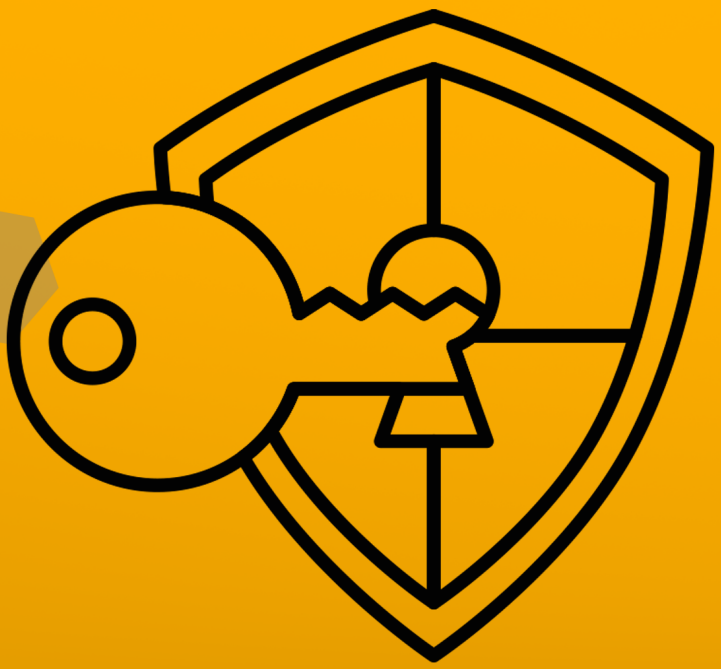
Seri Internet dan HAM

Perlindungan Data Pribadi
KONSEP, INSTRUMEN, DAN PRINSIPNYA



Wahyudi Djafar
M. Jodi Santoso

ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

Perlindungan Data Pribadi
KONSEP, INSTRUMEN, DAN PRINSIPNYA

Lembaga Studi dan Advokasi Masyarakat (ELSAM)

PERLINDUNGAN DATA PRIBADI:

Konsep, Instrumen, dan Prinsipnya

Penulis:
Wahyudi Djafar
M. Jodi Santoso

Pertama kali dipublikasikan dalam bahasa Indonesia oleh:
Lembaga Studi dan Advokasi Masyarakat (ELSAM), dengan dukungan dari Australian Government-Department of Foreign Affairs and Trade (DFAT), 2019.

Semua penerbitan ELSAM didedikasikan kepada para korban pelanggaran hak asasi manusia selain sebagai bagian dari upaya pemajuan dan perlindungan hak asasi manusia di Indonesia.

DAFTAR ISI

A. PENGANTAR

Majelis Umum PBB pada tahun 2013, melalui resolusi 68/167 tentang *the right to privacy in the digital age*, mengingatkan banyaknya praktik pengawasan (*surveillance*) dan intersepsi komunikasi yang dilakukan secara sewenang-wenang dan melawan hukum (*unlawfull*), termasuk pengumpulan data pribadi secara sewenang-wenang, yang merupakan bentuk pelanggaran terhadap hak privasi.[1] Lebih jauh, mengacu pada Pasal 17 Kovenan Internasional Hak-Hak Sipil dan Politik (ICCPR), dalam konteks pengumpulan dan penyimpanan data pribadi, sebagaimana dijelasnkan dalam Komentar Umum No. 16, disebutkan bahwa pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan perangkat lain, baik oleh otoritas publik atau individu atau badan pribadi, harus diatur oleh hukum. Langkah-langkah efektif harus diambil oleh negara untuk memastikan bahwa informasi mengenai kehidupan pribadi seseorang tidak sampai ke tangan orang yang tidak diizinkan oleh hukum untuk menerima, memproses dan menggunakannya.[2]

Perlindungan data pribadi sendiri merupakan aspek dinamis yang akan terus berhadapan dan dan dipengaruhi oleh kemajuan dan inovasi teknologi serta praktik bisnis. Salah satu faktor munculnya kejahatan dan penggunaan data pribadi secara melawan hukum disebabkan oleh perkembangan teknologi, Informasi, dan komunikasi. Saat ini, teknologi, Informasi, dan komunikasi telah merambah hampir semua aspek kehidupan dan mengubah perilaku kehidupan masyarakat menuju interaksi masyarakat berbasis elektronik dan internet. Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global dan menyebabkan interaksi antar-manusia menjadi tanpa batas *(borderless)*. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus juga menjadi sarana efektif perbuatan melawan hukum.[3]

Lebih jauh perkembangan teknologi, informasi, dan komunikasi secara langsung telah mempengaruhi perkembangan hukum. Untuk mengantisipasi kejahatan dan dampak perkembangan teknologi, informasi, dan komunikasi serta upaya perlindungan data pribadi maka dibutuhkan pembangunan dan pembentukan peraturan perundang-undangan *(legal framework)* yang ber-perspektif luas dan tepat guna. Ditinjau dari sudut pembentukan hukum, instrumen hukum yang mengikuti perkembangan teknologi informasi dan komunikasi pada hakekatnya merupakan bentuk dari formalisasi *(formalizing)* dinamika yang sudah berjalan dalam masyarakat, melalui proses *bottom up*. Dengan kata lain, bahwa hukum yang berkembang mengikuti perkembangan teknologi informasi dan komunikasi dewasa ini merupakan cerminan dari dinamika dari peradaban masyarakat itu sendiri.[4]

---

[1] United Nations, Resolution 68/167: The right to privacy in the digital age, A/RES/68/167.

[2] Indonesia telah mengaksesi ICCPR melalui UU No. 12/2005, selengkapnya lihat *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, available at: https://www.refworld.org/docid/453883f922.html.

[3] Penjelasan Umum UU No.11 Tahun 2008 Tentang informasi dan Transaksi Elektronik.

[4] BPHN, Laporan: Analisis Perencanaan Hukum Bidang Teknologi Informasi Dan Komunikasi, 2008, hlm 6.

Secara khusus, hukum perlindungan data pribadi sejatinya juga berkembang bersamaan dengan perkembangan teknologi itu sendiri, khususnya teknologi informasi dan komunikasi. Sebagaimana disinggung sebelumnya, rezim perlindungan data lahir di Eropa sebagai akibat dari ketiadaan definisi yang jelas mengenai privasi dan kehidupan pribadi, yang diatur oleh ketentuan Pasal 8 Konvensi Eropa. Hak atas perlindungan data ini sendiri bertujuan untuk melindungi individu di era masyarakat informasi. Negara yang pertama kali mengesahkan UU Perlindungan Data adalah Jerman pada tahun 1970, yang kemudian diikuti oleh Inggris pada tahun yang sama, dan kemudian sejumlah negara-negara Eropa lainnya, seperti Swedia, Prancis, Swiss, dan Austria. Perkembangan serupa juga mengemuka di Amerika Serikat, dengan adanya UU Pelaporan Kredit yang Adil pada tahun 1970, yang juga memuat unsur-unsur perlindungan data.

Pada dekade berikutnya, sejumlah organisasi regional juga mulai memberikan respon terkait dengan perlindungan data pribadi, seperti lahirnya *The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (No. 108), pada 1981 (diamandemen pada 2018). Sebelumnya juga lahir The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, pada 1980 (diamandemen 2013), dan The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72). Sedangkan APEC (Asia Pacifif Economic Cooperation) baru mengeluarkan APEC Privacy Framework pada 2004, yang kemudian diamandemen pada 2015.

Perkembangan signifikan hukum perlindungan data terjadi ketika Uni Eropa melakukan unifikasi hukum perlindungan datanya melalui Peraturan Perlindungan Data Umum Uni Eropa (EU GDPR—*General Data Protection Regulation*) pada 2016, dan mulai berlaku pada 25 Mei 2018. GDPR bersifat komprehensif, mencakup hampir semua pemrosesan data pribadi. Selain itu, implementasinya juga tidak hanya akan mempengaruhi pengendali dan prosesor data yang berbasis di Uni Eropa, tetapi juga mereka yang menawarkan barang atau jasa kepada, atau memantau perilaku, individu warga negara Uni Eropa. Sebagai hukum nasional, sampai dengan akhir tahun 2019, setidaknya lebih dari 125 negara telah mengadopsi undang-undang perlindungan data.

B. KONSEPTUALISASI PRIVASI DAN PERLINDUNGAN DATA PRIBADI

Data pribadi merupakan bagian dari privacy yang harus dilindungi, sebagaimana ditegaskan dalam berbagai instumen hukum internasional, regional, mapun nasional, yang memberikan jaminan pentingnya perlindungan data pribadi. Secata definitif dan pasti memang tidak ditemukan definisi yang baku tentang privasi dan data pribadi. Baik dalam pendapat para ahli maupun hukum positif di berbagai negara, memberikan kategori dan lingkup yang berbeda, mengenai privasi dan data pribadi. Situasi ini tentunya merefleksikan betapa dinamisnya definisi dan cakupan ruang lingkup keduanya, yang berkembang sesuai dengan konteks dan situasi masyarakatnya, termasuk pengaruh dari inovasi teknologi dalam kehidupan sehari-hari.

B.1. Memahami Konsep Privasi

Secara konseptual, tidak ditemukan dan tidak akan ditemukan satu definisi baku tentang konsep privasi karena istilah *privacy* merupakan *an essentially contested concept* (konsep yang diperdebatkan secara mendalam dan terus menerus).

Dalam hal ini, Mulligan, Koopman, & Doty (2016)[5] berpendapat bahwa Privasi 'adalah konsep solusi untuk masalah yang kami tidak yakin bagaimana menyelesaikannya; dan konsepsi tandingan adalah usulan saingan untuk menyelesaikannya atau untuk melakukan yang terbaik, dalam hal ini mengingat bahwa masalahnya tidak dapat dipecahkan.[6]

Menurut Adam D. Moore, *privacy* adalah gagasan yang sulit untuk didefinisikan.[7] Akhirnya, dengan semua konsep privasi yang saling bersaing ini, beberapa orang berpendapat bahwa tidak ada konsep privasi yang menyeluruh, melainkan beberapa konsep inti berbeda yang telah disatukan.[8] Hal yang sama dikemukakan Judith Jarvis Thomson yang skeptis tentang konsep privasi. Menurut Thomson, *privacy* adalah gagasan yang sulit untuk didefinisikan. Mungkin hal yang paling nampak tentang hak privasi adalah bahwa tidak ada orang yang memiliki ide yang jelas tentang hal tersebut.[9]

Perdebatan tentang *right to privacy*, di Eropa dan Amerika Serikat, menurut Daniel J. Solove[10] setidaknya memunculkan enam konsepsi *privacy* yang berkembang dan mewarnai pemikiran tentang hak atas *privacy*. Keenam konsepsi tersebut adalah:

(1) *right to privacy* dikonsepsikan sebagai *the right to be let alone*—hak untuk dibiarkan sendiri. Konsepsi ini dipopulerkan oleh Samuel Warren dan Louis Brandeis yang mengadopsi gagasan hakim Thomas Cooley dalam tulisnnya *Treatise on the Law of Torts* (1880). Tulisan Warren & Brandeis dengan konsepsi *the right to be let alone*[11] menjadi tonggak munculnya pemikiran hukum privasi modern dan mempengaruhi pemikiran dan praktik hukum di Amerika dan Eropa.

(2) *right to privacy* dikonsepsikan sebagai *limited access to the self* - akses terbatas pada diri. Konsepsi ini menekankan pada keinginan individu untuk menyembunyikan diri dan terpisah dari yang lain. Akan tetapi, konsepsi akses terbatas bukan kesendirian (*solitude*} pengasingan, atau penarikan diri dari orang lain. Kesendirian adalah komponen dari konsepsi akses terbatas serta konsepsi hak untuk dibiarkan sendiri. Konsepsi akses terbatas lebih luas yang mencakup kebebasan dari campur tangan pemerintah serta dari intrusi oleh pers dan lainnya. E.L. Godkin, ahli yang mengajukan versi awal teori akses terbatas, mengatakan bahwa hak setiap orang untuk menjaga urusannya sendiri, dan untuk memutuskan sendiri sejauh mana mereka akan menjadi subjek pengamatan dan diskusi publik. Sementara itu, menurut Ernest Van Den Haag," Privasi adalah akses eksklusif seseorang (atau badan hukum lainnya) ke ranah miliknya sendiri. Hak privasi memberi hak seseorang untuk mengecualikan orang lain dari: (a) menonton, (b) memanfaatkan, (c) menyerang (mengganggu, atau masuk cara lain yang memengaruhi) wilayah pribadinya.[12] Pengikut pandangan ini antara lain: Sissela Bok (1983), Anita Allen (1988), and Ruth Gavison (1980). Van Den Haag, 1971).

---

[5] Deirdre K. Mulligan1, Colin Koopman2 and Nick Doty, "Privacy is an Essentially Contested Concept: a Multidimensional Analytic for Mapping Privacy. *Phil. Trans. R. Soc. A* 374: 2016.0118.

[6] Pendapat Mulligan, Koopman, & Doty menggunakan pemikiran Waldron yang mengatakan "*essentially contested concepts can be 'solution-concept*(s)' as well as 'achievement-concept(s)'. Waldron J menganalisis konsep Demokrasi dalam kerangkan "*essentially contested concepts*" yang dikemukakan Gallei. Waldron J, dalam "Is the rule of law an essentially contested concept (in Florida)?" *Law Philos.* 21 2002 ,137–164.

[7] Adam D. Moore, "Privacy", Library Hi Tech, Vol. 25, pp. 58-78, 2007 (available at: http://ssrn.com/abstract=1980871)

[8] Adam D. Moore, "Privacy: Its Meaning and Value", American Philosophical Quarterly, Volume 40, Number 3, July 2003 (215-227).

[9] Judithj Arvis Thomson, "The Right to Privacy", Philosophy and Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 295-314.

[10] Daniel J. Solove, "Conceptualizing Privacy", California Law Review, Vol. 90, Issue 4 Article 2, 2002, [p.1087- 1155].

[11] Samuel D. Warren; Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

[12] Solove, Conceptualizing Privacy… *Op.Cit.*

Bok menulis bahwa, "privasi adalah kondisi dilindungi dari akses yang tidak diinginkan oleh orang lain - baik akses fisik, informasi pribadi, atau perhatian".[13]

(3) *right to privacy* dikonsepsikan sebagai *secrecy*—kerahasiaan: penyembunyian hal-hal tertentu dari orang lain. Salah satu pemahaman privasi yang paling umum adalah bahwa kerahasiaan itu merupakan kerahasiaan hal-hal tertentu. Menurut Hakim Richard Posner, kata 'privasi' tampaknya mengandung dua kepentingan yang berbeda yaitu kepentingan dibiarkan sendiri (being left alone) dan penyembunyian informasi (concealment of information). Konsep privasi sebagai kerahasiaan dapat dipahami sebagai bagian dari akses terbatas ke diri sendiri (*limited access to the* self). Kerahasiaan informasi pribadi adalah cara untuk membatasi akses ke diri sendiri. Konsepsi privasi sebagai penyembunyian informasi (*concealment of information*) tentang diri menjadi fondasi hak konstitusional atas informasi pribadi.

(4) *right to privacy* dikonsepsikan sebagai *Control Over Personal Information*. Salah satu teori privasi yang paling dominan adalah kontrol atas informasi pribadi (*Control Over Personal Information)* yang sampaikan sejumlah ilmuwan. Menurut Alan Westin: "Privasi adalah klaim individu, kelompok, atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain." Arthur Miller menyatakan bahwa "atribut dasar dari hak privasi yang efektif adalah kemampuan individu untuk mengontrol sirkulasi informasi yang berkaitan dengannya. Richard Parker mendefinisikan ruang lingkup informasi pribadi dengan sangat luas yaitu privasi adalah kendali atas kapan dan oleh siapa bagian dari kita dapat dirasakan oleh orang lain. Kontrol atas kapan dan siapa yang dapat melihat kita, mendengar kita, menyentuh kita, mencium bau kita, dan rasakan, kita, secara keseluruhan, mengendalikan siapa yang dapat merasakan kita, adalah inti dari privasi.

(5) *right to privacy* dikonsepsikan sebagai *Personhood*—perlindungan kepribadian, individualitas, dan martabat. Teori privasi ini dibangun berdasarkan gagasan Warren dan Brandeis tentang "kepribadian yang tidak dapat diganggu gugat." Menurut pandangan ini privasi melindungi kepribadian dan tindakan otonom. Paul Freund (1971), Jeffrey Reiman (1976), Stanley Benn (1971) telah mempertahankan konsepsi privasi berdasarkan kepribadian Paul Freund menciptakan istilah "kepribadian" untuk merujuk pada "atribut-atribut individu yang tidak dapat direduksi dalam kediriannya." Menurut Edward Bloustein, Privasi adalah konsep terpadu dan koheren yang melindungi dari perilaku yang "merendahkan kepribadian," 'penghinaan terhadap martabat pribadi, atau "serangan terhadap kepribadian manusia." Jeffrey Reiman menyatakan, hak atas privasi .., melindungi minat individu untuk menjadi, menjadi, dan tetap menjadi seseorang".[14]

(6) *right to privacy* dikonsepsikan sebagai *intimacy*—kontrol atas, atau akses terbatas ke, hubungan seseorang atau aspek kehidupan. Teori ini mengakui bahwa privasi tidak hanya penting untuk penciptaan diri individu, tetapi juga untuk hubungan manusia. Salah satu keutamaan privasi sebagai intimacy adalah itu "Perluas kepribadian moral di luar otonomi rasional yang sederhana." teori memandang privasi terdiri dari beberapa bentuk akses atau kontrol terbatas, dan itu menempatkan nilai privasi dalam pengembangan hubungan pribadi.[15]

---

[13] Adam D. Moore, "Privacy", Library Hi Tech, Vol. 25, pp. 58-78, 2007 (available at: http://ssrn.com/abstract=1980871).

[14] *Ibid*.

[15] Daniel J. Solove, Conceptualizing Privacy.... *Op.Cit*.

Dalam konteks hukum, dari berbagai pemikiran yang muncul tentang konseptualisasi *privacy*, ada dua pemikran ahli hukum yang secara signifikan mempengaruhi perkembangan pemikiran dan praktik hukum, yaitu: *pertama,* Samuel Warren dan Louis Brandeis dalam tulisannya *Right to* Privacy, yang dianggap sebagai pencetus munculnya *right of privacy* modern. *Kedua* adalah William L. Prosser melalui tulisannya "*Privacy"* yang berpengaruh terhadap perkembangan hukum privasi di Amerika sampai sekarang.[16]

Sebagaimana telah disinggung di atas, Warren dan Brandeis mengkonseptualisasikan *privacy* sebagai *the right to be let alone*. Konsepsi ini mengadopsi gagasan hakim Thomas Cooley dalam tulisnnya *Treatise on the Law of Torts* (1880). Tulisan Warren & Brandeis dengan konsepsi *the right to be let alone*[17] menjadi tonggak munculnya pemikiran hukum privasi modern dan mempengaruhi pemikiran dan praktik hukum di Amerika dan Eropa. Menurut mereka, "*The right to life has come to mean the right to enjoy life, --the right to be let alone; the right to liberty secures the exercise of extensive civil privelges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible*".[18]

Lebih jauh, dalam pandangan Warren dan Brandeis, individu harus memiliki perlindungan penuh secara pribadi dan property. Prinsip ini ada bersamaan dengan munculnya *common law*. Akan tetapi perlindungan penuh tersebut tidak langsung hadir tetapi perlu dari waktu ke waktu untuk mendefinisikan kembali sifat dan tingkat perlindungan. Terjadi pergeseran dan perluasan perlindungan hukum terhadap individu. Perubahan politik, sosial, dan ekonomi memerlukan pengakuan hak-hak baru untuk memenuhi tuntutan masyarakat.

Pada awalnya, hukum memberi solusi hanya untuk gangguan fisik dengan kehidupan dan harta benda, karena pelanggaran vi et armis. Hak untuk hidup hanya berfungsi untuk melindungi subjek dari gangguan dalam berbagai bentuknya. Kebebasan dimaknai sebatas kebebasan dari pengekangan nyata, dan hak atas properti untuk melindungi tanah dan ternaknya (liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle). Namun, dalam perkembangan selajutnya, munculah pengakuan akan sifat spiritual manusia, perasaan dan kecerdasannya. Akibatnya, secara bertahap ruang lingkup hak-hak hukum ini meluas. Sekarang, hak untuk hidup telah berarti hak untuk menikmati hidup - hak untuk dibiarkan sendiri, hak kebebasan untuk mengamankan pelaksanaan hak-hak sipil yang luas; dan istilah "properti" telah berkembang menjadi setiap bentuk kepemilikan—tidak berwujud—termasuk data, dan juga berwujud.

1. Hak privasi tidak melarang publikasi materi apa pun yang merupakan kepentingan umum.
2. Hak privasi tidak melarang komunikasi masalah apa pun, meskipun sifatnya pribadi, ketika publikasi dibuat dalam keadaan yang akan membuatnya komunikasi istimewa menurut hukum fitnah dan pencemaran nama baik.
3. Undang-undang mungkin tidak akan memberikan ganti rugi atas pelanggaran privasi melalui publikasi lisan tanpa adanya kerusakan khusus.
4. Hak privasi berhenti setelah publikasi fakta oleh individu, atau dengan persetujuannya.
5. Kebenaran dari masalah yang diterbitkan tidak mampu membela diri.
6. Tidak adanya "kedengkian" di penerbit tidak mampu membela diri.

---

[16] Vernon Valentine Palmer, Three Milestones in the History of Privacy in the United States, Tulane European & Civil Law Forum [Vol. 26, 2011], p-67-97.

[17] Samuel D. Warren and Louis D. Brandeis, The Right to Privacy ... *Op.Cit.*

[18] Ibid.

Tentang konsepsi *the right to be let alone*, Hakim Fortas dalam perkara *Time, Inc. v. Hill, (385 U.S. 374,413)* menjelaskan bahwa, "untuk menjalani kehidupan seseorang seperti yang dipilihnya, bebas dari serangan, intrusi atau invasi kecuali karena mereka dapat dibenarkan oleh kebutuhan yang jelas di bawah pemerintahan hukum."[19] Sementara itu Hakim Douglas berpendapat bahwa: "Hak privasi seperti yang disampaikan Mr. Justice Brandeis yaitu hak "untuk dibiarkan sendiri." Hak itu termasuk hak istimewa seorang individu untuk merencanakan urusannya sendiri, karena di luar wilayah perilaku yang jelas-jelas berbahaya, setiap orang Amerika dibiarkan membentuk hidupnya sendiri seperti yang ia pikir terbaik, melakukan apa yang diinginkannya, pergi ke mana pun ia mau."[20]

Meski berpengaruh kuat perkembangan hukum tetapi muncul kritik terhadap konsepsi ini. Menurut Daniel J. Solove, Tujuan Warren dan Brandeis bukanlah untuk memberikan konsepsi komprehensif tentang privasi tetapi menjelajahi akar hak atas privasi dan menjelaskan bagaimana hak semacam itu dapat berkembang. Artikel itu merupakan awal menuju pengembangan konsepsi privasi. Perumusan privasi sebagai hak untuk dibiarkan, semata-mata menggambarkan atribut privasi tetapi gagal memberikan jabaran tentang bagaimana privasi harus dihargai *vis-Avis* kepentingan lain, seperti kebebasan berbicara, penegakan hukum yang efektif, dan nilai-nilai penting lainnya.[21]

Artikel yang ditulis Warren dan Brandeis telah menginspirasi pemikiran dan praktik hukum hampir seabad atau 90 tahun sejak 1890-1970. Bahkan konsep perlindungan hak atas privasi yang dirumuskan di dalam Deklarasi Universal Hak-Hak Asasi Manusia (DUHAM) 1948, secara khusus merujuk pada konsep yang diajukan oleh Warren dan Brandeis tersebut. William Prosser mencatat bahwa lebih dari 300 putusan menggunakan menggunakan pemikiran Warren and Brandeis, hanya beberapa yang *decided*. Perkembangan hukum berubah setelah William Prosser menulis artikel yang berjudul "Privacy" dipublikasikan pada tahun1960.[22]

Menurut William L. Prosser, Pemikiran Warren & Brandeis dianggap belum memberikan detail konsepsi *privacy*. Hal ini mendoring William L. Prosser mengkonsepsikan *Privacy* secara lebih mendalam melalui tulisannya yang berjudul "Privacy". Menurut Prosser, hukum privasi terdiri dari empat jenis invasi yang berbeda dari empat kepentingan yang berbeda dari seseorang, yang diikat bersama dengan nama yang sama, Keempat gugatan ini dapat diuraikan sebagai berikut:

1. Intrusi atas pengasingan atau kesendirian seseorang, atau gangguan dalam urusan pribadinya.
2. Pengungkapan kepada publik tentang fakta pribadi yang memalukan.
3. Publisitas yang menempatkan seseorang dalam *false light* di mata publik.
4. Pengambilalihan, untuk kepentingan terdakwa, atas nama atau persamaan penggugat.

Gagasan William L. Prosser yang dikenal *Prosser's four privacies* banyak berpengaruh dalam praktik hukum privasi di Amerika Serikat. The Restatement (Second) of Torts mengadopsi gagasan Prosser's four privacies in 1979 tersebut. Dalam Restatement (Second) oF Torts 652A (2) (1979) disebutkan bahwa: (a) *Unreasonable intrusion upon the seclusion of another (b) Appropriation of the other's name or likeness (c) Unreasonable publicity given to the other's private life (d) Publicity that unreasonably places the other in a false light before the public.*

---

[19] Time, Inc. v. Hill, 385 U.S. 374,413 (1967).

[20] Doe v. Bolton, 410 U.S. 179, 213 (1973) (Douglas, J., concurring) (citations omitted) (quoting Kent v. Dulles, 357 U.S. 116, 126 (1958)).

[21] Daniel J. Solove, Conceptualizing Privacy... *Op.Cit*.

[22] Menurut Vernon Valentine Palmer, Three Milestones in the History of Privacy ... *Op.Cit*.

Sementara dalam hukum Indonesia, UU ITE juga telah mendefinisikan pengertian hak pribadi yang dipersamakan dengan hak privasi. Dalam Penjelasan Pasal 26 Ayat (1) UU ITE disebutkan bahwa hak pribadi mengandung pengertian: hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan; hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai; dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

B.2. Konseptualisasi Data Pribadi

Data pribadi sering dipadankan dengan istilah *personal data* (berkembang di Eropa) atau *personal information* (Amerika Serikat). Malaysia menggunakan Istilah *data peribadi*, Singapura menggunakan istilah *personal data,* sementara Philipina menggunakan istilah *Personal Information*, seperti halnya Jepang dan Korea Selatan*.* Berbagai istilah yang digunakan tersebut secara substansial bermakna sama. Sementara menurut Kamus Besar Bahasa Indonesia, Data pribadi berarti *data yang berkenaan dengan ciri seseorang, misalnya nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.*

Sedangkan negara-negara Uni Eropa dalam EU General Personal Data Regulation (EU GDPR) mendefinisikan *personal data* adalah berkaitan erat dengan berbagai informasi yang berkaitan dengan orang individu yang 'diidentifikasi' atau 'dapat diidentifikasi'. Gagasan tentang 'data pribadi' memang sengaja didefinisikan secara luas sehingga memungkinkan badan legislatif negara-negara Eropa dapat memasukkan semua data yang mungkin terkait dengan seorang individu.[23]

Lebih jauh, menurut Orla Lynskey, terdapat dua perbedaan mengenai data dalam ruang lingkup 'data pribadi' dan privacy: *Pertama*, tidak seperti gagasan 'gangguan privasi', gagasan tentang 'data pribadi 'tidak tergantung pada konteks. *Kedua*, pengertian tentang data pribadi termasuk data yang berkaitan dengan individu yang tidak dikenal namun dapat diidentifikasi.[24] Sementara Charles Fried menautkan definisinya tentang ruang lingkup informasi pribadi sama dengan nilai privasi. Dia mendefinisikan privasi sebagai "kontrol atas pengetahuan tentang diri sendiri" yang diperlukan untuk melindungi "hubungan mendasar" dari "rasa hormat, cinta, persahabatan dan kepercayaan." Teorinya berbicara tentang nilai privasi (mempromosikan rasa hormat, cinta, persahabatan, dan kepercayaan) dan mungkin, akan mendefinisikan ruang lingkup informasi sebagai informasi "intim" (informasi yang diperlukan untuk membentuk dan membina hubungan yang melibatkan rasa hormat, cinta, persahabatan, dan kepercayaan). Namun, melihat hanya informasi intim yang mengecualikan informasi penting seperti catatan keuangan.

Pada akhirnya, seseorang dapat membatasi ruang lingkup informasi pribadi hanya untuk yang berhubungan dengan individu. Richard Murphy mendefinisikan ruang lingkup informasi pribadi sebagai terdiri dari "setiap data tentang seorang individu yang dapat diidentifikasi oleh individu tersebut". Namun demikian definisi Murphy terlalu luas karena ada sejumlah besar informasi yang dapat diidentifikasi kepada kita dan yang kita lakukan. Perlindungan Data pribadi merupakan hak asasi manusia sebagai bagian dari hak *privacy* yang mendapatkan jaminan perlindungan baik instrument hukum internasional dan konstitusi negara.

---

[23] Orla Lynskey, "*Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order*". International and Comparative Law Quarterly, (2014) 63 (3). pp. 569-597.

[24] *Ibid.*

Dari pengertian data pribadi di atas, dapat terlihat bahwa seseorang yang dapat diidentifikasi adalah seseorang yang dapat dikenali/diidentifikasi secara langsung maupun tidak langsung berdasarkan nomor tanda pengenal atau berdasarkan satu atau lebih faktor spesifik dari identifikasi fisik, psikologi, mental, budaya atau sosial. Entitas yang dilindungi dalam mekanisme perlindungan data pribadi adalah "orang perorangan" (*natural person*) bukan "badan hukum" (*legal person*).

C. PERLINDUNGAN DATA PRIBADI SEBAGAI HAK ASASI MANUSIA: INSTRUMEN RUJUKAN

Hak privasi adalah hak dasar yang dijamin dan dilindungi dalam berbagai instrumen hukum internasional dan konstitusi di seluruh dunia. Perlindungan data pribadi merupakan bentuk penghormatan khusus hak privasi.[25] Dalam hukum internasional hak asasi manusia, perlindungan hak atas privasi diatur secara khusus dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM), yang menegaskan:

> *Tidak seorangpun boleh diganggu secara sewenang-wenang dalam urusan pribadi, keluarga, rumah tangga atau hubungan surat-menyuratnya, juga tidak boleh dilakukan serangan terhadap kehormatan dan reputasinya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau penyerangan seperti itu.*

Kemudian dalam Pasal 17 Kovenan Internasional Hak-hak Sipil dan Politik (ICCPR) yang menjadi instrumen hukum mengikat (legally binding) bagi negara-negara peserta perjanjian, perlindungan hak atas privasi, termasuk di dalamnya perlindungan data pribadi, disebutkan:

(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 seperti tersebut di atas.*

Berkaitan dengan keberlakuan Pasal 17 ICCPR, *General Comment No. 16: Article 17 (Right to Privacy),* pada paragraf 10 menegaskan bahwa pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan perangkat lain, baik oleh otoritas publik atau individu atau badan pribadi, harus diatur oleh hukum. Langkah-langkah efektif harus diambil oleh Negara untuk memastikan bahwa informasi mengenai kehidupan pribadi seseorang tidak sampai ke tangan orang yang tidak diizinkan oleh hukum untuk menerima, memproses dan menggunakannya, dan tidak pernah digunakan untuk tujuan yang tidak sesuai dengan Kovena.[26]

Lebih lanjut, ditegaskan bahwa untuk mendapatkan perlindungan paling efektif dari kehidupan pribadinya, setiap individu harus memiliki hak untuk: (1) memastikan dalam bentuk data pribadi apa yang disimpan dalam file data otomatis, (2) memastikan untuk tujuan pengumpulan dan penyimpanan data pribadi; (3) Setiap individu juga harus dapat memastikan otoritas publik atau individu atau badan atau pribadi mana yang mengendalikan atau dapat mengontrol file mereka; dan (4) jika file tersebut-

---

[25] 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. para 58 (May 16, 2011).

[26] 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, available at: https://www.refworld.org/docid/453883f922.html [accessed 27 March 2019]

berisi data pribadi yang salah atau telah dikumpulkan atau diproses bertentangan dengan ketentuan hukum, setiap individu harus memiliki hak untuk meminta perbaikan atau penghapusan.[27] Hal ini ditegaskan kembali oleh *UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* yang menyebutkan dalam laporannya pada 2011, bahwa Perlindungan data pribadi merupakan bentuk penghormatan khusus hak privasi.[28] Oleh karenanya negara harus menghormati kewajiban hak asasi manusia internasional mengenai hak privasi [...] ketika mereka membutuhkan pengungkapan data pribadi dari pihak ketiga, termasuk perusahaan swasta.

Selain Deklarasi Umum Hak Asasi Manusia dan Kovenan Internasional Hak-hak Sipil dan Politik, beberapa Instrumen hukum hak asasi manusia di tingkat regional juga mengatur tentang hak atas privasi, antara lain:

- ***The American Convention on Human Rights,*** yang pada Pasal 11, menyebutkan: (1) *Everyone has the right to have his honor respected and his dignity recognized;* (2) *No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation*; (3) *Everyone has the right to the protection of the law against such interference or attacks.*

- ***The Arab Charter on Human Rights***, pada Pasal 17 menyatakan: *Private life is sacred, and violation of that sanctity is a crime. Private life includes family privacy, the sanctity of the home, and the secrecy of correspondence and other forms of private communication.*

- ***The ASEAN Human Rights Declaration***, pada paragraf 21 menyebutkan: *Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.*

- ***The European Convention on Human Rights***, dalam Pasal 8 mengatakan: *Right to respect for private and family life:* (1) *Everyone has the right to respect for his private and family life, his home and his correspondence*; (2) *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

- ***The EU Charter on Fundamental Rights and Freedoms***, pada Pasal 6 (Right to liberty and security) menyatakan "*Everyone has the right to liberty and security of person.* Kemudian pada Pasal 7 *(Respect for private and family life)* disebutkan "*Everyone has the right to respect for his or her private and family life, home and communications*". Berikutnya Pasal 8 (*Protection of personal data*) menegaskan:

---

[27] *Ibid* Paragraf 10.

[28] 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*. para 58 (May 16, 2011).

(1) *Everyone has the right to the protection of personal data concerning him or her.*
(2) *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
(3) *Compliance with these rules shall be subject to control by an independent authority.*

Selain berbagai instrumen hukum hak asasi manusia internasional dan regional di atas, hukum perlindungan data juga bermunculan di negara-negara Eropa. Dimulai tahun 1970-an, beberapa negara Eropa merespon perkembangan teknologi, informasi, dan komunikasi dengan mengeluarkan undang-undang perlindungan data. Swedia merupakan negara pertama di dunia yang mengeluarkan UU Perlindungan Data 1973 (sebelumnya di Jerman baru di tingkat negara bagian). Undang-undang ini merupakan undang-undang pertama yang memperkenalkan elemen dasar yang kemudian dikenal sebagai hukum perlindungan data pribadi.[29] Hingga saat ini, lebih dari 125 Negara telah mengeluarkan undang-undang perlindungan data pribadi.

Dalam Perkembangannya negara-negara dunia melalui berbagai bentuk Kerjasama merespon dengan mengeluarkan instrumen baik dalam bentuk petunjuk/*guidelines* maupun kerangka kerja/*framework* baik yang mengikat maupuan yang tidak mengikat, seperti instrumen berikut:

- ***The OECD's Privacy Guidelines (1980)***

Pada tahun 1980, Organisation for Economic Co-operation and Development (OECD), sebuah organisasi kerjasama ekonomi yang didirikan Amerika Serikat, Canada dan 18 negara Eropa,[30] mengeluarkan *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines 1980).[31] Selanjutnya pada tahun 2013 OECD Council mengadopsi Revisi OECD Privacy Guidelines 1980 yang dikenal dengan OECD Privacy Guidelines 2013.[32] Meski sifatnya tidak mengikat (*non-binding*) The OECD's Privacy Guidelines (1980-amandemen 2013) memberi pengaruh signifikan terhadap perkembangan hukum perlindungan data pribadi termasuk negara-negara di kawasan Asia.[33] Di Amerika Serikat, prinsip-prinsip OECD Privacy Guidelines digunakan sebagai rujukan perlindungan data pribadi yang dikenal dengan *Fair Information Practices.*[34]

- ***Instrumen Regional Uni Eropa***

Pada tahun 1981, Uni Eropa mengesahkan Convensi Perlindungan data yaitu *Convention for the Protection*

[29] Graham Greenleaf, *Asian Data Privacy Laws:Trade and Human Rights Perspectives*, (Oxford: Oxford University Press, 2014), hlm. 6.

[30] Organaisasi yang didirikan pada tahun 1960 oleh 18 negara eropa, USA, dan Canada. Pada May 2007, Indonesia bersama Brazil, India, the People's Republic of China and South Africa menjadi negara-negara Key Partners the OECD's. http://www.oecd.org/about/membersandpartners/.

[31] Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data adopted by OECD Council on 23 September 1980 (OECD Doc. C (80)58/FINAL).

[32] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013). [C (80)58/FINAL, as amended on 11 July 2013 by C(2013)79] (OECD Guidelines governing the

[33] GrahamGreenleaf *Asian Data Privacy Laws... op.cit hlm 10.*

[34] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*. P.13. Apendix B.

of Individuals with Regard to Automatic Processing of Personal Data (CoE Convention 108).[35] Selanjutnya pada tahun 2015, dilakukan amandeman Convention 108 berdasarkan *Council of Europe Treaty Series - No. 223* diadopsi the Committee of Ministers of the Council of Europe pada 18 May 2018 dikenal dengan Modernised Convention 108.[36]

Kemudian pada tahun 1995, Parlemen Eropa dan Council EU mengeluarkan Directive 95/46/EC on *the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* [37] yang merupakan embrio dari EU GDPR. Selanjutnya berkembang pada tahun 2016, Parlemen Eropa dan Council EU mengeluarkan Regulation (EU) 2016/679 *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 yang dikenl dengan EU General Data Protection Regulation.[38]

- ***UN Guidelines for the Regulation of Computerized Personal Data Files 1995***

Pada tahun 1995, Majelis Umum PBB mengadopsi *Guidelines for the Regulation of Computerized Personal Data Files (*Resolution 45/95 of 14 December 1990). Dalam *Guidelines* diatur prinsip-prinsip perlindungan data/file.[39] Kemudian pada tahun 2018, UN High-Level Committee on Management (HLCM) mengadopsi *Personal Data Protection and Privacy Principles*.[40]

- ***The Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004 (Revisi 2015)***

Pada tahun 2004 APEC mengeluarkan APEC Privacy Framework 2004 yang bertujuan untuk mempromosikan perdagangan elektronik di seluruh wilayah Asia Pasifik dan menegaskan kembali nilai dari privasi bagi individu dan masyarakat informasi.[41] APEC Privacy Framework 2004 mendasarkan pada nilai-nilai inti OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines 1980. Tahun 2015, dilakukan revisi yang dikenal APEC Privacy Framework (2015).

Baik APEC Privacy Framework 2004 maupun 2015, sifatnya tidak mengikat bagi negara anggota. APEC Privacy Framework memberikan kelonggaran pada anggota untuk menentukan bahwa Prinsip perlindungan data pribadi dan menggunakan pendekatan sesuai dengan negara masing-masing. Apa pun pendekatan

---

[35] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108; adopted 28 January 1981) ('CoE Convention 108').

[36] *Council of Europe Treaty Series - No. 223* Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 10.X.2018, adopted by the Committee of Ministers of the Council of Europe on 18 May 2018 on the occasion of its 128th session held in Elsinore, Denmark. ('Modernised Convention 108').

[37] EU, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.

[38] EU. Regulation (EU) 2016/679 of The European Parliament And Of The Council of 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).

[39] 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.

[40] *Personal Data Protection and Privacy Principle,* Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018.

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

yang diadopsi dalam keadaan tertentu, tujuan keseluruhannya adalah mengembangkan pendekatan perlindungan privasi yang kompatibel di kawasan APEC.

- ***ASEAN Framework on Personal Data Protection***

Pada tahun 2016, negara-negara ASEAN menandatangani *ASEAN Framework on Personal Data Protection* yang berisi kesepahaman negrara-negara ASEAN untuk memperkuat perlindungan data pribadi di ASEAN dan untuk memfasilitasi kerja sama di antara para Peserta, dengan tujuan untuk berkontribusi pada promosi dan pertumbuhan perdagangan regional dan global dan aliran informasi. Meski demikian, ASEAN *Framework on Personal Data Protection* hanya berfungsi sebagai catatan keinginan negara-negara ASEAN dan bukan merupakan atau menciptakan, dan tidak dimaksudkan untuk membentuk atau membuat, kewajiban di bawah hukum domestik atau internasional dan tidak akan menimbulkan proses hukum apa pun dan tidak akan dianggap untuk membentuk atau membuat kewajiban yang mengikat atau dapat ditegakkan secara hukum, tersurat maupun tersirat.[42]

Berangkat dari mandat berbagai instrumen hak asasi manusia internasional dan regional, maupun berbagai standar yang dikembangkan, pembentukan UU Perlindungan Data pribadi hari ini merupakan kewajiban penting bagi negara. Menurut *Human Rights Council dalam Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* menegaskan bahwa Negara-negara Pihak diharuskan mengatur melalui undang-undang yang diartikulasikan dengan jelas, pencatatan, pemrosesan, penggunaan dan penyampaian data pribadi otomatis dan untuk melindungi mereka yang terkena dampak penyalahgunaan oleh organ-organ negara serta swasta. Negara, selain melarang pemrosesan data untuk tujuan yang tidak sesuai dengan Kovenan, undang-undang perlindungan data harus menetapkan hak atas informasi, koreksi dan, jika perlu, penghapusan data dan memberikan tindakan pengawasan yang efektif….., untuk mendapatkan perlindungan yang paling efektif terhadap kehidupan pribadinya, setiap individu harus memiliki hak untuk memastikan dalam bentuk yang dapat dipahami, apakah, dan jika demikian, data pribadi apa yang disimpan dalam file data otomatis, dan untuk tujuan apa. Setiap individu juga harus dapat memastikan otoritas publik atau individu atau badan atau pribadi mana yang mengendalikan atau dapat mengendalikan file mereka.[43]

Hingga saat ini, lebih dari 125 negara telah mengeluarkan undang-undang perlindungan data pribadi. Dimulai tahun 1970-an, undang-undang perlindungan data muncul di Eropa barat (Austria, Denmark, Greenland, Jerman, Prancis, Norwegia, Swedia, dan Luksemburg) dan Amerika Serikat dengan dengan US Fair Credit Reporting Act dan US Privacy Act. Pada 1980-an, Finlandia, Islandia, Irlandia, Belanda, San Marino, Inggris, Israel, Australia, Kanada, dan Jepang membuat undang-undang 'sektor publik' saja.

Berikutnya pada 1990-an, sebagian besar negara Eropa Barat seperti Belgia, Italia, Yunani, Monaco, Portugal, Spanyol, dan Swiss memberlakukan undang-undang perlindungan data. Bersamaan dengan runtuhnya Uni Soviet banyak negara bekas 'blok timur' memberlakukan undang-undang privasi data yaitu Albania, Republik Ceko, Hongaria, Polandia, Slovakia, dan Slovenia, Azerbaijan dan Lithuania. Penyebaran di luar Eropa juga dimulai, Chili adalah negara pertama di Amerika Latin yang menerapkan UU Perlindungan Data. Di Asia-Pasifik, Hong Kong, Selandia Baru, Taiwan, Thailand dan Korea Selatan merupakan negara-negara yang paling awal menerapkan UU Perlindungan Data Pribadi.

---

[42] ASEAN *Framework on Personal Data Protection 2016,* (Effect of the Framework).

[43] *Ibid.*

Pada tahun 2000 percepatan berlanjut, dan meningkat di hampir semua wilayah di dunia mengeluarkan uu perlindungan data pribadi. Paling mencolok adalah di bekas blok timur dan negara-negara republik Soviet yaitu Bosnia & Herzegovina, Bulgaria, Kroasia, Estonia, Latvia, Makedonia (FYROM), Moldova, Rumania, Serbia dan Montenegro, ditambah Rusia. Negara-negara Eropa Barat yang tersisa Andorra, Siprus, Gibraltar, Liechtenstein dan Malta memberlakukan UU perlindungan data. Di luar Eropa, seperti negara Asia Pasifik (Macao, Nepal, dan penyempurnaan dilakukan beberapa negara seperti Australia, Korea Selatan, dan Jepang), Amerika Latin (Argentina, Kolombia, Paraguay dan Uruguay), dan Karibia (Bahama, St Vincent & Grenadines). Perkembangan pesat terjadi di Afrika dengan undang-undang baru di Tunisia dan Maroko (Afrika Utara) dan Benin, Burkina Faso, Tanjung Verde, Mauritius, Senegal, Seychelles, dan hukum sektor publik Zimbabwe (Afrika Sub-Sahara).

Republik Kirgistan menjadi negara pertama di Asia Tengah yang membuat undang-undang pada 2008, dan Pusat Keuangan Dubai dan Qatar menambahkan undang-undang pertama di Timur Tengah. Pada Tahun-tahun terakhur, semua negara Eropa yang tersisa memberlakukan hukum dengan pengecualian Turki, Belarus dan Vatikan. Negara-negara di luar Eropa banyak memberlakukan UU perlindungan data pribadi seperti: India, Filipina, Malaysia, Vietnam, dan Singapura (Asia); Kosta Rika, Nikaragua, Meksiko, dan Peru (Amerika Latin); Angola, Gabon, dan Ghana, (Afrika); St Lucia dan Trinidad & Tobago, (Karibia); dan Yaman (Timur Tengah). Negara-negara ASEAN juga mengeluarkan peraturan serupa, misalnya Malaysia pada 2010, Filipina dan Singapura pada 2012, Laos pada 2017, dan Thailand mengesahkan UU Perlindungan Data Pribadi pada 2019.

D. LANDASAN DAN TUJUAN UU PERLINDUNGAN DATA

D.1. Landasan Pengaturan UU Perlindungan data

Landasan pembentukan undang-undang perlindungan data didasarkan landasan filosofis negara masing-masing. Meski hukum privasi dan perlindungan data pribadi berasal dari Barat (Eropa dan Amerika Serikat), akan tetapi terdapat perbedaan mendasar landasan hukum privasi AS dan negara-negara Eropa, khususnya pada aspek filosofisnya. Di Amerika Serikat, undang-undang privasi berfokus pada memperbaiki kerusakan dan kerugian konsumen serta menyeimbangkan privasi dengan transaksi komersial yang efisien. Sedangkan di Uni Eropa, privasi diposisikan sebagai hak fundamental yang dapat mengalahkan kepentingan lain.[44]

Pun Indonesia secara filosofis berbeda dengan Amerika Serikat dan EU. Meski demikian terdapat standar universal yang harus dipenuhi dengan tetap memperhatikan materi muatan yang berlaku di Indonesia. Secara umum pembentukan hukum perlindungan data pribadi mengikuti teknik penyusunan peraturan perundang-undangan sebagaimana diatur dalam UU Pembentukan Peraturan Perundang-undangan. Oleh karenanya pembentukan UU Pelindungan Data juga harus didasarkan pada landasan filosofis, sosiologis, dan yuridis.

Pertama, landasan filosofis UU Perlindungan data dididasarkan pada cita hukum dalam Pembukaan UUD 1945 yaitu tujuan pembentukan Pemerintahan Negara salah satunya adalah "*Negara melindungi segenap bangsa Indonesia, dan seluruh tumpah darah Indonesia*….". Hal ini berarti, negara berkewajiban

[44] Paul M. Schwartz & Daniel J. Solove, "Reconciling Personal Information in the United States and European Union", in *California Law Review* [Vol. 102:877-916, 2014].

memberikan perlindungan dan menjamin hak-hak asasi manusia termasuk perlindungan data pribadi. pelindungan privasi atas data pribadi merupakan hak asasi yang diamanatkan langsung oleh konstitusi yang dituangkan dalam Pasal 28 G ayat (1). Selain itu, perlindungan data pribadi merupakan hak asasi yang ditegaskan baik dalam instrumen hak asasi manusia baik internasional maupun regional, dimana Indonesia salah satunya terikat secara yuridis pada The International Covenant on Civil and Political Rights (ICCPR) 1966 dan The ASEAN Human Rights Declaration. Selain itu, perlindungan data pribadi juga diatur dalam instrumen perjanjian kerjasama internasioanl yang Indonesia terlibat di dalamnya antara lain the Asia-Paci ic Economic Cooperation (APEC) Privacy Framework 2004.

Kedua, pada landasarn sosiologis masyarakat Indonesia saat ini juga bagian dari masyarakat informasi, dalam sebuah ruang interkoneksi global. Oleh karenanya perlindungan privasi atas data pribadi merupakan kebutuhan untuk memberikan keamanan bagi setiap indvidu baik warga negara Indonesia maupuan warga negara asing yang ada di Indonesia berkaitand dengan pengumpulan, pemrosesan, penyelenggaraan, dan penyebarluasan Data Pribadi.

Ketiga, landasan yuridis, terdapat bebagai peraturan perundang-undangan di Indonesia yang terkait dan secara parsial mengatur perlindungan data pribadi, tetapi belum secara optimal memberikan perlindungan dan kepastian hukum data pribadi. Studi yang dilakukan Lembaga Studi dan Advokasi Masyarakat (ELSAM) misalnya mengidenti ikasi setidaknya 30 undang-undang di Indonesia yang kontennya terkait dengan data pribadi.[45] Oleh karena itu dibutuhkan sebuah undang-undang perlindungan data yang dapat memberikan jaminan perlindungan data pribadi dan memberikan kepastian hukum.

D.2. Tujuan Perlindungan Data Pribadi

Tujuan utama dari pengaturan perlindungan data pibadi adalah melindungi dan menjamin setiap individu terlepas dari kebangsaan, suku, tempat tinggal/domisili, berkaitan dengan penyimpanan dan pemrosesan data pribadi dan hak dan kebebasan khususnya hak privasi. Meski tujuan utama adalah setiap orang (subjek data), tetapi operasionalisasi perlindungan data pribadi melibatkan entitas lain baik perorangan maupun kelompok/organisasi, dan negara. Untuk itu, tujuan dari pembentukan undang-undang perlindungan data adalah bertujuan:

a. melindungi hak-hak dasar dan kebebasan warga negara, khususnya hak untuk melindungi data pribadi;
b. menjamin kepatuhan pemerintah, pelaku bisnis dan Organisasi Kemasyarakatan lainnya untuk memberi untuk melindungi data pribadi bagi warga negara;
c. mendorong kepastian hukum dan pertumbuhan industri teknologi, informasi dan komunikasi.

D.3. Rung Lingkup, Keberlakuan, dan Pengecualian

- **Lingkup Material**

Sebuah undang-undang perlindungan data pribadi bertujuan untuk melindungi hak privasi individu berkaitan dengann data pribadi dari tindakan penyelengaraan data baik yang dilenggarakan oleh lembaga publik maupun swasta. Untuk itu, perlu Undang-undang perlindungan data komprehensif yang berlaku

[45] Wahyudi Djafar, dkk., Perlindungan Data Pribadi di Indonesia: Usulan Pelembagaan Kebijaan dari Perspektif HAM, (Jakarta: ELSAM, 2016).

dan mengikat badan publik dan swasta. Dalam keadaan apa pun badan publik atau swasta tidak akan sepenuhnya dibebaskan dari prinsip-prinsip perlindungan data dan menghormati hak-hak individu. Namun demikian terhadap perseorangan (individu), diterima secara luas bahwa pemrosesan untuk keperluan perseorangan atau rumah tangga (yang dilakukan secara mandiri) dikecualikan dari berlakunya UU Perlindungan Data Pribadi. Artinya individu dan rumah tangga tidak masuk dalam kualifikasi sebagai pengendali atau prosesor data. UU Perlindungan Data Pribadi mengatur hak dari subjek data (individu pemilik data), tidak memberikan pengaturan mengenai kewajiban dari subjek data (individu), tetapi kewajiban bagi mereka yang melakukan pemrosesan data dalam jumlah tertentu, yang disebut sebagai pengendali/prosesor data.

Keberlakuan undang-undang perlindungan data pribadi juga mengikat lembaga-lembaga publik seperti penegak hukum dan badan-badan intelijen. Pengaturan pengecualian terhadap penegak hukum dan badan-badan intelijen harus diatur secara jelas tidak memberikan ketentuan pasal yang terlalu longgat atau tafsir yang luas atau menimbulkan multitafsir yang dapat berdampak pada pelanggaran hak privasi dan data pribadi warga negara.

Sebagai gambaran, EU GDPR[46] pada Pasal 2 ayat (1) menyatakan bahwa undang-undang perlindungan data berlaku untuk pemrosesan data pribadi seluruhnya atau sebagian dengan cara otomatis dan untuk pengolahan selain dengan cara otomatis data pribadi yang merupakan bagian dari sistem pengarsipan atau dimaksudkan untuk membentuk bagian dari sistem pengarsipan.

- **Lingkup Teritorial**

Pembentukan Undang-undang perlindungan data harus mempertimbangkan bahwa data, termasuk data pribadi, bergerak lintas batas. Hal ini menimbulkan masalah yurisdiksi yang signifikan dan kompleks, termasuk kemungkinan benturan undang-undang antara satu negara dengan negara lain.

Undang-undang perlindungan data harus menempatkan individu sebagai pusatnya: ini berarti memastikan bahwa data pribadi individu dilindungi, terlepas dari apakah data mereka diproses di dalam atau di luar wilayah di mana mereka berada. Perlindungan ini dapat dicapai dengan berbagai cara, termasuk dengan menetapkan bahwa hukum:

a. Berlaku untuk pengontrol dan prosesor yang didirikan di negara tersebut, bahkan jika pemrosesan dilakukan di luar wilayah hukum negara.
b. Berlaku untuk pemrosesan data pribadi oleh pengontrol dan prosesor yang didirikan di luar yurisdiksi negara tempat individu tersebut berada.
c. Mengatur kondisi untuk mentransfer data pribadi di luar wilayah negara.[47]

Dalam prktik, EU GDPR (prinsip extraterritorial, Art 3 EU GDPR[48]) dan undang-undang beberapa negara memberlakukan prinsip extraterritorial, seperti Jepang (prinsip extraterritorial – Art 75 Amandend APPI Act)

---

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 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).

[47] Privacy International, *The Keys to Data Protection,* hlm, 17.

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 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).

dan Philipina (prinsip extraterritorial, Section 6 Republic Act No. 10173 – Data Privacy Act of 2012). Akan tetapi, Malaysia dan beberapa negara lain tidak menerapkan extraterirotial.

E. KETENTUAN UMUM: ISTILAH-ISTILAH KUNCI

Penggunaan istilah dan definisi yuridis dari data pibadi berbeda dari satu negara dengan negara lain. Amerika Serikat, pada level Federal, tidak memiliki undang-undang perlindungan data tersendiri tetapi tersebar pada beberapa undang-undang. Akan tetapi, pada level negara bagian (*state*), sebagian diantaranya telah memiliki undang-undang khusus perlindungan data pribadi, seperti halnya Californian Consumer Privacy Act (CCPA) 2019, yang materinya banyak mengadopsi EU GDPR. Istilah yang lazim digunakan di Amerika adalah informasi pribadi (*personal information*).

Negara-negara Eropa secara umum, khususnya anggota Uni Eropa tunduk pada ketentuan yang diatur dalam EU General Data Protection Regulation (Regulation (EU) 2016/679 *of the European Parliament and of the Council*) (EU GDPR). EU GDPR kemudian menjadi rujukan dunia internasional dalam hal pembentukan uu perlindungan data pribadi. Selain EU GDPR, beberapa organisasi kerjasama internasional seperti Organisation for Economic Co-operation and Development (OECD) dan Asia Pasific Economic Cooperation (APEC) mengeluarkan *Guidelines on the Protection of Personal Data*.

E.1. Data Pribadi

Beberapa instrumen hukum regional dan perjanjian kerjasama internasional memberikan definisi yang sederhana. Hal ini memberi kemungkinan kepada negara-negara untuk mengembangkan definisi tersebut.

- **Definisi data Pribadi Menurut OECD dan APEC**

OECD dalam *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, mendefinisikan data pribadi adalah "…segala informasi yang berkaitan dengan individu (subjek data) yang diidentifikasi atau dapat diidentifikasi (*any information relating to an identified or identifiable individual (data subject)*.[49] Sementara APEC memilih menggunakan istilah atau konsep *personal information* atau informasi pribadi yang berarti setiap informasi yang mengidentifikasi atau mengidentifikasi individu tertentu (*any information about an identified or identifiable individual*). Termasuk di dalamnya informasi yang dapat digunakan untuk mengidentifikasi seseorang, namun tidak hanya informasi saja, akan tetapi juga informasi yang ketika disatukan dengan informasi lain akan mengidentifikasi seorang individu. Misalnya, jenis metadata tertentu, yang pada saat dikumpulkan, dapat mengungkapkan informasi pribadi dan dapat memberikan infromasi tentang perilaku, hubungan sosial, preferensi pribadi, dan identitas individu.[50]

- **Definisi data Pribadi Menurut EU GDPR**

Definisi OECD tersebut di atas hampir sama dengan definisi yang diatur dalam EU General Data Protection Regulation dengan menambah pengertian "data individu yang dapat diidentifikasi. Secara jelas EU General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council), pada Article 4 (4), menguraikan bahwa yang dimaksud dengan *personal data* adalah "*segala informasi yang berkaitan dengan identifikasi atau dapat mengidentifikasi seorang individu (subyek data); an identifiable person adalah yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal online/satu atau lebih faktor*

[49] OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

[50] APEC Privacy Framework 2015.

spesifik untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau identitas sosial dari orang tersebut".

- **Definisi Data Pribadi di Beberapa Negara**

a. Definsi Data Pribadi di Amerika Serikat

Di Amerika Serikat, isitilah yang umum digunakan "personally information" sebagai padanan istilah "*Data pribadi*". Pada level negara Federal terdapat bebrapa undang-undang yang mengatur perlindungan data pribadi. TIdak ada keseragaman dalam mendefinisikan informasi pribadi secara konsisten. Undang-undang privasi di Amerika Serikat menawarkan beberapa definisi yang saling bersaing. Menurut Paul M. Schwartz & Daniel J. Solove, masalah awal yang muncul dari berbagai definisi yang tidak seragam di Amerika Serikat terkadang menghilangkan perbedaan antara "*identifiable*" and "*identified*."

b. Singapore Personal Data Protection Act 2012 (No. 26 of 2012),

Data pribadi atau "*personal data*" diartikan bahwa data, *whether true or not, about an individual who can be identified —*
(a) from that data; or
(b) from that data and other information to which the organisation has or is likely to have access;

c. Malaysia, Akta Perlindungan Data Peribadi 2010

Pengertian "*Data Peribadi*" menurut Akta 709: Akta Perlindungan Data Peribadi 2010, mendefinisikan data pribadi dalam kontek transaksi comersial, yaitu: "*apa-apa maklumat yang berkenaan dengan transaksi komersial, yang—*

(a) sedang diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan yang dikendalikan secara automatik sebagai tindak balas kepada arahan yang diberikan bagi maksud itu;
(b) direkodkan dengan niat bahawa ia sepatutnya diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan itu; atau
(c) direkodkan sebagai sebahagian daripada sistem pemfailan yang berkaitan atau dengan niat bahwa ia sepatutnya menjadi sebahagian daripada sistem pemfailan yang berkaitan,
(d) yang berhubungan secara langsung atau tidak langsung dengan seorang subjek data, yang dikenal pasti atau boleh dikenal pasti daripada maklumat itu atau daripada maklumat itu dan maklumat lain dalam milikan seorang pengguna data, termasuk apa-apa data pribadi sensitif dan pernyataan pendapat tentang subjek data itu; tetapi tidak termasuk apa-apa maklumat yang diproses bagi maksud suatu perniagaan pelaporan kredit yang dijalankan oleh sesuatu agensi pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010;"

d. Pilipina, Republic Act No. 10173 – Data Privacy Act of 2012

Undang-Undang Data Privasi menggunakan istilah "*Personal Information",* yang didefinisikan *Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual*.

- **Elemen-Elemen dalam Merumuskan Data Data Pribadi**

The Article 29 Working Party (Art. 29 WP) sebuah kelompok kerja independen Uni Eropa, dalam Opinion 4/2007 on the concept of personal data,[51] memberikan opini berkaitan dengan Article 4 (4) Directive 95/46/EC (ketentuan ini kemudian dimasukkan dalam EU General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council), yang berberbunyi *"Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); ……*

a. *personal data* adalah "*segala informasi yang berkaitan dengan seorang individu (subyek data) yang didentifikasi atau dapat mengidentifikasi*
b. *an identifiable person adalah yang dapat 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 untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau identitas sosial dari orang tersebut;"*

Terhadap ketentuan ini, The Article 29 Working Party/Art. 29 WP dalam Opinion 4/2007 on the concept of personal data, memberikan opini yang intinya tujuan pengaturan data pribadi adalah untuk melindungi individu. Ruang lingkup aturan perlindungan data tidak boleh terlalu berlebihan dan meluas akan tetapi membatasi interpretasi konsep data pribadi secara sempit juga harus dihindari. Terdapat 4 elemen dalam merumuskan definisi data pribadi, yaitu: "*Personal data/*data pribadi", "*any information*/informasi apa pun", "*relating to*/yang berkaitan dengan", "*identified or identifiable*/diidentifikasi atau dapat diidentifikasi", dan "*natural person*/orang individu". Elemen-elemen tersebut saling terkait dan bersama-sama menentukan apakah sebuah informasi harus dianggap sebagai "data pribadi".

Pertama, "*any information*/informasi apa pun", ini membutuhkan interpretasi yang luas, terlepas dari sifat atau isi informasi, dan format teknis yang disajikan. Ini berarti bahwa informasi yang obyektif dan subyektif tentang seseorang dalam kapasitas apa pun dapat dianggap sebagai "data pribadi", dan secara teknis terlepas dari media di mana data tersebut dituangkan.

Kedua, "*relating to*/yang berkaitan dengan", elemen kedua ini sering diabaikan, tetapi memiliki peran penting dalam menentukan ruang lingkup substantif konsep, terutama dalam kaitannya dengan objek. Pendapat tersebut memberikan tiga elemen alternatif - yaitu konten, tujuan, dan hasil - untuk menentukan apakah informasi "berkaitan dengan" seseorang. Ini juga mencakup informasi yang mungkin memiliki dampak yang jelas pada cara seseorang.

Ketiga, "*identified or identifiable*", elemen ketiga ini berfokus pada kondisi di mana seseorang harus dianggap sebagai "dapat diidentifikasi", dan terutama pada "sarana yang mungkin secara wajar akan digunakan" oleh pengontrol atau oleh orang lain untuk mengidentifikasi orang itu. Konteks dan keadaan khusus dari kasus tertentu memainkan peran penting dalam analisis ini. Pendapat tersebut juga berkaitan dengan "*pseudonymised data*/data samaran".

Keempat, "*natural person*/orang individu", ini berkaitan dengan persyaratan bahwa "data pribadi" adalah tentang "individu yang hidup". Pendapat itu juga membahas antarmuka dengan data orang yang meninggal, anak yang belum lahir dan orang hukum.

---

[51] EU Article 29 Data Protection Working Party, Opinion 4/2007 *on "the concept of personal data",* 01248/07/EN WP 136.

E.2. *Identifiable* Data

Salah satu elemen dalam mendefinisikan data pribadi menurut EU GDPR adalah *identified or identifiable natural person*. Pengertian *identifiable natural person* menurut EU GDPR adalah orang orang yang dapat 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 untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau sosial dari orang alami itu. [52]

Seorang individu dapat dianggap sebagai "*identified*/teridentifikasi" ketika, di dalam sekelompok orang, ia "dibedakan" dari semua anggota kelompok lainnya.[53] Seorang individu orang alami "dapat diidentifikasi/ *identifiable*" ketika, meskipun orang tersebut belum diidentifikasi, adalah mungkin untuk melakukannya (melakukan pengidentifikasian). Dalam hal ini, pengidentifikasian berada pada kondisi menentukan apakah informasi berada dalam ruang lingkup. *"Identifikasi"* biasanya dicapai melalui potongan informasi tertentu yang dapat disebut "*identifiers*" dan yang memiliki hubungan istimewa dan dekat dengan individu tertentu, seperti tinggi badan, warna rambut, pakaian (tanda-tanda lahiriah dari penampilan orang).[54]

Di Amerika Serikat, tidak terdapat definisi baku menurut undang-undang tentang *identifiable* data atau dalam literatur Amerika dikenal dengan istilah *Personally Identifiable Information*. Sebagai rujukan, *United States Government Accountability Office* (GAO) tahun 2008 merumuskan *Personally Identifiable Information*[55] yang kemudian diadopsi *US National Institute of Standards and Technology* (NIST) dalam *Guide to Protecting the Confidentiality of Personally Identifiable Information*. Menurut panduan ini *Personally Identifiable Information* adalah informasi apapun tentang seorang individu yang dikelola oleh suatu agen, termasuk:

(a) informasi apa pun yang dapat digunakan untuk membedakan atau melacak identitas seseorang, seperti nama, nomor jaminan sosial, tanggal dan tempat lahir, informasi ibu nama gadis, atau catatan biometrik; dan
(b) informasi lain yang terkait atau ditautkan dengan seseorang, seperti informasi medis, pendidikan, keuangan, dan pekerjaan. Employment.[56]

To distinguish an individual/membedakan seorang individu adalah mengidentifikasi seorang individu. Beberapa contoh informasi yang dapat mengidentifikasi individu termasuk, tetapi tidak terbatas pada, nama, nomor paspor, nomor jaminan sosial, atau data biometrik. Sebaliknya, daftar yang hanya berisi skor kredit tanpa informasi tambahan mengenai individu yang kepadanya mereka berhubungan tidak memberikan informasi yang cukup untuk membedakan individu tertentu.

To trace an individual/melacak individu adalah untuk memproses informasi yang cukup untuk membuat penentuan tentang aspek tertentu dari aktivitas atau status individu. Misalnya, log audit yang berisi catatan tindakan pengguna dapat digunakan untuk melacak aktivitas individu.

---

[52] EU *General Data Protection Regulation* (Regulation (EU) 2016/679). Dalam praktik perlindungan data di Amerika Serikat, data/ information dapat dipilah menjadi tiga yaitu (1) identified, (2) identifiable, or (3) non-identifiable person. Akan tetapi ketiga katergiri tersebut tidak mempunyai batasan yang jelas.

[53] Article 29 Data Protection Working Party, Opinion 4/2007.

[54] Article 29 Data Protection Working Party, Opinion 4/2007.

[55] United States Government Accountability Office (GAO Report to Congressional Requesters, *Privacy: Alternatives Exist for Enhancing Protection of Personall Identifiable Information*, May 2008, Memorandums 07-16 and 06-19. GAO Report 08-536.

[56] The Department of Justice (DOJ) *Privacy Impact Assessments Official Guidance* (Rev. 7/15); US NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*. P.13. Apendix B.

Linked information/informasi tertaut adalah informasi tentang atau terkait dengan seorang individu yang secara logis dikaitkan dengan informasi lain tentang individu tersebut. Sementara itu, "linkable information */informasi yang dapat ditautkan*" adalah informasi tentang atau yang terkait dengan individu yang kemungkinan terkait secara logis dengan informasi lain tentang individu tersebut.

Beberapa contoh-contoh informasi yang dapat dianggap *Personally Identifiable Information* adalah:[57]

- Nama, seperti nama lengkap, nama gadis, nama gadis ibu, atau alias.
- *Personal identification number*, seperti nomor jaminan sosial (SSN), nomor paspor, nomor SIM, nomor identifikasi pembayar pajak, nomor identifikasi pasien, dan nomor rekening keuangan atau kartu kredit.
- Informasi alamat, seperti alamat jalan atau alamat email.
- Asset information, seperti alamat Protokol Internet (IP) atau *Media Access Control* (MAC) atau pengidentifikasi statis persisten spesifik host yang secara konsisten menautkan ke orang tertentu atau sekelompok kecil orang yang didefinisikan dengan baik.
- Nomor telepon, termasuk nomor seluler, bisnis, dan pribadi.
- Personal characteristics/Karakteristik pribadi, termasuk gambar fotografis (terutama wajah atau karakteristik pembeda lainnya), sinar-X, sidik jari, atau data biometrik atau data lainnya (mis., Pemindaian retina, tanda tangan suara, geometri wajah).
- Informasi yang mengidentifikasi properti yang dimiliki secara pribadi, seperti nomor registrasi kendaraan atau nomor judul dan informasi terkait.
- Informasi tentang seseorang yang terhubung dengan salah satu di atas (mis., Tanggal lahir, tempat lahir, ras, agama, berat badan, kegiatan, indikator geografis).

E.3. Data Pribadi Sensitif

Secara umum, data pribadi dapat dilakukan kategoriasi untuk membedakan data umum dan data 'sensitif' atau spesifik. Sebuah informasi menjadi data sensitif atau kategori khusus, ketika pemrosesan memerlukan tingkat perlindungan tambahan atau membutuhkan tingkat perlindungan yang lebih tinggi, termasuk adanya alasan diizinkan untuk memprosesnya. Sulit memang menemukan definisi baku tentang Data Pribadi Sensitif. Sebagian besar undang-undang tidak memberikan definisi, tetapi sebaliknya memberikan daftar data yang dikategorikan sebagai data pribadi sensitif atau daftar kategori khusus data pribadi.

Rujukan awal untuk menetukan kategori data yang diidentifikasi sensitif adalah ketentuan yang mengatur jenis diskriminasi yang dimuat dalam instrumen hak asasi manusia dan ketentuan dasar konstitusional masing-masing negara yang mengabadikan hak untuk non-diskriminasi. Sebab seringkali sejumlah data (sensitif) teresebut menjadi basis atau dasar terjadinya praktik diskriminasi dan ekslusivisme atau pengucilan terhadap seseorang atau kelompok.

Oleh karenanya terhadap data pribadi sensitif atau kategori data khusus, perlu perlindungan untuk menjaga terhadap risiko yang mungkin timbul dari pemrosesan data sensitif berkaitan dengan resiko kepentingan, hak, dan kebebasan mendasar dari subjek data, terutama risiko diskriminasi. (Pasal 6 ayat 2 EU Modernised Convention 108). Data sensitif atau kategori data khusus menurut Pasal 6 EU Modernised Convention 108 mencakup:

---

[57] NIST Special Publication 800-122 ibid. Baca juga European Commission, What is personal data? *ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.*

- *data genetik;*
- *data pribadi yang berkaitan dengan pelanggaran, proses pidana dan hukuman, dan tindakan keamanan terkait;*
- *data biometrik yang secara unik mengidentifikasi seseorang;*
- *data pribadi untuk informasi yang mereka ungkap terkait dengan ras atau asal etnis, pendapat politik, keanggotaan serikat pekerja, kepercayaan agama atau lainnya, kesehatan atau kehidupan seksual, hanya akan diizinkan jika perlindungan yang sesuai diabadikan dalam hukum, yang melengkapi Konvensi ini.*

Sementara itu Pasal 9 ayat (1) EU GDPR menenentukan kategori khusus data pribadi, yang terdiri atas: asal ras atau etnis, pendapat politik, kepercayaan agama atau filosofis, atau keanggotaan serikat pekerja, dan data genetik, data biometrik untuk tujuan mengidentifikasi secara unik orang alami, data mengenai kesehatan atau data mengenai kehidupan seks atau orientasi seksual.

Dalam konteks, nasional, beberapa negara dimungkinkan memiliki pandangan tersendiri tentang data sensitif yang perlu mendapatkan perlindungan tambahan karena 'sensitivitas' dalam konteks nasional mereka sendiri masing-masing negara mungkin memasukkan data pribadi lain yang masuk sebagai kategori data pribadi sensitif, misalnya, data keuangan, nomor jaminan sosial, dan data yang berkaitan dengan anak-anak. Penambahan kategori data sensitive dan membutuhkan perlindungan tambahan dapat dilakukan dalam konteks negara masing-masing.. Misalnya, di India, memperlakukan 'informasi kasta' sebagai data pribadi yang sensitif,[58] sementara Filipina menempatkan status perkawinan (marital status) sebagai bagian dari data sensitif,[59] juga Trinidad Tobago menjadikan umur atau status perkawinan sebagai data sensitif.[60] Oleh karena itu pertimbangan konteks dan realitas lokal adalah langkah penting dalam memastikan bahwa perlindungan yang relevan disediakan dalam undang-undang.

Tidak ada daftar lengkap dan sama disemua negara tentang data pribadi yang masuk dalam kategori data pribadi sensitif. Namun, data yang berkaitan dengan informasi berikut ini telah secara luas dianggap sebagai data pribadi yang sensitif:[61]

a. asal ras atau etnis individu
b. opini politik
c. keyakinan agama atau filosofis atau keyakinan lain yang sifatnya serupa
d. keanggotaan serikat pekerja
e. kesehatan fisik atau mental
f. orientasi seksual
g. tindakan kejahatan atau dugaan tindakan kejahatan atas pelanggaran apa pun, atau tindakan apa pun atas pelanggaran apa pun yang dilakukan atau diduga telah dilakukan, pelepasan proses semacam itu atau hukuman pengadilan mana pun dalam proses tersebut
h. data biometrik
i. data genetik.

---

[58] Privacy International, *The Keys to Data Protection …….*hlm 26

[59] Sec. 3(l) of the Data Privacy Act of Phillipines,

[60] Trinidad Tobago, The Data Protection Act 2011.

[61] Privacy International, *The Keys to Data Protection …….*hlm 26

E.4. Pemrosesan (*Processing*) Data

Definisi 'pemrosesan' harus luas dan inklusif, bukan lengkap. Ini akan mendorong negara-negara untuk berpikir secara inovatif dan progresif dalam menanggapi kemajuan teknologi dalam metode analisis data. Modernised Convention 108 memberikan dua pemaknaan tentang data processing/pemrosesan data, yaitu:

- Pasal 2 huruf b mendefinisikan *data processing* pada kondisi pemrosesan menggunakan cara otomatis/*automated processing*. Dalam hal ini data processing/pemrosesan data berarti setiap akatifitas atau serangkain aktifitas yang dilakukan terhadap data pribadi, seperti pengumpulan, penyimpanan, pelestarian, perubahan, pengambilan, pengungkapan, membuat tersedia, penghapusan, atau perusakan, atau pelaksanaan logika dan/atau aritmatika operasi pada data tersebut;
- Pasal 2 huruf c mendefinisikan data processing pada kondisi pemrosesan menggunakan cara manual/*not-automated processing*. Dikatakan "Jika pemrosesan otomatis tidak digunakan, "pemrosesan data" berarti operasi atau serangkaian operasi yang dilakukan atas data pribadi dalam set terstruktur dari data tersebut yang dapat diakses atau diambil sesuai dengan kriteria tertentu";

Sementara itu dalam Pasal 4 ayat (2) EU GDPR memberikan definisi *processing*/pemrosesan yaitu setiap kegiatan atau serangkaian kegiatan yang dilakukan pada data pribadi atau pada serangkaian data pribadi, baik dengan cara otomatis atau tidak, seperti pengumpulan, pencatatan, organisasi, penataan, penyimpanan, adaptasi atau perubahan, pengambilan, konsultasi, menggunakan, mengungkapkan melalui transmisi, penyebaran atau menyediakan, penyelarasan atau kombinasi, pembatasan, penghapusan atau penghancuran. Ketentuan Pasal 2 angka 1 EU GDPR berlaku untuk pemrosesan data pribadi seluruhnya atau sebagian dengan cara otomatis dan untuk pemrosesan selain dengan cara otomatis, yang merupakan bagian dari sistem pengarsipan atau dimaksudkan untuk membentuk bagian dari sistem pengarsipan.

Dengan mempertimbangkan hal tersebut, penting juga memasukan gagasan untuk secara khusus mengintegrasikan pembuatan data dalam definisi pemrosesan. Ini adalah kegiatan yang sejauh ini belum secara eksplisit dibahas dalam undang-undang perlindungan data, dan harus diatur dan diawasi, dan untuk itu individu harus diberikan perlindungan.

E.5. Pengendali (*Controller*) dan Prosesor (*Processor*) Data

Terdapat perbedaan dalam mendefinsikan *controller* dan *processor*. Tidak hanya tentang definisi dari *controller* dan *processor* itu sendiri tetapi juga tentang keberadaan *controller* dan *processor*. OECD Privacy Guidelines, Modernised Convention 108 , EU GDPR, dana beberapa undang-undang di berbagai negara membedakan dalam mendefinsikan maupun pengaturan *controller* dan *processor*.

Akan tetapi UU Perlindungan Data Pribadi Jepang (Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) tidak membedakan antara *controller* dan *processor* tetapi menggunakan istilah *a Handling Operator* (*Kojin Joho Toriatsukai Jigyosha*) yang bertindak sebagai *controller* dan *processor*. Disebutkan *Handling Operator* (*Kojin Joho Toriatsukai Jigyosha*) *may be comparable to a Controller or a Processor in that it is subject to obligations to protect Personal Information*.

Sementara OECD mendefinisikan *data controller* sebagai pihak yang menurut hukum domestik, kompeten untuk memutuskan tentang konten dan penggunaan data pribadi terlepas dari apakah data tersebut dikumpulkan, disimpan, diproses atau disebarluaskan oleh pihak itu atau oleh agen atas namanya.

Kemudian Modernised Convention 108 mendefisinisikan *controller* dan *processor* sebagai berikut:

- *Controller* pada Pasal 2 huruf d, berarti seorang individu atau badan hukum, otoritas publik, layanan, agensi atau badan lain yang, secara sendiri atau bersama-sama dengan lainnya, memiliki kekuasaan membuat keputusan sehubungan dengan pemrosesan data;
- *Processor* pada Pasal 2 huruf f berarti orang individu atau badan hukum, otoritas publik, layanan, agensi atau badan lain apa pun yang memproses data pribadi atas nama *controller* atau pengendali.

Sementara dalam EU GDPR, *controller* dan *processor* didifinisikan pada Pasal 4 angka 7 dan angka 8, yang menyebutkan:

- *Controller* berarti orang perseorangan atau badan hukum, otoritas publik, agensi atau badan lain yang, secara sendiri atau bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan data pribadi; di mana tujuan dan cara pemrosesan tersebut ditentukan oleh hukum EU atau Negara Anggota, ……;
- *Processor* 'pengolah' berarti orang alami atau badan hukum, otoritas publik, agensi atau badan lain yang memproses data pribadi atas nama pengontrol;

Lebih jauh dengan merujuk pada definisi EU GDPR dan Modernised Convention 108, elemen *controller* dan *processor*, yaitu:

(a) "orang individu atau badan hukum, otoritas publik, agensi atau badan lainnya";
(b) "sendiri atau bersama-sama dengan orang lain"; dan
(c) "menentukan tujuan dan cara pemrosesan data pribadi".

Dari ketiga elemen tersebut, elemen ketiga yaitu menentukan tujuan dan cara pemrosesan data pribadi (*determines the purposes and means of the processing of personal data*) merupakan elemen penting untuk membedakan pengendali/*controller* dari aktor lain.[62] Elemen "*determines*,…." dalam definisi the body "*who is competent ... to decide*.." berkaitan dengan tiga kondisi, yaitu:[63]

- Kontrol berasal dari kewenangan yang ditentukan secara explisit oleh hukum (*Control stemming from explicit legal competence*). Undang-undang menentukan secara pasti kewenangan dan kewajiban pengendali/kontroler.
- Kontrol berasal dari kewenangan yang tidak ditentukan secara explisit oleh hukum (*Control stemming from implicit competence*). Kewenangan menentukan pemrosesan tidak secara eksplisit ditetapkan oleh undang-undang, atau bukan konsekuensi langsung dari ketentuan hukum. Akan tetapi, berasal dari ketentuan hukum umum atau praktik hukum yang berkaitan dengan bidang yang lain (hukum perdata, hukum dagang, hukum perburuhan , dll). Dalam hal ini, tanggung jawab atau kapasitas untuk menentukan pemrosesan melekat pada peran fungsional organisasi yang pada akhirnya mengharuskan tanggung jawab juga dari sudut pandang perlindungan data,misalnya, pengusaha terkait dengan data karyawannya, atau asosiasi terkait dengan data anggotanya.
- Kontrol berasal dari pengaruh faktual (*Control stemming from factual influence*). Tanggung jawab sebagai pengendali dikaitkan situasi faktual. Dalam hal ini, tanggung jawab pengendali/*controller* dikaitkan dan berdasarkan pada situasi faktual, seperti hubungan kontraktual antara pihak yang terlibat. Kondisi ini memungkinkan adanya peran dan tanggung jawab pengontrol karena pengontrol menjadi ke satu pihak dalam kontrak.

---

[62] EU Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor". 00264/10/EN. WP 169 Adopted on 16 February 2010 (EU WP 00264/10/EN. WP 169).

[63] *Ibid.*

Determination of the "purpose" of processing/penentuan "tujuan" pemrosesan diberikan atau menjadi kewenangan pengendali/*controller*. Oleh karena itu siapa pun yang membuat keputusan ini adalah pengendali (*de facto*). *The determination of the "means" of processing*/menentukan "sarana" pemrosesan dapat didelegasikan oleh pengendali, sejauh menyangkut masalah teknis atau organisasi. Keputusan dapat didelegasikan ke prosesor, seperti misalnya "perangkat keras atau perangkat lunak mana yang akan digunakan?", "data mana yang akan diproses?" , "untuk berapa lama mereka akan diproses?", "siapa yang akan memiliki akses ke mereka?", dan seterusnya.

Sementara kaitannya dengan prosesor, merupakan "*orang yang secara hukum terpisah bertindak atas namanya*". Keberadaan prosesor tergantung pada keputusan yang diambil oleh pengendali (pihak yang dapat memutuskan memproses data di lakukan oleh internal organisasinya atau pihak yang dapat mendelegasikan semua atau sebagian dari kegiatan pemrosesan ke organisasi eksternal). Sedangkan dalam kaitan hubungan pengendali/*controller* dan prosesor, terdapat dua posisi prosesor yaitu di satu sisi menjadi pihak yang terpisah dengan pengendali dan di sisi lain memproses data atas nama dirinya. Kegiatan pemrosesan ini mungkin terbatas pada tugas atau konteksnya. Dalam kondisi tertentu pada saat yang sama, pihak yang sama dapat bertindak sebagai pengendali untuk operasi pemrosesan tertentu dan sebagai prosesor untuk orang lain, dan kualifikasi sebagai pengendali atau prosesor harus dinilai terkait dengan rangkaian tindakan proses data tertentu.[64]

E.6. Subjek Data Pribadi

Secara sederhana subjek data adalah setiap orang yang data pribadinya dikumpulkan, ditahan, atau diproses. Penggunaan istilah subjek data (*data subject*) berbeda dengan pemilik data (data owner), sebab secara konsep juga berbeda makna. Subjek data mengacu pada kontrol atas data yang mengidentifikasi atau diidentifikasi melekat pada individu tertentu, sedangkan pemilik data lebih mengacu pada penguasaan atas data, yang tidak secara khusus mengidentifikasi individu tertentu. Perbedaan konsep ini pula yang membedakan rezim perlindungan data yang menggunakan istilah subjek data yang menekankan pada kontrol, dengan rezim hak kekayaan intelektual yang menekankan pada kepemilikan (*ownership*).[65]

Dari intrumen hukum perlindungan data, termasuk juga undang-undang perlindungan data di berbagai negara, subjek data umumnya mengacu pada setiap individu yang dapat diidentifikasi, secara langsung atau tidak langsung, melalui pengidentifikasi seperti nama, nomor ID, data lokasi, atau melalui faktor-faktor spesifik pada fisik, fisiologis, genetik, mental, ekonomi, budaya atau identitas sosial. Sementara pemilik data adalah individu yang bertanggung jawab atas aset data. Termasuk di dalamnya badan publik pemerintah, organisasi, atau unit bisnis yang memiliki aset data. Artinya konsep pemilik data (data owner) justru lebih mengacu pada pengendali data (data controller) yang dibebani serangkaian tanggung jawab, seperti: kepatuhan pada undang-undang, mengontrol data, administrasi data, akses data, hingga keamanan data tersebut (*data security*).

Dalam kaitannya dengan pelaksanaan prinsip-prinsip transparansi dan akuntabilitas dalam pemrosesan data pribadi, hukum perlindungan data pribadi harus dilengkapi dengan seperangkat hak dari subjek data. Sejumlah hak subjek data (*rights of data subject*) umumnya terdiri atas: hak atas informasi, hak akses;

---

[64] *Ibid*.

[65] Teresa Scassa, Data Ownership, CIGI Papers No. 187, September 2018, available at https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf.

hak untuk memperbaiki, memblokir, dan menghapus; hak untuk menyangkal (*right to object*); hak atas portabilitas data; hak yang terkait dengan pemrofilan dan pengambilan keputusan secara otomatis; hak atas pemulihan yang efektif; serta hak atas kompensasi dan pertanggungjawaban.

E.7. Pembuatan Profil (*Profiling*)

Ketersediaan data pribadi di internet dan kemampuan perangkat internet untuk menemukan korelasi dan membuat tautan data, memungkinkan aspek-aspek pribadi atau perilaku, minat, dan kebiasaan individu dianalisis dan diprediksi. Kemajuan teknologi, kemampuan analitik big data, dan kecerdasan buatan (*artificial intelligence*) mempermudah untuk membuat profil dan membuat keputusan secara otomatis yang secara signifikan berpotensi memengaruhi hak dan kebebasan individu. Pembuatan profil dan pengambilan keputusan otomatis dapat bermanfaat bagi individu dan organisasi dan memberikan manfaat seperti peningkatan efisiensi dan penghematan sumber daya. Namun, pembuatan profil dan pengambilan keputusan otomatis dapat menimbulkan risiko signifikan bagi hak dan kebebasan individu yang membutuhkan perlindungan yang tepat.Individu mungkin tidak tahu bahwa mereka sedang diprofilkan. [66]

EU GDPR mendefinisikan pembuatan profil pada Pasal 4 (4). Definisi ini digunakan Undang-Undang Privasi Data Filipina 2012 (bagian 1. (p)) yang menyebutkan sebagai berikut:

> *segala bentuk pemrosesan data pribadi secara otomatis yang terdiri dari penggunaan data pribadi untuk mengevaluasi aspek-aspek pribadi tertentu yang berkaitan dengan orang individu, khususnya untuk menganalisis atau memprediksi aspek-aspek mengenai kinerja orang tersebut di tempat kerja, situasi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi atau pergerakan.*

Terhadap definsi tersebut, EU Article 29 Data Protection Working Party, "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation*" memberikan uraian bahwa *profiling* terdiri dari tiga elemen:[67]

- harus bentuk pemrosesan otomatis (*it has to be an automated form of processing*);
- harus dilakukan pada data pribadi (*it has to be carried out on personal data*); dan
- tujuan dari pembuatan profil harus untuk mengevaluasi aspek - aspek pribadi tentang orang individu (*the objective of the profiling must be to evaluate personal aspects about a natural person*).

Pembuatan profil harus melibatkan beberapa bentuk pemrosesan otomatis—walaupun keterlibatan manusia tidak serta-merta menghilangkan aktivitas dari definisi tersebut. *Profiling* merupakan prosedur yang mungkin melibatkan serangkaian deduksi statistik. Ini sering digunakan untuk membuat prediksi tentang orang, menggunakan data dari berbagai sumber untuk menyimpulkan sesuatu tentang seseorang, berdasarkan pada kualitas orang lain yang tampak serupa secara statistik. Secara umum, membuat profil berarti mengumpulkan informasi tentang seseorang (atau sekelompok individu) dan mengevaluasi karakteristik atau pola perilaku mereka untuk menempatkan mereka ke dalam kategori atau kelompok tertentu, khususnya untuk menganalisis dan/atau membuat prediksi.[68]

---

[66] Baca EU ARTICLE 29 DATA PROTECTION WORKING PARTY, "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*", 17/EN-WP251rev.01, Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018 (EU WP 17/EN-WP251rev.01).

[67] *Ibid.*

[68] *Ibid.*

F. PRINSIP-PRINSIP PERLINDUNGAN DATA

Berbagai organisasi dan kerjasama internasional dan regional telah mengeluarkan petunjuk/kerangka kerja perlindungan data pribadai baik yang mengikat (*binding*) sebagai sebuah *hard law*, maupun yang tidak mengikat (*non-binding*) dalam bentuk *soft law*. Dalam perjalanan waktu, dari berbagai instrumen tersebut secara simultan saling beradaptasi dan dilakukan revisi, beberapa diantaranya adalah:

1. ***UN Guidelines for the Regulation of Computerized Personal Data File***, terbatas pada prinsip standard, tidak mengikat.
2. ***UN Personal Data Protection and Privacy Principles***, tidak mengikat.
3. ***EU General Data Protection Regulation***, memuat aturan penyelenggaraan data pribadi yang bersifat mengikat negara-negara anggota Uni Eropa.
4. ***OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*** 1980 (amandement 2013), memuat petunjuk perlindungan data pribadi, tidak mengikat tetapi Amerika Serikat menggunakan beberapa materi sebagai rujukan regulasi dan implementasi perlindungan data di Amerika Serikat.
5. ***APEC Privacy Framework*** (2015), memuat petunjuk perlindungan data pribadi, tidak mengikat.
6. ***ASEAN Framework on Personal Data Protection*** 2016, memuat petunjuk perlindungan data pribadi, tidak mengikat.

Berbagai petunjuk dan kerangka kerja tersebut menggunakan istilah yang berbeda tetapi beberapa substansinya sama. *EU General Data Protection Regulation* (Regulation 2016/679) sebagai peraturan yang mengikat bagi negara anggotanya merupakan instrumen yang dianggap paling rinci memuat materi perlindungan data pribadi. Dalam konteks ini, penulisan naskah ini menggunakan rujukan *EU General Data Protection Regulation* sebagai rujukan penting yang di komparasi dari berbagai instrumen yang ada.

Tabel Perbandingan Prinsip-Prinsip Perlindungan Data Pribadi

UN Guidelines for the Regulation of Computerized Personal Data Files	**UN Personal Data Protection And Privacy Principles**	**EU *General Data Protection Regulation***	**OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**	**APEC Privacy Framework**	**ASEAN Framework On Personal Data Protection**
1. Lawfulness and fairness 2. Accuracy 3. The purpose-specification 4. Interested-person access 5. Interested-person 6. Power to make exceptions 7. Security 8. Supervision and sanctions 9. Transborder data flows	1. Fair and legitimate processing 2. Purpose specification 3. Proportionality and necessity 4. Retention 5. Accuracy 6. Confidentiality 7. Security 8. Transparency 9. Transfers 10. Accountability	1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimisation; 4. Accuracy 5. Storage limitation 6. Integrity and confidentiality 7. Accountability	1. Collection Limitation 2. Data Quality 3. Purpose Specification 4. Use Limitation 5. Security Safeguards 6. Individual Participation 7. Accountability	1. Preventing Harm 2. Notice 3. Collection Limitation 4. Uses of Personal Information 5. Choice 6. Integrity of Personal Information 7. Security Safeguards 8. Access and Correction	1. Consent, Notification and Purpose 2. Accuracy of Personal Data 3. Security Safeguards 4. Access and Correction 5. Transfers to Another Country or Territory 6. Retention 7. Accountability

Dari perbandingan prinsip-prinsip di atas, setidaknya kita dapat menginventarisasi tujuh prinisip yang hampir pasti muncul dalam setiap peraturan mengenai perlindungan data pribadi, ketujuh prinsip tersebut adalah:

1. prinsip keabsahan dan transparansi (*lawfulness and transparency principle*)
2. prinsip batasan tujuan (*purpose limitation principle*)
3. prinsip minimalisasi data (*data minimization principle*)
4. prinsip akurasi(*accuracy principle*)
5. prinsip retenti/batasan penyimpanan (*retention/storage limitation principle*);
6. prisip kerahasiaan dan keamanan (*confidentiality* and *security principle*)
7. prinsip akuntabilitas (*accountability principle*)

Secara detail uraian dan penjelasan dari ketujuh prinsip tersebut, hubungan dengan setiap tahapan pemrosesan data pribadi, pengendali dan prosesor data, maupun kaitannya dengan hak-hak subjek data akan dijelaskan berikut ini:

F.1. Prinsip Keabsahan dan Transparansi (*Lawfulness, Fairness and Transparency*)

Urgensi penerapan prinsip ini adalah individu harus diberi informasi dan mengetahui dengan jelas bagaimana data mereka akan diproses, dan oleh siapa data diproses dan disimpan. Individu harus mengetahui apakah data akan dibagi pada pihak ketiga. Jika individu tidak diberi informasi dengan jelas dan tidak mengetahu tentang fakta tersebut, maka kemungkinan bahwa data pribadi orang tersebut diperoleh secara tidak adil, dan proses dianggap tidak transparan.[69]

Dalam UN *Guidelines for the Regulation of Computerized Personal Data Files* digunakan istilah *principle of lawfulness and fairness,* yaitu Informasi tentang orang tidak boleh dikumpulkan atau diproses dengan cara yang tidak adil atau melanggar hukum, juga tidak boleh digunakan untuk tujuan yang bertentangan dengan tujuan dan prinsip-prinsip Piagam PBB.[70]

Sementara UN *Personal Data Protection And Privacy Principles* menggunakan istilah *Fair and Legitimate Processing* yaitu memrosesan data pribadi dengan cara yang adil, sesuai dengan mandat dan instrumen pemerintahan mereka dan berdasarkan hal-hal berikut:

(a) persetujuan subjek data;
(b) kepentingan terbaik dari subjek data, konsisten dengan mandat Organisasi Sistem Perserikatan Bangsa-Bangsa yang bersangkutan;
(c) mandat dan instrumen pemerintahan dari Organisasi Sistem Perserikatan Bangsa-Bangsa yang bersangkutan; atau
(d) setiap dasar hukum lainnya yang secara khusus diidentifikasi oleh Organisasi Sistem Perserikatan Bangsa-Bangsa yang bersangkutan.

Sementara OECD dalam *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Amandement 2013), memasukkan substansi *lawfulness, fairness and transparency* dalam *Collection Limitation Principle,* yang substansinya sama dengan *principle of lawfulness, fairness and transparency,* yaitu penyelenggaraan data pribadi harus dilakukan secara sah, adil, dan transparan dalam kaitannya

---

[69] Privacy International, The Keys to Data Protection (2018), hlm 38.

[70] UN, "*Guidelines for the Regulation of Computerized Personal Data Files",* Adopted by General Assembly resolution 45/95 of 14 December 1990. A. 1. Principle of lawfulness and fairness.

dengan subjek data (*There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject)*.[71]

Sedangkan APEC dalam Privacy Framework (2015), menggunakan prinsip *principle of collection limitation* yang secara substansi sama dengan Prinsip Keabsahan, keadilan dan Transparansi. Dalam hal ini APEC berpendapat, *Pengumpulan informasi pribadi harus dibatasi pada informasi yang relevan dengan tujuan pengumpulan dan setiap informasi tersebut harus diperoleh dengan cara yang sah dan adil, dan jika perlu, dengan pemberitahuan, atau persetujuan dari, orang yang bersangkutan.*[72]

Dalam EU GDPR, Prinsip ini diatur pada Pasal 5 huruf a yaitu *processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)*. Pada Pasal 6 ayat (1) diuraikan bahwa Pemrosesan sah jika dilakukan:

(a) subjek data telah memberikan persetujuan untuk pemrosesan data pribadinya untuk satu atau lebih tujuan spesifik (*consent of the data subject*);
(b) pemrosesan diperlukan untuk pelaksanaan kontrak dimana subjek data menjadi pihak atau untuk mengambil langkah-langkah atas permintaan subjek data sebelum masuk ke dalam kontrak (*necessity to enter a contract*);
(c) pemrosesan diperlukan untuk kepatuhan dengan kewajiban hukum yang harus dikontrol oleh pengendali (*a legal obligation*);
(d) pemrosesan diperlukan untuk melindungi kepentingan vital subjek data atau orang perorangan lainnya (*necessity to protect the vital interests of the data subject or of another person*);
(e) pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali (*necessity for performing a task in the public interest*);
(f) pemrosesan diperlukan untuk tujuan kepentingan sah yang diminta oleh pengendali atau oleh pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak dasar dan kebebasan dari subjek data yang membutuhkan perlindungan data pribadi, khususnya di mana data tersebut subjek adalah seorang anak (*necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject*). Ketentuan ini tidak berlaku untuk pemrosesan yang dilakukan oleh otoritas publik dalam melaksanakan tugasnya.[73]

Dalam Modernised Convention 108, *the lawfulness principle* menentukan bahwa data pribadi yang sedang diproses akan diproses secara sah (*personal data undergoing processing shall be processed lawfully*), data pribadi yang sedang diproses harus diproses secara adil dan transparan (*(personal data undergoing processing shall be …. (a) processed fairly and in a transparent manner*).[74] Pada Pasal 5 EU Modernised Convention 108 dsebutkan bahwa:

- Setiap pihak harus menetapkan bahwa pengendali menginformasikan kepada subjek data tentang:
  a. identitasnya dan tempat tinggal atau pendirian kebiasaan;

---

[71] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013). [C (80)58/FINAL, as amended on 11 July 2013 by C(2013)79] Anex. Para 7.

[72] APEC, The APEC Privacy Framework, 2015: APEC Information Privacy Principles (III. Collection Limitation).

[73] EU GDPR, Regulation (EU) 2016/679 Of The European Parliament And Of The Council 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) Art. 5 – 6.

[74] EU Modernised Convention 108, Article 5 (3), Article 5 (4) (a).

b. dasar hukum dan tujuan pemrosesan yang dimaksud;
c. kategori data pribadi yang diproses;
d. penerima atau kategori penerima data pribadi, jika ada; dan
e. cara melaksanakan hak yang diatur dalam Pasal 9, serta informasi tambahan yang diperlukan untuk memastikan pemrosesan data pribadi yang adil dan transparan.

- Paragraf 1 tidak berlaku di mana subjek data sudah memiliki informasi yang relevan.
- Jika data pribadi tidak dikumpulkan dari subyek data, pengontrol tidak diharuskan untuk memberikan informasi seperti itu di mana pemrosesan secara tegas ditentukan oleh hukum atau ini terbukti tidak mungkin atau melibatkan upaya yang tidak proporsional.

F.2. Prinsip Batasan Tujuan (*Purpose Limitation*)

Subtansi dari *purpose limitation pinciple* adalah bahwa penyelenggara data pribadi dapat mengumpulkan, menggunakan atau mengungkapkan data pribadi tentang seorang individu hanya untuk tujuan yang masuk akal.[75] Semua data pribadi harus dikumpulkan untuk tujuan yang ditentukan secara sah dan spesifik. Pemrosesan harus sesuai dengan tujuan yang ditentukan sejak awal dan tidak boleh digunakan untuk tujuan lain tanpa pemberitahuan atau persetujuan subjek data. Tujuan pemrosesan, penggunaan data harus jelas dan diberitahukan kepada subjek data. Jika data akan digunakan untuk tujuan selain tujuan awal, maka subjek data harus diberi informasi yang memadai tentang hal ini dan memerlukan persetujuan lebih lanjut dari pemilik data. Data pribadi yang sensitif tidak diproses untuk tujuan selain yang ditentukan sebelumnya. Data pribadi tidak boleh diungkapkan, disediakan, atau digunakan untuk tujuan selain yang ditentukan, sesuai dengan 'Prinsip Batasan Tujuan'.[76]

Terdapat dua pengecualian umum untuk prinsip ini yaitu dapat diterima jika: (1) dilakukan dengan persetujuan subjek data; persetujuan harus valid; itu tidak boleh bersyarat atau memiliki tujuan lain yang disembunyikan dalam cetakan kecil atau *legalese* (tidak dapat diakses oleh subjek data); dan (2) dilakukan oleh otoritas hukum. Akan tetapi perlu ditegaskan bahwa pengecualian seperti itu mengancam dan melemahkan perlindungan yang ditawarkan oleh undang-undang perlindungan data, sehingga sangat penting bahwa ketentuan pengecualian dibuat secara ketat.[77]

UN Guidelines for the Regulation of Computerized Personal Data Files memuat Prinsip spesifikasi tujuan/*the purpose-specification principle*, yaitu tujuan untuk pelayanan dan penggunaan data/file harus ditentukan secara spesifik, sah dan ketika pergunakan untuk publikasi harus sepengatahuan orang yang bersangkutan, dan selanjutnya untuk memastikan bahwa:[78]

(a) Semua data pribadi yang dikumpulkan dan direkam tetap relevan dan memadai untuk tujuan yang ditentukan (*pen*. berkaitan dengan *data minimization principle*);
(b) Tidak ada data pribadi yang digunakan atau diungkapkan untuk tujuan yang tidak sesuai dengan yang ditentukan, kecuali dengan persetujuan dari orang yang bersangkutan (*pen*. berkaitan dengan *Purpose limitation Principle*);
(c) Periode penyimpanan data pribadi tidak melebihi periode yang memungkinkan pencapaian tujuan yang ditentukan (*pen*. berkaitan dengan '*Storage Limitation Principle*).

---

[75] ASEAN *Framework on Personal Data Protection: Principle of Consent, Notification and Purpose.*

[76] Privacy International, The Keys to Data Protection (2018), hlm 39-40.

[77] *Ibid*.

[78] UN, "*Guidelines for the Regulation of Computerized Personal Data Files",* Adopted by General Assembly Resolution 45/95 of 14 December 1990 A.3. *the purpose-specification principle*.

UN Personal Data Protection And Privacy Principles, dalam *purpose specification principle* dijelaskan bahwa data pribadi harus diproses untuk tujuan tertentu, memperhitungkan keseimbangan hak, kebebasan, dan kepentingan yang relevan. Data pribadi tidak boleh diproses dengan cara yang tidak sesuai dengan tujuan tersebut.[79] Sedangkan *ASEAN Framework on Personal Data Protection*, dalam prinsip *consent, notification and purpose*, menguraikan secara singkat prinsip *purpose* yaitu bahwa suatu organisasi dapat mengumpulkan, menggunakan atau mengungkapkan data pribadi tentang seorang individu hanya untuk tujuan yang masuk akal yang sesuai keadaan.[80]

Kemudian dalam *APEC Privacy Framework* (2015), digunakan istilah *uses of personal information* yaitu informasi pribadi yang dikumpulkan harus digunakan hanya untuk memenuhi tujuan pengumpulan dan tujuan lain yang sesuai atau terkait, kecuali:

a. dengan persetujuan individu yang informasi pribadinya dikumpulkan;
b. bila perlu untuk menyediakan layanan atau produk yang diminta oleh individu; atau
c. oleh otoritas hukum dan instrumen hukum lainnya, proklamasi dan pernyataan dampak hukum.[81]

Selanjutnya *OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (Amandement 2013), menggunankan istilah *purpose specification principle*, yaitu tujuan pengumpulan data pribadi harus ditentukan secara spesifik selambat-lambatnya pada saat pengumpulan data dan penggunaan data pribadi selanjutnya terbatas pada pemenuhan tujuan tersebut atau yang sesuai dengan tujuan tersebut dan sebagaimana ditentukan pada setiap perubahan tujuan.[82] Pada *detailed comment* menguraikan bahwa *purpose specification principle* memuat, sebelum atau selambat-lambatnya pada saat pengumpulan data, dimungkinkan untuk mengidentifikasi tujuan penggunaan data, dan bahwa perubahan tujuan kemudian harus juga ditentukan. Tujuan baru tidak boleh diperkenalkan secara sewenang-wenang. Kebebasan melakukan perubahan harus menyiratkan kesesuaian dengan tujuan aslinya. ketika data tidak lagi sesuai tujuan, perlu untuk dihancurkan (dihapus) atau diberikan formulir anonim. Alasannya adalah bahwa pengawasan atas data dapat hilang ketika data tidak lagi dibutuhkan. Hal ini dapat menyebabkan risiko pencurian, penyalinan tidak resmi atau sejenisnya.[83]

Sementara EU GDPR pada Pasal 5 ayat (1) huruf b menjelaskan bahwa data pribadi harus dikumpulkan untuk tujuan yang ditentukan, eksplisit dan sah dan tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut; pemrosesan lebih lanjut untuk keperluan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistik (sesuai Pasal 89 (1)) harus dianggap sesuai dengan tujuan awal.[84]

Semua penggunaan dan pemrosesan data diluar tujuan awal harus mendapat persetujuan dari subjek data. Tentang persetujuan dari individu, EU GDPR pada Pasal 7 menentukan bahwa ketentuan untuk persetujuan:

(a) Jika pemrosesan didasarkan pada persetujuan, pengendali harus dapat menunjukkan bahwa subjek data telah menyetujui untuk memproses data pribadinya.

---

[79] UN *Personal Data Protection And Privacy Principles,* Adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018.

[80] ASEAN *Framework on Personal Data Protection: Principle of Consent, Notification and Purpose.*

[81] APEC, The APEC Privacy Framework, 2015: APEC Information Privacy Principles (*Uses of Personal Information).*

[82] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013). [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] Anex. Para 11.

[83] *Ibid.*, *Original Explanatory Memorandum* (1980): *Detailed Comments,* Para.9: *Purpose Specification Principle.*

[84] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 – 6.

(b) Jika persetujuan subjek data diberikan dalam konteks pernyataan tertulis yang juga menyangkut masalah lain, permintaan persetujuan harus disajikan dengan cara yang jelas dapat dibedakan dari masalah lain, dalam bentuk yang mudah dipahami dan mudah diakses, menggunakan formulir yang jelas dan mudah diakses. bahasa sederhana. Bagian mana pun dari pernyataan tersebut yang merupakan pelanggaran terhadap Peraturan ini tidak akan mengikat.
(c) Subjek data memiliki hak untuk menarik persetujuannya kapan saja. Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya. Sebelum memberikan persetujuan, subjek data harus diberitahu tentangnya. Akan mudah untuk menarik diri dengan memberikan persetujuan.
(d) Ketika menilai apakah persetujuan diberikan secara bebas, harus dipertimbangkan apakah, antara lain, kinerja kontrak, termasuk penyediaan layanan, tergantung pada persetujuan terhadap pemrosesan data pribadi yang tidak diperlukan untuk kinerja kontrak itu.[85]

F.3. Prinsip Minimalisasi Data (*Data Minimization*)

Prinsip-prinsip ini mengharuskan pihak yang memproses data untuk mempertimbangkan jumlah data minimum yang diperlukan untuk mencapai tujuan tersebut. Prosesor tidak dapat menerima dan mengumpulkan data tambahan karena ada kemungkinan berguna atau karena alasan lain. Pada era *big data*, Prinsip minimalisasi data sangat dibutuhkan karena kemajuan dan kemampuan teknologi secara radikal meningkatkan teknik analisis untuk mencari dan mengumpulkan untuk mengembangkan kecerdasan dan pengetahuan. Pengesampingan prinsip minimalisasi data akan berdampak pada kepemilikan data yang lebih banyak dan memungkinkan menambah akurasi tentang perilaku manusia. Karena hal tersebut ada kebutuhan mendesak untuk mencegah penyalagunaan data dengan memastikan bahwa hanya data yang diperlukan dan relevan untuk tujuan tertentu yang harus diproses.[86]

UN Guidelines for the Regulation of Computerized Personal Data Files tidak memuat secara eksplisit prinsip Minimalisasi data/*data minimization*. Substansi prinsip ini dalam *principle of the purpose-specification*/Prinsip spesifikasi tujuan yaitu semua data pribadi yang dikumpulkan dan direkam tetap relevan dan memadai untuk tujuan yang ditentukan.[87] Sementara *UN Personal Data Protection And Privacy Principles,* dalam *principles of proportionality and necessity* menguraikan bahwa pemrosesan data pribadi harus relevan, terbatas, dan memadai dengan apa yang diperlukan sehubungan dengan tujuan khusus pemrosesan data pribadi (*the processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing*).[88]

Dalam *OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (Amandement 2013), menggunakan *Data Quality Principle*/Prinsip Kualitas Data, yaitu data pribadi harus relevan dengan tujuan penggunaannya, dan, sejauh yang diperlukan untuk tujuan tersebut, harus akurat, lengkap, dan terus diperbarui relevan, dan tidak berlebihan sehubungan dengan tujuan pemrosesannya.[89]

---

[85] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 7.

[86] Baca Privacy International, The Keys to Data Protection…. hlm 40 – 41.

[87] UN, *"Guidelines for the Regulation of Computerized Personal Data Files"* Adopted by General Assembly resolution 45/95 of 14 December 1990 A.3. *the purpose-specification principle.*

[88] UN *Personal Data Protection and Privacy Principles.*

[89] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013). [C (80)58/

Dalam instrumen hukum Uni Eropa, *the data minimization principl*e ditemukan dalam *General Data Protection Regulation*, Article 5 (1) (c) dan Modernised Convention 108, Article 5 (4) (c). Ketentuan Pasal 5 (1) huruf c EU GDPR menyebutkan "*Data pribadi harus memadai, relevan dan terbatas pada apa yang diperlukan sehubungan dengan tujuan untuk mana mereka diproses*".[90] Sedangkan Modernised Convention 108, Article 5 (4) (b) menentukan bahwa data pribadi yang sedang diproses adalah dikumpulkan untuk tujuan eksplisit, spesifik dan sah dan tidak diproses dengan cara yang tidak sesuai dengan tujuan tersebut; pemrosesan lebih lanjut untuk tujuan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistik, tunduk pada perlindungan yang sesuai, kompatibel dengan tujuan tersebut.

F.4. Prinsip Akurasi (*Accuracy*)

Secara sederhana *UN Personal Data Protection And Privacy Principles,* menjelaskan bahwa data pribadi harus akurat dan, jika perlu, data terkini untuk memenuhi tujuan yang ditentukan.[91] Sedangkan *UN Guidelines for the Regulation of Computerized Personal Data Files* dalam uraian *principle of accuracy* menjelaskan bahwa orang yang bertanggung jawab untuk mengumpulkan file atau mereka yang bertanggung jawab untuk menyimpannya memiliki kewajiban untuk melakukan pemeriksaan berkala pada keakuratan dan relevansi data yang direkam dan untuk memastikan bahwa data/ file disimpan selengkap mungkin untuk menghindari kesalahan kelalaian dan bahwa mereka tetap diperbarui secara berkala atau ketika informasi yang terkandung dalam file digunakan, selama mereka sedang diproses.

Sementara *ASEAN Framework on Personal Data Protection*, dalam *Accuracy of Personal Data principle*, menguraikan secara singkat bahwa data pribadi harus akurat dan lengkap sejauh yang diperlukan untuk tujuan penggunaan data pribadi tersebut.[92] Kemudian OECD dalam *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (Amandement 2013), menggunakan isitilah *data quality principle*, yaitu data pribadi harus relevan dengan tujuan penggunaannya, dan, sejauh yang diperlukan untuk tujuan tersebut, harus akurat, lengkap, dan terus diperbarui (*Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date*).[93]

Berikutnya APEC dalam *Privacy Framework* (2015), menggunakan *principle of integrity of personal information* yaitu informasi pribadi harus akurat, lengkap, dan terus diperbarui sejauh diperlukan untuk keperluan penggunaan. [94] Prinsip ini menekankan bahwa pengontrol informasi pribadi wajib menjaga akurasi dan kelengkapan catatan dan simpan yang diperlukan untuk memenuhi tujuan penggunaan.[95]

EU GDPR pada Pasal 5 ayat (1) huruf b menyebutkan bahwa data pribadi harus akurat dan, jika perlu,

FINAL, as amended on 11 July 2013 by C (2013)79] Anex. Para 7.

[90] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art Article 5 (1) (c).

[91] UN *Personal Data Protection and Privacy Principles.*

[92] ASEAN *Framework on Personal Data Protection: Principle of Accuracy of Personal Data.*

[93] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013), Anex. Para 8 *Data Quality Principle.*

[94] APEC, The APEC Privacy Framework, 2015: APEC Information Privacy Principles (VI. Integrity of Personal Information) Para 27.

[95] APEC, The APEC Privacy Framework, 2015: comentar VI. Integrity of Personal Information) Para 27.

selalu diperbarui; setiap langkah yang masuk akal harus diambil untuk memastikan bahwa data pribadi yang tidak akurat, sehubungan dengan tujuan pengolahannya, dihapus atau diperbaiki tanpa penundaan.[96] Sedangkan Konvensi 108 menyebutkan: "Data pribadi yang sedang diproses harus akurat dan, jika perlu, selalu diperbarui." [Pasal 5 (4) (d).

Menurut *Privacy International*, terdapat berbapa elemen penting dalam prinsip akurasi ini, yaitu:

- Akurasi: Semua data yang diproses harus akurat sepanjang siklus hidup data;
- Lengkap: Setiap kategori data harus lengkap sejauh mungkin bahwa penghilangan data yang relevan mungkin tidak mengarah pada inferensi informasi yang berbeda dengan informasi yang dapat diperoleh jika data lengkap;
- Mutakhir: Setiap data yang disimpan dan dapat diproses lebih lanjut sesuai dengan ketentuan yang diatur dalam undang-undang perlindungan data serta harus selalu diperbarui; dan
- Terbatas: Data pribadi hanya boleh diproses (dan disimpan) selama periode waktu yang diperlukan untuk tujuan pengumpulan dan penyimpanan data. [97]

F.5. Prinsip Retensi/Batasan Penyimpanan (*Retention*/*Storage Limitation*)

Storage limitation principle muncul dalam EU GDPR dan Modernised Convention 108. Sementara *UN Personal Data Protection and Privacy Principles* dan *ASEAN Framework on Personal Data Protection* menggunakan istilah *retention principle.* Dalam dokumen perlindungan privacy lain seperti OECD dan APEC tidak ditemukan prinsip pembatasan penyimpanan.

Substanasi dari *retention*/*storage limitation* adalah data pribadi disimpan dalam bentuk yang memungkinkan tidak lebih dari yang diperlukan untuk keperluan pemrosesan. Data pribadi dapat disimpan untuk waktu yang lebih lama sejauh data pribadi akan diproses semata-mata untuk tujuan pengarsipan demi kepentingan umum, tujuan penelitian ilmiah, historis atau tujuan statistic. *UN Personal Data Protection and Privacy Principles,* dalam *retention principle* diuraikan bahwa data pribadi hanya boleh disimpan untuk waktu yang diperlukan untuk tujuan yang ditentukan.[98]

Sedangkan *UN Guidelines for the Regulation of Computerized Personal Data Files* tidak memuat secara eksplisit *retention*/*storage limitation principle* tetapi menjadi bagian *the purpose-specification principle.* Salah satu aspek dari *the purpose-specification principle* adalah tujuan untuk melayani suatu file dan penggunaannya dalam hal tujuan tersebut harus ditentukan dan selanjutnya untuk memastikan bahwa: ....(c) Periode penyimpanan data pribadi tidak melebihi periode yang memungkinkan pencapaian tujuan yang ditentukan.[99]

Modernised Convention 108, Article 5 (4) (e) menentukan bahwa: "*Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*" [Article 5(e)].[100] Sementara EU GDPR,

---

[96] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 – 6.

[97] Baca Privacy International, The Keys to Data Protection (2018), hlm 42.

[98] UN *Personal Data Protection and Privacy Principles.*

[99] UN, "*Guidelines for the Regulation of Computerized Personal Data Files",* Adopted by General Assembly resolution 45/95 of 14 December 1990 A.3. *the purpose-specification principle.*

[100] Modernised Convention 108, Article 5.

dalam Article 5 (1) huruf (e) menyatakan bahwa data pribadi yang sedang diproses harus disimpan tidak lebih dari yang diperlukan untuk keperluan; data pribadi dapat disimpan untuk waktu yang lebih lama sejauh data pribadi akan diproses semata-mata untuk keperluan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau tujuan statistik sesuai dengan Pasal 89 (1), yang tunduk pada implementasi teknis dan organisasi yang sesuai langkah-langkah yang diperlukan oleh Peraturan (EU GDPR) ini untuk melindungi hak dan kebebasan subjek data (batasan penyimpanan).[101]

Sementara *ASEAN Framework on Personal Data Protection*, dalam *retention principle,* menguraikan secara singkat bahwa suatu organisasi harus berhenti menyimpan dokumen yang berisi data pribadi, atau menghapus sarana yang dengannya data pribadi dapat dikaitkan dengan individu tertentu, segera setelah berasumsi bahwa retensi tidak lagi diperlukan untuk hukum atau bisnis.[102] Data pribadi hanya boleh disimpan untuk periode waktu ketika data tersebut diperlukan untuk tujuan pengumpulan dan penyimpanannya.

Oleh karenanya, undang-undang harus secara jelas menetapkan bahwa data tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan semula. Setiap pengecualian untuk ini harus sangat terbatas dan dide inisikan dengan jelas. Individu harus diberi tahu berapa lama data mereka akan disimpan, oleh karena itu penting bahwa undang-undang memberi insentif kepada pengendali data untuk menerapkan prinsip minimalisasi data dengan meminimalkan pengumpulan data pribadi, dan tidak menyimpannya lebih lama dari yang diperlukan.

F.6. Prinsip Kerahasiaan dan Keamanan (*Con identiality and Security*)

Prinsip kerahasian atau *confidentiality* ditemukan dalam *UN Personal Data Protection and Privacy Principles*, yang memisahkan dengan dari prinsip keamanan atau *security*. Menurut *UN Personal Data Protection And Privacy Principles*, *principle of confidentiality* adalah bahwa data pribadi diproses dengan memperhatikan kerahasiaan. Sementara itu prinsip keamanan adalah bahwa perlindungan dan prosedur organisasi, administrasi, fisik, dan teknis yang sesuai harus diterapkan untuk melindungi keamanan data pribadi, termasuk terhadap atau dari akses tidak sah atau tidak disengaja, kerusakan, kehilangan atau risiko lain yang ditimbulkan oleh pemrosesan data.[103]

Dalam EU GDPR secara eksplisit diatur prinsip *integrity and confidentiality.* Akan tetapi, jabaran dari *integrity and confidentiality* lebih pada keamaan dara pribadi. Dalam Articles 5 (1) (f) EU GDPR menjelaskan bahwa Data pribadi diproses dengan cara yang memastikan keamanan data pribadi yang tepat, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan terhadap kehilangan, kerusakan, atau kerusakan yang tidak disengaja, menggunakan tindakan teknis atau organisasi yang sesuai (integritas dan kerahasiaan).[104] Sedangkan Modernised Convention 108 dalam Article 7 menyatakan:

- Setiap Pihak harus menetapkan bahwa pengontrol, dan, jika dapat diterapkan prosesor, mengambil tindakan pengamanan yang tepat terhadap risiko seperti akses yang tidak disengaja atau tidak sah ke, perusakan, kehilangan, penggunaan, modifikasi, atau pengungkapan data pribadi.
- Setiap Pihak harus menetapkan bahwa pengontrol memberitahukan, tanpa penundaan, setidaknya otoritas pengawas yang kompeten dalam arti Pasal 15 Konvensi ini, tentang pelanggaran data yang dapat secara serius mengganggu hak dan kebebasan mendasar dari subyek data.

---

[101] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 (1) (e).

[102] ASEAN *Framework on Personal Data Protection: Principle of Retentionn.*

[103] UN *Personal Data Protection and Privacy Principles*: *confidentiality principle - security principle.*

[104] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 (1) (f).

ASEAN Framework on Personal Data Protection menguraikan bahwa data pribadi harus dilindungi dengan baik terhadap kehilangan dan akses tidak sah, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, perusakan atau risiko serupa.[105] Kemudian APEC dalam Privacy Framework (2015), menguraikan bahwa *controller* harus melindungi informasi pribadi yang mereka pegang dengan pengamanan yang tepat terhadap risiko, seperti kehilangan atau akses tidak sah ke informasi pribadi, atau perusakan yang tidak sah, atau penyalahgunaan lainnya. Perlindungan seperti itu harus proporsional dengan kemungkinan dan tingkat bahaya yang mengancam, kepekaan informasi dan konteks di mana informasi itu disimpan, dan harus ditinjau secara berkala dan penilaian ulang.[106]

Sementara *OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (Amandement 2013), menggunakan *Security Safeguards Principle* yang menyatakan bahwa Data pribadi harus dilindungi dengan perlindungan keamanan yang wajar dari risiko seperti kehilangan atau akses tidak sah, perusakan, penggunaan, modifikasi atau pengungkapan data.[107] Implementasi *Prinsip Perlindungan Keamanan* memiliki cakupan luas. "Kehilangan" data mencakup kasus-kasus seperti penghapusan data yang tidak disengaja, penghancuran media penyimpanan data (dan dengan demikian penghancuran data) dan pencurian media penyimpanan data. "Dimodifikasi" harus ditafsirkan untuk mencakup input data yang tidak sah, dan "digunakan" untuk mencakup penyalinan yang tidak sah. Pengamanan terhadap data pribadi mencakup tindakan fisik, tindakan organisasi (seperti tingkat otoritas terkait dengan akses ke data) dan, terutama dalam sistem komputer, langkah-langkah informasi (seperti *enciphering* dan pemantauan ancaman terhadap aktivitas yang tidak biasa dan tanggapan mereka). Harus ditekankan bahwa kategori tindakan organisasi mencakup kewajiban personil pengolah data untuk menjaga kerahasiaan.[108]

Lebih jauh, data pribadi harus dilindungi terhadap risiko seperti akses, penggunaan dan pengungkapan yang melanggar hukum atau tidak sah, serta kehilangan, kehancuran, atau kerusakan data. Perlindungan keamanan dapat mencakup:

- Langkah-langkah fisik, misalnya pintu terkunci dan kartu identitas;
- Langkah-langkah organisasi, yaitu kontrol akses;
- Langkah-langkah informasi, yaitu penyandian (pengubahan teks menjadi bentuk kode), dan pemantauan ancaman; dan
- Langkah-langkah teknis, yaitu enkripsi, pseudonimisasi, anonimisasi.
- Langkah-langkah organisasi lainnya termasuk pengujian berkala terhadap kecukupan langkah-langkah ini, implementasi perlindungan data dan kebijakan keamanan informasi, pelatihan, dan kepatuhan terhadap kode perilaku yang disetujui.[109]

F.7. Prinsip Akuntabilitas (*Accountability*)

Akuntabilitas merupakan inti penyelenggaraan dan perlindungan data pribadi. Prinsip akuntabilitas berkaitan dengan tanggung jawab dan kepatuhan penyelenggaraan data pribadi. Pengendali data merupakan pihak

---

[105] ASEAN *Framework on Personal Data Protection: security safeguards principle.*

[106] APEC, The APEC Privacy Framework, 2015: comentar VII. Security Safeguards Para 28.

[107] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Amandement 2013), Anex. Para 11: *Security Safeguards Principle.*

[108] OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data), Anex. Para B. *Detailed Comments* Para 11 angka 56.

[109] Privacy International, *The Key Concept of Data Protection* (2018), hlm. 45.

yang bertanggung jawab atas penyelenggaraan data pribadi dan dapat menunjukkan kepatuhan terhadap prinsip-prinsip pemrosesan data pribadi (akuntabel).[110] Oleh karena itu undang-undang harus mengatur pertanggungjawaban pengendali data. *Data Controller* tidak boleh dibebaskan dari kewajiban dan tanggung jawab hanya karena pemrosesan data dilakukan atas namanya oleh pihak lain. Pertanggungjawaban ini mengacu pada pertanggungjawaban yang didukung oleh sanksi hukum, serta pertanggungjawaban yang ditetapkan oleh kode etik. Data pribadi harus diproses dengan cara yang adil, berdasarkan persetujuan subjek data dan kepentingan terbaik dari subjek data.[111]

Dengan mengacu pada prinsip-prinsip tersebut, pemrosesan data pribadi baru dapat dilakukan apabila ada sejumlah alasan hukum berikut ini: ada persetujuan atau konsen dari subjek data; memastikan perlunya pemrosesan untuk berlakunya kontrak dengan subjek data; kepatuhan terhadap kewajiban hukum; melindungi kepentingan vital subjek data atau orang lain; pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali (data); atau tujuan kepentingan sah (*legitimate interest*), yang dilakukan oleh pengendali atau pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan, hak atau kebebasan dari subjek data.

Sementara kewajiban bagi pengendali dan prosesor data secara umum harus mengambil langkah-langkah teknis dan organisasional untuk memastikan dan menunjukkan bahwa pengolahan data yang mereka lakukan telah sesuai hukum. Secara detail kewajiban mereka umumnya meliputi: menyediakan audit data terkini; kebijakan & prosedur perlindungan data yang komprehensif; privasi *by design* dan *by default*; petugas perlindungan data (DPO); prosedur yang jelas bagi pemilik data; penilaian dampak perlindungan data (*data protection assessment*); peningkatan kapasitas staf-stafnya; langkah keamanan data yang kuat; prosedur terkait palanggaran, merekam dan melaporkan pelanggaran; prosedur penilaian untuk meninjau dan memperbaharui langkah-langkah yang telah diambil. Sedangkan hak-hak dari pemilik data (*rights of data subject*) terdiri dari: hak atas informasi, hak akses; hak untuk memperbaiki, memblokir, dan menghapus; hak untuk menyangkal (*right to object*); hak atas portabilitas data; hak yang terkait dengan pemrofilan dan pengambilan keputusan secara otomatis; hak atas pemulihan yang efektif; serta hak atas kompensasi dan pertanggungjawaban.

***

[110] EU GDPR, Regulation (EU) 2016/679 (General Data Protection Regulation) Art. 5 (2).

[111] UN Personal Data Protection and Privacy Principles: Accountability Principle.

PROFIL ELSAM

Lembaga Studi dan Advokasi Masyarakat (ELSAM) atau *Institute for Policy Research and Advocacy,* adalah sebuah organisasi hak asasi manusia, yang berdiri di Jakarta, sejak Agustus 1993. Tujuannya turut berpartisipasi dalam usaha menumbuhkembangkan, memajukan dan melindungi hak-hak sipil dan politik serta hak-hak asasi manusia pada umumnya – sebagaimana diamanatkan oleh UUD 1945 dan Deklarasi Universal Hak Asasi Manusia. Sejak awal, semangat perjuangan ELSAM adalah membangun tatanan politik demokratis di Indonesia melalui pemberdayaan masyarakat sipil melalui kegiatan penelitian, advokasi dan promosi hak asasi manusia.

Saat ini ELSAM memiliki tiga kegiatan utama, yang terdiri atas: (1) pengarusutamaan hak asasi manusia dalam pengambilan kebijakan; (2) studi dan produksi pengetahuan hak asasi untuk mendukung advokasi kebijakan; dan (3) Pendidikan Hak Asasi Manusia.

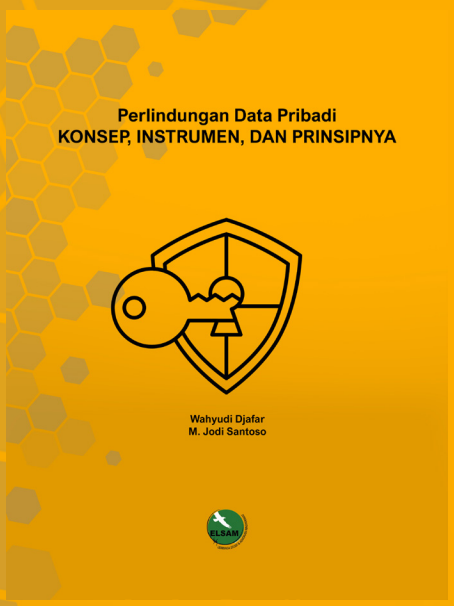
Dalam kegiatan pengarusutamaan hak asasi manusia dalam pengambilan kebijakan, ELSAM secara terus-menerus mendorong pengintegrasian prinsip-prinsip hak asasi manusia dalam setiap proses pembentukan kebijakan, seperti: (i) Memberikan masukan dan rekomendasi bagi lembaga legislatif dan pemerintah; (ii) Menyusun catatan kritis melalui berbagai policy brief atas suatu rancangan kebijakan; (iii) Monitoring pelaksanaan fungsi legislasi; (iv) Menyediakan pendampingan teknis keahilan bagi lembaga-lembaga pemerintah; dan (v) Melakukan berbagai kemitraan strategis dengan berbagai lembaga.

Berikutnya pada kegiatan studi dan produksi pengetahuan hak asasi untuk mendukung advokasi kebijakan, ELSAM melakukan berbagai penelitian dan produksi pengetahuan untuk mendorong pembentukan kebijakan berbasis bukti *(evidence based policies)*, dengan pendekatan hak asasi manusia *(human rights based approach)*. Fokus-fokus studi ELSAM antara lain:

- Bisnis dan hak asasi manusia: Mengkaji dampak operasi korporasi terhadap hak asasi, termasuk mendorong lahirnya berbagai kebijakan untuk mengaplikasikan *UN Guiding Principles on Business and Human Rights*.
- Internet dan hak asasi manusia: Meneliti mengenai implikasi kemajuan teknologi infromasi dan komunikasi terhadap perlindungan hak asasi, termasuk isu tatakelola internet, kebijakan konten, perlindungan data pribadi, keamanan siber, dan respon terhadap berbagai perkembangan terbaru inovasi teknologi *(intech, e-commerce, big data, artificial intelligence)*.
- Perlindungan kebebasan sipil: ELSAM ingin memastikan penghormatan dan perlindungan terhadap kebebasan sipil di Indonesia melalui berbagai kegiatan studi dan advokasi kebijakan, khususnya yang terkait dengan kebebasan berekspresi, kebebasan berkumpul/berorganisasi, kebebasan beragama, termasuk respon terhadap makin maraknya praktik-praktik intoleransi.
- Penyelesaian pelanggaran HAM masa lalu: ELSAM secara intensif mempromosikan pengadopsian pendekatan keadilan transisional untuk menyelesaikan berbagai kasus pelanggaran HAM yang berat di masa lalu. Tujuannya untuk memastikan keadilan dan pemulihan bagi korbannya, serta mencegah keberulangan.

Kemudian sebagai bagian dari upaya promosi dan penguatan kapasitas pemangku kepentingan, ELSAM terus menyelenggarakan berbagai pendidikan hak asasi manusia, melalui unit khusus pelatihannya. Pendidikan ini seperti Kursus HAM untuk Pengacara; Penyelenggaraan pelatihan dengan topik-topik khusus, seperti penanganan kasus HAM yang berat, kursus hak asasi manusia bgai aparat penegak hukum; dan Pelatihan untuk mempromosikan penggunaan pendekatan berbasis hak, bagi pengambil kebijakan, dan sektor bisnis, termasuk di dalamnya pelatihan bisnis dan hak asasi manusia, serta pelatihan yang terkait dengan perlindungan data pribadi.

Alamat:
Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA
Telepon: (+62 21) 797 2662; Telefax: (+62 21) 7919 2519
Email: office@elsam.or.id; Website: www.elsam.or.id
Twitter: @elsamnews, @elsamlibrary; Facebook: @elsamjkt



Revolusi digital telah menciptakan sebuah inovasi baru dalam kapasitas untuk memperoleh, menyimpan, memanipulasi dan mentransmisikan volume data secara nyata (*real time*), luas dan kompleks. Oleh karenanya revolusi digital seringkali dianggap identik dengan revolusi data. Perkembangan tersebut telah mendorong pengumpulan berbagai data, tidak lagi tergantung pada pertimbangan data apa yang mungkin berguna di masa depan. Perlindungan data pribadi sendiri merupakan aspek dinamis yang akan terus berhadapan dan dan dipengaruhi oleh kemajuan dan inovasi teknologi serta praktik bisnis. Salah satu faktor munculnya kejahatan dan penggunaan data pribadi secara melawan hukum disebabkan oleh perkembangan teknologi, Informasi, dan komunikasi. Saat ini, teknologi, Informasi, dan komunikasi telah merambah hampir semua aspek kehidupan dan mengubah perilaku kehidupan masyarakat menuju interaksi masyarakat berbasis elektronik dan internet. Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global dan menyebabkan interaksi antar-manusia menjadi tanpa batas *(borderless)*. Oleh karena itu, hukum perlindungan data harus dikerangkakkan secara tepat untuk mencegah penyalahgunaan atau kesalahan penanganan data. Tegasnya, bila peningkatan massif dalam pengumpulan data ini tidak dilakukan dalam kerangka penghormatan hak, maka mau tidak mau proses dan tujuannya akan digunakan dengan cara yang mengesampingkan hak-hak—privasi masyarakat.

Alamat:
Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA Tel.: (+62 21) 797 2662, Fax.: (+62 21) 7919 2519
Email: office@elsam.or.id, Website: www.elsam.or.id

Twitter: @elsamnews, @elsamlibrary Facebook: @elsamjkt | Instagram: @elsamnews