SKRIPSI

PENGATURAN HUKUM INTERNASIONAL TENTANG TRANSFER DATA PRIBADI LINTAS NEGARA

Disusun dan diajukan oleh

SITI NURHALIMA LUBIS
B11115389

DEPARTEMEN HUKUM INTERNASIONAL

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

HALAMAN JUDUL

PENGATURAN HUKUM INTERNASIONAL TENTANG TRANSFER DATA PRIBADI LINTAS NEGARA

OLEH

SITI NURHALIMA LUBIS

B11115389

SKRIPSI

Sebagai Tugas Akhir dalam Rangka Penyelesaian Studi Sarjana pada Departemen Hukum Internasional Program Studi Ilmu Hukum

DEPARTEMEN HUKUM INTERNASIONAL

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

LEMBAR PENGESAHAN SKRIPSI

PENGATURAN HUKUM INTERNASIONAL TENTANG TRANSFER DATA PRIBADI LINTAS NEGARA

Disusun dan diajukan oleh

SITI NURHALIMA LUBIS

B11115389

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Departemen Hukum Internasional Program Stud Ilmu Hukum Fakultas Hukum Universitas Hasanuddin pada tanggal 22 April 2021 dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui

Pembimbing Utama,	Pembimbing Pendamping,
Prof. Dr. Judhariksawan, SH., MH	Dr. Maskun, SH., LL.M
NIP. 196907291999031002	NIP. 197611291999031005

Ketua Program Studi Sarjana Ilmu Hukum,

Dr. Maskun, SH., LL.M

NIP. 197611291999031005

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM
KAMPUS UNHAS TAMALANREA, JALAN PERINTIS KEMERDEKAAN KM. 10
TELEPON (0411) 587219, 546686, FAX. (0411) 587219, 590846
MAKASSAR 90345
E-mail : hukumunhas@unhas.ac.id

PESETUJUAN PEMBIMBING SKRIPSI

Diterangkan bahwa Skripsi mahasiswa:

Nama	: Siti Nurhalima Lubis
Nomor Induk Mahasiswa	: B11115389
Departemen	: Hukum Internasional
Judul	: Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara

Telah diperiksa dan disetujui untuk diajukan pada ujian skripsi.

Makassar, April 2021

Pembimbing Utama,	Pembimbing Pendamping,
Prof. Dr. Judhariksawan, SH., MH	Dr. Maskun, SH., LL.M
NIP. 196907291999031002	NIP. 197611291999031005

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM
KAMPUS UNHAS TAMALANREA, JALAN PERINTIS KEMERDEKAAN KM.10
Telp : (0411) 587219,546686, FAX. (0411) 587219,590846 Makassar 90245
E-mail: hukumunhas@unhas.ac.id

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: SITI NURHALIMA LUBIS
N I M	: B11115389
Program Studi	: Ilmu Hukum
Departemen	: Hukum Internasional
Judul Skripsi	: Kajian Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, April 2021

a.n. Dekan,
Wakil Dekan Bidang Akademik,Riset dan Inovasi

Prof. Dr. Hamzah Halim SH.,MH
NIP. 19731231 199903 1 003

PERNYATAAN KEASLIAN PENULIS

Yang bertanda tangan di bawah ini :

Nama	: Siti Nurhalima Lubis
NIM	: B11115389
Program Studi	: Ilmu Hukum
Jenjang	: S1

Menyatakan dengan ini bahwa Skripsi dengan judul Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara adalah karya saya sendiri dan tidak melanggar hak cipta pihak lain. Apabila dikemudian hari Skripsi karya saya ini terbukti bahwa sebagian atau keseluruhannya adalah hasil karya orang lain yang saya pergunakan dengan cara melanggar hak cipta pihak lain, maka saya bersedia menerima sanksi.

Makassar, Mei 2021

Yang Menyatakan

Siti Nurhalima Lubis

ABSTRAK

Siti Nurhalima Lubis (B11115389) dengan judul Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara. Di bawah bimbingan Judhariksawan sebagai Pembimbing I dan Maskun sebagai Pembimbing II.

Penelitian ini bertujuan untuk mengetahui pengaturan hukum internasional tentang perlindungan hukum terhadap transfer data pribadi lintas negara, dan untuk mengetahui praktik negara dalam transfer data pribadi lintas negara. Kajian ini penting di era kemajuan teknologi dan informasi mengingat data pribadi memiliki nilai ekonomi tinggi dan menjadi tolak ukur negara dalam menegakkan kedaulatannya melalui perlindungan terhadap data pribadi warga negaranya.

Penelitian ini menggunakan metode penelitian yuridis normatif dengan jenis data sekunder dikumpulkan melalui studi pustaka berupa instrumen hukum internasional, peraturan perundang-undangan, putusan pengadilan, buku, jurnal, dan karya ilmiah lainnya yang berkaitan dengan topik penelitian. Dalam hasil penelitian ini dianalisis kemudian disajikan secara deskriptif.

Adapun hasil penelitian ini, yaitu (1) Transfer data pribadi telah diatur dalam beberapa hukum internasional seperti OECD Guidelines, GDPR, APEC Privacy Framework dan Privacy Shield. (2) Mayoritas negara di dunia telah mengatur terkait perlindungan transfer data pribadi dalam praktik hukum nasionalnya sebagai wujud keseriusan negara dalam mengatur transfer data pribadi lintas negara.

Kata kunci: Data Pribadi, Transfer, Hukum Internasional, Praktik Negara.

ABSTRACT

Siti Nurhalima Lubis (B11115389) International Law Regulations Regarding Cross-Country Personal Data Transfers. Under the supervision of Judhariksawan as Advisor I and Maskun as Advisor II.

This study aims to determine international legal arrangements regarding legal protection of the transfer of personal data across countries, and to determine state practices in the transfer of personal data across countries. This study is important in an era of advances in technology and information, considering that personal data has high economic value and is a benchmark for the state in upholding its sovereignty through the protection of the personal data of its citizens.

This study uses a normative juridical research method with secondary data collected through literature studies in the form of international legal instruments, laws and regulations, court decisions, books, journals, and other scientific works related to the research topic. In the results of this study were analyzed then presented descriptively.

The results of this study indicate that: (1) Personal data transfers has been regulated in several international laws such as the OECD Guidelines, GDPR, APEC Privacy Framework and Privacy Shield; and (2) The majority of countries in the world have regulated the protection of personal data transfers in their national legal practices as a manifestation of their seriousness in regulating the transfer of personal data across countries.

Keywords: Personal Data, Transfers, International Law, State Practices.

KATA PENGANTAR

Bismillahirrahmanirahim.

Segala puji dan syukur senantiasa penulis panjatkan kehadirat Allah SWT, atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul Pengaturan Hukum Internasional Tentang Transfer Data Pribadi Lintas Negara yang merupakan tugas akhir dalam rangka menyelesaikan studi strata satu untuk mendapatkan gelar Sarjana Hukum di Fakultas Hukum Universitas Hasanuddin.

Penulis dengan sepenuh hati menyampaikan terima kasih yang sebesar-besarnya kepada beberapa pihak yang senantiasa mendampingi penulis dalam proses penyelesaian skripsi ini. Terkhusus kepada Oma dan Opa, *Almarhummah* **Hasna M. Bumulo** dan *Almarhum* **Abubakar Maksum** yang telah membesarkan penulis dengan penuh kesabaran dan ketulusan. Kepada orang tua penulis, yang telah berusaha memberikan perhatian dan kasih sayangnya.

Selain itu, penulis juga menampaikan rasa hormat dan terima kasih kepada:

1. Bapak Prof. Dr. Judhariksawan, SH.,MH. dan Bapak Dr. Maskun, SH., LL.M., selaku pembimbing skripsi yang senantiasa meberikan ilmu, waktu dan tenaga dalam membimbing penulis sehingga skripsi ini dapat diselesaikan.
2. Bapak Prof. Dr. Juajir Sumardi, SH., MH., dan Bapak Dr. Laode Abd. Gani, SH., MH., selaku penguji skripsi atas segala masukan dan arahannya dalam penyelesaian skripsi ini.
3. Ibu Dr. Andi Tenri Famauri, SH., MH., selaku penasehat akademik penulis yang telah memberikan bimbingan kepada penulis selama di bangku kuliah.

4. Tim Penelitian Siber Agresi, Bapak Dr. Maskun, S. H, L. L. M., Dr. Ahmad, S. H., Dr. Naswar, S. H., Hasbi Asidiq dan Armelia Syafira atas pelajaran, pengalaman dan dukungannya untuk penulis.
5. Segenap dosen Fakultas Hukum Universitas Hasanuddin yang telah memberikan ilmu pengetahuan kepada penulis.
6. Seluruh pegawai akademik yang telah sabar membantu penulis selama melakukan pemberkasan dalam penyelesaian skripsi ini.
7. Seluruh Pegawai Perpustakaan Pusat Universitas Hasanuddin dan Perpustakaan Fakultas Hukum Universitas Hasanuddin yang telah menyediakan waktu, tempat, dan dukungan selama proses penyelesaian skripsi ini.

Semoga Allah SWT membalas segala kebaikan yang telah diberikan. Akhir kata, penulis memohon maaf atas segala kekurangan dalam skripsi ini, semoga para pembaca dapat mengambil manfaat yang berarti.

Makassar, April 2021

Siti Nurhalima Lubis

DAFTAR ISI

halaman

BAB I

PENDAHULUAN

A. Latar Belakang

Data pribadi dapat dianggap sebagai kekayaan bernilai jual tinggi bagi perusahaan, pemerintah atau perorangan yang ingin memprediksikan perilaku individu atau untuk memenuhi rasa ingin tahu tentang data pribadi seseorang. Data pribadi adalah data yang mengidentifikasi seseorang dengan karakteristik orang tersebut misalnya alamat tempat tinggal, pendidikan, nama, usia, jenis kelamin, pekerjaan, serta peran dalam kehidupan berkeluarga. Dalam hal lain data pribadi juga diartikan sebagai suatu informasi, dimana informasi tersebut melekat pada pribadi orang, pada umumnya informasi yang dimaksudkan digunakan dalam menemukan seorang sebagai pemiliknya.

Pencipta atau admin perangkat, sistem operasi, dan aplikasi yang kita gunakan merupakan pemegang kendali atas informasi data pribadi yang telah dikumpulkan. Hal ini menunjukkan pada dasarnya setiap kita baik secara *Online* maupun *Offline* diawasi oleh pihak tertentu seperti perusahaan atau pemerintah yang memiliki kepentingan dengan atau tanpa sepengetahuan pihak yang bersangkutan. Data pribadi dapat diambil melalui kolom periksa atau setelan privasi pada suatu perangkat, sistem operasi atau aplikasi yang digunakan. Selain itu data pribadi seseorang dapat dikumpulkan pula melalui postingan yang telah dipublikasikan di dunia maya baik disengaja ataupun tidak disengaja.

Pengumpulan data ini dapat dilakukan secara diam-diam tanpa disadari oleh orang yang bersangkutan merupakan pelanggaran terhadap hak privasi seseorang. Pelanggaran tersebut mempunyai aspek negatif yang terjadi dalam kejahatan siber, seperti pencurian, penipuan, pemerasan, dan penyalahgunaan data pengguna misalnya diakses secara melanggar hukum yang dilakukan oleh seseorang ataupun pihak lainnya yang tidak bisa bertanggung jawab.

Akses ilegal sendiri merupakan salah satu kejahatan siber yang tercantum di dalam Bab II Pasal 2 *Budapest Covention on Cybercrime*, 2001[1]. Pasal ini menyebutkan bahwa Para Pihak harus menerapkan peraturan tersebut serta langkah-langkah lainnya jika dianggap perlu teruntuk menjalankan sebagai pelanggaran kriminal bersumber pada undang-undang domestiknya, dalam hal ini apabila dilakukan dengan terencana, akses ke semua atau sebagian sistem komputer tanpa hak. Sesuatu Pihak dapat mensyaratkan suatu pelanggaran dilakukan dengan melanggar langkah-langkah pengamanan, dengan tujuan untuk memperoleh informasi dari komputer atau dengan iktikad tidak jujur yang lain, ataupun terkait dengan sistem komputer yang terhubung ke sistem komputer yang lain.[2]

[1] Dikenal juga dengan *Council of Europe Convention on Cybercrime* (ETS No. 185)
[2] Muhamad Amirullah, Ida Padmanegara, dan Tyas Dian Anggraeni, 2009, *"Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi",* Laporan Akhir Penulisan Karya Ilmiah, Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia RI, Jakarta, hlm. 34.

Semua data pribadi yang telah dikumpulkan dapat menghasilkan sebuah laporan yang kemudian dapat dijual dan dibagikan sesuai dengan keinginan pihak-pihak tertentu. Hal ini mengapa penting adanya hukum yang dapat menjamin perlindungan data pribadi. Hukum yang melindungi data pribadi seseorang diperlukan untuk melindungi data pribadi dan hak-hak pemiliknya untuk tahu apa yang terjadi dengan data-data tersebut sehingga terhindar dari penyalahgunaan oleh pihak-pihak tertentu.

Pengaturan hukum atas data di seluruh dunia sangat beragam, lebih dari 100 negara telah menerapkan berbagai tingkat hukum perlindungan data, tetapi semua itu tidak mencakup semua sektor bisnis atau fungsi pemerintah. Karena informasi bergerak ke seluruh dunia melalui jaringan yang tak terbatas, bahkan sekalipun seseorang hidup di suatu tempat dimana data dilindungi, data tersebut kemungkinan besar akan berakhir di negara-negara yang mempunyai hukum yang berbeda ataupun bahkan tidak terdapat peraturan sama sekali, artinya jika hak data pribadi tersebut dilanggar tidak akan mendapat pemulihan. Hal ini menjangkau area kompleksitas baru ketika kita menyadari bahwa hampir seluruh informasi dunia melewati pusat kendali teknologi dan hampir semuanya terletak di Amerika Serikat (AS) serta berada di bawah hukum AS. Payung hukum AS tentunya tidak berlaku bagi masyarakat di luar negara tersebut, sehingga jika data pribadi seseorang di luar Amerika telah masuk ke dalam pusat kendali teknologi Amerika melemahkan hak terhadap data tersebut.

Hal demikian menunjukkan bagaimana hukum perlindungan data pribadi dilemahkan akan membatasi hak yang dimiliki terkait informasi data pribadi. Jika pengaturan hukum mengenai perlindungan data pribadi menguat maka lebih banyak hak yang dimiliki oleh seseorang terkait data pribadinya. Kemudian akan lebih tinggi kontrol yang dimiliki sehingga lebih kecil kemungkinan penyalahgunaan data pribadi. Perihal ini tidak hanya berlaku pada perusahaan tertentu, akan tetapi berlaku pada pemerintah yang membatasi kontrol seseorang terhadap data pribadinya.

Penguatan hukum perlindungan data pribadi diperlukan agar tidak ada *database* rahasia dan tujuan pendataan dan penggunaan data diatur spesifik pada kurun waktu tertentu serta hanya data penting yang dapat dikumpulkan. Data tersebut harus selalu diperbaharui, aman dan dihapus ketika tidak lagi dibutuhkan. Tidak ada informasi yang dapat disalurkan tanpa persetujuan dari pihak yang bersangkutan.

Kebocoran atau penyalahgunaan data pribadi tidak hanya menjadi persoalan di Indonesia.[3] Laporanyang ditulis oleh Rachna Khaira (*The Tribune India*) berisi tentang data warga berjumlah sekitar satu miliar yang dimuat dalam program *Aadhaar* mengalami bocor.[4] Program ini merupakan program identitas elektronik yang diselenggarakan *UIDAI*[5]*.* Kesimpulan kebocoran data warga ini ditemukan setelah *Tribune India*

[3] Ahmad Zaenudin – 8 Maret 2018. *Di Balik Kabar Kebocoran Data Registrasi Ulang Kartu SIM*. https://tirto.id/di-balik-kabar-kebocoran-data-registrasi-ulang-kartu-sim-cFQj (berita online)
[4] Rachna Khaira – Jan 04, 2018. *Rs 500, 10 minutes, and you have access to billion Aadhaar details.* https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361 (online news)
[5] *Unique Identification Authority of India*

menemukan bahwa dalam program *Aadhaar* datanya dapat diakses dari sumber anonim yang didapatkan dari pesan *WhatsApp* dengan bayaran sebesar $8. Harga tersebut merupakan jumlah yang digunakan untuk memperoleh data pribadi warga. Namun berita ini kemudian dinyatakan merupakan "berita palsu."

Kebocoran data juga terjadi di Meksiko di bulan April tahun 2016, dimana ada data pribadi warga yang terdapat dalam rekam data untuk registrasi pemilu berjumlah 93,4 juta telah mengalami kebocor[6]. Berita tentang hal ini dimuat dalam *Digital Trends*, data bocor tersebut selanjutnya dihapus setelah beredar secara umum selama lebih dari satu minggu. Kebocoran yang sama juga dialami pada Oktober 2917 oleh Afrika Selatan. Dimana puluhan juta data warga Afrika Selatan dalam *file* berukuran 27 GB mengalami kebocoran[7]. Seorang konsultan keamanan bernama Troy Hunt merupakan orang yang mengungkapkan kebocoran ini. Data yang beredar tersebut diantaranya nomor kependudukan, status pernikahan, hingga kepemilikan properti. Kasus-kasus di atas merupakan bukti bahwa masalah data pribadi yang terjadi di negara-negara dunia merupakan permasalahan yang serius

Pada Juli 2020, Kesepakatan dimana perusahaan teknologi dapat mentransfer data pribadi dari *server* yang berada di Uni Eropa ke *server*

[6] Lulu Chang – April 23, 2016. *The latest data breach involves the voting records of 93.4 million Mexican citizens.* https://www.digitaltrends.com/computing/mexico-voting-breach/ (online news)

[7] Iafrikan – Oct 18, 2017. *South Africa's biggest data breach affects over 30 million citizens – and nobody knows where it come from.* https://thenextweb.com/contributors/2017/10/18/south-africas-biggest-data-breach-affects-30-million-citizens-nobody-knows-came/ (online news)

yang ada di Amerika Serikat telah ditolak oleh Mahkamah Eropa.[8] Gugatan dalam kasus terbaru ini yang dilakukan oleh Maximilian Schrems, seorang warga Austria yang menuntut Komisi Perlindungan Data Pribadi Irlandia dan Pihak Facebook. Dalam kasus ini melalui kesepakatan *Privacy Shield* dimungkinkan terjadinya transfer atau perpindahan data antar-*server*.[9] Isi gugatan menyatakan standar perlindungan data pribadi lebih rendah di Amerika Serikat jika dibandingkan di Uni Eropa, hal ini disebabkan oleh kemungkinan data pribadi yang dapat diakses oleh intelijen walaupun tidak ada pengawasan serta tidak terdapat mekanisme banding apabila terjadi sesuatu pada data-data tersebut. Dalam putusannya Mahkamah Eropa berpandangan bahwa perlu adanya lembaga pengawas independen yang dapat menentukan dan mengatur mekanisme dalam penyelesaian sengketa serta pemulihan hukum yang diperlukan. Kasus ini menjadi penting tidak hanya kepada pihak yang terkait, melainkan secara khusus penting untuk Indonesia karena sedang dalam penyelesaian Rancangan Undang-undang (RUU) tentang Perlindungan Data Pribadi (PDP).

Dalam Hukum internasional yang telah diketahui sebelumnya menerangkan bahwa suatu data pribadi tunduk di bawah hukum dimana *server* dari data pribadi tersebut berada. Namun dalam kenyataannya saat

[8] JUDGMENT OF THE COURT (Grand Chamber) - 16 July 2020. Akses online di https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62018CJ0311

[9] DW – Kamis, 16 Juli 2020. Mahkamah Eropa Larang Mekanisme Transfer Data Pengguna Facebook ke Server di AS. https://www.tempo.co/dw/2956/mahkamah-eropa-larang-mekanisme-transfer-data-pengguna-facebook-ke-server-di-as (berita online)

ini negara tujuan pengiriman data pribadi bisa merupakan negara dengan kapasitas perlindungan data pribadi yang lebih lemah, bahkan tidak memiliki perlindungan data pribadi.

Melihat contoh aturan Inggris tentang perlindungan data pribadi yang tercantum pada undang-undang Perlindungan Data 1998 (*The Data Protection Act* 1998).[10] Dalam isi undang-undangnya menyebutkan suatu badan pelaksana yang dikenal sebagai *The Data Protection Commisioner* memiliki wewenang dalam pengawasan terhadap pengguna data yang berkuasa atas data pribadi. Perlindungan hak privasi pula terdapat pada *Data Protection Act* 1998 dimana dalam aturan tersebut mengizinkan subjek data dalam memiliki informasi pengolahan data pribadi miliknya serta hal ini juga bisa mencegah beberapa pengolahan data untuk dilakukan apabila hal tersebut diperkirakan dapat membahayakan.[11]

Data pribadi di Inggris dilindungi secara kuat dan tegas oleh aturannya, dimana bahkan terdapat larangan transfer data pribadi ke luar Eropa kecuali terdapat jaminan yang cukup. Inggris tidak mengizinkan ataupun memberikan data pribadi yang dimiliki ke negara lain dalam tujuan apa pun walaupun dengan cara sah dalam hukum, apabila negara

[10] Lia Sautunnida, 2018, "Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia", Kanun Jurnal Ilmu Hukum, Fakultas Hukum Universitas Syiah Kuala, Vol 20, No. 2 (Agustus 2018), hlm. 375

[11] Edmin Makarim, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, dalam Radian Adi Nugraha, 2012, "*Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari UU Informasi dan Transaksi Elektronik"*, Skripsi, Fakultas Hukum Universitas Indonesia, hlm. 50.

tersebut tidak memiliki undang-undang khusus tentang perlindungan data pribadi.[12]

Negara Malaysia juga telah memiliki aturan khusus Perlindungan Data Pribadi. Aturan tersebut tertuang dalam *Personal Data Protection Act* (PDPA) 2010. Hukum PDPA yang ada di Malaysia ini memiliki tujuan tujuan mengatur pengolahan data pribadi di sektor transaksi komersial oleh pengguna data, memiliki maksud menjaga kepentingan subjek data pribadi. Mengenai hal ini hanya dapat dicapai melalui adanya persetujuan oleh yang bersangkutan yang telah dimiliki sebelum pengolahan data dan juga memberikan data dengan subjek hak untuk mengakses secara benar dan kontrol pengolahan data pribadi oleh yang bersangkutan. Sama dengan apa yang tertuang dalam Pasal 26 UU ITE Indonesia.[13]

Pemberlakuan PDPA 2010 memberikan setiap individu beberapa hak contohnya hak dalam mendapatkan informasi terkait data pribadi yang bersangkutan serta hak akses atas data pribadi tersebut, mengoreksi serta memiliki kontrol dalam pengolahan atau bagaimana data pribadi digunakan oleh pihak lain. Dalam PDPA ditetapkan bahwa tidak boleh terjadi transfer atau perpindahan data pribadi ke wilayah di luar Malaysia, transfer hanya dapat dilakukan apabila telah disetujui dan ditetapkan oleh Menteri Informasi, Kebudayaan dan Komunikasi. Selanjutnya negara

[12] Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, Vol. 10 No. 2, 2019, hlm. 222.
[13] Zuryati Mohamed Yusoff, "The Malaysian Personal Data Protection Act 2010: A Legislation Note", New Zealand Journal of Public and International Law, Vol. 9, No. 1, 2011, hlm. 6.

tujuan tempat ditransfernya data harus telah memenuhi tingkat perlindungan yang cukup baik, atau minimal sama dengan tingkat perlindungan yang telah diterapkan dalam PDPA Malaysia.

Internet telah berjasa dalam menghubungkan komunikasi dan transfer data lintas batas negara. Data pribadi kemudian dapat diolah sehingga menghasilkan keuntungan atau di-*monetisasi*, misalnya dengan menciptakan profil pribadi tentang seseorang untuk digunakan dalam keperluan iklan ataupun yang lainnya. Data pribadi yang telah dikumpulkan oleh perusahaan teknologi, berkemungkinan dapat ditransfer ke wilayah negara lain di luar jangkauan hukum negara asal pengguna data pribadi. Dalam hal ini data pribadi kita berpotensi untuk digunakan dengan cara yang salah oleh pihak ketiga tanpa ada pengawasan yang sesuai. Sampai saat ini tidak ada regulasi tingkat global berisi standar perlindungan data pribadi yang berlaku terhadap seluruh negara di dunia. Inilah yang menjadikan penulis terdorong dan tertarik untuk melakukan penelitian dengan judul “Kajian Hukum Internasional tentang Transfer Data Pribadi Lintas Negara”.

B. Rumusan Masalah

Melalui latar belakang yang telah diuraikan di atas, maka penulis menarik rumusan masalah yaitu:

1) Bagaimana pengaturan hukum internasional tentang perlindungan hukum terhadap transfer data pribadi?
2) Bagaimana praktik negara-negara dalam transfer data pribadi?

C. Tujuan Penelitian

Adapun Tujuan dari penelitian ini, yaitu:

1. Untuk mengetahui pengaturan hukum internasional tentang perlindungan hukum terhadap transfer data pribadi;
2. Untuk mengetahui praktik negara-negara dalam transfer data pribadi.

D. Kegunaan Penelitian

Kegunaan dari penelitian ini, yaitu:

1. Dengan penelitian ini dapat diketahui pengaturan hukum internasional tentang perlindungan hukum terhadap transfer data pribadi;
2. Dengan penelitian ini dapat diketahui praktik negara-negara dalam transfer data pribadi.

E. Keaslian Penelitian

1. Lia Sautunnida - Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia (Artikel Ilmiah)

Artikel ini telah menjawab bagaimana pentingnya penetapan hukum yang bersifat tegas dan komprehensif serta memberikan perlindungan untuk data pribadi melalui media elektronik. Beberapa negara contohnya Uni Eropa, Amerika, Inggris, Hongkong, Singapura, dan Malaysia, telah mempunyai hukum yang bersifat tegas dan komprehensif terkait dengan data pribadi. Namun sejauh ini Indonesia belum memiliki hukum khusus yang mengatur hal tersebut. Terkait perlindungan data pribadi Indonesia memiliki aturan dalam Pasal 26 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan beberapa aturan lainnya.

Sedangkan penelitian yang penulis lakukan melalui skripsi ini membahas bagaimana aturan hukum internasional terhadap transfer data pribadi lintas negara serta penulis meneliti bagaimana praktik yang ada di negara-negara pada masa kini. Penulis tidak memfokuskan penelitian hanya pada negara tertentu seperti yang terdapat pada artikel sebelumnya, melainkan secara keseluruhan namun fokus pada satu topik yaitu transfer data pribadi itu sendiri.

2. Fanny Priscyllia - Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum (Artikel Ilmiah)

Penelitian ini memiliki tujuan untuk menganalisis perlindungan privasi data pribadi dalam perspektif perbandingan hukum. Dalam hasil penelitian menunjukkan dimana konsep perlindungan hak privasi merupakan hak penuh pada seseorang serta pemenuhannya tidak

didasarkan pada hak orang lain, manun hak tersebut dapat hilang jika dikehendaki pemiliknya. Ketiadaan hukum secara komprehensif terkait perlindungan privasi atas data pribadi memiliki potensi meningkatkan pelanggaran pada hak konstitusional warga negara.

Pada penelitian sebelumnya di artikel ini mengaitkan data pribadi dan perlindungan privasi, sedangkan pada penelitian yang penulis lakukan memaparkan bagaimana transfer data pribadi lintas batas dalam pengaturan hukum internasional. Perspektif perbandingan hukum yang terdapat pada penelitian sebelumnya masih menjadi perspektif yang penulis lakukan dalam penelitian ini namun lebih fokus pada transfer data pribadi itu sendiri.

3. Oktaviani Sugiarto - Tinjauan Hukum Internasional Terkait Perlindungan Data dan Informasi Pribadi (Skripsi)

Penelitian ini membahas tentang bagaimana pengaturan hukum internasional terkait perlindungan data privasi dan kaitan tentang pelanggaran atas hak privasi yang bertentangan dengan HAM. Hasil penelitian dalam tulisan ini menunjukkan bahwa hak atas privasi tidak bertentangan dengan HAM melainkan merupakan bagian dari HAM yang fundamental, namun dalam penerapannya hak privasi dapat dibatasi/dilanggar secara sah oleh undang-undang.

Pada skripsi di atas membahas terkait perlindungan data dan informasi pribadi yang dilihat melalui perspektif HAM sedangkan yang penulis utarakan dalam penelitian ini lebih mengarah pada bagaimana hukum internasional itu sendiri mengatur tentang transfer data pribadi lintas negara yang lebih lanjut membahas bagaimana praktik-praktik negara mengenai transfer data pribadi tersebut.

F. Metode Penelitian

1. Jenis Penelitian

   Penelitian ini dilakukan dengan metode penelitian yuridis normatif. Pendekatan yuridis normatif berdasarkan pendapat Soerjono Soekanto adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur yang berkaitan dengan permasalahan yang diteliti.[14]

2. Jenis Data

   Adapun jenis data yang terdapat dalam penelitian ini yaitu jenis data sekunder. Data ini setelah penelitian digunakan sebagai data pendukung dalam menganalisis dan menginterpretasikannya permasalahan yang dibahas dalam skripsi ini.

3. Sumber Data

[14] Soerjono Soekanto & Sri Mamudji, 2001, *Penelitian Hukum Normatif (SuatuTinjauanSingkat)*, Rajawali Pers, Jakarta, hlm 13-14.

Sumber data yang digunakan penulis dalam penelitian ini adalah: konvensi-konvensi internasional, buku-buku dan literatur lain seperti jurnal ilmiah, hasil penelitian, maupun sumber informasi lainnya yang berhubungan dengan judul skripsi ini. Sumber data yang digunakan berbentuk *hard copy* maupun *soft copy* yang penulis dapatkan secara langsung maupun melalui penelusuran dari internet.

4. Teknik Pengumpulan Data

Penelitian ini dilakukan dengan teknik pengumpulan data studi literatur (*literature research*) berupa buku, jurnal, surat kabar, majalah, internet, dan sumber-sumber lainnya. Teknik ini bertujuan untuk memperoleh bahan-bahan dan informasi-informasi sekunder yang diperlukan dan relevan dengan penelitian.

5. Analisis Data

Adapun analisis data, penulis melakukan analisis data-data yang diperoleh dari studi literatur yang bersumber dari konvensi-konvensi internasional, buku-buku dan literatur lain yang berhubungan dengan judul skripsi ini dengan cara kualitatif dan disajikan secara deskriptif analisis.

BAB II

TINJAUAN PUSTAKA DAN ANALISIS PERMASALAHAN PERTAMA

A. Tinjauan Pustaka

1) Informasi Pribadi dan Data Pribadi

a. Pengertian Informasi Pribadi

Pengertian informasi pribadi tercantum dalam *APEC Privacy Framewok Part II Number 9*:

> *"Personal information means any information about an identified or identifiable individual"*

Selain *APEC Privacy Framework*, pengertian informasi pribadi juga tercantum di *Australian Privacy Act 1988 Section 6:*

> *"personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."*

Dalam *Children's Online Privacy Protection Act (COPPA) of 1998,*

> *"section 1302 (8)---the term "personal information" means individually identifiable information about an individual collected online, including---"*
> *a) a first and last name:*
> *b) a home or other physical address including street name and name of a city or town;*
> *c) an e-mail address;*
> *d) a telephone number;*
> *e) a Social Security number;*
> *f) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or*
> *g) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.*

Menurut definisi yang digunakan oleh *National Institute of Standard and Technology (NIST)* yang termasuk kategori informasi pribadi, antara lain[15]:

1. Nama lengkap;
2. Wajah;
3. Alamat rumah;
4. Alamat *email*;
5. Nomor identifikasi nasional (misalnya nomor jaminan sosial di Amerika Serikat);
6. Nomor paspor;
7. Nomor plat registrasi kendaraan;
8. Nomor SIM;
9. Sidik jari atau tulisan tangan;
10. Nomor kartu kredit;
11. Identitas digital;
12. Tanggal lahir;
13. Tempat kelahiran;
14. Informasi genetik;
15. Nomor telepon;
16. Nama *login*, nama layar, nama panggilan, atau pegangan.

[15] NIST, *"Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"* (PDF). Special Publication 800-122.

Selain yang disebutkan di atas, berikut ini juga berpotensi untuk dikategorikan sebagai informasi pribadi namun jarang digunakan untuk membedakan identitas individu:

1. Nama depan atau belakang;
2. Negara, negara bagian, kode pos, atau kota tempat tinggal;
3. Usia;
4. Gender atau ras;
5. Nama sekolah atau tempat kerja ;
6. Gaji atau posisi pekerjaan ;
7. Catatan kriminal;
8. *Cookie Web.*

b. Pengertian Data Pribadi

Tiap-tiap negara menggunakan peristilahan yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantif kedua istilah tersebut mempunyai pengertian yang hampir sama sehingga kedua istilah tersebut sering digunakan bergantian. Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi sedangkan negara-negara Uni Eropa dan Indonesia sendiri dalam UU ITE menggunakan istilah data pribadi.[16] Suatu data adalah data pribadi apabila data tersebut

[16] Shinta Dewi, 2009, *CyberLaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Widya Padjadjaran, Bandung,hlm. 71.

berhubungan dengan seseorang, sehingga dapat digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data.[17]

Definisi data pribadi banyak terdapat dalam berbagai regulasi, baik regional maupun nasional, antara lain:

1. Dalam Undang-undang Republik Indonesia Nomor 24 Tahun 2013 tentang Perubahan atas Undang-undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Pasal 1 angka 23 yang berbunyi:

   "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta dilindungi kerahasiaannya."

2. Menurut *Draft* RUU Perlindungan Data Pribadi Pasal 1 angka 3:

   "Data Pribadi adalah setiap data tentang kehidupan seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik."

3. Menurut *European Union General Data Protection Regulation (GDPR) Article 4 (1)*:

   "'personal data' means 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 such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

   Terjemahan bebas:

[17] European Union Agency for Fundamental Rights and Council of Europe, 2014, *Handbook on European Data Protection Law*, Belgium, hlm. 36.

data pribadi adalah segala informasi yang berkaitan dengan seseorang (subjek data) yang teridentifikasi atau dapat diidentifikasi; seseorang yang dapat diidentifikasi adalah orang yang bisa diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal *online* atau satu atau lebih faktor spesifik seperti fisik, fisiologis, genetik , identitas mental, ekonomi, budaya atau sosial dari orang itu.

4. Menurut *Personal Data Act 1998 Section 3*:

   "Personal Data means all kinds of information that directly or indirectly may be referable to a natural person who is alive."

   Terjemahan bebas:

   Data Pribadi berarti semua jenis informasi yang secara langsung atau tidak langsung yang merujuk kepada orang yang masih hidup.

5. Dalam beberapa instrumen, definisi data pribadi hampir memiliki pengertian yang sama , seperti dalam *Data Protection Directives, Data Protection Convention,* dan *the Organisation for Economic Co-operation and Development (OECD) Guidelines*,

   "information relating to an identified or identifiable natural person"[18]

2) Data Kependudukan

Pada umumnya data memiliki arti yaitu sebagai suatu kumpulan informasi dapat dimiliki dengan cara mengamati dapat berbentuk angka, lambang dan atau sifat digunakan sebagai gambaran mengenai suatu keadaan dan atau persoalan. Definisi lain dari data yaitu sekumpulan

[18] Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia", Yustisia Vol.5, No.1, Januari - April 2016, hlm. 29.

informasi atau nilai yang diperoleh dari pengamatan (observasi) suatu objek. Sehingga oleh definisi di atas data yang baik adalah data yang bisa dipercaya kebenarannya (*reliable*), tepat waktu dan mencakup ruang lingkup yang luas atau bisa memberikan gambaran tentang suatu masalah secara menyeluruh merupakan data relevan. Dengan demikian data kependudukan adalah segala tampilan data penduduk dalam bentuk resmi maupun tidak resmi yang diterbitkan oleh badan-badan pencatatan kependudukan (pemerintah maupun non pemerintah), dalam berbagai bentuk baik angka, grafik, gambar dan lain-lain.

Penduduk adalah warga negara Indonesia dan orang asing yang bertempat tinggal di Indonesia. Kependudukan adalah hal ihwal yang berkaitan dengan jumlah, struktur, umur, jenis kelamin, agama, kelahiran, perkawinan, kehamilan, kematian, persebaran, mobilitas dan kualitas serta ketahanannya yang menyangkut politik, ekonomi, sosial, dan budaya. Berdasarkan Undang-undang Republik Indonesia Nomor 24 tahun 2013 Pasal 1 nomor 9, Data Kependudukan adalah data perseorangan dan/atau data agregat yang terstruktur sebagai hasil dari kegiatan Pendaftaran Penduduk dan Pencatatan Sipil.

Dalam UU Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, data dikelompokkan menjadi :

1. Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya (Pasal 1 Poin 22).

2. Database adalah kumpulan berbagai jenis data kependudukan yang tersimpan secara sistematik, terstruktur dan saling berhubungan dengan menggunakan perangkat lunak, perangkat keras dan jaringan komunikasi data (Pasal 1 Poin 29 PP No. 37 Tahun 2007).

3. Data Kependudukan adalah data perseorangan atau data agregat yang terstruktur sebagai hasil kegiatan pendaftaran penduduk dan pencatatan sipil.

4. Data perseorangan menurut UU No. 24 Tahun 2013, Pasal 58 ayat 2, meliputi nomor Kartu Keluarga; Nomor Induk Kependudukan; nama lengkap; jenis kelamin; tempat lahir; tanggal/bulan/tahun lahir; golongan darah; agama/kepercayaan; status perkawinan; status hubungan dalam keluarga; cacat fisik dan/atau mental; pendidikan terakhir; jenis pekerjaan; NIK ibu kandung; nama ibu kandung; NIK ayah; nama ayah; alamat sebelumnya; alamat sekarang; kepemilikan akta kelahiran/surat kenal lahir; nomor akta kelahiran/nomor surat kenal lahir; kepemilikan akta perkawinan/buku nikah; nomor akta perkawinan/buku nikah; tanggal perkawinan; kepemilikan akta perceraian; nomor akta perceraian/surat cerai; tanggal perceraian; sidik jari; iris mata; tanda tangan; dan elemen data lainnya yang merupakan aib seseorang.

B. Analisis Permaalahan Pertama

1) Pengaturan Hukum Internasional Terkait Data Pribadi

Lebih dari puluhan aturan internasional seperti konvensi dan perjanjian internasional lainnya memiliki unsur-unsur data pribadi di dalamnya yang telah digunakan di negara pada tingkatan regional atau tingkatan internasional. Berikut penjelasan mengenai beberapa konvensi dan perjanjian tersebut:[19]

a. *The Organisation for Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

Perkembangan pemrosesan data memungkinkan data dalam jumlah besar dikirim dalam hitungan detik melintasi perbatasan nasional, dan bahkan lintas benua menjadikan perlunya pertimbangan perlindungan privasi dalam kaitannya dengan data pribadi. Undang-undang perlindungan privasi telah diperkenalkan, atau akan segera diperkenalkan, di sekitar setengah negara Anggota OECD (Austria, Kanada, Denmark, Prancis, Jerman, Luksemburg, Norwegia, Swedia, dan Amerika Serikat telah mengesahkan undang-undang. Belgia, Islandia, Belanda, Spanyol, dan Swiss telah menyiapkan rancangan undang-undang) untuk mencegah pelanggaran hak asasi manusia yang fundamental, seperti penyimpanan

[19] Oktaviani Sugiarto, 2019, "Tinjauan Hukum Internasional Terkait Perlindungan Data dan Informasi Pribadi", Skripsi, Fakultas Hukum Universitas Hasanuddin, Makassar, hlm. 9.

data pribadi secara tidak sah, penyimpanan data pribadi tidak akurat, penyalahgunaan atau pengungkapan data tersebut tanpa izin.[20]

Terdapat bahaya dalam perbedaan peraturan-peraturan perundang-undangan nasional yang dapat menghambat arus bebas transfer data pribadi lintas batas. Hal ini dapat menyebabkan gangguan serius sektor-sektor penting ekonomi, seperti perbankan dan asuransi. Untuk alasan ini negara-negara Anggota OECD menganggap perlunya untuk mengembangkan Panduan yang akan membantu menyelaraskan undang-undang privasi nasional serta menegakkan hak asasi manusia, di saat yang bersamaan juga akan mencegah interupsi dalam arus data internasional. Mereka mewakili konsensus tentang prinsip-prinsip dasar yang dapat dimasukkan ke dalam undang-undang nasional yang ada atau berfungsi sebagai dasar undang-undang di negara-negara yang belum memilikinya. Panduan ini dalam bentuk Rekomendasi oleh Dewan OECD, dikembangkan oleh sekelompok ahli pemerintah di bawah ketua *The Hon. Mr. Justice M.D. Kirby*, Ketua Komisi Reformasi Hukum Australia. Rekomendasi ini diadopsi dan berlaku pada tanggal 23 September 1980.[21]

Sejak beberapa dekade, *The Organisation for Economic Co-Operation and Development* (OECD) telah berperan penting mempromosikan penghormatan terhadap privasi sebagai nilai fundamental dan syarat untuk arus bebas transfer data pribadi lintas

[20] Kata Pengantar dalam OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Akses digital : http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top

[21] *Ibid.*

batas. Pada tahun 2013 OECD merevisi Panduan Privasi untuk pertama kalinya setelah diluncurkan pada 1980, *The OECD's Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* merupakan pembaruan pertama dari versi asli 1980 yang berfungsi sebagai kesepakatan internasional pertama mengenai seperangkat prinsip privasi.[22]

Dua tema yang dijalankan melalui Panduan yang telah diperbarui:[23]

- Fokus pada penerapan praktis perlindungan privasi melalui pendekatan yang didasarkan pada **manajemen risiko (*risk management)***, dan
- Kebutuhan untuk menangani dimensi privasi global melalui **peningkatan karakteristik, kelebihan, dan kekurangan (*improved interoperability*).**

Sejumlah konsep baru diperkenalkan, termasuk :[24]

- **Strategi privasi nasional *(National Privacy Strategies*).** Meskipun undang-undang yang efektif itu penting, kepentingan strategis privasi saat ini juga membutuhkan strategi nasional beragam (multifaset) yang dikoordinasikan di tingkat pemerintahan tertinggi.

[22] OECD Privacy Guidelines, http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm. Diakses pada tanggal 12 Februari 2021.
[23] *Ibid.*
[24] *Ibid.*

- **Program manajemen privasi (*Privacy Management Programmes*).** Ini berfungsi sebagai mekanisme operasional inti yang melaluinya organisasi menerapkan perlindungan privasi.
- **Pemberitahuan pelanggaran keamanan data (*Data Security Breach Notification)*.** Ketentuan ini mencakup pemberitahuan kepada otoritas dan pemberitahuan kepada individu yang terkena dampak pelanggaran keamanan yang memengaruhi data pribadi.

Pada bagian empat di bawah judul *"Basic Principles of Internasional Application: Free Flow and Legitimate Restrictions",* dalam *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[25] berisi bahwa pengontrol data tetap bertanggung jawab atas data pribadi yang berada di bawah kendalinya tanpa memperhatikan lokasi data. Pada poin ke-17, suatu negara Anggota tidak dapat membatasi arus lintas batas data pribadi antara anggota lain apabila negara lain secara substansial mematuhi pedoman ini atau memiliki perlindungan yang memadai, termasuk mekanisme penegakan yang efektif dan tindakan yang tepat oleh pengontrol data, serta memastikan tingkat perlindungan berkelanjutan yang konsisten dengan panduan ini. Apabila melakukan pembatasan transfer data pribadi harus proporsional dengan risiko yang

[25] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188

ada dengan mempertimbangkan sensitivitas data dan tujuan serta konteks pemrosesan.

b. *Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data*

The Convention for the Protection of Individual with regard to Automatic Processing of Personal Data (ETS No.108) dibuat oleh komite ahli pemerintah di bawah kewenangan *The European Commitee on Legal Co-operation* (CDCJ), dibuka untuk ditandatangani oleh Negara Anggota Dewan Eropa pada tanggal 28 Januari 1981 di Stasbourg. Instrumen hukum internasional ini merupakan konvensi yang berisi perlindungan terhadap *data privacy*. COE 108 terbuka untuk negara mana pun termasuk negara bukan anggota Dewan Eropa.[26] Pada tahun 2018 konvensi ini diperbaharui untuk mengatasi tantangan yang ditimbulkan oleh teknologi informasi dan komunikasi baru serta untuk memperkuat penegakan konvensi. Pembaruan ini dikenal dengan *The Modernized Convention 108* atau *Convention 108+.*

Tujuan dari Konvensi ini untuk memperkuat perlindungan data – perlindungan hukum individu terkait dengan pemrosesan otomatis informasi pribadi. Konvensi 108 (1981) mencerminkan kebutuhan aturan hukum baru dalam menghadapi ketergantungan yang meningkat pada data digital karena kapasitas penyimpanan yang lebih tinggi, biaya pemrosesan yang lebih rendah, dan pertumbuhan yang meroket dalam

[26] https://epic.org/privacy/intl/coeconvention/ diakses pada tanggal 26 Februari 2021.

transaksi data. Banyak sistem hukum nasional yang tidak memiliki aturan umum perlindungan data yang komprehensif tentang pengumpulan, penyimpanan, dan penggunaan informasi pribadi. Konvensi 108 ini telah ditandatangani dan diratifikasi oleh seluruh 47 anggota Dewan Eropa dan diratifikasi oleh tujuh negara non anggota.[27]

Sebagaimana yang dinyatakan dalam *Explanatory Memorandum*, konvensi ini memiliki tiga bagian (1) ketentuan hukum substantif berupa asas-asas; (2) aturan khusus tentang aliran data lintas batas; (3) mekanisme untuk saling membantu dan konsultasi antara Para Pihak.

Konvensi ini juga mengharuskan para pihak untuk mengesahkan ke dalam hukum domestik prinsip-prinsip perlindungan data yang diatur dalam Konvensi. Ini termasuk:

- Kualitas data.
- Larangan pemrosesan data kategori khususras.[28]
- Keamanan data.
- Hak individu untuk mengakses, mengoreksi, dan menghapus jika hak dilanggar.

Konvensi ini juga mendorong aliran data yang bebas, mencegah pihak-pihak yang memerlukan otoritas khusus kepada pihak lain kecuali

[27] *Ibid.*
[28] politik, kesehatan, agama, kehidupan seksual, catatan kriminal seseorang, jika tidak ada perlindungan hukum yang tepat.

untuk keadaan yang memaksa. Terakhir, Konvensi ini menetapkan sistem kerja sama dalam mengimplementasikan sistem tersebut, dan membentuk *Consultative Committee* untuk mengawasi dan melaksanakan konvensi.

Setelah proses peninjauan yang panjang sejak 2013 menghasilkan *2018 amending protocol*. Protokol ini dikenal dengan *The Modernized Privacy Convention or Convention 108+.* Tujuan modernisasi adalah untuk mengatasi tantangan privasi dari teknologi baru dan untuk memperkuat penegakan hukum.

Di antara perubahan lainnya, Konvensi yang dimodernisasi:

- Memerlukan pemberitahuan cepat atas pelanggaran data.
- Menetapkan otoritas pengawas nasional untuk memastikan kepatuhan.
- Mengizinkan transfer ke negara non-pihak hana jika data pribadi memiliki perlindungan yang cukup.
- Memberikan hak pengguna baru seputar pengambilan keputusan otomatis, termasuk transparansi algoritme.
- Membutuhkan proporsionalitas dan minimalisasi data.

Revisi dibuka untuk ditandatangani pada 11 Oktober 2018. Sejauh ini, dua puluh enam anggota dan satu non-anggota telah menandatangani protokol amandemen.

Pada bagian laporan penjelasan, Tujuan *Article 14* di bawah judul *“Transborder flows of personal data”* dalam *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* adalah untuk memfasilitasi kebebasan aliran informasi terlepas dari batas-batasannya sekaligus memastikan perlindungan yang sesuai bagi individu terkait dengan pemrosesan data pribadi. Transfer data lintas batas terjadi ketika data pribadi diungkapkan atau disediakan untuk penerima yang tunduk pada yurisdiksi negara lain atau organisasi internasional.

Tujuan rezim aliran lintas batas adalah untuk memastikan bahwa data pribadi awalnya diproses dalam yurisdiksi suatu pihak (misalnya data yang dikumpulkan atau disimpan di sana) yang selanjutnya berada yurisdiksi suatu negara yang bukan pihak dari Konvensi, diproses dengan pengamanan yang sesuai. Penting adanya bahwa data yang diproses dalam yurisdiksi suatu pihak selalu dilindungi oleh prinsip-prinsip perlindungan data yang relevan dari Konvensi. Meskipun terdapat berbagai macam sistem perlindungan, perlindungan yang diberikan harus memiliki kualitas sedemikian rupa untuk memastikan bahwa hak asasi manusia tidak terpengaruh oleh globalisasi dan aliran data lintas batas.

Pasal 14 hanya berlaku untuk arus keluar data, bukan arus masuknya, karena arus masuk dicakup oleh rezim perlindungan data dari pihak penerima.

Paragraf 1 berlaku untuk aliran data antara Para Pihak pada Konvensi. Aliran data tidak boleh dilarang atau dikenai otorisasi khusus "dengan tujuan semata-mata untuk melindungi data pribadi". Namun, Konvensi tidak membatasi kebebasan suatu Pihak untuk membatasi transfer data pribadi kepada Pihak lain untuk tujuan lain, termasuk misalnya keamanan nasional, pertahanan, keselamatan publik, atau kepentingan publik penting lainnya (termasuk perlindungan kerahasiaan negara).

Dasar pemikiran dari ketentuan dalam ayat 1 adalah bahwa semua Pihak yang telah berlangganan inti umum dari ketentuan perlindungan data yang ditetapkan dalam Konvensi, diharapkan menawarkan tingkat perlindungan yang dianggap tepat dan oleh karena itu pada prinsipnya memungkinkan data untuk beredar secara bebas. . Namun, mungkin ada kasus-kasus luar biasa di mana terdapat risiko yang nyata dan serius bahwa peredaran data pribadi secara bebas ini akan mengakibatkan pengelakan terhadap ketentuan-ketentuan Konvensi. Sebagai pengecualian, ketentuan ini harus ditafsirkan secara terbatas dan Para Pihak tidak dapat mengandalkannya dalam kasus di mana risikonya bersifat hipotetis atau kecil. Oleh karena itu, suatu Pihak hanya dapat meminta pengecualian dalam kasus tertentu jika ia memiliki bukti yang jelas dan dapat diandalkan bahwa mentransfer data ke Pihak lain dapat secara signifikan merusak perlindungan yang diberikan kepada data tersebut berdasarkan Konvensi, dan kemungkinan terjadinya hal ini tinggi.

Ini mungkin terjadi, misalnya, ketika perlindungan tertentu yang diberikan berdasarkan Konvensi tidak lagi dijamin oleh Pihak lain (misalnya karena otoritas pengawasnya tidak lagi dapat secara efektif menjalankan fungsinya) atau ketika data kemungkinan besar akan ditransfer ke Pihak lain. untuk dipindahkan lebih lanjut (transfer selanjutnya) tanpa tingkat perlindungan yang sesuai dijamin. Pengecualian lebih lanjut yang diakui dalam hukum internasional ada di mana Para Pihak terikat oleh aturan perlindungan yang harmonis yang dimiliki oleh para negara yang telah bergabung dalam organisasi regional (ekonomi) yang mencari tingkat integrasi yang lebih dalam.

Antara lain, ini berlaku untuk negara anggota UE. Namun, sebagaimana secara eksplisit dinyatakan dalam Peraturan Perlindungan Data Umum (UE) 2016/679, aksesi negara ketiga ke Konvensi 108 dan implementasinya akan menjadi faktor penting saat menerapkan rezim transfer internasional UE, khususnya saat menilai apakah negara ketiga menawarkan tingkat perlindungan yang memadai (yang pada gilirannya memungkinkan aliran data pribadi dengan bebas).

Paragraf 2 mengatur kewajiban untuk memastikan, pada prinsipnya, bahwa "tingkat perlindungan yang sesuai berdasarkan ketentuan Konvensi dijamin". Pada saat yang sama, menurut paragraf 4, Para Pihak dapat mentransfer data meskipun tidak ada tingkat perlindungan yang sesuai di mana hal ini dibenarkan, antara lain, oleh “kepentingan sah yang berlaku, khususnya kepentingan publik yang

penting” sejauh ini disediakan karena menurut hukum dan transfer semacam itu merupakan tindakan yang perlu dan proporsional dalam masyarakat demokratis. Data pribadi dengan demikian dapat ditransfer dengan alasan yang serupa dengan yang tercantum dalam Pasal 11, paragraf 1 dan 3. Dalam semua kasus, Para Pihak tetap bebas berdasarkan Konvensi untuk membatasi transfer data kepada non-Pihak, baik itu untuk tujuan perlindungan data atau karena alasan lain.

Paragraf 2 mengacu pada arus lintas batas data pribadi ke penerima yang tidak tunduk pada yurisdiksi suatu Pihak. Untuk setiap data pribadi yang mengalir di luar batas negara, tingkat perlindungan yang sesuai harus dijamin. Dalam kasus di mana penerima bukan merupakan Pihak pada Konvensi, Konvensi menetapkan dua mekanisme untuk memastikan bahwa tingkat perlindungan data memang sesuai; baik oleh hukum, atau *ad hoc* atau pengamanan standar yang disetujui yang mengikat dan dapat ditegakkan secara hukum, serta diterapkan sebagaimana mestinya.

Paragraf 2 dan 3 berlaku untuk semua bentuk perlindungan yang sesuai, baik yang disediakan oleh hukum atau oleh pengamanan standar. Undang-undang harus memasukkan elemen-elemen perlindungan data yang relevan sebagaimana diatur dalam Konvensi ini. Tingkat perlindungan harus dinilai untuk setiap transfer atau kategori transfer. Berbagai elemen transfer harus diperiksa seperti: jenis data; tujuan dan durasi pemrosesan data yang ditransfer; penghormatan terhadap aturan

hukum oleh negara tujuan akhir; aturan hukum umum dan sektoral yang berlaku di Negara atau organisasi yang bersangkutan; dan aturan profesional dan keamanan yang berlaku di sana.

Konten perlindungan *ad hoc* atau standar harus mencakup elemen perlindungan data yang relevan. Selain itu, persyaratan kontrak dapat berupa, misalnya, subjek data diberikan dengan narahubung pada staf orang yang bertanggung jawab atas transfer data, yang bertanggung jawab untuk memastikan kepatuhan dengan standar perlindungan substantif. Subjek data akan bebas untuk menghubungi orang ini kapan saja dan tanpa biaya terkait dengan pemrosesan atau transfer data dan, jika memungkinkan, mendapatkan bantuan dalam menggunakan haknya.

Penilaian mengenai apakah tingkat perlindungan yang tepat harus mempertimbangkan prinsip-prinsip Konvensi, sejauh mana mereka dipenuhi di Negara atau organisasi penerima - sejauh relevan untuk kasus transfer tertentu - dan bagaimana subjek data dapat mempertahankan kepentingannya jika ada ketidakpatuhan. Keberlakuan hak subjek data dan penyediaan ganti rugi administratif dan yudisial yang efektif untuk subjek data yang data pribadinya sedang ditransfer harus dipertimbangkan dalam penilaian. Demikian pula, penilaian dapat dilakukan untuk seluruh Negara Bagian atau organisasi sehingga memungkinkan semua transfer data ke tujuan tersebut.

Paragraf 4 memungkinkan Para Pihak untuk menyimpang dari prinsip yang membutuhkan tingkat perlindungan yang sesuai dan untuk memungkinkan transfer ke penerima yang tidak menjamin perlindungan tersebut. Pengurangan seperti itu diizinkan hanya dalam situasi terbatas: dengan persetujuan subjek data atau kepentingan tertentu dan / atau di mana terdapat kepentingan sah yang ditetapkan oleh undang-undang dan / atau pengalihan merupakan tindakan yang diperlukan dan proporsional dalam masyarakat demokratis untuk kebebasan berekspresi. Penurunan tersebut harus menghormati prinsip kebutuhan dan proporsionalitas.

Paragraf 5 menetapkan ketentuan untuk pengamanan tambahan: yaitu bahwa otoritas pengawas yang berwenang diberikan semua informasi yang relevan mengenai transfer data sebagaimana dimaksud dalam ayat 3.b, dan, atas permintaan 4.b dan 4.c. Pihak berwenang harus berhak meminta informasi yang relevan tentang keadaan dan justifikasi transfer ini. Di bawah kondisi yang ditetapkan dalam Pasal 11, ayat 3, pengecualian terhadap Pasal 14, ayat 5 diperbolehkan.

Menurut ayat 6, otoritas pengawas harus berhak meminta agar efektivitas tindakan yang diambil atau keberadaan kepentingan sah yang berlaku didemonstrasikan, dan untuk melarang, menangguhkan atau memaksakan persyaratan pada transfer jika hal ini terbukti perlu dalam melindungi hak dan kebebasan fundamental subjek data. Di bawah kondisi yang ditetapkan dalam Pasal 11, ayat 3 pengecualian untuk Pasal 14, ayat 6 diperbolehkan.

Arus data yang terus meningkat dan kebutuhan terkait untuk meningkatkan perlindungan data pribadi juga memerlukan peningkatan kerja sama penegakan hukum internasional di antara otoritas pengawas yang kompeten.

c. *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows*

Teks tersebut akan meningkatkan perlindungan data pribadi dan privasi dengan meningkatkan Konvensi asli tahun 1981 (ETS No. 108) di dua bidang. Pertama, menyediakan pengaturan otoritas pengawas nasional yang bertanggung jawab untuk memastikan kepatuhan terhadap undang-undang atau peraturan yang diadopsi sesuai dengan konvensi, mengenai perlindungan data pribadi dan aliran data lintas batas. Perbaikan kedua menyangkut aliran data lintas batas ke negara ketiga. Data hanya dapat ditransfer jika Negara penerima atau organisasi internasional mampu memberikan tingkat perlindungan yang memadai.[29]

Pada Laporan Penjelasan Protokol Tambahan[30], menjelaskan Pasal 2 yang berisi pengaturan mengenai aliran data pribadi lintas batas ke penerima yang tidak tunduk pada yurisdiksi pihak pada konvensi ini.

[29] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181
[30] Additional Protocol to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, 2001

Pasal 12 Konvensi menetapkan prinsip aliran bebas data pribadi antara Para Pihak tunduk pada kemungkinan pengurangan yang diatur dalam sub-paragraf 3. Hal ini menyiratkan, khususnya, bahwa prinsip-prinsip Konvensi telah dilaksanakan.

Aliran data pribadi lintas batas ke penerima yang tidak tunduk pada yurisdiksi suatu Pihak hanya terkait secara tidak langsung. Menurut Pasal 12 ayat 3b, suatu negara dapat menyimpang dari prinsip sirkulasi bebas data antara wilayahnya dan penerima yang tidak tunduk pada yurisdiksi suatu Pihak melalui Pihak lain, untuk menghindari pengalihan tersebut yang mengakibatkan pengelakan undang-undang dari Pihak asal. Oleh karena itu, tidak ada ketentuan khusus tentang arus data lintas batas berkenaan dengan negara atau organisasi yang bukan Pihak Konvensi.

Oleh karena itu, Para Pihak pada Konvensi dapat membuat ketentuan dalam sistem hukum mereka untuk otorisasi eksplisit transfer data pribadi kepada penerima yang tidak tunduk pada yurisdiksi suatu Pihak dengan tingkat perlindungan yang berbeda terhadap Konvensi. Pada saat Protokol ini dibuat, meskipun mereka tidak memiliki kewajiban eksplisit untuk melakukannya, beberapa Pihak telah memasukkan aturan ke dalam hukum domestik mereka tentang transfer data ke penerima yang tidak tunduk pada yurisdiksi suatu Pihak. Perbedaan dalam praktik, terutama dalam kaitan dengan Pasal 12 ayat 3b yang disebutkan di atas, dapat menyebabkan pembatasan substansial pada peredaran bebas data antara Para Pihak, yang juga akan bertentangan dengan tujuan Konvensi.

Oleh karena itu perlu, tindakan seperti itu ditentukan di satu sisi oleh keinginan untuk menjamin perlindungan yang efektif atas data pribadi di luar batas negara dan, di sisi lain, oleh tekad Para Pihak untuk memastikan peredaran bebas informasi antar masyarakat, sesuai dengan kata-katanya dari Pembukaan Konvensi.

Arus data lintas batas ke penerima yang tidak tunduk pada yurisdiksi suatu Pihak tunduk pada kondisi suatu memadai tingkat perlindungan di negara atau organisasi penerima. Paragraf 70 dari laporan penjelasan Konvensi mengacu pada "Negara non-pihak (memiliki) a memuaskan rezim perlindungan data ". Penerima yang tidak tunduk pada yurisdiksi suatu Pihak pada Konvensi hanya dapat dianggap memiliki rezim perlindungan data yang memuaskan jika diberikan tingkat perlindungan yang memadai.

Kecukupan tingkat perlindungan harus dinilai berdasarkan semua keadaan yang berkaitan dengan pengalihan. Tingkat perlindungan harus dinilai berdasarkan kasus per kasus untuk setiap transfer atau kategori transfer yang dilakukan. Dengan demikian, keadaan transfer harus diperiksa dan, khususnya, jenis data, tujuan dan durasi pemrosesan data yang ditransfer, negara asal dan negara tujuan akhir, aturan hukum umum dan sektoral, berlaku di negara bagian atau organisasi yang bersangkutan dan aturan profesional dan keamanan yang diperoleh di sana.

Penilaian kecukupan juga dapat dilakukan untuk seluruh negara bagian atau organisasi sehingga memungkinkan semua transfer data ke tujuan ini. Dalam hal ini, tingkat perlindungan yang memadai ditentukan oleh otoritas yang berwenang dari masing-masing Pihak.

Penilaian tingkat perlindungan yang memadai harus mempertimbangkan prinsip-prinsip Bab II Konvensi dan Protokol ini dan sejauh mana mereka dipenuhi di negara atau organisasi penerima - sejauh itu relevan untuk tujuan tertentu. Kasus transfer - dan bagaimana subjek data dapat mempertahankan kepentingannya jika terjadi ketidakpatuhan dalam kasus tertentu.

Komite Konsultatif Konvensi dapat, atas permintaan salah satu Pihak, memberikan pendapat tentang kecukupan tingkat perlindungan data di negara atau organisasi ketiga.

Para pihak memiliki keleluasaan untuk menentukan pengurangan dari prinsip tingkat perlindungan yang memadai. Namun, ketentuan hukum domestik yang relevan harus menghormati prinsip yang melekat dalam hukum Eropa bahwa klausul yang membuat pengecualian ditafsirkan secara terbatas, sehingga pengecualian tidak menjadi aturan. Oleh karena itu, pengecualian hukum domestik dapat dibuat untuk kepentingan sah yang berlaku. Kepentingan itu mungkin untuk melindungi kepentingan publik yang penting, seperti yang ditentukan dalam konteks Pasal 8 ayat 2 Konvensi Eropa tentang Hak Asasi Manusia dan Pasal 9 ayat 2 Konvensi

ETS No. 108; pelaksanaan atau pembelaan klaim hukum; atau ekstraksi data dari register publik. Pengecualian juga dapat dibuat untuk kepentingan spesifik subjek data seperti untuk pemenuhan kontrak dengan subjek data atau untuk kepentingannya, atau untuk melindungi kepentingan vitalnya atau ketika dia telah memberikan persetujuannya. Dalam hal ini, sebelum memberikan persetujuan, subjek data harus diberi tahu dengan cara yang tepat tentang transfer yang dimaksud.

Masing-masing pihak dapat memberikan transfer data pribadi kepada penerima yang tidak tunduk pada yurisdiksi suatu Pihak dan tidak memastikan tingkat perlindungan yang memadai, asalkan orang yang bertanggung jawab atas transfer memberikan pengamanan yang memadai. Pengamanan ini harus dianggap memadai oleh otoritas pengawas yang kompeten menurut hukum domestik. Perlindungan tersebut secara khusus mungkin merupakan hasil dari klausul kontrak yang mengikat pengontrol yang melakukan transfer dan penerima yang tidak tunduk pada yurisdiksi suatu Pihak.

Isi kontrak terkait harus mencakup elemen perlindungan data yang relevan. Selain itu, dalam istilah prosedural, persyaratan kontrak dapat berupa, misalnya, subjek data memiliki kontak person pada staf orang yang bertanggung jawab atas transfer, yang bertanggung jawab untuk memastikan kepatuhan dengan standar perlindungan yang substantif. Subjek bebas untuk menghubungi orang ini kapan saja dan tanpa biaya

dan, jika memungkinkan, mendapatkan bantuan dalam menggunakan haknya.

d. *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*

Tujuan dari Protokol amandemen adalah untuk memodernisasi dan meningkatkan Konvensi (ETS No.108), dengan mempertimbangkan tantangan baru terhadap perlindungan individu dalam hal pemrosesan data.[31]

Modernisasi Konvensi Perlindungan Individu terkait Pemrosesan Otomatis Data Pribadi, merupakan satu-satunya perjanjian internasional yang bersifat mengikat secara hukum dengan relevansi global di bidang ini, mengatasi tantangan privasi yang diakibatkan dari menggunakan teknologi informasi dan komunikasi baru, serta memperkuat mekanisme konvensi untuk memastikan implementasi yang efektif.

Protokol memberikan kerangka hukum multilateral yang kuat dan fleksibel untuk memfasilitasi aliran data lintas batas sambil memberikan perlindungan yang efektif saat data pribadi digunakan. Ini merupakan jembatan antara berbagai wilayah di dunia dan kerangka normatif yang berbeda, termasuk undang-undang Uni Eropa yang baru yang akan

[31] Council of European Portal, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 diakses pada tanggal 1 Maret 2021.

berlaku penuh pada 25 Mei 2018 dan yang mengacu pada Konvensi 108 dalam konteks aliran data lintas batas.

Beberapa inovasi yang terkandung dalam Protokol adalah sebagai berikut:[32]

- Persyaratan yang lebih kuat mengenai proporsionalitas dan prinsip minimisasi data, dan keabsahan pemrosesan;
- Perluasan jenis data sensitif, yang sekarang akan mencakup data genetik dan biometrik, keanggotaan serikat pekerja dan asal etnis;
- Kewajiban untuk mengumumkan pelanggaran data;
- Transparansi yang lebih besar dari pemrosesan data;
- Hak-hak baru untuk orang-orang dalam konteks pengambilan keputusan algoritmik, yang sangat relevan dalam kaitannya dengan pengembangan kecerdasan buatan;
- Akuntabilitas pengontrol data yang lebih kuat;
- Persyaratan bahwa prinsip "privasi menurut desain" diterapkan;
- Penerapan prinsip-prinsip perlindungan data untuk semua aktivitas pemrosesan, termasuk untuk alasan keamanan nasional, dengan kemungkinan pengecualian dan pembatasan yang tunduk pada ketentuan yang ditetapkan oleh Konvensi, dan dalam hal apa pun dengan tinjauan dan pengawasan independen dan efektif;
- Rezim yang jelas dari aliran data lintas batas;

[32] *Ibid.*

- Kekuasaan yang diperkuat dan kemandirian otoritas perlindungan data dan meningkatkan dasar hukum untuk kerja sama internasional.

e. *European Union on Data Protection Directive (Uni Eropa, 24 Oktober 1995) digantikan dengan European Union General Data Protection Regulation (GDPR)*

Komisi Eropa mencetuskan reformasi perlindungan data pada 25 Januari 2012.[33] Usulan reformasi ini melingkupi dua hal utama, yaitu: regulasi yang secara umum berkaitan pada perlindungan data (*GDPR*), serta sebuah direktif yang bertautan pada pemrosesan data pribadi di dalam lingkup peradilan pidana.[34] Pada 8 April 2016, GDPR ada sebagai penganti Direktif Perlindungan Data 1995, bersamaan dengan hal itu pula lahirlah sebuah Direktif Perlindungan Data baru. Berikut adalah uraian singkat mengenai hal tersebut:[35]

- "Regulasi (EU) 2016/679 *GDPR"*: aturan ini merupakan tindakan yang diambil oleh UE dalam menegaskan kekuatan hak asasi warga pada zaman digital serta memberi kemudahan di bidang bisnis melalui cara penyederhanaan aturan untuk perusahaan dalam "*digital single*

[33] European Union (2014). *Handbook on European data protection law* (dalam bahasa Inggris). Belgium: Publications Office of the European Union. Hlm. 21.
[34] Dorraji, Seyed Ebrahim; Barcys, Mantas (2014). "Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations". *Social Technologies* (dalam bahasa Inggris). Lithuania: Mykolas Romeris University.**4** (3): 306–317. Hlm. 310.
[35] European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en . Diakses tanggal 1 Maret 2021.

market". *GDPR* adalah suatu aturan komprehensif dalam semua wilayah UE dimana bisa meniadakan fragmentasi dan juga mahalnya beban administrasi. *GDPR* berlaku bagi pihak yang memproses atau mengendalikan data pribadi. Dikarenakan sangat penting dalam ekonomi data sehingga perusahaan mengalami pengaruh yang signifikan karena adanya GDPR. Regulasi ini berlaku sejak 24 Mei 2016 dan diterapkan sejak 25 Mei 2018.

- "Direktif (EU) 2016/680": arahan dengan tujuan melindungi hak asasi warga negara dalam hal perlindungan data apabila data pribadi digunakan oleh otoritas penegak hukum pidana. Dengan tujuan memastikan perlindungan yang memadai terhadap data pribadi korban, saksi, maupun tersangka kejahatan serta mempermudah kerja sama lintas batas dalam hal memerangi kejahatan dan terorisme. Arahan ini melindungi individu dalam eksekusi hukuman pidana, dimana data pribadi dilindungi ketika diproses oleh pihak berwenang untuk tujuan pencegahan, penyelidikan, deteksi atau penuntutan pelanggaran pidana.[36] Direktif ini mulai berlaku pada tanggal 5 Mei 2016 dan negara-negara UE harus mengubahnya ke dalam hukum nasional mereka pada 6 Mei 2018.

GDPR sebagai suatu regulasi memiliki perbedaan dengan direktif, *GDPR* akan langsung berlaku dan dapat diterapkan di negara-negara UE walaupun tidak ada penyusunan direktif terlebih dahulu atau

[36] European Union (2016b). *How will the data protection reform help fight international crime?*. *Factsheet* (dalam bahasa Inggris). Brussels: Publication Office.

tidak perlu pembuatan peraturan pelaksanaan oleh negara anggota tersebut.[37] Melalui pemerataan aturan dalam perlindungan data ini, *GDPR* memiliki kepastian hukum serta menghilangkan potensi halangan terhadap aliran bebas data pribadi.[38] *GDPR* sendiri membawa beberapa perubahan antara lain*:*[39]

- Peningkatan ruang lingkup teritorial
- Syarat penyimpanan data yang ditingkatkan
- Peningkatan penalti
- Penunjukan Petugas Perlindungan Data (*Data Protection Officer/DPO)*
- Kewajiban yang lebih luas untuk Pengontrol Data (organisasi yang mengumpulkan dan mengelola data warga UE)
- Kewajiban yang lebih luas untuk Pengolah Data (setiap perusahaan yang memproses data pribadi atas nama Pengontrol Data)
- Pelaporan pembobolan data yang lebih tepat waktu
- Hak atas portabilitas data
- Hak untuk dihapus (hak untuk dilupakan atau *right to be forgotten*)
- Izin subyek data yang diperkuat

[37] Lambert, Paul (2017). *Understanding the new European data protection rules* (dalam bahasa Inggris). Boca Raton: CRC Press. hlm. 98.
[38] Voigt, Paul & Bussche, Axel von dem (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (dalam bahasa Inggris). Switzerland: Springer International Publishing AG. Hlm. 2.
[39] Russell, Chad & Fuller, Shane (2017). *GDPR For Dummies®, MetaCompliance Special Edition* (PDF) (dalam bahasa Inggris). UK: John Wiley & Sons, Ltd. Hlm. 6.

GDPR dalam kaitannya dengan teritorial tidak memiliki beda antara pengendali (*controller*) dan prosesor (*processor*), dengan arti lain keduanya memiliki lingkup teritorial yang sama. Terutama *GDPR* memiliki peran dalam situasi berikut:[40]

- Pihak yang memproses data sebagai bagian dari kegiayan salah satu cabangnya yang didirikan di UE, hal ini terlepas dari mana data diproses, atau
- perusahaan dan atau pihak lain yang didirikan di luar UE memiliki penawaran barang/jasa (berbayar atau gratis) atau para pengamat perilaku individu di UE.

Arus data pribadi ke dan dari negara di luar Uni Eropa dan organisasi internasional diperlukan untuk perluasan perdagangan internasional dan kerja sama internasional. Hal ini menimbulkan tantangan dan kekhawatiran baru terkait dengan perlindungan data pribadi. Namun, ketika data pribadi ditransfer dari Uni Eropa ke pengontrol, pemroses, atau penerima lainnya di negara ketiga atau ke organisasi internasional, tingkat perlindungan orang perorangan yang dijamin oleh Peraturan ini tidak boleh dirusak, termasuk dalam kasus transfer selanjutnya. Dalam hal apa pun, transfer data pribadi ke negara ketiga dan organisasi internasional lainnya hanya dapat dilakukan dengan sepenuhnya memenuhi peraturan ini. Pengalihan hanya dapat dilakukan jika, dengan tunduk pada ketentuan

[40] Voigt & Bussche (2017), hlm. 22.

lain peraturan ini, persyaratan yang ditetapkan dalam ketentuan peraturan ini terkait dengan pengalihan data pribadi ke negara ketiga atau organisasi internasional dipatuhi oleh pengontrol atau pemroses.

Bab V GDPR[41] dengan judul bab "Transfer data pribadi ke negara ketiga atau organisasi internasional"[42], berisi Pasal 44 hingga Pasal 50 peraturan tersebut.

> Terjemahan bebas *Article 44 "General Principle for Transfers"*:
>
> "Setiap transfer data pribadi yang sedang diproses atau dimaksudkan untuk diproses setelah transfer ke negara ketiga atau ke organisasi internasional hanya akan terjadi jika, dengan tunduk pada ketentuan lain dari Peraturan ini, kondisi yang ditetapkan dalam Bab ini dipenuhi oleh pengontrol dan pemroses, termasuk untuk penerusan data pribadi dari negara ketiga atau organisasi internasional ke negara ketiga lain atau ke organisasi internasional lain. Semua ketentuan dalam Bab ini akan diterapkan untuk memastikan bahwa tingkat perlindungan orang perseorangan yang dijamin oleh Regulasi ini tidak dirusak."

Menurut Pasal 44 yang berjudul "Asas umum transfer", setiap transfer data pribadi yang sedang diproses atau dimaksudkan untuk diproses setelah transfer ke negara ketiga atau ke organisasi internasional hanya akan terjadi jika, tunduk pada ketentuan lain dari peraturan ini, persyaratan yang ditetapkan dalam bab ini dipenuhi oleh pengontrol dan pemroses, termasuk untuk penerusan data pribadi dari negara ketiga atau

[41] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (27 April 2016) 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)

[42] *CHAPTER V* : *Transfers of personal data to third countries or international organisations*

organisasi internasional ke negara ketiga lain atau ke organisasi lain. Semua ketentuan dalam bab ini akan diterapkan untuk memastikan bahwa tingkat perlindungan orang perseorangan yang dijamin oleh regulasi ini tidak dirusak.

Pasal 45 GDPR dengan judul “Transfer berdasarkan keputusan kecukupan”, mengatur dalam paragraf 1 hingga 3, dimana transfer data pribadi ke negara ketiga atau organisasi internasional dapat terjadi jika Komisi telah memutuskan bahwa negara ketiga, wilayah atau satu atau lebih sektor tertentu di negara ketiga tersebut, atau organisasi internasional yang bersangkutan memastikan tingkat yang memadai dari perlindungan transfer semacam itu tidak memerlukan otoritas khusus.

Saat menilai kecukupan tingkat perlindungan, Komisi harus secara khusus mempertimbangkan elemen-elemen berikut:

a) Supremasi hukum, penghormatan terhadap hak asasi manusia dan kebebasan fundamental, perundang-undangan yang relevan, baik umum maupun sektoral, termasuk tentang keamanan publik, pertahanan, keamanan nasional dan hukum pidana dan akses otoritas publik ke data pribadi serta penerapannya. Undang-undang, aturan perlindungan data, aturan profesional dan langkah-langkah keamanan, termasuk aturan untuk penelusuran data pribadi ke negara ketiga lain atau organisasi internasional yang dipatuhi di negara atau organisasi internasional, hukum kasus,

serta data yang efektif dan dapat dilaksanakan hak subjek dan ganti rugi administratif dan yudisial yang efektif untuk subjek data yang data pribadinya sedang ditransfer;

b) Keberadaan dan fungsi efektif dari satu atau lebih otoritas pengawas independen di negara ketiga atau di mana organisasi internasional tunduk, dengan tanggung jawab untuk memastikan dan menegakkan kepatuhan dengan aturan perlindungan data, termasuk kekuatan penegakan yang memadai, untuk membantu dan memberi nasihat tentang subjek data dalam menggunakan hak mereka dan untuk bekerja sama dengan otoritas pengawas dari Negara Anggota; dan

c) Komitmen internasional yang telah dibuat oleh negara ketiga atau organisasi internasional terkait, atau kewajiban lain yang timbul dari konvensi atau instrumen yang mengikat secara hukum serta dari partisipasinya dalam sistem multilateral atau regional, khususnya terkait dengan perlindungan data pribadi.

Komisi setelah menilai kecukupan tingkat perlindungan dapat memutuskan dengan menetapkan tindakan, bahwa negara ketiga, wilayah atau satu atau lebih sektor tertentu di negara ketiga atau organisasi internasional memastikan tingkat yang memadai. Perlindungan yang dimaksudkan dalam pasal ini yaitu tindakan pelaksana harus menyediakan mekanisme untuk tinjauan berkala, setidaknya setiap empat

tahun, yang harus mempertimbangkan semua perkembangan yang relevan di negara ketiga atau organisasi internasional. Tindakan pelaksana harus menentukan penerapan teritorial yang dirujuk dalam poin (b) ayat 2 pasal ini.

Pasal 46 GDPR dengan judul “Transfer tunduk pada pengamanan yang sesuai”, memiliki tiga paragraf berisi jika tidak ada keputusan yang sesuai dengan Pasal 45(3), pengontrol atau pemroses dapat mentransfer data pribadi ke negara ketiga atau organisasi internasional hanya jika pengontrol atau pemroses telah memberikan pengamanan yang sesuai, dan dengan syarat bahwa hak subjek data yang dapat diberlakukan dan solusi hukum yang efektif untuk subjek data tersedia.

Pengamanan yang sesuai sebagaimana dimaksud dalam ayat 1 dapat disediakan, tanpa memerlukan otoritas khusus dari otoritas pengawas, oleh:

a) Instrumen yang mengikat dan dapat ditegakkan secara hukum antara otoritas atau badan publik;

b) Mengikat aturan perusahaan sesuai dengan Pasal 47;

c) Klausul perlindungan data standar yang diadopsi oleh komisi sesuai dengan prosedur pemeriksaan sebagaimana dimaksud dalam Pasal 93 (2);

d) Klausul perlindungan data standar yang diadopsi oleh otoritas pengawas dan disetujui oleh komisi sesuai dengan prosedur pemeriksaan sebagaimana dimaksud dalam Pasal 93 (2);

e) Kode etik yang disetujui sesuai dengan Pasal 40 bersama dengan komitmen yang mengikat dan sapat dilaksanakan dari pengontrol atau pemroses di negara ketiga untuk menerapkan pengamanan yang sesuai, termasuk dalam hal hak subjek data; atau

f) Mekanisme sertifikasi yang disetujui sesuai dengan Pasal 42 bersama dengan komitmen yang mengikat dan dapat dilaksanakan dari pengontrol atau pemroses di negara ketiga untuk menerapkan pengamanan yang sesuai termasuk dalam hal hak subjek data.

Tunduk pada otoritas dari otoritas pengawas yang kompeten, pengamanan yang sesuai sebagaimana dimaksud dalam ayat 1 juga dapat disediakan untuk khususnya oleh:

a) Klausa kontrak antara pengontrol atau pemroses dan pengontrol, pemroses atau penerima data pribadi di negara ketiga atau organisasi internasional; atau

b) Ketentuan yang akan dimasukkan ke dalam pengaturan administratif antara otoritas atau badan publik yang mencakup hak subjek data yang dapat dilaksanakan dan efektif.

f. African Union Convention on Cyber Security and Personal Data Protection

Konvensi Uni Afrika tentang Keamanan Siber dan Perlindungan Data Pribadi diadopsi pada Sesi Biasa ke-23 dari KTT Uni Afrika yang ditutup di Malabo, Guinea Ekuatorial pada 27 Juni 2014. Konvensi, yang secara substansial mengusung bahasa 'privasi' pada tingkat ini berupaya untuk membangun kerangka hukum untuk Keamanan Siber dan Perlindungan Data Pribadi sebagai kelanjutan dari komitmen yang ada dari Negara Anggota Uni Afrika di tingkat sub-regional, regional dan internasional untuk membangun Masyarakat Informasi.[43]

Pada Pasal 28 Konvensi Uni Afrika tentang Keamanan Siber dan Perlindungan Data Pribadi[44] membahas tentang Kerja Sama Internasional yang berisi empat poin yaitu :

Pertama, Harmonisasi *(Harmonization).* Negara-negara Pihak harus memastikan bahwa tindakan legislatif dan/atau peraturan yang diadopsi untuk melawan kejahatan dunia maya akan memperkuat harmonisasi regional dari tindakan-tindakan ini dan menghormati prinsip tanggung jawab pidana ganda (*the principle of double criminal liability)*.

[43] African Declaration on Internet Rights and Freedom, diakses online pada tanggal 2 Maret 2021 https://africaninternetrights.org/en/resource/african-union-convention-cybersecurity-and-personal-data-protection

[44] AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, Article 28 - International Cooperation

Kedua, Bantuan Hukum Bersama *(Mutual Legal Assistance).* Negara-negara Pihak yang tidak memiliki perjanjian tentang bantuan timbal baik dalam kejahatan dunia maya harus berupaya untuk mendorong penandatanganan perjanjian tentang bantuan hukum timbal balik sesuai dengan *the principle of double criminal liability,* sambil mempromosikan pertukaran informasi serta pembagian data yang efisien antara organisasi-organisasi Negara Pihak secara bilateral dan multilateral.

Ketiga, Pertukaran Informasi *(Exchange od Information).* Negara-negara Pihak harus mendorong pembentukan lembaga yang bertukar informasi tentang ancaman dunia maya dan penilaian kerentanan seperti *Computer Emergency Response Team (CERT)* atau *Computer Security Incident Response Team (CSIRTs)*

Keempat, Sarana Kerja Sama *(Means of Cooperation).* Negara-negara Pihak harus menggunakan sarana yang ada untuk kerja sama internasional dengan tujuan untuk menanggapi ancaman dunia maya, meningkatkan keamanan dunia maya dan merangsang dialog antara para pemangku kepentingan. Mungkin secara internasional, antar pemerintah atau regional, atau berdasarkan kemitraan swasta dan publik.

g. Privacy Shield Frameworks

Kerangka Kerja Perlindungan Privasi UE-AS dan Swiss-AS dirancang oleh Departemen Perdagangan AS, Komisi Eropa, dan

Administrasi Swiss, yang masing-masing memberikan mekanisme kepada perusahaan di kedua sisi Atlantik sebagai pemenuhan persyaratan dalam perlindungan data pada saat melakukan transfer data pribadi dari Uni Eropa dan Swiss hingga Amerika Serikat untuk mendukung perdagangan translantik.[45]

Pada 12 Juli 2016, Komisi Eropa menganggap *UE-US Privacy Shield Framework* memadai untuk memungkinkan transfer data berdasarkan hukum UE.[46] Pada 12 Januari 2017 Pemerintah Swiss mengumumkan persetujuan *Swiss-US Privacy Shield Framework* sebagai mekanisme hukum yang valid untuk mematuhi persyaratan Swiss pada saat melakukan transfer data pribadi dari Swiss ke Amerika Serikat.[47]

Komisi Eropa dan Amerika Serikat menyetujui kerangka kerja baru untuk aliran data transatlantik yaitu UE-US *Privacy Shield* sebagai pengganti *Safe Harbor Framework* melalui keputusan Pengadilan Eropa pada 6 Oktober 2015.[48] Pengaturan ini memberikan kewajiban yang lebih kuat kepada perusahaan di AS untuk melindungi data pribadi orang Eropa serta memperkuat pemantauan dan penegakan oleh *The U.S Departement of Commerce* dan *Federal Trade Commission (FTC)*,

---

[45] *Privacy Shield Framework Overview* - *https://www.privacyshield.gov/Program-Overview* diakses pada tanggal 8 Maret 2021

[46] Lihat *adequancy determination – Commission Implementing Decision (UE) 2016/1250* - *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG*

[47] *Privacy Shield Framework Overview*

[48] European Commission - Press release: political agreement on framework, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216

termasuk melalui peningkatan kerja sama dengan *European Data Protection Authorities*.

Privacy Shield mencakup elemen-elemen berikut:[49]

- Kewajiban yang kuat perusahaan dalam menangani data pribadi orang Eropa dan penegakan hukum yang tegas.
- Perlindungan yang jelas dan kewajiban transparansi pada akses pemerintah AS.
- Perlindungan efektif hak warna negara UE dengan beberapa kemungkinan ganti rugi.

Pada 16 Juli 2020 Pengadilan Eropa mengeluarkan putusan yang menyatakan Keputusan Komisi Eropa[50] tentang kecukupan perlindungan yang diberikan oleh *UE-US Privacy Shield*, "tidak valid/ *invalid".* Akibatnya, *UE-US Privacy Shield Framework* tidak lagi menjadi mekanisme valid untuk mematuhi persyaratan perlindungan data UE saat mentransfer data pribadi dari Uni Eropa ke Amerika Serikat. Keputusan tersebut tidak membebaskan peserta dalam *UE-US Privacy Shield* dari kewajiban mereka berdasarkan *UE-US Privacy Shield Framework.*[51]

Pada 8 September 2020, *the Federal Data Protection and Information Commissioner (FDPIC)* Swiss mengeluarkan pendapat yang berisi bahwa *Swiss-US Privacy Shield Framework* tidak memberikan

[49] *Ibid.*
[50] Keputusan Komisi Eropa 2016/1250 pada tanggal 12 Juli 2016
[51] *Privacy Shield Framework Overview*

tingkat perlindungan yang memadai untuk transfer data dari Swiss ke Amerika Serikat sesuai dengan Undang-

Undang Federal Swiss tentang Perlindungan Data (FADP). Berdasarkan hal tersebut, organisasi yang ingin mengandalkan Perlindungan Privasi Swiss-AS untuk mentransfer data pribadi dari Swiss ke Amerika Serikat harus meminta panduan dari FDPIC atau penasihat hukum. Pendapat tersebut tidak membebaskan peserta dalam *the Swiss-US Privacy Shield* dari kewajiban mereka berdasarkan *the Swiss-US Privacy Shield Framework.*[52]

h. Asia-Pacific Economic Cooperation (APEC) Privacy Framework

APEC Privacy Framework merupakan pendekatan fleksibel terhadap perlindungan privasi di seluruh negara anggota APEC tanpa membentuk penghalang arus bebas informasi yang tidak diperlukan. Kerangka kerja yang dimaksud mencakup :

- Meningkatkan berbagi informasi di antara lembaga pemerintah dan regulator;
- Menyediakan fasilitas transfer informasi yang aman antar ekonomi;
- Menetapkan seperangkat privasi umum;

[52] *Privacy Shield Framework Overview*

- Mendorong penggunaan data elektronik sebagai sarana untuk meningkatkan dan memperluas bisnis; dan
- Memberikan bantuan teknis kepada negara-negara yang belum menangani privasi dari perspektif peraturan atau kebijakan.

Sembilan prinsip dalam *APEC Privacy Framework* yaitu : *preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability.* Kesembilan prinsip tersebut telah dikembangkan kode etik dimana bisnis akan memperoleh sertifikat pihak ketiga atas kepatuhan mereka. Otoritas penegakan privasi dari ekonomi APEC yang berpartisipasi seperti FTC akan dapat mengambil tindakan penegakan hukum terhadap perusahaan yang melanggar komitmen mereka berdasarkan kode etik.[53]

Para menteri ekonomi anggota APEC pada September 2007 mendukung *APEC Privacy Pathfinder* yang merupakan bentuk komitmen untuk bekerja sama mengembangkan sistem dalam penyediaan aliran data lintas batas yang dapat dipertanggungjawabkan sesuai dengan *APEC Privacy Framework.* Kesepakatan dilakukan dengan mempertimbangkan mekanisme implementasi internasional dengan melihat bagaimana aturan privasi lintas batas (CBPR) dapat memfasilitasi

[53] Siaran Pers, FTC, *"FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region"* (14 Nov 2011). https://www.ftc.gov/news-events/press-releases/2011/11/ftc-welcomes-new-privacy-system-movement-consumer-data-between diakses pada tanggal 5 Maret 2021.

arus informasi lintas batas yang fleksibel, jika dilakukan dalam sistem yang memberikan pengawasan yang kredibel dan memastikan penegakan aturan privasi ini. Pathfinder menetapkan serangkaian tujuan yang harus dicapai dalam proses ini: Ini mengimplementasikan komitmen terpadu anggota-ekonomi untuk mengembangkan sistem yang menyediakan penggunaan CBPR oleh bisnis. Selain itu, proyek Pathfinder membangun sistem yang memungkinkan bisnis untuk membuat CBPR mereka sendiri, sambil melindungi konsumen dengan "agen akuntabilitas" dan regulator, di wilayah APEC sistem yang memastikan bisnis bertanggung jawab atas janji privasi mereka. Selanjutnya, Kerangka kerja diperbarui pada tahun 2015 dengan menggambar konsep yang diperkenalkan ke dalam Pedoman *Organisation* for Economic Co-operation and Development (OECD) pada tahun 2013 dengan pertimbangan untuk berbagai fitur hukum dan konteks wilayah APEC. Pada dasarnya, kerangka kerja ini meningkatkan berbagi informasi di antara lembaga pemerintah dan regulator; memfasilitasi transfer informasi yang aman antar perekonomian; menetapkan seperangkat prinsip privasi yang sama; mendorong penggunaan data elektronik untuk meningkatkan dan memperluas bisnis; dan memberikan bantuan teknis kepada ekonomi yang belum mengatasi privasi dari perspektif peraturan atau kebijakan.[54]

The APEC Cross-Border Privacy Rules System (CBPR) atau sistem Aturan Privasi Lintas Batas APEC dikembangkan oleh 21 ekonomi forum

[54] APEC, 2015, *"APEC Data Privacy Pathfinder"* - https://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx diakses pada tanggal 13 Maret 2021.

Kerjasama Ekonomi Asia-Pasifik (APEC), sistem CBPR adalah sertifikasi berbasis akuntabilitas sukarela, dapat dilaksanakan, yang memungkinkan transfer data pribadi yang bertanggung jawab lintas batas dan antar negara yang berpartisipasi. CBPR memberikan kerangka kerja siap pakai yang diakui secara internasional kepada pemerintah dan organisasi untuk memastikan perlindungan yang memadai atas informasi pribadi sambil memungkinkan aliran data yang aman dan dengan demikian memberikan manfaat penuh dari ekonomi digital global saat ini.[55]

2) Penyelesaian Sengketa Internasional Terkait Data Pribadi

Penyelesaian sengketa internasional berdasarkan Pasal 33 Piagam Persatuan Bangsa-Bangsa (Piagam PBB), berisi bahwa pihak yang terlibat pertama-tama harus mencari penyelesaian dengan cara perundingan, penyelidikan, mediasi, konsiliasi, arbitrase, penyelesaian menurut hukum (badan yudisial), menggunakan pengaturan-pengaturan atau badan-badan regional, atau dengan cara damai lainnya yang dipilih mereka sendiri.

Oleh karena itu berdasarkan hukum internasional dalam hal ini Pasal 33 Piagam PBB diatas, setiap negara-negara atau pihak yang terlibat dalam sengketa diberi kebebasan untuk memilih mekanisme penyelesaian sengketa secara damai. Namun berdasarkan Pasal 36 ayat 3 Piagam PBB, dinyatakan bahwa sengketa hukum pada umumnya harus

[55] APEC, 2018, *THE APEC CBPRs: PROTECTING INFORMATION, DRIVING GROW TH, ENABLING INNOVATION,* C&M International

diajukan oleh para pihak ke Mahkamah Internasional dalam hal ini merupakan organ yudisial utama dalam PBB.[56]

Berdasarkan Statuta Mahkamah Internasional, Mahkamah dalam memberikan putusan terhadap sengketa-sengketa yang diajukan padanya, harus melakukan:[57]

a. Konvensi-konvensi/Perjanjian internasional baik umum maupun khusus yang diakui oleh para pihak;
b. Kebiasaan-kebiasaan internasional, sebagai bukti dari praktek-praktek umum yang diterima sebagai hukum;
c. Prinsip-prinsip hukum yang diakui oleh bangsa-bangsa beradab; dan
d. Keputusan-keputusan hakum (dengan memperhatikan ketentuan bahwa putusan Mahkamah Internasional tidak mengikat selain kepada pihak yang bersengketa) dan ajaran-ajaran dari para ahli hukum yang terpandang di berbagai negara sebagai pelengkap untuk penentuan peraturan-peraturan hukum.

Dalam Pasal 40 ayat (1) Statuta Mahkamah Internasional, dijelaskan bahwa:

> *"Cases are brought the Court, as the case may be, either by the notification of the special agreement or by a written*

[56] Pasal 92 Piagam PBB
[57] Pasal 38 Statuta Mahkamah Internasional

application addressed to the Registrar. In either case the subject of the dispute and the parties shall be indicated."

Berdasarkan kutipan pasal di atas, jika terjadi sengketa internasional, para pihak dapat membuat perjanjian untuk menyelesaiakan sengketanya melalui Mahkamah Internasional. Sehingga berdasarkan ketentuan-ketentuan tersebut, perjanjian internasional menjadi salah satu rujukan utama dalam penyelesaian sengketa hukum antar negara berdasarkan hukum internasional, juga menjadi dasar pengajuan penyelesaian sengketa melalui Mahkamah Internasional.

Selain itu, masing-masing perjanjian internasional atau perjanjian regional terkait yang bersifat mengikat secara tegas terkait perlindungan data pribadi memiliki mekanisme khusus dalam penyelesaian sengketa yang diatur di dalamnya.