IMPLEMENTASI DESAIN PRIVASI SEBAGAI PELINDUNGAN PRIVASI ATAS DATA BIOMETRIK

Patricia Edina Sembiring
Fakultas Hukum, Universitas Padjadjaran
email: patriciaedina16@gmail.com

Ahmad M. Ramli
Fakultas Hukum, Universitas Padjadjaran
email: ahmad.ramli@unpad.ac.id

Laina Rafianti
Fakultas Hukum, Universitas Padjadjaran
email: laina@unpad.ac.id

disampaikan 18/01/2024 – di-*review* 21/03/2024 – diterima 08/06/2024
DOI: 10.25123/vej.v10i1.7622

Abstract
Attention to biometric data security has become urgent for protecting user privacy. In the context of the Protection of Data Privacy (PDP) Law, biometric data are classified as specific data, requiring extra protection due to their unique, non-exchangeable characteristics. This study uses a normative approach, analyzing legislation and legal comparisons through regional and international regulations, to examine two issues: the position of biometric data as specific data under the Electronic Information and Transactions Law and PDP Law, and the technical solutions through privacy by design to protect biometric data. The research findings are: (1) Biometric data are correlated with privacy and personal rights, classifying them as specific data. Their use for public and private interests raises the potential for privacy violations. (2) Technical solutions through privacy by design can begin with implementing consent at the registration stage by personal data controllers, ensuring the processing of biometric data achieves specific purposes.

Keywords:
biometric data; privacy by design; privacy right; sensitive data

Abstrak
Perhatian terhadap keamanan data biometrik telah menjadi urgensi bagi pelindungan privasi pengguna. Dalam konteks Undang-Undang (UU) Perlindungan Data Pribadi, data biometrik diklasifikasikan sebagai data spesifik sehingga dibutuhkan pelindungan lebih selama pemrosesan disebabkan karakteristik khas seseorang yang tidak dapat dipertukarkan. Dengan pendekatan yuridis-normatif perundang-undangan dan perbandingan hukum aturan regional dan internasional, terdapat dua permasalahan yang akan dikaji, yakni kedudukan data biometrik sebagai data spesifik dari perspektif UU Informasi-Transaksi Elektronik dan UU Perlindungan Data Pribadi; serta solusi teknis melalui konsep desain privasi sebagai upaya pelindungan privasi atas data biometrik. Tiga hasil penelitian ini yaitu: (1) data biometrik berkorelasi dengan hak atas privasi dan hak pribadi sehingga diposisikan sebagai data spesifik, tetapi penggunaan bagi kepentingan publik dan privat meningkatkan resiko pelanggaran privasi, (2) solusi teknis melalui desain privasi dapat dimulai dari penerapan persetujuan pada tahap registrasi oleh pengendali data pribadi sebagai upaya mencapai tujuan spesifik atas pemrosesan data biometrik.

Kata Kunci:
data biometrik; data spesifik; desain privasi; hak atas privasi

Pendahuluan

Kepemilikan atas data pribadi kini telah menjadi satu kesatuan dari diri manusia. Kehadirannya sebagai penunjang bagi individu di dalam menjalankan aktivitasnya pada dunia teknologi. Akibatnya, manusia bukan lagi dikatakan sebagai *Homo Sapiens*, akan tetapi bergeser menjadi *Homo Digitalis*. Berbeda dari *homo sapiens* dengan berorientasi untuk meningkatkan kemampuan berburu dan meramu hingga berhasil memperoleh pasokan makanan,[1] *homo digitalis* memandang data seperti makanan baru, sehingga aspek kehidupannya tidak terlepas dari penggunaan data.[2] Hal ini dibuktikan dari segala aktivitas dunia maya yang telah dilakukan oleh penggunanya seperti sebanyak 20.780.928 postingan di Facebook, 262.332 unggahan di Instagram, 19.278 pembelian di Amazon, dan lain sebagainya.[3] Dapat dibayangkan seberapa banyak penggunaan data demi melaksanakan aktivitas berselancar di atas.

Data pribadi yang berkorelasi terhadap privasi, merupakan satu kesatuan dari hak asasi manusia sebagai hak yang krusial. Keberadaan dari privasi atas data pribadi menjadi elemen bagi kebebasan dan harga diri individu.[4] Bila penyebaran atas data informasi melalui teknologi begitu cepat dan mudah, pembatasan bagi seorang individu untuk memiliki kontrol atas informasinya menjadi terbatas. Hingga dimungkinkan terdapat potensi pelanggaran yang nantinya akan dilakukan oleh pihak lain. Pengaruh dari pelanggaran data pribadi akan menimbulkan kerugian terhadap reputasi dan harga diri, sehingga bukan semata-mata melukai aspek materil, tetapi memasuki ranah psikis korban.[5]

Pelindungan atas data pribadi sebelumnya juga diatur dalam berbagai instrumen hukum di Indonesia yakni Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan,

---

1 *Evelyn de Souza, The Era of Homo Digitus, in Women in Security, Women in Engineering and Science, Springer Cham, Europe, 2018, hlm. 48.*

2 Id.

3 *Social Media Today, The Internet in Real Time [Live Infographic],* diakses pada 14 Januari 2024, https://www.socialmediatoday.com/content/internet-real-time-live-infographic.

4 Sinta Dewi Rosadi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia, 5 *Yustisia* 1, 25., 2016.

5 *Samuel D. Warren dan Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 5, hlm. 198.*

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

Kemudian apabila memandang pelindungan data pribadi, maka terdapat tuntutan pula untuk melihat kembali kepada penggolongan data pribadi, yang terdiri dari data umum dan data khusus sehingga secara tidak langsung memberikan perbedaan dampak di dalam pemrosesannya. Atas pertimbangan inilah, timbul dorongan baik dari instrumen hukum internasional seperti *General Data Protection Regulation* (GDPR), *Organisation for Economic Co-operation* (OECD) dan instrumen hukum di Indonesia yang secara eksplisit memisahkan data umum dan data spesifik salah satunya data biometrik. Mengapa hal ini terjadi? Pemisahan di atas timbul sebagai bentuk atensi terhadap pelindungan data umum dan data khusus, terlebih pada karakteristik data biometrik, berupa representasi 'keunikan biologis individu' sehingga tidak dapat digantikan oleh siapapun.[6] Persoalannya adalah bagaimana nantinya data biometrik ini dapat dinilai sebagai data bersifat spesifik sesuai kualifikasi dalam Undang-Undang dan hukum internasional lainnya. Siapa nantinya yang akan melindungi dampak dari data biometrik (pemerintah atau organisasi). Selanjutnya, bagaimana wujud implementasi pelindungan apabila data biometrik dipergunakan?

Perlu diperhatikan bahwa data pribadi sangat berkorelasi terhadap privasi. Begitu juga data biometrik sebagai satu kesatuan dari data pribadi. Karena itu, sejatinya penggunaan data ini perlu melibatkan persetujuan eksplisit dan hanya diberlakukan untuk tujuan spesifik.[7] Nyatanya pelanggaran bersinggungan pada data biometrik pernah terjadi, seperti pada kasus perusahaan Clearview AI Incorporation. Pelanggaran tersebut dilakukan oleh Clearview AI Incorporation sebagai perusahaan pengolahan kumpulan gambar yang beredar di web media publik dengan kemudian mengolah perolehan data-data di web media menjadi data biometrik berbentuk *face print*. Akan tetapi, selama prosesnya Clearview tidak

6 *Lawrence J. Fennelly, Effective Physical Security Fourth Edition, Elsevier, United Kingdom, 2013,* hlm. 255.
7 *Innovatrics, "Biometricks and Personal Data," (White Paper, 2004), hlm. 2.*

memberitahukan proses-proses penggunaan dari data biometrik serta tidak memberikan persetujuan kepada pemilik data biometrik yang telah dipergunakan.[8]

Di Indonesia sendiri, data biometrik pernah diaplikasikan bagi kepentingan pelayanan publik oleh PT Kereta Api Indonesia (PT KAI), mempergunakan pengenalan wajah (*face recognition*), namun pada 16 Januari 2024, dikabarkan kelompok peretas berhasil mengakses data spesifik milik PT KAI menampilkan informasi bertuliskan "Anda dapat menemukan memo umum KAI.ID disini! Harga 11.69 Bitcoin."[9] Hal ini memberikan kekhawatiran, apakah data identifikasi wajah miliknya tetap terlindungi atau menjadi salah satu bagian dari jual beli data oleh kelompok peretas. Mengingat, para pemilik data tidak diberikan peluang untuk menerima atau menolak pengumpulan, padahal data biometrik wajib memperoleh persetujuan dari subjek data pribadi menggunakan metode yang memadai.

Menelisik berbagai peristiwa yang ada, penulisan ini akan menelaah esensi kehadiran data biometrik dalam perspektif hukum positif di Indonesia dan hukum internasional lainnya, kemudian memberikan langkah solutif berupa desain privasi (*privacy by designs*). Terlebih GDPR sebagai regulasi pelindungan data terketat di dunia,[10] mengatur secara eksplisit persyaratan pelindungan data privasi berbentuk desain dan tampilan (*by designs and default*). Melalui konsep ini, mengarahkan untuk mengedepankan kontrol teknis dan tata kelola untuk meminimalkan risiko pelanggaran privasi sebelum menciptakan desain pemrosesan baru.[11] Oleh sebab itu, penulisan ini merumuskan permasalahan yang akan ditelisik, yaitu (1) bagaimana kedudukan data biometrik sebagai data spesifik ditinjau dari perspektif UU ITE dan UU PDP? (2) bagaimana solusi teknis melalui konsep desain privasi sebagai upaya pelindungan privasi atas data biometrik?

Penelitian ini bertujuan untuk memberikan jawaban atas esensi kehadiran data spesifik berupa data biometrik melalui regulasi hukum di Indonesia, adapun elaborasi penjelasan terkait upaya solutif melalui desain privasi diharapkan mampu

---

8 Miyuki Fattah Rizki dan Abdul Salam, Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris, 2 *Lex Patrimonium* 1, 2-3, 2023.

9 Id.

10 *Riza Roidila Mufti, "A Policy Brief EU General Data Protection Regulation (GDPR)," (Research Series Embassy of the Republic of Indonsia in Brussels, 2021), hlm. 2.*

11 *Ann Cavoukin, Ph.D., Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices, Information and Privacy Commissioner, Canada, 2012, hlm.* 8.

menjadi upaya solutif demi pelindungan pemrosesan data biometrik. Mengingat biometrik merupakan teknologi termutakhir saat ini dan tentunya akan berkembang semakin maju kedepannya, maka pada dasarnya penulisan artikel mendorong kepada pentingnya langkah pelindungan baik melalui hukum dan teknis demi membangun upaya pencegahan terhadap penguatan data pribadi bersifat spesifik yang kian hari semakin tergerus akan pengamanannya. Untuk menjawab tujuan tersebut, penelitian ini menggunakan metode pendekatan yuridis normatif bersifat deskriptif analitis dengan cakupan pembahasan terdiri atas asas-asas hukum, sistematika hukum, dan perbandingan hukum terkhusus merujuk kepada *General Data Protection Regulation* (GDPR), OECD, dan lainnya.[12] Kemudian, keseluruhan sumber berasal dari studi kepustakaan dari data primer, sekunder, dan tersier.[13]

Pembahasan

Kedudukan Biometrik Sebagai Data Spesifik Dalam Perspektif UU ITE dan UU PDP

Berdasarkan terminologi, kata biometrik berasal dari kata Yunani yakni *bios* dengan arti kehidupan dan *metron* yakni ukuran.[14] Oleh sebabnya, kehadiran dari biometrik dapat diilhami bagaikan 'kemasan kecil dari manusia' dikarenakan telah merepresentasikan identitas biologis dari seorang manusia, dalam artian biometrik berusaha memposisikan layaknya sebuah alat pemrofilan dari individual dengan menggunakan tiga aspek penelaahan (1) apa yang ia ketahui sebagai seorang individu yang hidup (2) apa yang dimilikinya dari luar (unsur ekstrinsik), dan (3) siapa dia dari dalam (unsur intrinsik).[15] Kemudian, melalui pandangan yuridis yakni UU ITE, data biometrik masuk kepada kategori Informasi Elektronik. Namun, UU ITE hanya memberikan pelindungan terhadap data biometrik jikalau pemrosesannya dilakukan melalui sistem elektronik berwujud informasi/dokumen elektronik.

Sebaliknya, pada UU PDP memberikan ruang secara khusus terhadap data biometrik dimana secara eksplisit mendefinisikan "data yang berkaitan dengan fisik,

12 H. Zainduddin Ali, Metode Penelitian Hukum, Sinar Grafika, Jakarta, 2015, hlm. 24.
13 Id., hlm. 22.
14 *Mark Maguire, The Birth of Biometric Security, 25 Anthropology 9, 9, 2009.*
15 *Anil K. Jain, et.al., Introduction to Biometrics, Springer Science Business Media, London, 2011, hlm. 2.*

fisiologis, atau karakteristik perilaku individu," dan memisahkan data sebagai kategori data spesifik. Oleh sebab itu, pada pokoknya, UU ITE dan UU PDP memberikan pelindungan terhadap data biometrik, perbedaannya adalah dengan cara seperti apa nantinya data tersebut akan diproses dan dimanfaatkan. Kondisi perbedaan ini berangkat dari hakikat kehadiran UU ITE, bahwa pembentukannya sebagai respon dari penegakan hukum siber terhadap berbagai kejahatan terkomputerisasi di dalam dunia internet.[16] Fokus utama pengaturan UU ITE merujuk pada kejahatan komputer dan siber dengan terdiri atas penipuan, penggelapan, peretasan, pidana komunikasi, perbuatan pidana perusakan sistem komputer, dan perbuatan pidana yang berkaitan dengan hak milik intelektual.[17]

Lain halnya pada segi pengaturan UU PDP, konstruksi aturan lebih menekankan kepada upaya pelindungan data pribadi milik entitas orang perorangan (*natural person*), sehingga cakupannya merujuk pada hak untuk menghormati kehidupan pribadi dari mahluk hidup (*the right to private life*).[18] Dengan kata lain, pemahaman pelindungan atas data biometrik jika dikaji melalui ke dua regulasi mempunyai maksud berbeda-beda, implikasinya adalah (1) bila pemanfaatan data biometrik digunakan untuk perbuatan pelanggaran ataupun kejahatan melalui sistem elektronik, maka penegakan menggunakan regulasi UU ITE, namun bila selama penggunaan dan/atau pemrosesan data biometrik telah terjadi pelanggaran terhadap data pribadi yang dapat diidentifikasi atau teridentifikasi, maka UU PDP akan berlaku.

Kemudian, berdasarkan klasifikasi data bersifat umum dan spesifik melalui UU PDP, data biometrik telah diatur secara eksplisit pada Pasal 4 ayat (1) dan ayat (2) dengan menegaskan bahwasannya data biometrik merupakan data pribadi yang bersifat spesifik. Dengan demikian, mengacu kepada definisi data spesifik telah secara jelas diterangkan dalam bagian penjelasan Pasal 4 ayat (1) UU PDP yakni data pribadi yang bersifat spesifik merupakan data pribadi yang apabila dalam pemrosesannya dapat mengakibatkan dampak lebih besar kepada subjek data pribadi. Dengan demikian, pemrosesan data dari informasi-informasi yang telah

---

16 Ibrahim Fikma Edrisy, *Pengantar Hukum Siber*, Sei Wawai Publishing, Lampung, 2019, hlm. 42.

17 Niniek Suparni*, Cyberspace, Problematika dan Antisipasi Pengaturannya, Penerbit Sinar Grafika*, Jakarta, 2009, hlm. 5-6.

18 Sinta Dewi Rosadi et.al., Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia, 4 *Veritas et Justitia* 1, 94, 2018.

diklasifikasikan sebelumnya tidak dapat dipergunakan secara universal dan hanya dipergunakan dalam kondisi tertentu, yakni bagi kebutuhan publik, kesehatan, keuangan, atau adanya persetujuan eksplisit dari pemilik data.[19]

Adanya pembatasan atas kondisi demikian pada hakikatnya dilandaskan atas alasan kuat dari hak fundamental atas privasi dan kebebasan naluriah manusia seperti dinyatakan pada *Recital* 51 EU GDPR:

> "*Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedom merit specific protection as the context of their processing could create significant risks to* ***the fundamental rights and freedoms***."

Melihat dari definisi EU, pemaknaan tersirat atas data spesifik bersinggungan erat pada kebebasan seorang subjek data pribadi untuk menikmati kehidupan dari segala macam gangguan, menghindari perilaku diskriminasi, dan menghargai hak atas privasinya. Pernyataan sebelumnya juga kembali diperjelas oleh *Council of Europe* di dalam penjelasan Konvensi 108, bahwa pemrosesan data spesifik harus meninjau kepada potensi risiko atas perbuatan diskriminasi atau mencederai martabat maupun fisik individu.[20] Terlebih, hak fundamental dan kebebasan berkaitan erat dengan hak atas privasi sebagai bagian dari hak asasi manusia.

Adapun, hak atas privasi diperkenalkan oleh Samuel D. Warren dan Louis D Brandeis. Menurut Warren dan Louis, hak atas privasi digambarkan sebagai hak untuk menikmati hidupnya dan dibiarkan sendiri sehingga dalam perkembangannya dibutuhkan pengakuan dari hukum dikarenakan hak demikian tidak dapat terlepas dari dirinya sebagai seorang manusia yang hidup.[21] Privasi juga dikatakan sebagai hak individu, grup, atau lembaga untuk memilih apakah informasi berkaitan dengan dirinya akan disampaikan atau tidak kepada pihak lain (*information privacy*).[22] Penguatan atas hak privasi kemudian dipertegas kembali

---

19 Janitra Haryanto, *Klasifikasi Data Untuk Pelindungan Data Pribadi*, Center for Digital Society, Yogyakarta, 2018, hlm. 14.

20 *Council of Europe, Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals With Refard to Automatic Processing of Personal Data, (Council of Europe Treaty Series No. 223, 2018), 10.*

21 Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, 2 *Jurnal Al-Wasath* 9, 21, 2021.

22 Sinta Dewi Rosadi, Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi, 9 *Arena Hukum* 403, 408, 2017.

oleh salah satu pernyataan dari *European Court of Human Rights* (ECtHR) dalam menangani kasus *S and Marper v United Kingdom*.[23]

Melalui kasus ini, pengadilan menyatakan bahwa meskipun pengumpulan serta penyimpanan sampel sidik jari, sampel seluler, dan DNA menjadi kepentingan bagi otoritas publik, akan tetapi tindakan tersebut masihlah menjadi bagian dari data pribadi terdakwa. Oleh sebabnya, berlandaskan atas *Article* 8 (1) ECtHR perbuatan demikian dinilai tidak proporsional serta telah melanggar hak privasi individu.[24] Walaupun penegakan privasi belum menjadi aspek perhatian dalam Negara Indonesia dibandingkan Negara Uni Eropa (khususnya penganut sistem *common law*), akan tetapi melalui konstitusi tertulis yakni Pasal 28G ayat (1) UUD 1945 menyiratkan kehadiran pelindungan hak atas privasi bagi warga negara Indonesia. Lebih lanjut, dalam pemanfaatan dunia teknologi, pelindungan privasi dari data pribadi telah hadir secara tersirat melalui penjelasan Pasal 26 UU ITE melalui frasa "Hak Pribadi."

Pengaruh dari eksistensi privasi terhadap hak pribadi menjadi kunci penting dalam melihat kedudukan data biometrik sebagai data spesifik. Hakikatnya, hak pribadi dipahami sebagai hak seorang manusia agar memiliki kebebasan atas kontrol dirinya sendiri. Namun, makna hak pribadi dapat diperluas menjadi kontrol kepemilikan atas hidupnya. Atau dengan kata lain, bahwa individu dapat memilih apakah bagian biologis (termasuk fisik, fisiologi, atau perilaku) dapat ia berikan kepada orang lain sebagai satu kesatuan utuh selama ia terlahir dan hidup.

John Locke berpandangan bahwa manusia memiliki hak untuk hidup, karena itu, hak tersebut merupakan bentuk pelindungan seseorang atas kepemilikan tubuhnya sendiri.[25] Oleh sebab itu, hak pribadi adalah hak asasi manusia yang diberikan oleh pencipta sebagai hak mendasar bagi kehidupan manusia dan menjadi aspek fundamental yang tidak dapat terlepas dari dalam diri manusia.[26] Atas pernyataan demikian, dapat diketahui bahwa maksud kehadiran data biometrik

---

23 *Lauren Dancer, et.al. Biometric Identification and Privacy, Comparative Research Prepared for the Center for Law and Policy Research, India, 2013, hlm*. 4.

24 Id.

25 Rai Mantili dan Remigus Jumalan, Eksistensi Teori Hak Milik Pribadi Dalam Kepemilikan Perseroan Terbatas (Dari Perspektif Sistem Kapitalisme dan Sistem Ekonomi Pancasila, 5 *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 2, 255, 2022.

26 Upik Mutiara dan Romi Maulana, Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Data Pribadi, 1 *Indonesian Journal of Law and Policy Studies* 1,47, 2020.

masuk sebagai data spesifik, sebagai wujud pelindungan atas fisik dan psikis dari pemilik data yang telah menjadi satu kesatuan utuh di dalam hidupnya.

Selanjutnya, dalam menghadirkan pengklasifikasian data bersifat umum dan khusus, penyusun regulasi perlu mempertimbangkan keadaan sistem hukum di Indonesia, kerangka sistem hukum merupakan fondasi dasar dalam mengidentifikasi berbagai aktor yang mempengaruhi pembentukan hukum.[27] Bila ditelisik melalui pandangan Lawrence M. Friedman mengenai pendapatnya terhadap sistem hukum (*legal system*), membagi sistem hukum atas beberapa elemen, yaitu:[28]

(1) Struktur hukum (*legal structure*): pranata hukum yang menjadi daya penopang berdirinya sistem hukum (tatanan hukum, lembaga, aparat penegak hukum, beserta proses kinerja dalam menegakkan hukum);
(2) Substansi hukum (*legal substance*): keseluruhan isi aturan hukum baik tertulis maupun tidak tertulis dimana terkandung asas, norma, dan putusan pengadilan sebagai dasar pegangan oleh masyarakat dan pemerintah;
(3) Budaya hukum (*legal culture*): mengandung ide-ide, nilai-nilai, pemikiran, diikuti pula perilaku anggota masyarakat dalam implementasi hukum. Hal ini tidak terlepas dari adanya kesadaran dan penerimaan dari masyarakat terhadap ketentuan hukum yang nantinya diberlakukan kepada mereka.

Oleh sebabnya, ketika berbicara terhadap pemaknaan dari data spesifik seperti biometrik perlu adanya keterikatan kuat antara struktur hukum, yakni pengendali data pribadi beserta prosesor data pribadi (individu, pemerintah, dan pihak swasta), substansi hukum yakni UU PDP, UU ITE, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PPSTE), maupun berbentuk keputusan dari beberapa lembaga negara nantinya, kemudian instrumen hukum lunak (*soft law*) seperti GDPR, OECD, dan lainnya dapat dijadikan acuan mengingat GDPR telah mengatur data spesifik secara komprehensif, sedangkan budaya hukum menitikberatkan terhadap pola perilaku berupa aktivitas masyarakat di dunia internet, sebagaimana data dari *We Are Social*

---

27 *Mustafa, et.al. Legal System in the Perspectives of H.L.A Hart and Lawrence M. Friedman, 2 Peradaban Journal Law and Society 1, 57, 2023.*

28 Farida Sekti Pahlevi, Pemberantasan Korupsi di Indonesia: Perspektif Legal System Lawrence M. Freidman, 1 *Jurnal El-Dusturie* 23, 31-33, 2022.

merepresentasikan kehidupan dunia maya penduduk Indonesia, menghabiskan waktu rata-rata sekitar 7 jam 42 menit mengakses internet setiap harinya dan 3 jam 18 menit menghabiskan waktu di sosial media.[29]

Bila melihat panjelasan dari sistem hukum di atas, sebenarnya terdapat beberapa hal yang perlu dikaji terutama dalam menelusuri sudut pemahaman terhadap segi substansi dan budaya hukum atas data spesifik. Pertama, substansi hukum atas data spesifik pada setiap negara adalah berbeda, hingga saat ini tidak dapat ditemukan pada tiap-tiap negara yang memiliki kualifikasi atas data spesifik yang serupa ataupun seragam. Sebagai contoh di Negara Amerika Serikat mengkategorikan data spesifik terdiri atas: (a) ras dan etnis, (b) kepercayaan terhadap agama, (c) kondisi kesehatan mental dan diagnosis kesehatan, (d) orientasi seksual, (e) genetik dan data biometrik.[30] Berbeda jika di Negara California pada *California Consumer Privacy Act* mengenal data privasi dengan terdiri atas: (a) kartu identitas, lisensi pengemudi, kartu jaminan pelindungan sosial, akun finansial, kartu debit dan kredit, kepercayaan atas filosofi, keanggotaan serikat pekerja, dan konten email.[31]

Lain halnya di Indonesia dalam Pasal 4 ayat (1) dan ayat (2) UU PDP data spesifik dikualifikasikan atas: (a) data dan informasi kesehatan; (b) data biometrik, (c) data genetika, (d) catatan kejahatan, (e) data anak, (f) data keuangan pribadi; dan/atau (g) data lainnya sesuai dengan ketentuan peraturan perundangan-undangan. Mengacu pada berbagai perbedaan atas klasifikasi sebelumnya, perbedaan-perbedaan demikian, dipengaruhi oleh sistem hukum yang dimiliki negara tersebut, misalnya,negara California menempatkan lisensi pengemudi sebagai data spesifik dengan dua pertimbangan (1) kehadiran *Driver's Privacy Protection Act* (DPAA) merupakan regulasi pokok dalam mengatur pelindungan informasi personal pengemudi, (2) penyusunan hukum DPAA terbentuk setelah beberapa hukum negara bagian menyusun regulasi yang sama, beberapa terinspirasi melalui kasus pembunuhan Rebecca Shaeffer, dibunuh oleh penggemarnya setelah menemukan lokasi kediaman menggunakan catatan

---

29 We Are Social, Digital 2023 Indonesia, diakses pada 16 Januari 2024, https://wearesocial.com/id/blog/2023/01/digital-2023/.

30 *Daniel J. Solove, Data is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data, 118 Northwestern University Law Review 2, 12, 2023.*

31 Id., hlm. 13.

pembelian dari Departemen Kendaraan Bermotor California.[32] Oleh karena perbedaan substansi dan budaya hukum, maka secara tidak langsung akan mempengaruhi budaya hukum terhadap bagaimana masyarakat akan mematuhi pelindungan data biometrik sebagai data spesifik kedepannya.

Sehubungan dengan itu, penulis meyakini terdapat ketimpangan di antara keduanya. Jika melihat dari substansi hukum UU PDP yang disebut sebagai data spesifik apabila menimbulkan akibat lebih besar kepada subjek data pribadi, antara lain tindakan diskriminasi dan kerugian yang lebih besar terhadap subjek data pribadi, sedangkan berdasarkan perspektif budaya hukum mengacu pada pendapat Hilman Hadikusuma adalah sebuah tanggapan umum yang seragam dari sebuah masyarakat tertentu terhadap gejala/fenomena hukum,[33] menggambarkan orientasi yang sama terhadap kehidupan hukum yang dihayati masyarakat bersangkutan.[34]

Sayangnya, penanaman atas budaya hukum masyarakat dihubungkan pada penerimaan teknologi di tengah era digitalisasi tidak dapat disebut sebagai yang paling terdepan. Mengapa hal ini bisa terjadi? Jika melihat kepada data, pengguna internet di Indonesia telah mencapai 353.8 juta (77%) dari populasi Warga Negara Indonesia.[35] Implikasinya adalah Negara Indonesia menduduki peringkat 4 sebagai negara pengguna internet terbesar di dunia[36] pencapaian ini bisa dikatakan luar biasa dari sisi negara berkembang dikarenakan semestinya Negara Indonesia bisa memperoleh predikat literasi digital terbaik setidaknya di ASEAN yang kemudian memberikan andil pada perkembangan masyarakat ke arah modernisasi, akan tetapi realitas berkata lain, menurut INDEFAviliani menyebutkan tingkat literasi digital di Indonesia sebesar 62% berbeda dari rata-rata Negara ASEAN yang mencapai 70%.[37] Rendahnya literasi digital terlihat dari maraknya berbagai macam modus penipuan seperti penipuan lotre, pencurian identitas, serta pinjaman *online*.

---

32 *Paul Ohm, Sensitive Information, 88 Southern California Law Review, 1130, 2015.*

33 Mohd Yusuf D.M., et.al., Peranan Budaya dan Kebudayaan di Indonesia Dari Aspek Sosiologi Hukum, 6 *Jurnal the Jurist* 1, 2022, 276.

34 Id.

35 We Are Social, *supra no*. 25.

36 Agnes Z. Yonatan, Indonesia Peringkat 4, Ini Dia 7 Negara Pengguna Internet Terbesar di Dunia, diakses pada 4 Januari 2024, https://data.goodstats.id/statistic/agneszefanyayonatan/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-FLw6V.

37 Khorul Anam, Paling Rendah di ASEAN, Tingkat Literasi Digital RI Cuma 62%, diakses pada 4 Januari 2024, https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62.

Melalui studi CFDS, terhadap 1700 responden di 34 provinsi sebanyak, 66,6% pernah menjadi korban penipuan *online*,[38]. Tindakan lain, sebagaimana dipaparkan oleh Kominfo, terhitung jumlah *hoax* sebanyak 9.546 telah ditemukan melalui berbagai media sosial di internet.[39] Sehingga, sekalipun pada akhirnya Negara Indonesia menggaung-gaungkan adanya data bersifat umum dan data bersifat khusus melalui regulasi hukum, niscaya warga negaranya pun tidak memiliki kapasitas bahkan sederhananya tidak menyadari adanya eksistensi pelindungan dari ke-2 data itu

Timbul pula permasalahan baru apabila bersinggungan terhadap pola penegakan hukum Negara Indonesia saat ini yang masih cenderung reaktif dari berbagai segi baik kebijakan, penindakan, penegakan, dan lainnya (*reactive in one way*) terutama berhubungan pada pelindungan atas data pribadi warga negaranya. Berbagai macam kasus kebocoran data sebagai contoh kasus terbaru dengan pembobolan 337 juta data yang dikelola Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri.[40]

Analisa kedua, berangkat atas posisi data biometrik sebagai data pribadi harus bersinergi pada esensi keberlakuannya, apakah data biometrik hanya terbatas pada identitas saja atau dipergunakan sebagai alat identifikasi. Menjawab atas kedua elemen ini seyogyanya perlu dikembalikan pada asal muasal dari data biometrik sebagai sebuah data pribadi. Sebabnya, diperlukan pembedahan satu persatu atas setiap definisi agar memperoleh titik temu di antara satu sama lain, sebagai berikut: (1) data pribadi dapat dipahami sebagai sekumpulan informasi yang memuat identitas ril atas individu.

Oleh sebab itu, data pribadi dapat diumpamakan sebagai 'tanda pengenal' oleh seseorang jika berada pada ruang lingkup digital seperti internet. Bila menelusuri dari ketentuan OECD mendefinisikan data pribadi sebagai "...segala informasi berkaitan dengan individu (subjek data) yang diidentifikasi atau dapat diidentifikasi."[41]

---

38 Irnas Shafira dan Dhalia Ndaru Herlusiatri Rahayu, *Literasi Digital*, CFDS, Yogyakarta, 2021, hlm. 2.

39 Tempo.co, Hingga Awal 2022, Kominfo Temukan 9.546 Hoaks di Internet, diakses pada 30 Maret 2024, https://bisnis.tempo.co/read/1558213/hingga-awal-2022-kominfo-temukan-9-546-hoaks-di-internet.

40 BBC News Indonesia, "Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber:'Ini Peretasan Paling Parah," diakses pada 4 Januari 2024, https://www.bbc.com/indonesia/articles/c51v25916zlo.

41 Wahyudi Djafar dan M. Jodi Santoso, *Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya*, ELSAM, Jakarta, 2019, hlm. 16.

Selanjutnya, *EU General Data Protection* pada *Article* 4 (4) memberikan definisi data pribadi hampir serupa dengan OECD, namun menambahkan definisi atas identifikasi dari seseorang (*an identifiable person*) adalah yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasian seperti nama, nomor identifikasi, data lokasi, pengenal *online*/satu atau lebih faktor spesifik untuk fisik, fisiologis, identitas genetik, mental ekonomi, budaya atau identitas sosial dari orang tersebut."[42] Menelisik pada regulasi di Indonesia melalui Pasal 1 butir 1 "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik."

Kesimpulannya jika segala sesuatu memiliki muatan atas penggambaran informasi dari pemilik data memuat suatu materi yang dapat menentukan atau menetapkan identitas dari seorang pemilik data, hal demikian disebut sebagai data pribadi. Tetapi, perlu diperhatikan secara bersama-sama terhadap berbagai pendefinisian data pribadi seperti yang diterangkan sebelumnya apabila data pribadi telah memasuki kepada aktivitas pemrosesan, maka perolehan maka akan menimbulkan akibat yang lebih besar. Artinya, jika nantinya data bersifat spesifik diproses dalam rangka identifikasi akibatnya perolehan data pribadi bukanlah sekadar sebagai identitas bersifat umum (*general*) tetapi berkoneksi antara pokok kehidupan orang, benda, segala bagian dari dirinya yang pada prosesnya akan menciptakan sebab akibat atas kehidupannya. Contoh sederhana adalah ketika pasien menggunakan aplikasi *E-health* biasanya penginputan data pribadi tidak hanya terdiri atas nama lengkap, tanggal lahir, dan lainnya seperti dielaborasi pada data bersifat umum, namun lebih dari itu seperti kondisi medis pasien (tingkat alergi, gaya hidup, data kunjungan rumah sakit, riwayat penyakit, mental, dan lainnya).[43]

Jika kembali kepada masa pandemi, ketika peristiwa kebocoran 3.2 miliar data dari aplikasi Peduli Lindungi dengan terdiri atas data pengguna, data vaksinasi,

---

42 Id.

43 Sinta Dewi Rosadi, *supra note* 21, hlm. 213.

riwayat pelacakan, serta c*heck-in* pengguna.[44] Dimana pada akhirnya data-data yang ada dipergunakan oleh Bjorka untuk diperjual belikan. Kemudian, bagaimana imbas atas peristiwa tersebut kepada pemilik data yang diduga bocor? Tentu pada akhirnya tidak hanya data umum miliknya saja diketahui, senyatanya pun status dari kesehatan dirinya terkhusus keadaan dirinya baik terjangkit Covid-19 ataupun tidak, turut ikut menjadi sentral dari jual beli data pribadi oleh pelaku. Maka demikian, idealnya data-data ini menjadi sesuatu yang seyogyanya tidak perlu diketahui atau diproses lebih lanjut terutama bagi kebutuhan publik/umum karena merupakan identitas pribadi bersifat privasi dari dirinya (*one self privacy identity*).

Berbeda halnya apabila kategori data bersifat umum pada Pasal 4 ayat (3) UU PDP. Representasi dari data umum yakni bahwa keberadaannya memang melekat sebagai identitas, sehingga sekalipun data bersifat umum digabungkan untuk diperuntukkan sebagai daya pembeda (*to distinguish an individual*) tidak memberikan dampak signifikan terhadap individu.

Berangkat dari berbagai pisau analisa tersebut, telah sampailah pada satu titik pertemuan, seperti yang dinyatakan oleh Jon Bing atas kritiknya terhadap pengklasifikasian informasi data pribadi:[45]

> "*Certain key data (especially the personal number) are not sensitive per sem but derive, sensitivity from the information to which one gains access through the key. This means, in order to determine the sensitive of key data, it is not sufficient to consider the grading this data element has been give isolated; one must also take into account* ***what information one thereby may connect to the nexus-person.*** *This may provide a basis for data security deliberation-the submission of* ***the key represents in itself a threat to the protection of highly sensitive information, an increased risk of undesired access to personal information.***"

Untuk itu, permasalahan bukanlah kepada pengklasifikasian terhadap jenis data pribadi bersifat umum ataupun spesifik, kembali lagi, pengklasifikasian ini perlu memahami terhadap dampak dari pemroses data pribadi, esensi terhadap konektivitas antara data pribadi dengan citra dirinya sendiri, dan kemungkinan ancaman apabila data miliknya diproses lebih lanjut. Faktor-faktor demikian haruslah menjadi kunci penting bagi pemerintah, pengendali, dan prosesor data

---

44 Andri Saubani, CISSReC: 3,2 Miliar Data PeduliLindungi Bocor, diakses pada 3 Januari 2023, https://news.republika.co.id/berita/rle9di409/cissrec-32-miliar-data-pedulilindungi-bocor.

45 *Yue Liu, supra note 16, hlm.* 47.

pribadi, begitu pula terhadap implementasi pengaturan di dalam UU ITE dan UU PDP sebagai regulasi utama pelindungan data spesifik di Indonesia, dibutuhkan ketentuan bersifat *human centric* salah satunya ketentuan berisikan pengarahan penyematan desain privasi kepada pengendali selama pemrosesan data pribadi berlangsung.

Pelindungan Data Biometrik Sebagai Data Spesifik dan Kehadiran Desain Privasi Sebagai Optimalisasi Pelindungan Data Biometrik

1) Pelindungan Data Biometrik Sebagai Data Spesifik

Setelah mengulas mengenai fondasi dasar kedudukan biometrik sebagai objek dari data spesifik. Pembahasan selanjutnya akan memberikan pandangan terhadap pelindungan semestinya bagi data biometrik.

Pada dasarnya, data bersifat spesifik layaknya data biometrik perlu memperhatikan atas prinsip-prinsip pelindungan data pribadi. Akan tetapi poin penting dari berbagai prinsip lebih tepat ditekankan pada spesifikasi tujuan dari penggunaan data. Sebab tujuan atas penggunaan seyogyanya perlu memperhatikan kepada batasan pengumpulan yang mana hanya diperuntukkan bagi kepentingan rasional sebagaimana disebut sebagai batasan tujuan (*purpose limitation*).[46] Lebih lengkapnya, OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* merincikan batasan tujuan sebagai prinsip tujuan spesifik (*purpose specification principle*) yakni tujuan pengumpulan data pribadi wajib ditetapkan secara terperinci selambat-lambatnya ketika pengumpulan dan penggunaan data pribadi dilaksanakan sesuai dengan tujuan tersebut dan sebagaimana dinyatakan pada setiap perubahan tujuan.[47]

Pada ketentuan GDPR pun, pengontrol data, atau pengendali data pribadi dan maksud dari pemrosesan data pribadi, harus mampu mendemonstrasikan pemrosesan data dilaksanakan secara sah, adil, dan transparan berkorelasi kepada subjek data pribadi.[48] Maka, pelaksanaan penentuan prinsip pembatasan tujuan

---

46 *ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Personal Data Protection, Bandar Seri Begawan, Brunei Darussalam, 25 November 2016, hlm.* 3.

47 Wahyudi Djafar dan M. Jodi Santoso, *supra* no. 34, hlm. 31.

48 *Zhasmina Radkova Kostadinova, Purpose Limitation Under the GDPR: Can Article 6(4) Be Automated, Master Thesis in Tilburg University, Belanda, 2014, hlm.* 5.

wajib ditampilkan secara jelas, tegas, dan terperinci dimulai sebelum subjek data pribadi memberikan persetujuan (*consent*).

Hal ini telah diamanatkan pada Pasal 26 ayat (1) UU ITE kepada setiap penggunaan informasi melalui media elektronik menyangkut data pribadi harus berdasarkan persetujuan orang bersangkutan. Lalu melalui Pasal 14 ayat (3) butir b dan f Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) kepada "Pemrosesan Data Pribadi harus memenuhi ketentuan adanya persetujuan yang sah dari pemilik Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan kepada pemilik Data Pribadi." Dimana selanjutnya melalui Pasal 22 ayat (1) mengatur terhadap informasi persetujuan pemrosesan dilakukan melalui persetujuan tertulis atau terekam.

Dapat dilihat bahwa ketika penentuan pembatasan tujuan ini diberlakukan, pemberitahuan (*notice*) berkaitan tujuan pemrosesan data pribadi haruslah ditetapkan sejak awal data diberikan kemudian diikuti adanya persetujuan pemrosesan oleh subjek data pribadi. Namun demikian, adakalanya aturan-aturan persyaratan tersebut diabaikan, sebagai contoh, inovasi pengenalan wajah oleh PT KAI sebagai alat verifikasi penumpang.

Tindakan pengumpulan dinilai berisiko dikarenakan proses verifikasi data tidak diikuti persyaratan persetujuan yang memadai kepada penumpang,[49] padahal tindakan pengumpulan tersebut mempergunakan data biometrik yang merupakan data spesifik. Tentu, prosedur pengumpulan tanpa persetujuan sangat mengancam terhadap privasi individu, bilamana data biometrik diretas oleh pihak yang tidak bertanggung jawab, akan berpotensi membahayakan keselamatan pemiliknya.

Menurut sudut pandang penulis, prinsip pembatasan tujuan pun sangatlah penting, terkadang ketika perkembangan teknologi begitu masif, para pencipta atau pengembang tidak menyadari bahwa nantinya teknologi ciptaannya akan dipergunakan tidak hanya untuk satu tujuan saja, namun untuk berbagai tujuan lain. Maka demikian, jika tiada batasan dari pada tujuan pemrosesan pada data biometrik, mendorong persoalan yang nantinya akan menciptakan destruksi baru

[49] Yosepha Debrina Ratih Pusparisa, Inovasi Pengenalan Wajah, KAI Didorong Perbaiki Kebijakan Privasi Data, diakses pada 28 Maret 2024, https://www.kompas.id/baca/ekonomi/2023/11/20/inovasi-pengenalan-wajah-kai-didorong-perbaiki-kebijakan-privasi-data.

seperti rambatan fungsi (*function creep*). Rambatan fungsi dapat diartikan tahapan perluasan penggunaan suatu teknologi atau sistem di luar tujuan awalnya, terutama ketika hal ini mengarah pada potensi pelanggaran privasi.[50] Menurut Jentzsch mendeskripsikan rambatan fungsi sebagai tendensi mempergunakan informasi lebih dari tujuan awal pengumpulannya, termasuk di dalamnya terdapat ketidaksinambungan tujuan awal dari pengumpulan data."[51]

Kehadiran rambatan fungsi terhadap biometrik pernah terjadi melalui kasus *Rivera v. Google inc.* Lindabeth Rivera bersama Joseph Weiss menuduh Google telah mengumpulkan secara tidak sah, menyimpan, dan memanfaatkan pemindaian geometri wajah melalui aplikasi *Google Photo* berbasis layanan komputasi awan (*cloud*). Weiss menemukan akun *Google Photo* milikinya telah terasosiasi dengan tampilan wajahnya melalui fitur *face group*, selain itu terhubung ke akun Google miliknya tanpa notifikasi pemberitahuan.[52]

Di Indonesia, fitur sebelumnya menjadi ladang bisnis terbesar bagi Google. Direktur Layanan *Google Cloud South East Asia* menyatakan Indonesia adalah pasar terbesar *Google Cloud* di Asia Tenggara.[53] Dapat disimpulkan bahwa kehadiran fitur tersebut telah dipergunakan kepada pengguna di Indonesia. Tegasnya, ketika pada akhirnya biometrik dipergunakan, pembagian pembatasan tujuan perlu dilihat dalam dua segi sektor, yaitu pada sektor publik, batas tujuan penggunaan disesuaikan berdasarkan kepentingan sah dan melalui pengawasan otoritas, dan di sektor privat, masyarakat secara sukarela diberikan pilihan untuk memilih menggunakan biometrik atau tidak sama sekali.[54] Hal ini setidaknya akan memberikan batasan tujuan pada setiap ruang lingkup kehadiran data biometrik,

2) Implementasi Konsep Desain Privasi Sebagai Langkah Teknis Pelindungan Data Biometrik

Lawrence L. Lessig mengilustrasikan dunia siber sebagai ruang yang dapat mengatur dirinya sendiri terbebas dari intervensi pemerintah dan keterhubungan

---

50 *Bert-Jaap Koops, The Concept of Function Creep, 13 Law, Innovation, and Technology 29, 35, 2021.*

51 Id., hlm. 48.

52 *Rivera v. Google Inc No. 16 C 02714.*

53 Novina Putri Bestari, Google Beberkan Pendapatan Bisnis Cloud dari Indonesia, diakses pada 28 Maret 2024, https://www.cnbcindonesia.com/tech/20231011133337-37-479699/google-beberkan-pendapatan-bisnis-cloud-dari-indonesia.

54 *John D. Woodward Jr, Handbook of Biometrics, Springer, Boston, 2008, hlm*. 399.

politik. Dari kehadiran dunia siber, pengguna memiliki kebebasan menciptakan dunianya sendiri layaknya seorang arsitek.[55] Oleh sebabnya melalui kode memberikan pengaruh kepada dunia siber tergantung bagaimana sifat kode akan mempengaruhi perilaku dari penghuni dunia siber.[56]

Pernyataan di atas, berangkat dari teorinya bernama *Pathetic Dot*, dimana mengelaborasikan beberapa faktor yang mempengaruhi perilaku seseorang di dalam dunia siber, yaitu kehadiran bukum (*laws*), norma (*norms*), pasar (*market*), dan arsitektur (*architecture*).[57] Dengan demikian, sebagai jalan keluar dalam mengontrol ke-4 faktor, menghadirkan kode pada dunia siber mampu memberikan kontrol terhadap lalu lintas dunia siber.

Namun problematika muncul jika bertolak pada isu pemanfaatan data biometrik, dimana ke-4 faktor di atas terkadang saling bertolak belakang (1) pasar melihat data pribadi sebagai "tanah baru" atau "*as a new soil*,[58]" dalam hal ini perusahaan mencari berbagai peluang agar dapat merawat dan mendaur ulang data bagi kepentingan bisnis, (2) hukum kerap kali tidak bekerja secara efektif dalam mengikuti perkembangan teknologi. Hukum yang bersifat rigid berjalan lebih lambat dibandingkan perkembangan teknologi, (3) norma berpusat pada keyakinan bahwasannya data biometrik haruslah dilindungi dan dijaga, pengguna perlu memiliki kontrol terhadap data miliknya, dan (4) bentuk dan rupa arsitektur dari data biometrik merepresentasikan sisi biologis dari manusia yang berkarakteristik tidak dapat diubah ataupun digantikan.[59]

Untuk itu, demi menciptakan sinergisitas di antara faktor-faktor sebelumnya, memasukkan konsep desain privasi ke dalam sistem pelindungan data biometrik dapat menjadi langkah solutif. Mengapa desain privasi dianggap mampu melindungi data biometrik? Penyelenggara data tidak akan terlepas dari pengumpulan data pribadi, pengumpulan data yang kerap kali dilakukan oleh berbagai pihak baik privat maupun publik ditujukan ke dalam berbagai maksud dan tujuan tergantung sasaran dari kepentingan para pihak, sementara itu, terkadang banyak dari

---

55 *Lawrence Lessig, Code, Basic Books, New York, 1999, hlm*. 12.
56 Id., hlm. 20.
57 Id., 122-123.
58 Data sebagai tanah baru diperkenalkan pertama kali oleh David Mc Candless, ia melihat data sebagai media subur yang dapat ditingkatkan dan digunakan kembali seiring berjalannya waktu (tidak seperti minyak). *Berry Smart, Data is the New Soil*, diakses pada 27 Maret 2024, https://endjin.com/blog/2021/05/data-is-the-new-soil.
59 Marcus Smith et.al., *supra no.* 17, hlm. 8.

penyelenggara mengumpulkan data secara intrusif sampai memasuki pola kecenderungan memata-matai (*surveillance*) melalui pola-pola aktivitas pengguna di dunia maya. Dibutuhkan kerangka teknis selama proses pengembangan sistem perangkat terkhusus pada pemrosesan data biometrik. Hal demikian dimaksudkan agar keputusan terkait penanganan ancaman-ancaman dan jenis-jenis serangan terhadap sistem dapat ditangani sejauh mana sistem akan dioperasikan.[60] Kerangka teknis sebagaimana dimaksud adalah desain privasi. Pengertian desain privasi merupakan sebuah rancangan yang dimaksudkan dalam mencegah pelanggaran privasi dengan mengimplementasikan pelindungan privasi ke dalam desain informasi teknologi, jaringan, dan praktik bisnis.[61]

Melalui desain privasi, terdapat tujuh prinsip fondasi sebagai acuan praktis terdiri atas:[62]

a. Proaktif: desain privasi harus dipersiapkan agar dapat menjadi sarana pencegahan, oleh sebabnya sistem disusun secara komprehensif dan preventif (*before the fact*);
b. *Default setting*: sistem dan infrastruktur dengan secara otomatis memberikan pelayanan privasi maksimum pada tampilan bawaan, artinya mekanisme telah terbangun di melalui sistem itu sendiri;
c. *Design embedded*: pelindungan data privasi telah tersedia dalam desain teknologi IT dan telah diatur secara integral oleh kebijakan bisnis masing-masing perusahaan tanpa mengurangi fungsi;
d. Transparansi: desain privasi mengakomodir seluruh kepentingan sah dan objektivitas dari pemrosesan sistemnya, maka diharapkan terdapat solusi saling menguntungkan (*win-win solution*);
e. *End-to-end security*: desain privasi yang tertanam ke dalam sistem sebelum informasi dikumpulkan, menjangkau seluruh siklus perkembangan data bertujuan memperkuat privasi dimulai dari tahap awal sampai selesai;
f. Visibilitas dan transparansi (tetap terbuka): desain privasi berusaha meyakinkan semua pihak terkait bahwa setiap praktik bisnis atau teknologi yang

---

60 *Randal S. Milch et.al., Building Common Approaches for Cybersecurity and Privacy in a Globalized World, Center of Cybersecurity, New York, 2019, hlm. 135.*

61 *Ann Cavoukin dan Claudiu Popa, Embedding Privacy Into What's Next: Privacy by Design for the Internet of Things, Privacy and Big Data Institute, 2016, 4.*

62 Sinta Dewi Rosadi, *supra note* 10, hlm. 21-22.

terlibat telah disesuaikan berdasarkan tujuan pemrosesannya. Keseluruhan bagian dan operasi berdasarkan transparansi, kepercayaan, tapi tetap terverifikasi;

g. Menghargai pengguna (*respect the user*): melalui desain privasi memberikan persyaratan bagi penyelenggara data agar mampu menyimpan kepentingan dari individu dengan cara menyediakan pelayanan berupa kebijakan privasi yang kuat, notifikasi memadai, dan menawarkan opsi kemudahan bagi pengguna (*user centric*).

Keberadaan dari ke-7 prinsip desain privasi sejatinya mampu memberikan alternatif penyelesaian teknis terhadap tiap-tiap alur proses verifikasi maupun identifikasi data biometrik, di samping itu, pendekatan kerangka desain privasi menggantikan pendekatan sistem manajemen keamanan yang terintegrasi secara holistik seperti keamanan tersistematis, pendekatan solusi lebih kepada praktikal (adanya demonstrasi dari penggunaan), kreatif, inovatif, dan pengaturan tujuan privasi yang lebih jelas.[63]

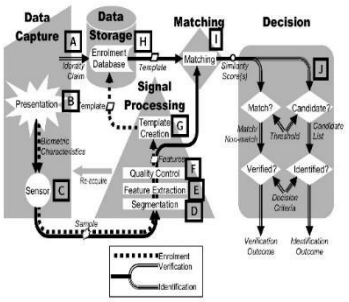
Dalam menelisik regulasi di Indonesia, desain privasi tidak secara eksplisit diatur sebagai ketentuan payung yang wajib diimplementasikan bagi setiap penyelenggara data pribadi, namun lebih kepada aturan rinci dengan menyematkan hal-hal tambahan seperti Pasal 28 butir f Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo No. 20 Tahun 2016) yang memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi (mengembalikan opsi kepada Pemilik Data Pribadi mengenai pilihannya membagikan data kepemilikannya), ataupun butir c mengelaborasi pemberitahuan tertulis kepada Pemilik Data Pribadi terkait kegagalan pelindungan rahasia Data Pribadi yang mana memuat berbagai langkah kepada Penyelenggara Data Pribadi bilamana terdapat kegagalan perlindungan rahasia Data Pribadi (tindakan preventif terhadap kegagalan pemrosesan data pribadi).

---

63 *Ann Cavoukin, Ph.D., supra note 11, hlm.* 9.

Konklusinya adalah pemberlakuan desain privasi dikembalikan kepada masing-masing Pengendali Data Pribadi, sehingga penyematan desain privasi perlu disesuaikan kepada model, bentuk, dan aturan internal bagi setiap Pengendali. Keberadaan regulasi tertulis seperti aturan hukum (undang-undang, peraturan pemerintah, peraturan menteri, keputusan, dan lain-lain) lebih diberlakukan sebagai pedoman universal (*guidance step*). Pernyataan ini juga diperkuat oleh Prof Paul A. Schwartz seorang ahli informasi dan privasi internasional pencetus desain privasi bahwasannya perusahaan merupakan sentral aturan manajemen informasi, pentingnya kebijakan awal (*pre-condition*) bagi pembangunan efektivitas serta akuntabilitas informasi kepada perusahaan ditujukan agar mampu mencapai pelindungan tertinggi privasi.[64] Adapun terkait langkah teknis terkait desain privasi di dalam pemrosesan data biometrik, penulis mengelaborasikan rangkaian alur terhadap data biometrik serta pengaplikasian desain privasi pada beberapa rangkaian operasinya.

Gambar 1. Tahapan Identifikasi Data Biometrik[65]



Seperti tampilan susunan verifikasi atau identifikasi dari data biometrik akan lebih mudah bila dipecah menjadi empat tahapan, sebagai berikut:[66]

a. Registrasi (*data capture*): permulaan penangkapan data biometrik. Bagian ini memberikan peran penting pada keseluruhan mekanisme sebagai awal mula data biometrik nantinya digunakan dan tersimpan di dalam kapasitas data (*data storage*);

---

64 *Ann Cavoukin, et.al., Privacy by Designs: Essential for Organizational Accountability and Strong Business Practices, 3 Identity in the Information Society 405, 406, 2010.*

65 *Andy Adler, Biometrics & Authentication Technologies: Security Issues*, diakses pada 10 Januari 2024, https://www.sce.carleton.ca/faculty/adler/talks/2008/adler-ornec-idt-5feb2008.pdf.

66 *Joseph N. Pato dan Lynette I. Millett, Biometric Recognition Challenges and Opportunities, The National Academic Press, Washington D.C., 2010, hlm*. 27.

b. Awal pemrosesan (*preprocessing*): setelah data dikumpulkan, dilakukan pemilahan data dimana pengoperasiannya dilakukan penghapusan data yang tidak dibutuhkan yang diyakini menyebabkan penurunan kinerja biometrik, kemungkinan terhadap penerimaan (*acceptance*) dan penolakan (*rejection*) registrasi pertama dapat diberlakukan;
c. Ekstraksi data (*feature extraction*): karakteristik data biometrik tidak dapat dipersamakan secara langsung. Artinya dibutuhkan kestabilan dan pemisahan di dalam fitur untuk dipilah dari perolehan sensor presentasi, hal ini bertujuan terhadap kinerja, interoperabilitas dari pemilik data biometrik yang diekstrak; dan
d. Pencocokan (*matching*): tahapan ini dilakukan melalui deteksi kecocokan pengumpulan data biometrik dari dua tahapan, pertama dikumpulkan pada proses registrasi awal dan kedua melalui tahap identifikasi atau otentikasi.

Bila dilihat melalui berbagai tahapan dan grafik atas proses data biometrik, hubungan antara desain privasi dan pelindungan data biometrik bisa ditempatkan pertama kali melalui tahapan registrasi, mengapa hal ini dapat dipertimbangkan? tahapan registrasi merupakan proses operasional awal sebelum sampel karakteristik data biometrik diproses lebih lanjut, bahkan tahapan ini dikatakan sebagai penentu sebelum data-data biometrik milik pengguna memasuki penyimpanan (*data storage*). Pada tahapan ini pula, terdapat dua proses yang perlu diperhatikan oleh Prosesor Data Pribadi yakni: (1) Verifikasi dan (2) Identifikasi.

Karena ke-2 proses adalah inti sebelum pengumpulan data biometrik dilakukan, konsekuensinya adalah (1) persetujuan (*consent*), (2) pemilihan (*choose*), (3) pembaharuan (*update*), dan (4) pencabutan (*retract*)[67] dari Pemilik Data Pribadi terhadap data biometrik miliknya akan diproses atau tidak, perlu dicantumkan sebagai awalan dari tahapan registrasi. Agar tercapainya persetujuan yang bersifat transparan, terutama mampu menjelaskan tujuan spesifik secara terperinci, memasukkan tata kelola desain privasi demi menunjang sistem keamanan data privasi menjadi suatu hal yang patut dipertimbangkan sebagai perwujudan kontrol atas privasi kepemilikan data pribadi.

[67] *Jaapp-Henk Hoepman, Privacy Design Strategies (The Little Blue Book), Redboud Universiteit, USA, 2022, hlm*. 16.

Penutup

Data biometrik sebagai data spesifik merepresentasikan laboratorium kehidupan seorang individu dimana menggambarkan karakteristik unik seseorang hingga pada akhirnya mempengaruhi hak privasi dan hak pribadi pengguna. Pengaruh keberadaan data spesifik tidak terlepas dari sistem hukum, namun demikian terdapat kelemahan terutama dalam substansi dan budaya hukum bahwasannya, walaupun UU PDP dan UU ITE telah mengupayakan ketentuan pelindungan data biometrik, akan tetapi belum tentu masyarakat sebagai aktor mampu menegakkan pelindungan data tersebut secara maksimal. Sejalan dari hal sebelumnya, kehadiran data biometrik perlu memperhatikan kepada fungsi peruntukkanya demi pencegahan penggunaan melebihi dari esensi dari data itu sendiri sehingga prinsip tujuan spesifik menjadi aspek esensial bagi prosesor dan pengendali.

Menimbang data biometrik bukanlah objek statis, dalam artian selama perkembangannya akan terus berubah-ubah mengikuti kemajuan inovasi teknologi dan manusia. Dengan ini, mempertimbangkan solusi teknis berupa kehadiran desain privasi sebagai jalan keluar dapat diberlakukan yang nantinya akan dikembalikan kepada pengendali data pribadi dengan tetap memperhatikan prinsip-prinsip pelindungan data pribadi, demi tercapainya hal demikian menghadirkan desain privasi pada tahapan registrasi pemrosesan data bisa menjadi pertimbangan lebih bagi penyelenggara data pribadi demi upaya preventif sebelum data biometrik disimpan dan dipergunakan demi kepentingan lain.

DAFTAR PUSTAKA

Buku:

Anil K. Jain, *et.al.*, *Introduction to Biometrics*, *Springer Science Business Media, London*, *2011.*

Ann Cavoukin, Ph.D., *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, *Information and Privacy Commissioner, Canada, 2012.*

Evelyn de Souza, The Era of Homo Digitus, in Women in Security, Women in Engineering and Science, Springer Cham, Europe, 2018.

H. Zainduddin Ali, *Metode Penelitian Hukum*, Sinar Grafika, Jakarta, 2015.

Ibrahim Fikma Edrisy, *Pengantar Hukum Siber*, Sei Wawai Publishing, Lampung, 2019.
Janitra Haryanto, *Klasifikasi Data Untuk Pelindungan Data Pribadi*, Center for Digital Society, Yogyakarta, 2018.
Jepp-Henk Hoepman, *Privacy Design Strategies (The Little Blue Book), Redboud Universiteit, USA, 2022.*
John D. Woodward Jr, *Handbook of Biometrics, Springer, Boston, 2008.*
Joseph N. Pato dan Lynette I. Millett, *Biometric Recognition Challenges and Opportunities, The National Academic Press, Washington D.C., 2010.*
Lawrence J. Fennelly, *Effective Physical Security Fourth Edition, Elsevier, United Kingdom, 2013.*
Lawrence Lessig, *Code*, *Basic Books, New York, 1999.*
Marcus Smith dan Seumas Miller, *Biometric Identification, Law, and Ethics, Springer, United Kingdom, 2021.*
Niniek Suparni, *Cyberspace, Problematika dan Antisipasi Pengaturannya, Penerbit Sinar Grafika*, Jakarta, 2009.
Robert Walters, et.al., *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches, Springer Nature Ltd, Singapore, 2019.*
Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, PT Refika Aditama, Bandung, 2015.
Wahyudi Djafar dan M. Jodi Santoso, *Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya*, ELSAM, Jakarta, 2019.

Jurnal:

Anahiby Becerril, The Value of Our Personal Data in the Big Data and the Internet of All Things Era," 7 ADCAIJ 71, 2018.
Ann Cavoukin, et.al., Privacy by Designs: Essential for Organizational Accountability and Strong Business Practices, 3 Identity in the Information Society 405, 2010.
Bert-Jaap Koops, The Concept of Function Creep, 13 Law, Innovation, and Technology 29, 2021.
Daniel J. Solove, Data is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data, 118 Northwestern University Law Review 2, 2023.
Farida Sekti Pahlevi, Pemberantasan Korupsi di Indonesia: Perspektif Legal System Lawrence M. Freidman, 1 *Jurnal El-Dusturie* 23, 2022.
Jeroen van Rest, et.al., Designing Privacy by Design, Annual Privacy Forum 55, 2012.
Mark Maguire, The Birth of Biometric Security, 25 Anthropology 9, 2009.
Miyuki Fattah Rizki dan Abdul Salam, Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris, 2 *Lex Patrimonium* 1, 2023.
Mohd Yusuf D.M., et.al., Peranan Budaya dan Kebudayaan di Indonesia Dari Aspek Sosiologi Hukum, 6 *Jurnal the Jurist* 1, 2022.
Muhammad Fikri dan Shelvi Rusdiana, Ruang Lingkup Pelindungan Data Pribadi: Kajian Hukum Positif Indonesia, 5 *Ganesha Law Review* 39, 2023.
Sekaring Ayumeida Kusnadi dan Andy Usmina Wijaya, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, 2 *Jurnal Al-Wasath* 9, 2021.

Sinta Dewi Rosadi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia, 5 *Yustisia* 1, 2016.

Samuel D. Warren dan Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Review 5, 1890.

Sinta Dewi Rosadi, Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi, 9 *Arena Hukum* 403, 2017.

Sinta Dewi Rosadi et.al., Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia, 4 *Veritas et Justitia* 1, 2018.

Situs Daring:

Agnes Z. Yonatan, Indonesia Peringkat 4, Ini Dia 7 Negara Pengguna Internet Terbesar di Dunia, diakses pada 4 Januari 2024, https://data.goodstats.id/statistic/agneszefanyayonatan/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-FLw6V.

Andri Saubani, CISSReC: 3,2 Miliar Data PeduliLindungi Bocor, https://news.republika.co.id/berita/rle9di409/cissrec-32-miliar-data-pedulilindungi-bocor, diakses pada 3 Januari 2023.

Andy Adler, Biometrics & Authentication Technologies: Security Issues, diakses pada 10 Januari 2024, https://www.sce.carleton.ca/faculty/adler/talks/2008/adler-ornec-idt-5feb2008.pdf.

BBC News Indonesia, Ratusan Juta Data Dukcapil Kemendagri Diduga Bocor, Pakar Siber:'Ini Peretasan Paling Parah, diakses pada 4 Januari 2024, https://www.bbc.com/indonesia/articles/c51v25916zlo.

Khorul Anam, Paling Rendah di ASEAN, Tingkat Literasi Digital RI Cuma 62%, diakses pada 4 Januari 2024, https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62.

Moh. Khory Alfarizi, "Data Internal PT KAI Diduga Dibobol Hacker dan Dijual Pakai Kripto, Ini Penjelasan Lengkap Manajemen," diakses pada 16 Januari 2024, https://bisnis.tempo.co/read/1821647/data-internal-pt-kai-diduga-dibobol-hacker-dan-dijual-pakai-kripto-ini-penjelasan-lengkap-manajemen.

Novina Putri Bestari, Google Beberkan Pendapatan Bisnis Cloud dari Indonesia, diakses pada 28 Maret 2024, https://www.cnbcindonesia.com/tech/20231011133337-37-479699/google-beberkan-pendapatan-bisnis-cloud-dari-indonesia.

Social Media Today, The Internet in Real Time [Live Infographic], diakses pada 14 Januari 2024. https://www.socialmediatoday.com/content/internet-real-time-live-infographic.

We Are Social, Digital 2023 Indonesia, diakses pada 4 Januari 2024, https://wearesocial.com/id/blog/2023/01/digital-2023/.

Forum:

ASEAN Telecommunications and Information Technology Ministers Meeting, Framework on Personal Data Protection, Bandar Seri Begawan, Brunei Darussalam, 25 November 2016.

Tesis dan Laporan:

Council of Europe, Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Refard to Automatic Processing of Personal Data, Council of Europe Treaty Series No. 223, 2018.

Lauren Dancer, et.al. Biometric Identification and Privacy, Comparative Research Prepared for the Center for Law and Policy Research, India, 2013.

Zhasmina Radkova Kostadinova, Purpose Limitation Under the GDPR: Can Article 6(4) Be Automated, Master Thesis in Tilburg University, Belanda, 2014.

Innovatrics, Biometricks and Personal Data, White Paper, Europe, 2004.

Riza Roidila Mufti, A Policy Brief EU General Data Protection Regulation (GDPR), Research Series Embassy of the Republic of Indonsia in Brussels, 2021.

Peraturan Perundang-undangan dan Instrumen Hukum Lain:

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

General Data Protection Regulation.

Rivera v. Google Inc No. 16 C 02714.