul pertanyaan terhadap kebutuhan dari kelompok/sindikat kejahatan tradisional untuk memasuki bidang ini dan kapasitas dari kelompok tersebut untuk mengamankan keuntungan dari aktivitas *cybercrime* ini.[97] Namun seiring dengan perkembangan teknologi dan sentralisasi dari kehidupan manusia terhadapnya, maka tidak dapat dibantah bahwa penggunaan *cyberspace* menjadi salah satu karakteristik baru dalam aktivitas organisasi kejahatan yang terorganisir. Dari dasar ini muncul kebutuhan untuk adanya separasi secara konseptual antara migrasi organisasi kejahatan terorganisasi tradisional ke dunia virtual (menggunakan fasilitas *cyberspace* dalam kegiatan kejahatan tradisional), dengan grup/organisasi yang murni bertujuan untuk kegiatan *cybercrime*.[98]

[97] Rob McCusker, *Transnational Organised Crime: Distinguishing Threat from Reality.* Journal Crime and Law Social Change 46, Hal. 257-273.

[98] Tatiana Tropina, *Organized Crime in Cyberspace*. Journal Transnational Issues of Cybercrime, Vol. 2, 2013. Hal. 48-57.

Perubahan terhadap komoditas yang diperebutkan juga memiliki perbedaan yang kontras antara sindikat kejahatan siber dan tradisional. Monetisasi komoditas *intangible* berupa data menjadi faktor pembeda utama antara sindikat kejahatan siber dan tradisional[99]. Hal ini juga yang menjadi perbedaan dalam karakteristik yang diturunkan dalam kegiatannya, dimana organisasi kejahatan tradisional pada umumnya memperebutkan kekuasaan atas suatu wilayah geografis, dan aset-aset ilegal di pasar gelap, melahirkan sebuah struktur kekuasaan yang formal, homogenis, dan birokratis.[100] Sementara dalam konteks organisasi kejahatan siber karakteristik tersebut tidak ditemukan, dengan data sebagai komoditas utama organisasi ini tidak membutuhkan lokasi geografis, konflik kepentingan, dan ketiadaan interaksi secara langsung. Alhasil aktivitas dari organisasi ini bersifat non kompetitif dan membuahkan kolaborasi antar jaringan-jaringan sindikat siber[101].

[99] *Ibid.*

[100] Council of Europe, *Summary of the Organised Crime Situation Report 2004: Focus on threat of cybercrime. Council of Europe Octopus Programme*. Strasbourg, September 6. Diakses dari: http://www.coe.int/.

[101] UK Home Office. *Cybercrime strategy. Stationery office limited on behalf of the controller of Her Majesty's Stationery Office*, 2010. Dikutip dari Tatiana Tropina, Op. Cit.

BAB III

PENERAPAN PRINSIP YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA SIBER PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA

A. Pengaturan Terkait Tindak Pidana Siber/*Cybercrime* Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara

Sebagaimana telah dijelaskan dalam bab sebelumnya, adalah mustahil untuk mengkategorikan tindak pidana siber sebagai kejahatan domestik atau hanya diafiliasikan terhadap satu wilayah kenegaraan. Fenomena internetisasi mengakibatkan interkoneksi jaringan global dimana bahkan apabila salah satu noda/titik koneksi dihancurkan jaringan tersebut masih akan tetap berjalan dengan noda-noda lainnya, yang menjadikan struktur ini menjadi kekuatan utama bagi pelaku tindak pidana siber yang dilakukan secara transnasional.[102]

Interkoneksi ini menghasilkan beberapa kelemahan dalam sisi preventasi dan penegakan yakni:[103]*Pertama,* potensi sasaran/target secara global selama terhubung dalam jaringan internet dan *kedua,* disparitas regulasi tindak pidana siber baik domestik dengan lemahnya kooperasi internasional terkait penegakan dan pencegahan dari jenis kejahatan ini menghasilkan salah satu faktor kesulitan terhadap penegakan dari tindak pidana siber. Sebagaimana salah satu kritik terkait

[102] William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*. 40 GA. Journal of. INT'L & COMP. Law 247, 2011. Hal. 252

[103] Meetali Rawat, *Transnational Cybercrime: Issue of Jurisdiction*. International Journal of Law Management & Humanities, Vol 4, Issue 2 No. 253, 2021. Hal. 254.

penegakan dari tindak pidana siber yang menyatakan bahwa sifat transnasionalitas dari *cybercrime* merepresentasikan tantangan yang besar bagi pemerintahan dunia, dikarenakan perpindahan dari materi dan lingkungan fisik kedalam immateriil/*intangible* mengakibatkan dogma-dogma hukum klasik/tradisional tidak sesuai untuk diterapkan.[104]Pada tahun 2005, 4 warga negara Amerika Serikat mengalami pencurian data keuangan sensitif yang mengakibatkan kerugian sebesar $3.50.000, yang dilakukan oleh 3 karyawan perusahaan BPO (*Business Process Outsourcing)* Citibank di India.[105] Beruntung, pemerintahan India dapat mengidentifikasi dan menindaklanjuti kejahatan tersebut, meskipun proses pengembalian kerugian yang alot antara dua wilayah kenegaraan tersebut. Namun, hal ini menggambarkan sifat transnasionalitas yang dimiliki oleh tindak pidana siber pencurian data pribadi. Harus kita bayangkan pula bagaimana penegakan terhadap kejahatan-kejahatan lainnya yang tidak ditindaklanjuti/diidentifikasi bahkan tidak diketahui oleh negara tempat pelaku berkediaman.

Penerapan yurisdiksi ektstrateritorial dan kerjasama internasional yang dilakukan secara intensif umumnya dilakukan untuk investigasi dan penegakan tindak pidana siber berupa pencurian data pribadi. Salah satu contoh keberhasilan dari terbentuknya kerjasama internasional yang efektif adalah terungkapnya sebuah sindikat *cybercrime* yang menyerang infrastruktur teknologi dari beberapa

[104] Gianpero Greco & Nicola Montinaro, *The Phenomenon of Cybercrime: From the Transnational Connotation to the Need of Globalization of Justice*. European Journal of Social Sciences Studies, Vol. 2 Issue 1, 2021. Hal. 2

[105] Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* Temple International and Comparative Law Journal Vol. 21 No. 103, 2007. Hal. 1

perusahaan di Prancis, Jerman dan Romania dengan serangan jenis *ransomware*, yakni penyaderaan dari data-data perusahaan sampai dibayarnya sejumlah uang tertentu, yang mengakibatkan kerugian sejumlah jutaan euro. Investigasi dan penegakan akhirnya dilakukan oleh tim gabungan dari Europol, kepolisian Prancis, Jerman, Romania dan Swiss dengan bantuan yudisial dari institusi Eurojust. Meskipun investigasi ini membuahkan hasil, namun diketahui bahwa dua pelaku yang tertangkap hanyalah sebuah bagian dari skema organisasi lebih besar, memfasilitasi alat-alat software untuk melakukan serangan siber dalam kasus-kasus *cybercrime* lainnya.[106]Contoh kasus lainnya adalah serangan siber bermotif finansial terhadap 1800 korban yang tersebar dari 71 negara, dengan metode pencurian data rahasia melalui *malware* atau program berbahaya.[107]

Selain kejahatan transnasional terorganisir dengan adanya sebuah sindikat kejahatan siber, *cybercrime* juga memiliki keunikan lain yakni tidak diperlukannya sebuah grup untuk melakukan kejahatan ini dengak skala transnasional. Salah satu kejahatan paling umum yang dilakukan oleh perorangan namun dapat berskala global adalah *phising*, yakni penipuan berbasis komputer yang bertujuan memperoleh data sensitif dari korban seperti password, nomor kartu kredit, nomor

[106] *European Union Agency for Criminal Justice Cooperation Press Release* pada tanggal 8 November 2021, bertajuk *Ransomware Gang Dismantled with Eurojust Support.* Diakses dari: https://www.eurojust.europa.eu/news/ransomware-gang-dismantled-eurojust-support

[107] Artikel oleh Henry Pope dalam laman *Organized Crime and Corruption Reporting Project* pada 2 November 2021. Diakses dari: https://www.occrp.org/en/daily/15419-ukraine-switzerland-arrest-12-suspects-of-international-cybercrime

PIN, dan informasi sensitif lainnya,[108] dengan tingkat korban mencapai 1 sampai 17% dari total populasi pengguna jaringan.[109]

Berangkat dari hal ini, akan kita telaah pengaturan terkait tindak pidana siber pencurian data pribadi baik secara internasional dan nasional untuk lebih memahami *status quo* dari pemberantasan terhadap tindak pidana siber pencurian data pribadi yang dilakukan secara transnasional/lintas batas negara.

1. Instrumen Hukum Pelindungan Data Pribadi terhadap Tindak Pidana Siber

Dalam pengaturan tindak pidana siber/*cybercrime* yang berkaitan dengan pencurian data pribadi ini, akan lebih mudah apabila dikaji menjadi beberapa sub-bab berkaitan dengan instrumen internasional yang digagaskan di tingkat global dan regional serta komparasinya dengan pengaturan di tingkat nasional, dilanjutkan beserta analisis mengenai keselarasan pengaturan tersebut dalam rangka pencegahan dan/atau penegakan tindak pidana siber pencurian data pribadi.

a. Instrumen Internasional

Dari berbagai konsepsi mengenai data pribadi yang sudah dijelaskan sebelumnya juga seiring berkembangnya fungsi hukum mengikuti kebutuhan dari zaman, data pribadi diakui sebagai hak fundamental dari seorang manusia yang awamnya disebut dengan hak

[108] Jan Kleijssen & Pierluigi Persi, *Cybercrime Evidence and Territorriality: Issue and Options.* Netherland Yearbook of International Law 47, Bab 7, 2016.
[109] UNODC, *Comprehensive Study on Cybercrime*. 2013. Hal. 25

asasi manusia. Pengakuan ini ditegaskan dalam Pasal 12 Deklarasi Hak Asasi Manusia, yang menyatakan bahwa: *"Tidak seorangpun dapat diganggu secara sewenang-wenang dalam urusan pribadi, keluarga dan rumah tangga atau hubungan surat-menyuratnya, juga tidak boleh dilakukan serangan terhadap kehormatan dan reputasinya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau penyerangan seperti itu."*

Pernyataan ini juga terkandung dalam Pasal 17 Kovenan Internasional Hak-hak Sipil dan Politik (*ICCPR*) yang menyatakan bahwa:

1) Tidak boleh seorang pun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya.
2) Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan tersebut di atas.

Terkait dengan Pasal diatas, dijelaskan lebih lanjut dalam *General Comment No. 16: Article 17 (Rights to Privacy)* yang menjabarkan bahwa pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan perangkat lain, baik oleh otoritas publik atau individu/badan pribadi, harus diatur oleh hukum. Penjelasan ini menegaskan pengakuan dunia internasional bahwa pelindungan terhadap informasi pribadi, baik berbentuk fisik maupun non-fisik,

merupakan sebuah bentuk hak yang harus dijaga oleh negara[110]. Dijelaskan juga dalam raport khusus *United Nations on the Promotion and Protection of the Right to Freedom of Opinion and Expression* pada tahun 2011 bahwa Pelindungan data pribadi merupakan salah satu bentuk khusus dari penghormatan dari hak privasi. Oleh karena itu negara harus menghormati hak asasi manusia mengenai privasi terkhusus ketika terdapat pengungkapan data pribadi kepada pihak ketiga[111]. Hal ini juga merupakan penegasan terhadap pemrosesan data pribadi sebagai bentuk perlindungan hak asasi manusia dalam bentuk data pribadi.

Salah satu instrumen hukum internasional yang vital bagi pelindungan data dalam ranah siber adalah *Organisation for Economic Co-operation and Development* (OECD) *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* yang dibuat pada tahun 1980 dan direvisi pada tahun 2013.[112] Mengapa instrumen ini menjadi vital karena sifatnya yang tidak mengikat dan berbentuk pedoman membuatnya lebih mudah untuk negara-negara pada umumnya, terkhusus negara-negara berkembang pada saat itu, untuk

[110] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, Diakses dari: https://www.refworld.org/docid/453883f922.html

[111] UN Doc.A/HRC/17/27, *Report of The Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression*, 16 Mei 2011. Paragraf 58.

[112] OECD (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.

membentuk sebuah regulasi terkait pelindungan dan transfer data. Pedoman ini terbagi menjadi 5 bagian yakni aturan umum, prinsip dasar untuk penggunaan nasional, prinsip dasar untuk penggunaan internasional: alir bebas dan pembatasan hukum (*free flow and legitimate restriction)*, implementasi nasional dan kerjasama internasional.

Adapun prinsip-prinsip dasar yang menjadi kerangka pendahulu bagi hukum pelindungan data dapat kita lihat dalam bagian ke-2, yaitu:

1) *Collection Limitation Principle* (prinsip pembatasan pengumpulan), yakni sebuah prinsip yang mengatur tentang harus adanya sebuah batasan terhadap pengumpulan data pribadi.[113]
2) *Data Quality Principle* (prinsip kualitas data), yakni sebuah prinsip yang mengatur tentang kebutuhan untuk pengecekan relevansi data terhadap tujuan dikumpulkannya data tersebut dan terhadap akurasi dari data.[114]
3) *Purpose Specification Principle (*prinsip spesifikasi tujuan), yakni sebuah prinsip yang mengatur tentang harus adanya pemberitahuan tentang tujuan dikumpulkannya data

[113] Pasal 7 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*
[114] Pasal 8 *Ibid.*

yang mengikat terhadap digunakannya data harus sesuai dengan pemenuhan tujuan yang diberitahukan.[115]

4) *Use Limitation Principle* (prinsip penggunaan terbatas), yakni prinsip yang menyatakan bahwa penggunaan data pribadi tidak boleh diluar dari hal yang diatur dalam Pasal 9 kecuali dalam hal tersebut disetujui oleh pemilik data (*data subject*) atau berdasarkan hukum yang berlaku.[116]

5) *Security Safeguards Principle* (prinsip penjaminan keamanan), menyatakan bahwa harus adanya sebuah system keamanan yang memadai terhadap ancaman kerusakan atau akses illegal, penghancuran, penggunaan, modifikasi atau pengungkapan terhadap data.[117]

6) *Openness Principle* (prinsip keterbukaan), yakni prinsip yang menyatakan harus adanya perkembangan yang dilakukan secara terbuka terkait dengan penggunaan data pribadi.[118]

7) *Individual Participation Principle* (prinsip partisipasi individu), yakni sebuah prinsip yang menyatakan terkait hak-hak individu dalam proses pengolahan, penyimpanan,

[115] Pasal 9 *Ibid.*
[116] Pasal 10 *Ibid.*
[117] Pasal 11 *Ibid.*
[118] Pasal 12 *Ibid.*

penggunaan, atau proses data lainnya yang menyangkut dirinya.[119]

8) *Accountability Principle* (prinsip akuntabilitas), menyatakan bahwa pengendali data harus bertanggungjawab atas memenuhi prinsip prinsip diatas.[120]

Selain OECD, Perserikatan Bangsa-Bangsa pernah membuat sebuah pedoman terkait dengan penggunaan data komputer yang menghasilkan beberapa dari prinsip-prinsip umum terkait penggunaan data yang digunakan secara global, dimana dapat kita lihat pengaruh dari pedoman OECD terhadap pedoman yang dihasilkan oleh PBB. Prinsip-prinsip tersebut dapat dilihat dalam bagian ke-2 yakni prinsip-prinsip terkait jaminan minimal dalam regulasi nasional yang terdiri dari beberapa prinsip yakni: [121]

1) *Principle of lawfulness and fairness* (prinsip legitimasi dan keadilan), yakni sebuah prinsip dimana data tidak boleh dikumpulkan dan diproses secara tidak sah dan tidak adil, juga dalam hal penggunaan yang bertentangan dengan tujuan dan prinsip Piagam Perserikatan Bangsa-Bangsa (*Charter of the United Nations).*

[119] Pasal 13 *Ibid.*

[120] Pasal 14 *Ibid.*

[121] UN Guidelines for the Regulation of Computerized Personal Data Files on '*the procedures for implementing regulations concerning computerized personal data files,'* Adopted by General Assembly resolution 45/95 of 14 December 1990.

2) *Principle of accuracy* (prinsip ketepatan), yakni sebuah prinsip dimana orang yang bertanggung jawab dalam hal pengumpulan atau penyimpanan data (*data controller* dan *processor*) memiliki kewajiban untuk melakukan pengecekan secara rutin terhadap akurasi dan relevansi data yang tersimpan untuk memastikan keutuhan dan kebenaran dari data.

3) *Principle of purpose-specification* (prinsip penggunaan spesifik), yakni sebuah prinsip dimana penggunaan data dalam sebuah tujuan tertentu harus dinyatakan secara spesifik/jelas, beralaskan hukum dan ketika ditetapkan haruslah diberitahukan kepada pihak yang bersangkutan untuk:

   a) Data pribadi yang dikumpulkan dan disimpan tetap relevan terhadap tujuan dari pengumpulan dan penyimpanan yang ditetapkan;

   b) Tidak terjadi penggunaan/penutupan terhadap data kecuali dengan sepersetujuan pemilik data, untuk tujuan yang tidak sesuai dengan yang dispesifikasikan;

   c) Penyimpanan data tidak melebihi jangka waktu setelah tujuan dari data tersebut terpenuhi.

4) *Principle of interested-person access* (prinsip akses orang terkait), yakni sebuah prinsip yang menyatakan bahwa setiap orang berhak memiliki akses terhadap data pribadi miliknya, dalam bentuk yang jelas dan tanpa penundaan yang tidak semestinya, serta berhak untuk melakukan perubahan atau penghapusan terhadap data tersebut dalam perihal ketidaksesuaian, ketidakabsahan, dan ketidakperluan penggunaan/penyimpanan data tersebut.

5) *Principle of non-discrimination* (prinsip non diskriminasi), yakni sebuah prinsip dimana data-data perihal individu yang dapat menjadi target dari diskriminasi dan perlakuan yang berbeda dilarang untuk dikumpulkan kecuali dalam kondisi tertentu.

6) *Power to make exceptions* (kewenangan untuk membuat pengecualian), yakni berisikan kondisi-kondisi dimana prinsip-prinsip yang sudah tertera sebelum ini dapat dikesampingkan, misalnya dalam hal keamanan dan ketertiban negara, kesehatan moral publik, serta hal seperti penjagaan hak dan kebebasan manusia.

7) *Principle of security* (prinsip keamanan), menyatakan bahwa harus ada langkah-langkah untuk menjaga data yang disimpan dari potensi ancaman yang natural/alamiah

maupun yang disebabkan oleh manusia, seperti akses ilegal, penyimpangan penggunaan data dan kontaminasi virus.

8) *Supervision and sanctions* (prinsip pengawasan dan sanksi), menyatakan perlunya sebuah lembaga yang bertindak dalam pengawasan dan penegakan terhadap pelaksanaan dan pelanggaran prinsip-prinsip ini. Lembaga ini harus bersifat independent, tidak memihak, dan memiliki kompetensi teknis.

9) *Transborder data flows* (aliran data antarnegara), menyatakan bahwa aliran data antar negara hanya bisa dilakukan ketika telah ada kerangka hukum privasi data yang memadai bagi dilakukannya peralihan data tersebut.

10) *Field of application* (ranah kerja pengaplikasian), bahwa prinsip-prinsip ini harus dapat diberlakukan untuk semua ranah komputerisasi baik publik ataupun privat.

Instrumen hukum lain hadir dalam bentuk sebuah konvensi yang dibentuk secara regional yakni Konvensi Budapest atau *Council of Europe Convention on Cybercrime*, merupakan sebuah konvensi yang digagas oleh Majelis Eropa namun mengundang negara non-anggota untuk ikut meratifikasi konvensi tersebut. *European Convention on Cybercrime* memberikan sebuah rancangan untuk regulasi yang dikhususkan terhadap kejahatan siber, dimana salah satunya merupakan pencurian data pribadi. Konvensi ini memiliki 4 bab yang terdiri dari

use of terms (definisi operasional), *measures to be taken at the national level* (langkah untuk diambil di tingkat nasional) *international cooperation* (kerjasama internasional) dan *final provision* (peraturan penutup). Dapat kita lihat dalam Bab 2 yang didalamnya berisikan "delik-delik" terhadap perbuatan yang dinyatakan sebagai tindakan pidana siber, pencurian data pribadi dapat dianotasikan dalam mayoritas dari Pasal yang terdapat didalamnya, yakni:

1) Kejahatan terhadap kerahasiaan, integritas dan ketersediaan dari data komputer dan sistem (*Offences against confidentiality, integrity and availability of computer data and systems).* Jenis kejahatan yang termasuk kedalam modus operandi ini adalah:

    a) *Illegal Access* atau akses illegal, yakni kejahatan yang disebabkan oleh akses tanpa hak terhadap suatu sistem komputer yang dilakukan untuk memperoleh suatu data atau maksud lain.[122]Dijelaskan juga bahwa bentuk-bentuk akses ilegal yang awamnya dilakukan seperti *hacking, cracking* ataupun penyerobotan komputer yang dilakukan secara melawan hukum

[122] Council of Europe, *Explanatory Reports to The Convention on Cybercrime.* European Treaty Series No. 185, 2001. Nomor 44.

merupakan salah satu bentuk dari akses ilegal tersebut.[123]

b) *Illegal Interception* atau pencegatan illegal, yang merupakan suatu tindakan pencegahan atau penahanan data yang dilakukan secara melawan hukum dimana perbuatan penahanan/pencegatan terhadap sebuah pergerakan data yang dilakukan secara pribadi yang dilakukan dalam segala bentuk transmisi elektronik. Meskipun tidak diartikulasikan secara eksplisit namun dalam penjelasan *CETS* menjadi jelas bahwa tujuan dibuatnya Pasal ini adalah sebagai jaminan bagi kebebasan komunikasi data, dan menjadi limitasi bagi kekuasaan negara dalam kontrol terhadap pergerakan data.[124] Hal tersebut dikarenakan adanya persyaratan kumulatif atas kesadaran/kesengajaan dan ketiadaan suatu hak/wewenang berdasarkan kata '*Rights'* yang dapat didefinisikan sebagai keduanya.

c) *Data Interference* atau gangguan data, yaitu merupakan sebuah klausul yang bertujuan untuk melindungi data komputer dan program komputer

[123] *Ibid.*
[124] *Ibid.* Nomor 51-59

terhadap ancaman sebagaimana dapat dinikmati oleh objek nyata/dapat dirasakan secara fisik. Kejahatan yang diatur dalam Pasal memiliki contoh pengrusakan, penghapusan, perubahan ataupun penekanan sebuah data yang dilakukan tanpa hak. Pemasukan dari kode-kode yang berbahaya seperti virus yang merusak atau merubah integritas dari sebuah data komputer termasuk kedalam kejahatan yang disebut dalam klausula ini.[125]

d) *System Interference* atau gangguan sistem adalah sebuah bentuk kejahatan yang dilakukan dengan memasukan, menyebarkan, menghapus atau menyembunyikan data komputer. Dalam laporan penjelasan yang dikeluarkan oleh ETS (*European Treaty Series),* kejahatan ini sering direferensikan sabotase komputer. Dalam kalimat resmi yang digunakan dalam Pasal ini yakni "*when committed intentionally, the serious hindering without the rights of the functioning of a computer system…",* kata '*hindering'* merujuk kepada tindakan yang mengganggu kepada fungsi asli dari komputer

[125] *Ibid.* Nomor 60-63.

dengan bentuk-bentuk seperti diatas. Klausula ini dibentuk secara netral agar dapat mengakomodasi segala fungsi komputer untuk menjaga hak-hak dari operator dan pengguna komputer, serta sistem pertelekomunikasian.[126]

e) *Misuse of Device* atau penyalahgunaan alat, merupakan sebuah Pasal yang berisikan tentang kejahatan penggunaan, penyebaran atau penjualan, impor dan menyediakan alat-alat yang bisa menyebabkan kejahatan-kejahatan yang terdapat pada Pasal 2-5 diatas (*The act of production, sale, procurement for use, import, distribution or otherwise making available of*). Pasal ini memberikan perlindungan terhadap ancaman yang berasal dari program-program komputer atau akses data yang meskipun secara tidak langsung namun dapat menyebabkan kejahatan siber yang diatur dan dijelaskan di Pasal 2-5 konvensi ini.[127]

2) Kejahatan terkait komputer (*computer related offences)*, adalah jenis kejahatan yang sejatinya merupakan kejahatan-kejahatan konvensional yang pada umumnya dilakukan

[126] *Ibid.* Nomor 65-70
[127] *Ibid.* Nomor 71-78

dengan media sebuah sistem komputer. Meskipun pada dasarnya negara dapat melakukan penafsiran ekstensif kepada hukum nasionalnya dalam mengakomodir bentuk-bentuk kejahatan yang termasuk dalam *computer related offences*, hukum tersebut mungkin tidak dapat melakukan ekstensifikasi terhadap situasi yang melibatkan jaringan komputer.[128] *United Nations Office on Drugs and Crime* (UNODC) mendeskripsikan *computer related offences* sebagai tindakan kejahatan dimana komputer atau alat digital merupakan alat yang inheren dengan modus operandi dari kejahatan tersebut.[129] Kejahatan yang termasuk dalam *computer related offences* adalah kejahatan yang bersifat didukung oleh siber (*cyber-enabled)* yang dilakukan dengan motif keuntungan atau kerugian finansial atau pribadi (*for personal or financial gain or harm).*[130] Dalam Konvensi *Cybercrime* 2001 kejahatan ini dikelompokan lebih jauh menjadi:

a) *Computer-related Forgery* atau pemalsuan yang berkaitan dengan komputer, merupakan tindakan-tindakan berupa pemasukan, perubahan,

[128] *Ibid.* Nomor 79.
[129] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime-Draft*. Vienna, 2013. Hal. 17.
[130] *Ibid.* Hal. 16.

penghapusan dan penekanan (*the input, alteration, deletion or suppression*) dari data komputer yang menyebabkan tidak terjamin keotentikanya (*inauthentic)* yang berujung pada penggunaan untuk tujuan hukum (*legal purposes)* sebagaimana apabila data tersebut dianggap otentik. Tujuan dari dibuatnya Pasal ini adalah sebagai kondisi pararel dari pemalsuan konvensional yang mungkin sudah diakomodasikan oleh hukum nasional negara. [131]

b) *Computer-related Fraud* atau penipuan yang berkaitan dengan komputer, merupakan kejahatan yang menyebabkan seseorang atas kehilangan terhadap propertinya kepada orang lain oleh tindakan-tindakan:

i. Pemasukan, perubahan, penghapusan atau penekanan apapun terhadap data komputer (*any input, alteration, deletion or suppression of computer data).*

ii. Gangguan apapun terhadap keberlangsungan fungsi dari sebuah sistem komputer.

[131] Council of Europe, *Explanatory Reports to The Convention on Cybercrime, Loc Cit.* Nomor 81-85.

Dari pemaparan Pasal-Pasal ini, pencurian data pribadi dapat dikategorikan dalam berbagai macam kondisi, yang mengakomodir penegakan yang progresif terhadap tindak pidana siber pencurian data pribadi, sebagaimana terdapat dalam *section* 2 dari Bab 2 *Convention on Cybercrime*. Beberapa contohnya adalah dengan mewajibkan negara anggota untuk mengakui data elektronik sebagai barang bukti dalam sebuah penyelidikan,[132]juga dengan adanya kewenangan tertentu kepada lembaga independen terkait dengan penegakan hukum terkait data dan pelanggaran terhadapnya.[133]

Dalam *section* 3 terdapat pengaturan terkait yurisdiksi yang menjadi bagian integral dari penegakan di bidang siber sebagai kejahatan transnasional. Tercantum dalam Pasal 22 tentang yurisdiksi dimana selain dari penerapan yurisdiksi dalam hal-hal yang biasa diterapkan pada umumnya,[134] konvensi ini menganut asas personalitas aktif dalam penyelesaian penerapan yurisdiksi ekstrateritorial dengan syarat adanya dual kriminalitas. Namun penerapan dari Pasal ini juga tidak ketat karena limitasi yang terdapat dalam ayat setelahnya, contohnya pada ayat 2 yang menyebutkan bahwa para pihak berhak untuk menerapkan atau tidak

[132] *Convention on Cybercrime*, Pasal 14 tentang *Scope of Procedural Provisions.*

[133] *Ibid.* Pasal 19 tentang *Search and Seizure of Stored Computer Data* (Penarikan dan Pengambilan Data Komputer Tersimpan)

[134] Yang dimaksud sebagai penerapan yurisdiksi dalam hal biasa adalah dalam Pasal 22 tentang *Jurisdiction*, konvensi ini memberikan yurisdiksi terhadap kejahatan yang berada: 1. Dalam sebuah teritori negara; 2. Dalam sebuah kapal yang memiliki bendera negara tertentu dan; 3. Dalam sebuah pesawat terbang yang teregistrasi dalam sebuah hukum negara tertentu.

menerapkan peraturan tentang yurisdiksi dalam kondisi dan keadaaan tertentu saja, juga pada ayat 4 yang menyebutkan bahwa konvensi ini tidak mengecualikan yurisdiksi pidana yang diberlakukan dalam hukum domestik negara masing-masing.

Dalam konteks regional khususnya Asia dan Asia Tenggara, kita memiliki *the Asia-Pacific Economic Cooperation (APEC) Privacy Framework* yang dibuat pada tahun 2004 dan direvisi pada tahun 2015. Tujuan dari kooperasi ini adalah untuk meningkatkan perdagangan elektronik di wilayah Asia Pasifik dan untuk mengukuhkan serta menguatkan nilai-nilai privasi bagi individu dan masyarakat informasi.[135] *Framework* ini diambil berdasarkan nilai-nilai inti dari *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data* yang diciptakan oleh *the Organization for Economic Co-Operation and Development* (OECD). Baik APEC *Privacy Framework* 2004 dan revisinya pada tahun 2015, sama-sama memiliki sifat tidak mengikat bagi negara anggotanya. Selain itu kita juga memiliki *ASEAN Declaration to Prevent and Combat Cybercrime*, sebuah deklarasi regional yang menyepakati kebutuhan dari negara-negara di Asia Tenggara untuk sebuah instrumen hukum yang mengakomodasi penegakan hukum lintas

[135] *APEC Privacy Framework 2004*, 16th APEC Ministerial Meeting, Santiago, Chile, 17-18 November 2004, 2004/AMM/014rev1, Agenda Item: V.4.

negara dan penegakan terhadap bukti elektronik untuk memerangi *cybercrime*.[136]

Selain dari instrumen regional yang terbuka diatas, Indonesia juga memiliki perjanjian berbentuk bilateral dengan beberapa negara sebagai upaya untuk mengakomodir jalannya penegakan terhadap kejahatan yang berbasis lintas negara, yakni dengan melakukan perjanjian *Mutual Legal Assistance* atau bantuan hukum timbal balik dengan negara-negara seperti Australia dengan UU No. 1 Tahun 1999,[137]China dengan UU No. 8 Tahun 2006,[138]Hongkong dengan UU No. 3 Tahun 2012,[139]Korea dengan UU No. 8 Tahun 2014, [140]India dengan UU No. 9 Tahun 2014 ,[141]Uni Emirat Arab dengan UU No. 6 2019,[142]dan Swiss dengan UU No. 5 Tahun 2022.[143]Untuk perjanjian bilateral dengan negara anggota ASEAN sendiri, Indonesia baru mengesahkan perjanjian bilateral dengan Republik Sosialis Vietnam dengan

[136] *ASEAN Declaration to Prevent and Combat Cybercrime,* Manila 13 November 2017. 31st Asean Summit. Dapat diakses melalui: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

[137] UU No. 1 Tahun 1999 tentang Pengesahan Perjanjian antara Republik Indonesia dan Australia mengenai Bantuan Timbal Balik Dalam Masalah Pidana.

[138] UU No. 8 Tahun 2006 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Rakyat China mengenai Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

[139] UU No. 3 Tahun 2012 tentang Pengesahan Perjanjian antara Republik Indonesia dan Pemerintah Daerah Administrasi Khusus Hong Kong Republik Rakyat China tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

[140] UU No. 8 Tahun 2014 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Korea tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

[141] UU No. 9 Tahun 2014 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik India tentang Bantuan HukumTimbal Balik Dalam Masalah Pidana.

[142] UU No. 6 Tahun 2019 tentang Pengesahan Perjanjian antara Republik Indonesia dan Persatuan Emirat Arab mengenai Bantuan Timbal Balik Dalam Masalah Pidana.

[143] UU No. 5 Tahun 2022 tentang Pengesahan Perjanjian antara Republik Indonesia dan Konfederasi Swiss tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

UU No. 13 Tahun 2015,[144]sementara lainnya masih didalam tahap pembahasan. Namun perlu diingat betapa vital untuk diperlukannya sebuah konvensi yang bersifat mengikat dalam permasalahan penindakan pidana siber, sebagai upaya kolektif dalam pemberantasan kejahatan ini, dibandingkan dengan peningkatan perjanjian bilateral.

b. Instrumen Nasional

Indonesia memiliki UU No. 27 Tahun 2022 sebagai payung hukum utama dalam regulasi terkait perlindungan data dan serta terkait pencurian data pribadi, dan undang-undang inilah yang akan menjadi analisis utama kita dalam pembahasan mengenai pengaturan hukum terkait dengan pencurian data pribadi terkhusus dalam konteks transnasional.

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, memiliki 76 total Pasal di 15 bab yang merujuk kepada pembahasan berikut:

1) Definisi dan tipe data pribadi;
2) Hak dari pemilik data;
3) Pemrosesan data pribadi;
4) Kewajiban pengontrol data pribadi dan prosesor data pribadi ketika memproses data pribadi;
5) Pengalihan data pribadi;
6) Sanksi administratif;
7) Larangan beberapa penggunaan terhadap data pribadi;

[144] UU No. 15 Tahun 2008 tentang Pengesahan *Treaty on Mutual Legal Assistance in Criminal Matters* (Perjanjian tentang Bantuan Timbal Balik dalam Masalah Pidana)

8) Penyelesaian sengketa menyangkut data pribadi;

9) Kerja sama Internasional;

10) Ketentuan pidana, dan;

11) Peran pemerintah dan publik.[145]

Dari rujukan yang tersebar dalam 15 bab tersebut, dapat kita telusuri pengaturan baik preventif dan juga represif terhadap tindak pidana pencurian data pribadi. Namun, perlu kita ketahui terlebih dahulu apa yang didefinisikan sebagai data pribadi dalam UU No. 27 Tahun 2022. Menurut definisi yang didapat pada Pasal 4, data pribadi dikategorikan menjadi dua jenis yakni data pribadi bersifat sensitive dan bersifat umum. Perbedaan ini didasari oleh dampak yang lebih besar terhadap data sensitive kepada subjek data pribadi tersebut, antara lain tindakan diskriminatif dan kerugian yang lebih besar dibandingkan dengan data yang bersifat umum.[146]Adapun data sensitive tersebut merupakan data-data seperti:[147]

1) Data dan informasi kesehatan, dimana penjelasan dari data dan informasi kesehatan adalah catatan atau keterangan individu yang berkaitan dengan kesehatan fisik, kesehatan mental, dan/atau pelayanan kesehatan;

[145] Muhammad Firdaus, *A Review of Personal Data Protection Law in Indonesia*, Artikel *Interdisciplinary Program of Information Security, Graduate School PKNU,* diakses pada 10 Desember 2022 melalui: https://osf.io/tmnwg/download

[146] Penjelasan atas UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi Pasal 4 (1) huruf a.

[147] Penjelasan atas UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi Pasal 4(2) huruf a-f

2) Data biometrik, dimana penjelasan dari data biometrik adalah data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identilikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk narnun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA.

3) Data genetika, merupakan semua data jenis apa.pun mengenai karakteristik suatu individu yang diwariskan atau diperoleh selama perkembangan prenatal awal;

4) Catatan kejahatan, merupakan catatan tertulis tentang seseorang yang pernah melakukan perbuatan melawan hukum atau melanggar hukum atau sedang dalam proses peradilan atas perbuatan yang dilakukan, antara lain catatan kepolisian dan pencantunan dalam daftar pencegahan atau penangkalan;

5) Data anak, meskipun penjelasan dari data ini sangatlah krusial, namun penulis tidak menemukan penjelasan apapun terhadap jenis data ini, sehingga bisa kita asumsikan bahwa seluruh data yang dapat digunakan untuk mengidentifikasikan atau dikombinaksikan untuk mengidentifikasi seorang anak merupakan data sensitive;

6) Data keuangan pribadi, adalah termasuk narnun tidak terbatas kepada data jumlah simpanan pada bank termasuk tabungan, deposito, dan data kartu kredit;

7) Data lainnya sesuai dengan ketentuan perundang-undangan, yang bisa diartikan data-data yang diatur dalam undang-undang beserta peraturan turunannya yang dapat digunakan dalam mengidentifikasi seseorang.

Sementara, data non-spesifik atau disebut sebagai data umum adalah data yang dapat digunakan untuk mengidentifikasi seseorang namun dengan dampak yang secara relatif tidak besar terhadap subjek data pribadi. Data tersebut adalah:

1) Nama lengkap;
2) Jenis kelamin;
3) Kewarganegaraan;
4) Agama;
5) Status perkawinan; dan/atau
6) Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang, dengan contoh berupa nomor seluler atau alamat IP (*internet protocol*).

Klasifikasi jenis data ini sesuai dengan implementasi hukum pelindungan data di berbagai instrumen internasional, contohnya dalam pedoman *OECD* 1980 pada bagian/bab 4 tentang implementasi nasional huruf

e,[148]serta pedoman perserikatan bangsa-bangsa tentang regulasi untuk data komputer pribadi.[149]Serupa juga dengan instrumen hukum regional seperti GDPR (*general data protection regulation*) yang digunakan oleh negara-negara anggota Uni Eropa,[150] namun perbedaannya adalah agama/keyakinan seseorang ditempatkan dalam kategori umum, sementara pada instrumen lainnya klasifikasi keyakinan/agama umumnya diletakkan dalam data yang bersifat spesifik.

Masuk kepada inti dari permasalahan, yakni pengaturan terkait pencurian data pribadi. Hal ini dapat kita temukan dalam bab 13 tentang larangan dalam penggunaan data pribadi dalam UU No. 27 Tahun 2022 dalam Pasal 65 yang berbunyi:

1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
2) Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.

[148] OECD Guidelines on the Protection of Privacy and Transborder Flows of Data. Bagian 4 huruf (e), *ensure that there is no unfair discrimination against data subjects*/menjamin tidak ada diskriminasi tidak adil terhadap subjek data.

[149] UN Guidelines for the Regulation of Computerized Personal Data Files, Huruf A, No. 5.

[150] EU General Data Protection Regulation 2016/679 No. (51).

Serta Pasal 65 dalam undang-undang sama yang berbunyi:

1) Setiap orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

Dalam hal terjadi pencurian atau kebocoran terhadap data pribadi, umumnya terdapat sebuah kewajiban dari pengendali data pribadi untuk memberitahukan kegagalan ini kepada pemilik data pribadi yang disebut sebagai *Security Breach Notification*, hal ini diakomodir oleh UU No. 27 Tahun 2022 dalam Pasal 46 yang berbunyi:

1) Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada:
    a) Subjek Data Pribadi; dan
    b) lembaga.
2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat:
    a) Data Pribadi yang terungkap;
    b) Kapan dan bagaimana Data Pribadi terungkap; dan
    c) Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.

3) Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.

Lalu definisi terkait kegagalan Pelindungan Data Pribadi ini dijelaskan sebagai ‘kegagalan melindungi Data Pribadi seseorang dalam hal kerahasiaan, integritas dan ketersediaan Data Pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang dikirim, disimpan, atau diproses.’[151]Lalu dalam hal tertentu merupakan ‘jika kegagalan Pelindungan Data Pribadi menganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat.’[152]Bisa kita simpulkan bahwa kewajiban ini mengikat tidak hanya kepada swasta namun juga terhadap lembaga pemerintah yang menggunakan data pribadi dalam kegiatannya. Hal ini dapat dilihat dalam Pasal 2 (1) yang menyatakan bahwa:

1) Undang-Undang ini berlaku bagi Setiap Orang, Badan Publik, dan Organisasi Internasional yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini:
    a) yang berada di wilayah hukum Negara Republik Indonesia, dan;

[151] Penjelasan UU No. 27 Tahun 2022 Pasal 46 (1).
[152] Penjelasan UU No. 27 Tahun 2022 Pasal 46 (3)

b) di luar wilayah hukum Negara Republik Indonesia, yang memiliki akibat hukum:

i. di wilayah hukum Negara Republik Indonesia; dan/atau

ii. bagi Subjek Data Pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia.

Selain berlaku kepada setiap organ baik swasta maupun pemerintahan, dari pengaturan ini juga dapat kita simpulkan bahwa pemerintah mencoba untuk membuat peraturan ini bersifat ekstrateritorial, dengan catatan selama peristiwa hukum tersebut memiliki dampak kepada warga negara Indonesia atau subjek lain yang berada di bawah naungannya. Hal ini tentu saja membutuhkan kooperasi dengan negara lain, khususnya dalam hal penegakan. Dalam bab 10 Pasal 62 tentang 'kerja sama internasional' bisa kita temukan kerangka kooperasi tersebut yang berbunyi:

1) Kerja sama internasional dilakukan Pemerintah dengan pemerintah negara lain atau Organisasi Internasional terkait dengan Pelindungan Data Pribadi;
2) Kerja sama Internasional dalam rangka pelaksanaan Undang-Undang ini dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan dan prinsip hukum internasional.

Undang-Undang ini berlaku disamping dari 49 peraturan sektoral lainnya dari pengaturan Pelindungan Data Pribadi di Indonesia, dimana

peraturan ini akan menjadi *lex specialis*, berperan sebagai rujukan utama ketika menyinggung pengaturan terkait data di Indonesia.

2. Analisa Terhadap Pengaturan Pelindungan Data Pribadi Indonesia dalam hal Pencurian Data Pribadi

Dalam sub-bab ini kita akan membedah beberapa permasalahan yang terjadi dalam UU No. 27 Tahun 2022 sebagai payung hukum pengaturan pelindungan data pribadi di Indonesia. Permasalahan pertama merupakan ketiadaan lembaga otoritas yang bersifat independent dan keberadaan sebuah panduan teknis terkait pelindungan dari data pribadi. Ketiadaan ini akan berdampak pada penggunaan pasal pelindungan data pribadi yang tidak sesuai dengan penggunaannya. Contohnya merupakan pasal tentang larangan penggunaan data pribadi yakni memperoleh/mengumpulkan, mengungkapkan, menggunakan dan memalsukan data pribadi yang bukan miliknya secara melawan hukum. Dibutuhkan suatu panduan teknis terkait dengan macam-macam bentuk perolehan/pengumpulan, pengungkapan, penggunaan dan pemalsuan data pribadi yang adalah melawan hukum, mengingat bahwa UU ini ditujukan tidak hanya untuk dokumen konvensional atau non-elektronik semata, melainkan ditujukan untuk dokumen elektronik sehingga dibutuhkan panduan teknis, dimana ketiadaan dari panduan ini dapat berakibat pada kebingungan, kesalahan pendefinisian, serta kesalahan penegakan oleh aparatur penegak hukum.

Sebagai contoh kita ambil dalam model lembaga otoritas data yang diatur dalam *General Data Protection Regulation* Uni Eropa, dalam

Pasal/*article* 51 tentang *Supervisory Authority* dimana setiap negara anggota berkewajiban untuk membuat otoritas publik independen yang bertanggung jawab terhadap pengawasan implementasi dari *GDPR*. Bila kita bandingkan terhadap kelembagaan dari otoritas pengawas data yang dirancang dalam UU No. 27 Tahun 2022, dalam Bab IX Kelembagaan Pasal 58, 59, dan 60 yang menjelaskan terkait lembaga yang bertanggungjawab dalam otoritas data, menyatakan bahwa "(3) Lembaga sebagaimana dimaksud dalam ayat 2 ditetapkan oleh presiden", dan "(4) Lembaga sebagaimana dimaksud dalam ayat 2 bertanggung jawab kepada presiden."[153]Lebih lanjut lagi, ketentuan-ketentuan lainnya akan diatur dalam Peraturan Presiden menurut ayat 5 dari Pasal yang sama. Dalam Pasal 60, yang menjelaskan terkait pelaksanaan kewenangan dari lembaga ini dengan materi berupa penyusunan dan penetapan kebijakan dalam bidang data pribadi, penjatuhan sanksi administratif oleh lembaga, model kerjasama dengan lembaga perlindungan data negara lain dalam penegakan pelanggaran data lintas negara, dan materi-materi lainnya yang tercantum dalam Pasal 60 ini akan diatur dalam Peraturan Pemerintah.[154]

Apabila kita bandingkan dengan independensi yang dimiliki oleh lembaga otoritas data *GDPR*, dengan diaturnya baik tugas dan kewenangan dalam lembaga tersebut didalam regulasi tersebut akan menjamin kekuatan dan kewenangan dari lembaga tersebut bahkan ketika menindak pelanggaran

[153] Pasal 58 UU No. 27 Tahun 2022 Ayat 3 dan 4.
[154] Pasal 61 UU No. 27 Tahun 2022

yang dilakukan oleh badan negara/publik.[155] Hal ini juga akan menjadi penentuan bagi kekuatan atau kelayakan (*adequacy*) dari UU No. 27 Tahun 2022, dimana Amerika Serikat dalam laporannya menunjukkan kekhawatiran atas aplikasi Peduli Lindungi, yang digunakan untuk mengumpulkan data pribadi masyarakat dalam hal penyimpanan dan penggunaan.[156] Dalam hal tersebut, apabila lembaga pengawasan data secara yuridis tidak memiliki independensi, maka kadar kepercayaan dan legitimasi dari pengawasan terhadap institusi publik juga rawan akan bias hukum. Kasus lainnya yang merupakan kelalaian dari pemerintah terhadap pelindungan data pribadi adalah bocornya data aplikasi E-HAC pada Agustus 2021 dengan jumlah sebesar 1.3 juta data pengguna E-HAC yang dijualbelikan di *darkweb* bernama *raidforum*.[157] Hal ini membuktikan lemahnya pengawasan terhadap penggunaan data yang dilakukan oleh pemerintah, yang juga membutuhkan pengawasan dan pengendalian yang independen dari sebuah komisi/lembaga pengawas data.

Pedoman terkait tindakan pidana dalam ranah siber dapat kita temukan dalam Konvensi *Cybercrime* atau Konvensi Budapest beserta laporan penjelasannya (*explanatory report*) yang secara spesifik menjelaskan hal-hal apa saja yang merupakan bentuk-bentuk dari tindak pidana siber, serta

[155] *Article* 57 & 58 *General Data Protection Regulation.*

[156] *2021 Country Reports on Human Rights Practices: Indonesia*. Diakses dari: https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/indonesia/

[157] Jihyun Park, Dodik Setiawan Nur Heriyanto, *In Favor of an Immigration Data Protection Law in Indonesia and Its Utilization for Contact Tracing.* Prophetic Law Review Vol. 4 Issue 1, Juni 2022. Hal. 14.

penjelasan dari ruang lingkup penegakan terhadapnya. Atas dasar hal tersebut, pemerintah harus segera membuat peraturan pelaksana yang mencantumkan teknikalitas tersebut agar penegakan hukum dalam konteks siber menjadi terarah dan sistematis.

Permasalahan kedua adalah ketidakjelasan beberapa diksi dalam UU No. 27 Tahun 2022 yang bisa menimbulkan permasalahan dalam penerapannya dalam dunia internasional. Contohnya terdapat dalam Bab VII tentang 'Transfer Data Pribadi ke Luar Wilayah Hukum Negara Republik Indonesia'. Dalam Pasal 56 ayat 2 disebutkan bahwa dalam melakukan transfer data tersebut harus dipastikan bahwa negara tempat penerima transfer tersebut memiliki pelindungan data pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini, namun sampai saat ini tidak ada kejelasan terkait kualifikasi apa yang menjadi tingkatan keamanan tersebut. Meskipun pengaturan mengenai ketentuan tersebut akan diatur lebih lanjut dalam Peraturan Pemerintah, didalamnya harus mengatur secara rinci tingkatan apa saja yang menjadi prasyarat bagi transfer tersebut. Serta lembaga pengawas data yang akan dibentuk juga harus secara aktif memantau transfer data yang berlangsung.

Permasalahan ketiga merupakan kerja sama internasional yang dicanangkan oleh pemerintah belum memiliki landasan yuridis yang kuat. Apabila pembuatan perjanjian hukum bertimbal balik (*Mutual Legal Assistance)* menjadi sebuah solusi maka bisa dibayangkan berapa lama penegakan hukum terkait pencurian data dapat direalisasikan. Selain itu juga,

perjanjian tersebut tidak memiliki kesamaan antara satu dengan lainnya dan memiliki variabel yang tinggi karena harus menyesuaikan dengan hukum domestik masing-masing negara. Contohnya adalah pada UU No. 5 Tahun 2020 tentang pengesahan perjanjian Indonesia dengan Swiss tentang bantuan hukum timbal balik dalam masalah pidana. [158]Ketidakefektifan ini lacak dari sifat tindak pidana siber yang bersifat *borderless,* yang artinya pelaku dari kejahatan siber tidak akan jarang untuk berada di berbagai negara dalam satu kasus yang sama. Alhasil dapat dikatakan tidak tepat untuk mendasarkan kerja sama terkhusus dalam penegakan pencurian data didasari oleh perjanjian jenis tersebut.

B. Implementasi Prinsip Yurisdiksi Ekstrateritorial terhadap Pelaku Tindak Pidana Siber Pencurian Data Pribadi Secara Lintas Batas Negara

Sebagaimana telah dibahas sebelumnya bahwa tindak pidana siber merupakan suatu kejahatan yang bersifat *borderless* atau tanpa batasan, artinya yurisdiksi menjadi suatu penghalang bagi penegakan terhadap pelaku tindak pidana siber/*cybercrime*. Skala dari potensi pelaku dari tindak pidana siber ini tidak dapat kita klasifikasikan menjadi sebuah kelompok tertentu saja, dikarenakan skala dari kejahatan siber itu sendiri adalah global atau seluruh dunia, selama terjaring atau terkoneksi melalui jaringan internet.

[158] Lampiran UU No. 5 Tahun 2022 Bab II tentang Permintaan Bantuan Hukum Timbal Balik, Pasal 5 tentang Hukum yang berlaku, yang berbunyi “Permintaan harus dilaksanakan seusai dengan hukum nasional negara yang diminta”.

Maka dari itu, sebagaimana UU No. 27 Tahun 2022 sebagai payung hukum dalam pelindungan data pribadi menyebutkan dalam Pasal 2 bahwa UU tersebut berlaku baik didalam maupun diluar wilayah hukum Indonesia, selama menyangkut warga negara Indonesia.

Adapun demikian, implementasi dari yurisdiksi ekstrateritorialitas ini memang dianggap belum realistis, karena pada dasarnya UU yang dipakai dalam pelindungan data pribadi sebelum munculnya UU No. 27 Tahun 2022 yakni UU No. 19 Tahun 2019 tentang perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur hal yang sama pada Pasal 2 UU tersebut.[159]Pengaturan tersebut juga tidak membuahkan hasil yang efektif terhadap penegakan dari pencurian data pribadi dimana keduanya tidak memiliki kekuatan apapun dalam menegakkan yurisdiksi Indonesia diluar wilayah hukum Indonesia, dengan tidak adanya instrumen hukum internasional untuk menetapkan yurisdiksi Indonesia.

Hal ini dapat menimbulkan impunitas terhadap pelaku-pelaku tindak pidana siber yang dilakukan secara transnasional sebagaimana kasus yang dimiliki oleh Amerika Serikat dan Filipina pada tahun 2000 yakni '*I Love You'* virus. Kasus ini dimulai ketika seorang mahasiswa di Filipina Onel de

[159] Pasal 2 UU No. 19 Tahun 2019 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: "*Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia*".

Guzman yang merancang sebuah program untuk mencuri password akun internet, men-scan komputer untuk *log-in* password, menghancurkan data gambar dan suara, serta menyebarkan program virus secara otomatis kepada seluruh kontak dalam email tersebut. Alhasil, virus ini menimbulkan kerugian sebesar 10 milliar dollar, menyusupi sistem komputer dari setidaknya 14 agensi federal di Amerika Serikat, serta sistem parlemen Britania, Belgia, dan organisasi internasional. [160]Ketika de Guzman berhasil dilacak, pemerintahan Filipina yang pada awalnya menuntut de Guzman harus mencabut gugatannya dikarenakan Filipina tidak memiliki undang-undang tentang peretasan komputer, sementara pemerintah Amerika Serikat sendiri tidak bisa mengektradisi de Guzman karena tidak terpenuhinya syarat dual kriminalitas/kriminalitas ganda. Pada akhirnya, de Guzman mendapatkan impunitas dari tindakannya tersebut,[161] Apabila kita analisa, ketiadaan basis hukum Amerika untuk menetapkan yurisdiksinya merupakan penghalang bagi penegakan kasus ini. Dari penyebab ini penulis berpendapat bahwa keberadaan sebuah instrumen hukum yang diakui secara global menjadi salah satu faktor untuk keberhasilan penerapan yurisdiksi ekstrateritorial khususnya di bidang tindak pidana siber. Dalam konvensi Budapest Pasal 27 tentang Prosedur untuk pelaksanaan bantuan hukum bertimbal balik dalam

[160] *The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack: Hearing Before the Subcomm. on Tech. of the H. Comm. on Sci*, 106th Cong. 12 (2000) (pernyataan dari Keith A. Rhodes, Direktur dari Office of Computer and Information Technology Assessment Amerika Serikat).

[161] Alexandra Perloff-Girles, *Transnational Cyber Offenses: Overcoming Jurisdicitional Challenges.* 43 Yale Journal of International Law No. 191. 2018.

ketiadaan persetujuan/instrumen internasional,[162]dimana ditetapkan sebuah basis hukum yang dapat digunakan dalam kondisi yang dimiliki oleh Amerika Serikat dan Filipina, yakni sebuah ketiadaan landasan hukum internasional untuk digunakan.

Permasalahan terkait yurisdiksi merupakan masalah vital yang didapatkan dalam penegakan terkait dengan tindak pidana siber, dikarenakan lokasi geografis, skala perbuatan, dan unsur lain yang menjadikan tindak pidana siber berbeda dari pidana konvensional lainnya, membuat implementasi dari prinsip-prinsip yurisdiksi sulit untuk diterapkan. Kesulitan dari penegakan terhadap kejahatan lintas negara ini dapat diklasifikasikan menjadi tiga factor yakni kesulitan dalam penggunaan barang bukti, kesulitan dalam investigasi, dan kesulitan dalam melakukan pengadilan terhadap pelaku lintas negara.[163] Serupa, pandangan dari Barbara Etter menjelaskan terkait kesulitan dalam timbulnya masalah yurisdiksi dalam kejahatan siber transnasional yakni:[164]

1) Ketiadaan konsensus global mengenai jenis-jenis kejahatan komputer. Klasifikasi dari hukum domestik negara menyangkut permasalahan komputer cukup berbeda, seperti yang dibahas

[162] *Convention on Cybercrime, Art. 27 Procedure pertaining to mutual assistance request in the absence of applicable international agreements.*

[163] Ermanto Fahamsyah, Vicko Taniady, Kania Venisa Rachim, Novi Wahyu Riwayanti. *Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention.* Jurnal Hukum dan Syariah De Jure, Vol. 14 No. 1 2022. Hal. 150.

[164] Barbara Etter dalam *Critical Issues in High Tech Crime*. Dikutip dari Barda N. Arief, *Tindak Pidana Mayantara Perkembangan Cybercrime di Indonesia.* Jakarta: PT. Raja Grafindo Persana, 2006. Hal. 108.

dalam landasan teori mengenai *cybercrime*. Artinya, sebuah instrumen hukum yang menyatukan perbedaan tersebut harus hadir dalam rangka penyelenggaraan penegakan terhadap tindak pidana siber.

2) Kurangnya kualitas para penegak hukum terhadap penanganan tindak pidana siber.
3) Sifat transnasional yang dimiliki
4) Ketidakharmonisan hukum acara domestik negara terkait tindak pidana siber
5) Ketiadaan upaya sinkronisasi dalam penegakan dan penanganan tindak pidana siber (dalam hal ekstradisi, investigasi, dan upaya bantuan lainnya).

Sebagai solusi dari permasalahan ini, banyak pakar menyarankan untuk menganggap dunia siber sebagai sebuah ruang yang terpisah dari kedaulatan negara konvensional. Sebuah tulisan karya Joel P. Trachman menyatakan kesinambungan antara ruang siber dan kedaulatan negara, dimana dia berpendapat bahwa ruang siber merupakan sebuah ruang netral yang tidak menyokong maupun menyerang kedaulatan negara manapun.[165]Atas dasar tersebut, ruang siber harus diberlakukan dengan

[165] Joel P. Trachman. *Cyberspace, Sovereignty, Jurisdiction and Modernism.* Indiana Journal of Global Legal Studies Vol. 5, Issue 2, Art. 10, 1998. Hal. 564-565

parameter untuk pengelolaan/pemerintahan global, yakni pengaturan bersama yang didasari dengan beberapa parameter yakni:[166]

1) Pengalokasian pengaturan terkait yurisdiksi untuk negara-negara;
2) Harmonisasi regulasi terkait penegakan tindak pidana siber;
3) Sentralisasi organisasi yang berperan dalam pembuatan kebijakan dan kegiatan penegakan hukum terkait tindak pidana siber.

Parameter tersebut dapat menjadi solusi untuk mengatasi sulitnya penegakan hukum terhadap tindakan pada ruang siber, khususnya pencurian data pribadi dalam konteks transnasional. Pada poin ke 1 dan 2 dapat kita laksanakan dengan meratifikasi sebuah instrumen hukum internasional yang memiliki volume massa yang cukup memadai dan terbuka secara universal, yakni meratifikasi konvensi Budapest atau *Convention on Cybercrime* atau setidak-tidaknya, menginisiasikan model perjanjian multinasional dengan kerangka hukum Konvensi Budapest. Didalam konvensi tersebut terdapat pengaturan terkait yurisdiksi yang dapat dijadikan sebuah patokan dalam penggunaan dan konflik dalam penentuan. Selain itu. CoE juga menjadi metode harmonisasi bagi pengaturan terkait penegakan tindak pidana siber dengan spesifikasi penentuan hukum yang dipakai, dan pengakomodasian kerjasama internasional, ekstradisi, serta bantuan hukum lainnya.[167]

Dalam poin 3 dari parameter diatas yaitu keberadaan sebuah organ sentral dalam masalah penanganan tindak pidana siber dapat kita artikan

[166] *Ibid.* Hal. 570.
[167] Konvensi Budapest/*Convention on Cybercrime* Bab 3 tentang Kooperasi Internasional

dalam kancah domestik maupun internasional. Dalam ranah domestik, organ ini akan menjadi pengawas dan pengendali dalam sektor pelindungan data, serta penegakan terhadap pelanggarannya. UU No. 27 Tahun 2022 sudah menyiapkan rancangan pembuatan lembaga khusus yang akan mengawasi dan menegakkan fungsi pelindungan data, namun yang menjadi permasalahan adalah independensi dari lembaga yang dibuat. Hal ini disebabkan oleh struktur yang dimiliki oleh lembaga berada dibawah kewenangan eksekutif, sementara pada praktik umumnya negara-negara yang menggunakan GDPR sebagai model acuan membuat lembaga otoritas data ini menjadi independen, untuk mengawasi peran dari pemerintahan dalam pelindungan data.

Dalam konteks internasional, organ ini menjadi pusat untuk penegakan tindak pidana siber dalam konteks global, serta mengkonsolidasikan standar operasi atau pembuatan kebijakan yang bersifat preventatif dan responsif terhadap perkembangan penegakan tindak pidana siber. Dalam pendapat penulis, satu-satunya organ internasional yang dapat memiliki kekuatan tersebut adalah Perserikatan Bangsa-Bangsa, namun sampai saat ini belum ada instrumen mengikat dari PBB terkait upaya penanggulangan tindak pidana siber.

Sementara dalam fungsi penegakan, interpol sudah menjadi sarana koordinasi bagi penegakan upaya hukum terkait tindak pidana siber, serta pelatihan untuk negara anggota dalam penanganan tindak pidana siber. Salah satu contoh implementasi dari kooperasi yang berbasis penegakan kolaboratif

adalah operasi Avalanche, sebuah operasi kolaboratif antara interpol dan 30 negara lainnya dalam mengungkap dan menjatuhkan infrastruktur criminal siber yang telah menghasilkan kerugian senilai 6 juta Euro,[168] serta operasi Goznym, dinamakan atas sebuah malware yang disebar kepada institusi keuangan dan menghasilkan kerugian diatas seratus juta USD, yang berhasil meruntuhkan jaringan sindikat siber tersebut.[169]Hal ini dapat kita lakukan dengan dasar memiliki instrumen hukum binding/mengikat yang akan mengakomodasi kerjasama internasional dalam penegakan terhadap tindak pidana siber khususnya dalam bentuk pencurian data pribadi, yakni Konvensi Budapest atau *Convention on Cybercrime*.

Penerapan yurisdiksi ekstrateritorial terhadap warga negara asing yang melakukan tindak pidana siber yang berdampak secara transnasional juga dilakukan oleh Amerika Serikat terhadap suatu grup/organisasi *cybercriminal* yang bergerak dalam *carding*, pencurian identitas dan pencurian data finansial yang kemudian dijual dalam sebuah situs *darkweb*.[170]Penangkapan dan penutupan dari organisasi tersebut dilakukan dalam sebuah operasi gabungan bernama *Operation Shadow Web*, terdiri dari Amerika Serikat, negara-negara Eropa, Australia, dan negara Asia. Pelaku dari kejahatan ditangkap di beberapa negara seperti Australia, UK, Prancis, Italia, Kosovo,

[168]Dikutip dari: https://www.interpol.int/ar/1/1/2016/Avalanche-network-dismantled-in-international-cyber-operation

[169]Dikutip dari: https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

[170] United States District Court, D. Nevada: United States of America v Svyastoslav Bondarenko. Case No. 2:17-CR-306 JCM, 12 Juni 2019.

Serbia dan Amerika Serikat pada tahun 2018 silam.[171] Salah satu dari pelaku yakni Syvastoslav Bondarkeno, yang berkewarganegaraan Ukraina, dituntut dan diadili di pengadilan distrik Nevada, Amerika Serikat berdasarkan kejahatannya dengan menggunanan *extraterritorial application* dari statuta RICO (*Racketeerr Influenced and Corrupt Organizations Act)*. Patut diingat bahwa Amerika Serikat juga merupakan anggota dari konvensi Budapest, yang memudahkan koordinasi dan penggunaan instrumen penegak seperti Interpol sebagaimana disebutkan dalam *press release* kementerian kehakiman Amerika Serikat.[172] Selain Bondarkeno, Amerika Serikat juga menuntut lebih dari 30 pelaku lainnya yang berasal dari berbagai kenegaraan, contohnya Makedonia, Mesir, Pakistan, UK, Pantai Gading, Australia, dan lain-lain.

Harapan akan penegakan Pasal 2 UU No. 27 Tahun 2022 dimana kita dapat menerapkan yurisdiksi ekstrateritorial terhadap pelindungan data pribadi bagi warga negara Indonesia hanyalah angan belaka tanpa suatu instrumen hukum yang mengakomodir hal tersebut. Yurisdiksi akan tetap menjadi masalah utama dalam penegakan pencurian data pribadi lingkup

[171] The United States Departemen of Justice (DoJ) Press Release, *Thirty-six Defendants for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrime.* 7 Februari 2018. Diakses dari: https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

[172] Dalam Pasal 27 ayat (9) huruf b Konvensi Budapest/*Convention on Cybercrime*, Interpol merupakan salah satu instrumen koordinasi dan komunikasi penegakan hukum berbasis transnasional bagi negara anggota. "*Any request or communication under this paragraph may be made through the International Criminal Police Organisation* (Interpol) "

transnasional. Jawaban atas hal tersebut penulis ajukan dalam Konvensi Budapest didalam muqadimahnya yang menyatakan:

" *Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation ... Believing that an effective fight against cybercrime requires increased, rapid and wellfunctioning international co-operation in criminal matters"*[173].

Yang menyatakan atas dasar keharusan untuk mengejar sebuah kebijakan pidana yang serupa untuk melindungi masyarakat, dimana salah satu caranya adalah dengan mengadopsi regulasi yang memadai dan mengembangkan kooperasi internasional, juga bahwa perlawanan terhadap tindak pidana siber memerlukan peningkatan kerja sama internasional, cepat/pesat dan berfungsi dengan baik.

[173] Pembukaan Convention on Cybercrime Paragraf 4 dan 8.

BAB IV

PENUTUP

A. Kesimpulan

1. Pengaturan terhadap tindak pidana siber pencurian data pribadi di Indonesia saat sekarang telah dipayungi oleh UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, disamping ketentuan-ketentuan internasional yang menengarai pelindungan data serta aturan siber seperti konvensi Budapest. Muatan dalam UU tersebut memiliki pengaturan dimulai dari hak-hak subjek data, kewajiban prosesor dan pengendali subjek data, serta pengaturan tentang lalu lintas transfer data, struktur kelembagaan pengawas data, larangan penggunaan data, sanksi administrative dan pidana, juga ketentuan mengenai kerja sama internasional. Alhasil, UU ini merupakan langkah yang tepat bagi Indonesia akan tetapi bukan menjadi tujuan akhir melainkan sebuah awal bagi pelindungan terhadap data pribadi. Terdapat beberapa catatan kritis bagi UU ini khususnya dalam hal preventasi dan penegakan terhadap pencurian data pribadi. Yang pertama adalah diperlukannya rancangan aturan teknis terkait bentuk-bentuk dari pelanggaran terhadap data pribadi agar menjadi pedoman bagi penegakan hukum dan masyarakat dalam menyadari eksistensi dari tindak pidana siber. Hal ini bertujuan agar aparat dan masyarakat mengetahui apa saja yang dianggap sebagai tindak pidana khususnya dalam masalah pelanggaran terhadap data pribadi dan tidak asal dalam mengaplikasikan hukum

tersebut. Yang kedua merupakan bentuk kerja sama internasional yang dirancang dalam UU No. 27 Tahun 2022 perlu ditindak lanjuti dengan strategi yang baik untuk menanggulangi masalah pencurian data pribadi baik dalam ranah domestic maupun transnasional. Sampai sekarang Indonesia hanya memiliki perjanjian MLA (*mutual legal assistance)* dengan beberapa negara baik di wilayah Asia Tenggara dan diluarnya sebagai instrumen kerja sama internasional untuk mengaplikasikan penegakan hukum ekstrateritorial, namun cara tersebut memakan waktu dan biaya yang sangat tidak efisien, belum juga menilai efektifitas dari perjanjian tersebut yang relatif tidak berdampak dalam penegakan hukum di bidang siber. Sinergi antara instrumen hukum nasional dan internasional menjadi penentu untuk menjadikan pelindungan data terhadap tindak pidana siber khususnya pencurian data pribadi yang dilakukan secara lintas batas negara dapat dilakukan secara maksimal dan berkelanjutan.

2. Dalam hal penerapan yurisdiksi ekstrateritorial untuk penegakan terhadap pelaku tindak pidana pencurian data pribadi sebagaimana ditujukan oleh UU No. 27 Tahun 2022 dalam Pasal 2, hal ini mustahil dilakukan tanpa instrumen hukum yang kuat dan mengakomodasi mobilisasi negara dalam penegakan, dikarenakan unsur dari *cybercrime* itu sendiri yang tidak dapat diprediksi baik lokasi maupun potensi skala dari perbuatannya. Solusi dari ini adalah meratifikasi satu-satunya konvensi mengikat terkait dengan tindak pidana siber yakni *Council of*

Europe Convention on Cybercrime beserta protokol tambahan ke-2 yaitu protokol terkait peningkatan kooperasi dan pengungkapan bukti elektronik. Konvensi *Cybercrime* beserta protocol tambahannya dapat menjadi alat yang memudahkan Indonesia dalam menerapkan yurisdiksi ekstrateritorial untuk menanggulangi dan menegakkan hukum terkait pencurian data pribadi dalam konteks transnasional.

B. Saran

1. Penulis menyarankan agar pemerintah menyiapkan segala alat kelengkapan yang dibutuhkan dalam pengawasan dan penegakan pelindungan data pribadi seperti komisi/lembaga pengawas data yang merujuk kepada perkembangan teknologi dan dunia siber serta memberikan pemahaman kepada aparat dan masyarakat terkait bentuk ancaman terhadap data pribadi.
2. Penulis juga menyarankan agar pemerintah meratifikasi Konvensi Budapest tentang *cybercrime* dan Protokol tambahan ke-2 sebagai tindak lanjut dari UU Pelindungan Data Pribadi dalam bentuk kerja sama internasional serta menggunakannya sebagai basis/instrumen hukum internasional dalam mengaplikasikan yurisdiksi ekstrateritorial terhadap penegakan dari UU Pelindungan Data Pribadi kepada pelanggar lintas batas negara.

DAFTAR PUSTAKA

A. Buku

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Jakarta: PT. Refika Aditama, 2005.

Agus Raharjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bandung: Citra Aditya, 2002.

Ahmad Abdi Amsir, *Perjanjian Westphalia dan Momentum Pendirian Negara Modern,* dalam Jurnal Sulesana Vol. 15 No *Principles of Public*. (2021)

Al. Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika,* Yogyakarta: Penerbit Atma Jaya, Cet. Ke-5, 2014.

Burhan Bungin, *Pornomedia: Konstruksi Sosial Telematika dan Perayaan Seks di Media Massa*. Jakarta: Prenada Media, 2003.

Ian Brownlie, *International Law*, Oxford: Clarendon Press, 1990,.

Jawahir Thontowi, Pranoto Iskandar, *Hukum Internasional Kontemporer,* Bandung: PT. Refika Aditama, 2016.

John O'Brien, *International Law,* Great Britain: Cavendish Publishing Limited, 2004.

Joanna Buick dan Zoran Jevtic, *Mengenal Cyberspace for Beginners.* Bandung: Penerbit Mizan, 1997.

Jonathan Clough, *Principles of Cybercrime.* Cambridge: Cambridge University Press. 2015

Kenneth S. Gallant, *International Criminal Jurisdiction: Whose Law Must We Obey?* New York: Oxford University Press, 2022.

Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges, and Legal Response.* International Telecommunications Union, 2012.

Romli Atmasasmita, *Dampak Ratifikasi Konvevnsi Tranasnational Organized Crime (TOC),* Jakarta: Penerbitan Badan Pembinaan Hukum Nasional Departemen Kehakiman dan Hak Asasi Manusia RI, 2004.

Rothwell, Donald R., Stuart Kaye, Afshin Akhtarkhavari, dan Ruth Davis. *International Law: Cases and Materials with Australian Perspectives*. Cambridge: Cambridge University Press, 2010.

Sefriani, *Hukum Internasional: Suatu Pengantar*, Edisi ke-2, Cet. 6. Jakarta: Rajawali Press, 2016.

Suherman, Musnaini, Hadion Wijoyo, dan Irjus Indrawan. *Industry 4.0 vs. Society 5.0.* Purwokerto: CV. Pena Persada, 2020.

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara.* Yogyakarta: CV. Aswaja Pressindo, 2013.

Widodo, *Memerangi Cybercrime: Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*. Yogyakarta: CV. Aswaja Pressindo, 2013.

B. Jurnal

Alan Westin, *Privacy and Freedom*. New York: Atheneum Press. 1967, dan David Flaherty, *Privacy in Colonial New England.* Charlottesville: University of Virginia Press. 1972.

Alexandra Perloff-Girles, *Transnational Cyber Offenses: Overcoming Jurisdicitional Challenges*. 43 Yale Journal of International Law No. 191. 2018.

Barda N. Arief, *Tindak Pidana Mayantara Perkembangan Cybercrime di Indonesia.* Jakarta: PT. Raja Grafindo Persana, 2006.

Bert-Jaap Koops & Ronald Leenes, *ID Theft, ID Fraud and/or ID Related Crime. Definitions Matter.* Jurnal Datenschutz und Datensicherheit Vol. 9.

Charles Fred, *Privacy.* Yale Law Journal No. 77, 1968.

Christine van den Wyngaert, *Double Criminality as a Requirement to Jurisdiction. Nordisk Tidsskrift for Kriminalvidenskab,* Vol. *76* No. 5, 1989.

Daniel J. Solove, *Conceptualizing Privacy,* California Law Review, Vol. 90 No. 4, 1975.

David O'Brien, *Privacy, Law, and Public Policy.* New York: Praeger Special Studies. 1979 dan Ruth Gavison, *Privacy and the Limits of the Law.* Yale Law Journal No. 89. 1980.

David O. Friedrichs. *Transnational Crime and Global Criminology: Definitional, Typological, and Contextual Conundrums.* Social Justice, Vol. 34. No. 2 (108), Beyond Transnational Crime, 2007.

DJ Harris, *Cases and Materials on International Law,* Edisi ke-5, London: Sweet & Maxwell, 1998.

Ermanto Fahamsyah, Vicko Taniady, Kania Venisa Rachim, Novi Wahyu Riwayanti. *Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku*

Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention. Jurnal Hukum dan Syariah De Jure, Vol. 14 No. 1 2022.

Erlina Maria, Mery Christin Putri, *Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Indiustri 4.0*. Jurnal RechtsVinding Vol. 9 No. 2, 2020.

Farah Hanan Muhamad, dkk., *Awareness on Financial Cybercrime among Youth: Experience, Exposure and Effect.* Society 5.0 2021 Proceedings, Vol. II, 2021.

Ferdinand Schoeman, *Privacy: Philosophical Dimensions.* American Philosophical Quarterly Vol. 21, No. 3, 1984.

George du Pont, *The Criminalization of True Anonymity in Cyberspace.* Michigan Telecommunication and Technology Law Review, Vol. 7 No. 191.

Gercke, *The Slow Wake of a Global Approach Against Cybercrime,* Computer Law Review International 2006.

Gianpero Greco dan Nicola Montinaro, *The Phenomenon of Cybercrime: From the Transnational Connotation to the Need of Globalization of Justice*. European Journal of Social Sciences Studies, Vol. 2 Issue 1, 2021.

Joel P. Trachman. *Cyberspace, Sovereignty, Jurisdiction and Modernism.* Indiana Journal of Global Legal Studies Vol. 5, Issue 2, Art. 10, 1998.

Joshua Dressler, *Encyclopedia of Crime & Justice*, Vol. 4, 2002.

Kathleen A. Wallace, *Anonymity.* Journal of Ethics and Information Technology Vol. 1, 1999.

L. Cohen dan M. Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach*, dalam Jurnal American Sociology Review No. 44, 1979.

L. Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

Mann, *The Doctrine of Jurisdiction in International Law.* Recueil des Cours de l'Académie de Droit International (RCADI), Vol. 111 No.9, 1964.

Meetali Rawat, *Transnational Cybercrime: Issue of Jurisdiction*. International Journal of Law Management & Humanities, Vol 4, Issue 2 No. 253, 2021.

Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*. Springer, Studies in Computational Intelligence Vol. 593.

Raymond T. Nimmer & Patricia Ann Krauthaus, *Information as a Commodity: New Imperatives of Commercial Law*, Vol.55 *Law and Contemporary Problems,* 1992.

Rob McCusker, *Transnational Organized Crime: Distinguishing Threat from Reality.* Jurnal Crime and Law Social Change 46.

Roman V. Veresha, *Preventive Measures Against Computer Related Crimes: Approaching an Individual.* Jurnal Informatologia, Vol. 51 No. 3-4, 2018.

Sebastian Schmidt, *To Order the Minds of Scholars: The Discourse of the Peace of Westphalia in International Relations Literature,* International Studies Quarterly Vol. 55 No. 3 (September 2011).

Samuel D. Warren dan Louis Brandeis, *The Rights to Privacy.* Harvard Law Review Vol. IV No. 5. 15 Desember 1890.

Sigid Suseno, *Cybercrime, Pengaturan dan Penegakan Hukumnya di Indonesia dan Amerika Serikat,* Jurnal Ilmu Hukum Padjajaran Jilid XXXIII, 2009.

Sumaryo Suryokusumo, *Yurisdiksi Negara vs. Yurisdiksi Ekstrateritorial*, dalam jurnal Hukum Internasional Vol. 2 Nomor 4 Juli 2005.

Tatiana Tropina, *Organized Crime in Cyberspace*. Journal of Transnational Issues of Cybercrime, Vol. 2, 2013.

Tien Saefullah, *Hubungan antara Yurisdiksi Universal dengan Kewajiban Negara berdasarkan Prinsip Aut Dedere Aut Judicare Dalam Tindak Pidana Penerbangan dan Implementasinya di Indonesia.* Jurnal Hukum Internasional UNPAD. Vol. 1 No. 1 Tahun 2002.

Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* Temple International and Comparative Journal Vol. 21 No. 103, 2007.

William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*. 40 GA. Journal of. INT'L & COMP. Law 247, 2011.

Yoyon Efendi. "*Internet of Things (IoT) "Sistem Pengendalian Lampu Menggunakan Raspberry PI Berbasis Mobile*." Jurnal Ilmiah Ilmu Komputer, Vol. 4 No. 1 April 2018.

C. Makalah/Prosiding

Barbara Etter, *Critical Issues in High Tech Crime.* Report Study for Australasian Center for Policing Research. 2001.

Josia Paska Darmawan, dkk., Dalam riset *Center for Digital Society* berjudul *Persepsi Masyarakat Indonesia Terhadap Perlindungan Data Pribadi*, diakses dari: https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/11/Riset-RUU-PDP.pdf\

Presentasi Dr. Edmon Makarim, S. Kom., S.H., LL.M. dalam Penelitian Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia (LKHT) dalam RDPU RUU PDP. Diakses melalui: https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf

Takumi Kimura, Analis siber di NRI SecureTechnologies,Ltd. Dalam artikel dalam https://www.nri.com/en/journal/2020/0825

D. Peraturan Perundang-undangan

UU No. 1 Tahun 1999 tentang Pengesahan Perjanjian antara Republik Indonesia dan Australia mengenai Bantuan Timbal Balik Dalam Masalah Pidana.

UU No. 1 Tahun 2006 tentang Bantuan Hukum Timbal Balik dalam Masalah Pidana

UU No. 8 Tahun 2006 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Rakyat China mengenai Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

UU No. 3 Tahun 2012 tentang Pengesahan Perjanjian antara Republik Indonesia dan Pemerintah Daerah Administrasi Khusus Hong Kong Republik Rakyat China tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

UU No. 8 Tahun 2014 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Korea tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

UU No. 9 Tahun 2014 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik India tentang Bantuan HukumTimbal Balik Dalam Masalah Pidana.

UU No. 6 Tahun 2019 tentang Pengesahan Perjanjian antara Republik Indonesia dan Persatuan Emirat Arab mengenai Bantuan Timbal Balik Dalam Masalah Pidana.

UU No. 5 Tahun 2022 tentang Pengesahan Perjanjian antara Republik Indonesia dan Konfederasi Swiss tentang Bantuan Hukum Timbal Balik Dalam Masalah Pidana.

UU No. 15 Tahun 2008 tentang Pengesahan *Treaty on Mutual Legal Assistance in Criminal Matters* (Perjanjian tentang Bantuan Timbal Balik dalam Masalah Pidana)

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

UU No. 19 Tahun 2019 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

E. Konvensi/Sumber Hukum Internasional

APEC Privacy Framework 2004, 16th APEC Ministerial Meeting, Santiago, Chile, 17-18 November 2004, 2004/AMM/014rev1, Agenda Item: V.4.

ASEAN Declaration to Prevent and Combat Cybercrime, Manila 13 November 2017. 31st Asean Summit. Dapat diakses melalui: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

Convention for the Suppression of Terrorism, European Convention on the Transfer of Criminal Proceedings, European Convention on the International Validity of Criminal Judgments.

Council Of Europe, *Convention on Cybercrime*, Budapest, 23, XI. 2001.

Council of Europe, *Project on Cybercrime: Final Report*, dalam laporan bernomor ECD/567(2009)1, Council of Europe, 15 Juli 2009. Diakses melalui: https://rm.coe.int/16802fa0b7

Council of Europe, *Summary of the Organised Crime Situation* Report 2004: Focus on threat of cybercrime. Council of Europe Octopus Programme. Strasbourg, September 6. Available at: http://www.coe.int/.

Council of Europe, *Explanatory Reports to The Convention on Cybercrime.* European Treaty Series No. 185, 2001.

EU General Data Protection Regulation 2016/679 No. (51).

European Union Agency for Fundamental Rights and Council of Europe

Institut de Droit International, *Resolution on Universal criminal jurisdiction with regard to the crime of genocide, crime against humanity and war crimes.* Krakow Session, 2005. Diakses dari: https://www.idi-iil.org/app/uploads/2017/06/2005_kra_03_en.pdf

INTERPOL, *Global Action Plan Strategy Summary*. 2017. Diakses dari: https://www.interpol.int/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf

OECD (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.

Regulation (EU) 2016/679 of the European Parliament on the Protection of Natural Persons with Regard to The Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation).

UN Doc.A/HRC/17/27, *Report of The Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression,* 16 Mei 2011.

UN Guidelines for the Regulation of Computerized Personal Data Files on '*the procedures for implementing regulations concerning computerized personal data files,'* Adopted by General Assembly resolution 45/95 of 14 December 1990.

United Nation Office on Drugs Crime, *Comprehensive Study on Cybercrime*, 2013.

UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, Diakses dari: https://www.refworld.org/docid/453883f922.html

UN Guidelines for the Regulation of Computerized Personal Data Files, Huruf A, No. 5.

UK Home Office. Cybercrime strategy. Stationery office limited on behalf of the controller of Her Majesty's Stationery Office, 2010.

United Nation Office on Drugs and Office (UNODC), *Transnational Organized Crime-The Globalized Illegal Economy.* Flier/Facts Sheet UNODC, diakses dari: https://www.unodc.org/documents/toc/factsheets/TOC12_fs_general_EN_HIRES.pdf

Universal Declaration of Human Rights/Deklarasi Universal Hak Asasi Manusia (*UDHR*/DUHAM) *Article* 12

F. Media Elektronik

Arrijal Rachman, dalam tulisan berita Tempo.co berjudul "*1,3 Miliar Data Sim Card Bocor, Kominfo: Baru 15-20 Persen yang Cocok"* 5 September 2022. Diakses pada tanggal 20 November 2022 melalui: https://bisnis.tempo.co/read/1630609/13-miliar-data-sim-card-bocor-kominfo-baru-15-20-persen-yang-cocok#:~:text=Senin%2C%205%20September%202022%2014%3A48%20WIB&text=Dari%20hasil%20penelusuran%20sementara%20dengan,data%20SIM%20Card%20yang%20bocor

Interpol Press Release, *Avalanche Network dismantled in International Cyber Operation*. 1 Desember 2016. Diakses pada 12 Maret 2023 melalui:

https://www.interpol.int/ar/1/1/2016/Avalanche-network-dismantled-in-international-cyber-operation

European Union Agency for Law Enforcement Cooperation Press Release, 16 Mei 2019. Diakses pada 12 Maret 2023 melalui: https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

Cybercrime.org.za, *Data Theft Definition*. Diakses pada 10 Februari 2023 melalui: https://cybercrime.org.za/data-theft/

https://www.merriam-webster.com/dictionary/transnational

European Union Agency for Criminal Justice Cooperation Press Release pada tanggal 8 November 2021, bertajuk *Ransomware Gang Dismantled with Eurojust Support.* Diakses dari: https://www.eurojust.europa.eu/news/ransomware-gang-dismantled-eurojust-support

Henry Pope dalam laman *Organized Crime and Corruption Reporting Project* pada 2 November 2021. Diakses pada 22 November 2022 melalui: https://www.occrp.org/en/daily/15419-ukraine-switzerland-arrest-12-suspects-of-international-cybercrime

International Telecommunications Union, *Measuring digital development: ICT facts and figures 2021*, dalam publikasi serikat telekomunikasi internasional, 2021. Diakses pada 22 November 2022 melalui: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Muhammad Firdaus, *A Review of Personal Data Protection Law in Indonesia*, Artikel *Interdisciplinary Program of Information Security, Graduate School PKNU,* diakses pada 10 Desember 2022 melalui: https://osf.io/tmnwg/download

National Action Plans on Business and Human Rights, *Extraterritorial Jurisdiction*. Diakses pada tanggal 10 Maret 2023 melalui: https://globalnaps.org/issue/extraterritorial-jurisdiction/#:~:text=Extraterritorial%20jurisdiction%20is%20the%20situation,power%20beyond%20its%20territorial%20boundarieshttps://globalnaps.org/issue/extraterritorial-jurisdiction/#:~:text=Extraterritorial%20jurisdiction%20is%20the%20situation,power%20beyond%20its%20territorial%20boundaries

Susan Lund, James Manyika, James Bughin, *Globalization is Becoming More About Data and Less About Stuff*. Harvard Business Review, 14 Maret 2016. Diakses pada September 23 2022. Url: https://hbr.org/2016/03/globalization-is-becoming-more-about-data-and-less-about-stuff.

The United States Departemen of Justice (DoJ) Press Release, *Thirty-six Defendants for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrime.* 7 Februari 2018. Diakses pada 20 Maret 2023 melalui: https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

G. Putusan Pengadilan

United States District Court, D. Nevada: United States of America v Syvastolav Bondarenko. Case No. 2:17-CR-306 JCM, 12 Juni 2019.

H. Tugas Akhir

Widodo, *Kebijakan Kriminal terhadap Kejahatan yang Berhubungan dengan Komputer di Indonesia*, Disertasi, Pascasarjana Universitas Brawijaya.

FAKULTAS HUKUM
Gedung Fakultas Hukum
Universitas Islam Indonesia
Jl. Kaliurangkm 14,5 Yogyakarta55584
T. (0274)7070222
E. fh@uii.ac.id
W. law.uii.ac.id

SURAT KETERANGAN BEBAS PLAGIASI

No. : 330/Perpus-S1/20/H/VII/2023

Bismillaahhirrahmaanirrahaim

Yang bertanda tangan di bawah ini:

Nama	: **Joko Santosa, A.Md.**
NIK	**961002136**
Jabatan	: **Staf Perpustakaan Referensi Fakultas Hukum UII**

Dengan ini menerangkan bahwa :

Nama	: Mohammad Fadel Roihan Ba'abud
No Mahasiswa	18410656
Fakultas/Prodi	: Hukum
Judul karya ilmiah	: PENERAPAN PRINSIP YURISDIKSI EKSTRATERITORIAL TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI YANG DILAKUKAN SECARA LINTAS BATAS NEGARA.

Karya ilmiah yang bersangkutan di atas telah melalui proses uji deteksi plagiasi dengan hasil **20**.%

Demikian surat keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 24 Juli 2023 M
6 Muharram 1445 H

Perpustakaan Referensi FH UII

Joko Santosa, A.Md.