

## ANALISA CAKUPAN HUKUM PENGELOLAAN PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA

Fauzi Solihin

Fakultas Ilmu Sosial, Universitas Negeri Malang

Email: fauzymufc@gmail.com

### ABSTRAK

Kajian ini didasari atas pentingnya di era modern saat ini untuk memberikan perlindungan atas hak-hak privasi dan data seseorang agar dapat menghalau penyelewengan atau kekeliruan penanganan data. Tujuan penelitian ini adalah untuk menganalisa cakupan pengelolaan hukum perlindungan data pribadi di Indonesia. Metode penelitian yang dipakai yakni penelitian kualitatif yang sifatnya studi pustaka (*library research*) memakai beberapa buku, jurnal dan literasi lain untuk menjadi obyek pokok dalam mengupas permasalahan terkait dengan cakupan pengelolaan hukum perlindungan data pribadi di Indonesia. Hasil Penelitian menguraikan bahwasanya cakupan pengelolaan hukum perlindungan data pribadi di Indonesia telah memunculkan beberapa aturan UU yang dijalankan dan sah saat ini, yang punya keterikatan atau dalamnya muncul bahasan yang terkait dengan pengelolaan perlindungan data pribadi. Beberapa aturan UU itu bisa digolongkan jadi beberapa sektor, yakni: (1) telekomunikasi dan informatika; (2) kependudukan dan kearsipan; (3) keuangan, perbankan, dan perpajakan; (4) perdagangan dan industri; (5) layanan kesehatan; dan (6) keamanan dan penegakan hukum.

**Keywords:** *Data Pribadi, Perlindungan, Hukum*

### PENDAHULUAN

Transformasi digital sudah berhasil membuat banyak inovasi keren dalam hal guna mendapatkan, memasukkan, mengolah, menyunting dan menyebarkan kuantitatif data sesuai waktu sebenarnya, luas dan komprehensif. Oleh sebab itu, revolusi digital kerap kali dinilai sama dengan revolusi data. Kemajuan itu yang sudah menggiring penyatuan banyak jenis data, tak lagi terperangkap pada pemikiran-pemikiran data apa yang mungkin masih bisa dipakai di masa yang akan datang. Namun, hampir seluruh data disatukan, banyak instansi berlomba-lomba guna meluaskan ruang penyimpanan data sendiri-sendiri, dan makin jarang untuk membuang atau memasukkan data ke dalam sampah yang artinya menghapusnya.

Banyak orang menemui nilai baru dalam sebuah data, alhasil data dirawat seperti misalnya emas, uang, dan sebagainya. Periode baru tata kelola data ini yang kerap dinamakan dengan Big Data. Transformasi dalam desain tata kelola data ini juga yang sering disebut dengan pokok dari Revolusi Industri Ke-4. Adanya revolusi digital yang di karekteristikkan dengan kolaborasi teknologi yang memadukan garis dari sisi fisik, digital, dan biologi. Revolusi Industri ke-4 kerap dicerminkan menjadi kemunculan sebuah "*cyber-physical systems*", yang mengikutsertakan kecerdasan yang semuanya baru untuk umat manusia dan mesin, terkhusus dalam sifat cepatnya, ruangnya, dan efek dari sistemnya. (Khairani, & Irwansyah, 2018).

Kemajuan ini sudah memberikan ruang atas munculnya banyak inovasi teknologi yang jarang di sektor-sektor misalnya kecerdasan buatan, robot, IoT, kendaraan otomatis, pencetakan 3-D, dan sebagainya. Big Data pada dasarnya, kerap dinilai menjadi substansi dari keterbaruan teknologi. Maksudnya konsepsi ini hanya dikendalikan oleh atribut atau elemennya, yang di dalamnya mencakup sebuah data yang baru ditemui dan daya digital yang kompleks. (Schwab, 2017)

Benar bahwasanya konsepsi dari Big Data sendiri muncul dengan tak dimaknai sebagai definisi yang baku, yang di-amankan oleh seluruh ahli. Akan tetapi, secara umum dipahami bahwasanya Big Data tak sama dari analisa bisnis konvensional dan data skala kecil, ataupun yang kuantitasnya banyak. Hal ini menimbulkan kerap munculnya rasa bimbang dan kekeliruan persepsi dalam memberikan pemahaman atas Big Data ini, yang merupakan efek dari luasnya pengertiannya.

Terlebih, pada poin tertentu, pemaknaan itu kerap bertabrakan satu dengan yang lain. Pada sudut pandang Ilkom, Big Data pada dasarnya, kerap dinilai cuma sebatas substansi dari keterbaruan teknologi. Maksudnya konsepsi ini hanyalah ditentukan oleh elemen-elemen di dalamnya, yang memuat sebuah data yang baru ditemui dan daya pengolahan digital yang maju tersebut. Hal itu mirip dengan pengungkapan dari Manovich (2011) bahwasanya Big Data pada dasarnya memfokuskan pada set data yang sangat luas atau besar, yang memerlukan super komputer. Walaupun di waktu sekarang ini, proses itu cukup dianalisa memakai PC dengan memaksimalkan *software* standar.

Secara tegas diungkapkan oleh Kitchin (2014), bahwasanya Big Data merupakan *output* dari *development* dan *convergn* dari banyak macam transformasi teknologi. Memang, dalam maypritas kasus, makna dari 'Big Data' sering mengambil dari kolaborasi atas unsur *volume*, *velocity*, *variety*, *veracity* (4Vs), yang jadi konsepsi yang dibuat oleh Gärtner, & Hiebl, (2017) dan setelah itu mayoritas konsepsi itu dicomot oleh IBM. Metode data-sentris ini terkhusus memfokuskan pada banyaknya lonjakan data, bertambahnya kecepatan, pembuatan dan pemanfaatan data pada di waktu itu juga, serta kemajemukan format data yang dikelola. (Goes, 2014).

Nyatanya, dikutip dari McAfee & Brynjolfsson (2012) tiap detik di bumi ini memproduksi lebih banyak data daripada yang dijaga dari puluhan th yang lalu. Seluruhnya datang dari satuan data yang beragam, banyak sumber dan banyak jenis format, misalnya audio, interaksi sosmed, dan banyak macam konten lainnya. Kemudian, Big Data juga kerap dipakai guna menguraikan untuk implementasi teknik-teknik analisa guna menelaah, menyatukan dan mengutip secara silang gabungan dari data dalam jumlah kuantitas yang cukup luas guna menumbuh kembangkan sistem kecerdasan dan ilmu pengetahuan.

Gabungan data yang kuantitasnya cukup besar itu dapat diperoleh dari sumber umum, juga satuan data dari konsumen perusahaan atau instansi. Big Data seiring berjalannya waktu mencakup tak cuma data yang sifatnya umum, tapi juga terdiri atas keterangan informasi yang disatukan oleh bagian privat. Faktor ini yang setelah itu menjadi latar belakang kemunculan definisi Big Data menjadi kedatangannya satuan data baru dengan kuantitas yang besar dan bertransformasi dengan cepat, begitu kompleks, dan melebihi keterjangkauan kecerdasan analisa lingkungan *software* dan *hardware* yang kerap dipakai guna memproses sebuah data. Maksudnya, volume data jadi sangat besar jika dikelola oleh alat dan metode yang lama. (Akhgar, Dkk 2015).

Akan tetapi dalam pemanfaatan Big Data, ada berbagai unsur fundamental yang wajib diketahui dan dipahami, terkhusus yang berketerikatan dengan kerahasiaan dan

perlindungan data pribadi. Hal ini terkhusus menimbang akan luas dan banyaknya penyatuan dataset yang akan memberikan kemudahan dalam menelaah seseorang personal atau golongan, yang mempunyai potensi menimbulkan tindak bahaya dari orang tersebut. Oleh sebab itu, upaya-upaya perlindungan data yang sesuai wajib dijalankan guna meminimalisir bahkan menghalau penyelewengan atau kekeliruan penanganan data. Maksudnya, jika pelonjalakan besar-besaran di kala penyatuan dan penyimpanan data ini tak dijalankan dalam rangka menghormati hak, alhasil mau tak mau proses dan misinya akan dipakai dengan metode yang tak mementingkan hak-hak privasi banyak orang. Berangkat dari latar belakang tersebut, penulis tertarik guna menelaah pengelolaan Hukum Perlindungan atau Privasi dari Data Pribadi di Indonesia

## TINJAUAN PUSTAKA

Menjadi sebuah hak yang menempel pada diri seseorang, pembahasan terkait urgensi nya tindakan dalam melindungi hak atas privasi manusia pada awalnya datang di dalam putusan dari peradilan di Inggris dan setelah itu di AS. Sampai suatu waktu, Warren menulis sebuah pemikiran hukum hak atas privasi Kajian ini datang saat banyak majalah dan koran mulai memproduksi gambar manusia pertama kali. Dalam kajian itu, Warren dengan sederhana mengartikan bahwasanya hak atas privasi menjadi sebuah hak untuk dibiarkan berdiri sendiri. Definisi itu berdasar pada dua aras yakni kehormatan pribadi, juga nilai dan norma seperti kedudukan manusia secara personal, otonomi dan kemandirian pribadi. (Warren, 1890).

Pemikiran tersebut lalu memperoleh persetujuan dengan munculnya banyak gugatan hukum yang setelah itu memberi sebuah membenaran mengenai pentingnya perlindungan hak atas privasi, terkhusus dengan maksud menjaga nilai moral. Menindaklanjuti konsepsi yang disusun oleh Warren, Prosser (1960) kala itu lebih menjelaskan dengan rinci atas bahasan ruang lingkup dari hak privasi manusia, dengan mengutip dari empat wujud gangguan pada diri manusia secara personal, yakni: (a) gangguan kepada tingkah laku manusia menyendiri, atau gangguan kepada keterikatan personal nya, (b) mengungkap fakta pribadi yang membuat malu di dalam ruang publik (c) publikasi yang memposisikan orang tertentu dengan salah di depan publik (d) memiliki dan menguasai tanpa adanya perizinan atas keidentikan seseorang sebagai upaya mencari keuntungan.

Di sisi lain, Westin (1967) mengartikan bahwasanya hak atas privasi menjadi hak dari seseorang, golongan, juga sebuah organisasi guna memilih pribadi tentang tata kelola keterangan informasi mengenai mereka disodorkan kepada siapapun juga dimanapun. Luasnya cakupan privasi kerap membuat banyak sekali kebijakan terkait privasi di sebuah negara, mulai dari macamnya juga level tingkatannya. Kemudian, Innes (1996) mengartikan privasi menjadi sebuah keadaan saat orang mempunyai kendali atas ranah putusan pribadi di diri mereka sendiri, yang terdiri atas putusan atas pengelolaan privat, keterangan privat dan implementasi privat. Kemudian, privat sendiri diuraikan menjadi sebuah *output* dari rasa cinta, rasa suka dan rasa peduli kepada sesama.

Dari beberapa pemaknaan yang disusun terkait dengan privasi", terlihat banyak polarisasi yang muncul, yang benang merahnya memposisikan privasi menjadi sebuah hak, atau hak personal guna mengatur keterangan apa terkait pribadinya yang bisa dikeluarkan atau dipublikasikan pada khalayak publik. Privasi juga sudah ditelaah menjadi volume kontrol seseorang kepada beberapa unsur kepribadian nya, yang terdiri

dari (i) keterangan terkait diri pribadinya; (ii) sifat rahasia identitas pribadi; atau (iii) orang-orang punya yang kendala kepada pribadi tersebut.

Hal ini tak sama dengan yang ada di AS, yang memfokuskan pada keterangan dan interaksi pribadi guna menguraikan keberadaan dan ruang privasi, rezim Eropa memfokuskan pada segi perlindungan data pribadi kerap dinamakan dengan “data” saja, menjadi elemen dari perlindungan hidup secara personal. Pemaknaan itu berfokus pada aturan Pasal 8 Konvensi Eropa, yang sudah membuat munculnya beberapa tafsir tentang cakupan dari kehidupan persona seseorang, terkhusus lewat beberapa macam fenomena kasus, mulai dari Pengadilan HAM Eropa, juga pada Pengadilan Eropa. Cakupan bahasan terkait kehidupan pribadi yang diuraikan dalam Pasal 8 Konvensi Eropa salah satunya yakni akses ke dalam data pribadi. (Lukács, 2016).

## **METODE PENELITIAN**

Penelitian ini memakai penelitian kualitatif yang sifatnya studi pustaka (*library research*) memakai beberapa buku, jurnal dan literasi lain untuk menjadi obyek pokok dalam mengupas permasalahan dalam penelitian (Hadi, 1995). Penelitian ini memproduksi sebuah keluaran keterangan berwujud tulisan catatan data deskripsi yang ada pada bacaan yang dikaji (Mantra, 2008). Lewat penelitian kualitatif, butuh dijalankan sebuah analisa deskriptif. Metode analisa deskriptif memberi sebuah cerminan dan informasi dengan gamblang, obyektif, tersusun rapi, dan mendalam terkait dengan cakupan pengelolaan hukum perlindungan data pribadi di Indonesia. Pendekatan kualitatif yang berdasar pada *step* awal yang dilewati dengan menyatukan berbagai jenis data-data yang diperlukan, lalu dilaksanakan klasifikasi dan deskripsi, serta mengambil simpulan.

## **HASIL DAN PEMBAHASAN**

### **Cakupan Pengelolaan Hukum Perlindungan Data Pribadi di Indonesia**

Dalam okupansi publik di Indonesia, konsepsi privasi kerap ditelaah sebagai konsepsi barat (Eropa), misalnya yakni HAM. Alasan ini menjadi pembelaan atas minimnya rasa sadar akan publik terkait privasi, terlebih yang berkesinambungan dengan perlindungan data personal seseorang. Masyarakat dengan gampang megumbar cerita pada orang lain, alamat rumah, tanggal lahir, sampai pada keterkaitan antara pasangan, saudara, dan sebagainya. Kemudian, juga menjadi perilaku umum di Indonesia, dengan sangat gampang nya menguraikan KTP maupun biodata dirinya, yang di mencakup data personal, pada orang lain atau pihak lain contohnya saat misalnya masuk ke area tertentu, atau ruang-ruang tertentu.

Dalam bahasan terbaru, para pemakai media sosial di Indonesia, sering dengan gamblang dan tanpa kompromi dengan mudah mencantumkan tempat tinggal asli sengan selengkap-lengkap nya sampai nomor rumah pun di cantumkan; sampai juga keterikatan kedekatan dengan orang tua dan pasangan. Hal ini mengindikasikan akan masih luasnya permasalahan rasa sadar masyarakat dalam memberikan perlindungan data privasi secara personal yang menjadi aset dirinya. Pengakuan yang menjelaskan privasi menjadi konsepsi barat sebenarnya tak menyeluruh benar di Indonesia, studi yang dilaksanakan oleh Westin (1967), terkhusus saat dia menjelaskan cerminan terkait konsepsi privasi dalam era pra-modern atau pada tatanan masyarakat lama, justru memakai contoh privasi

rumah tangga pada tatanan penduduk Jawa dan Bali di Indonesia, dengan memfokuskan pada kajian yang dijalankan oleh Clifford Geertz.

Sebuah konsepsi hukum perlindungan kepada privasi orang memang baru muncul berbarengan dengan kemunculan aturan UU kolonial, terkhusus se-usai diberlakukannya KUHP pada 1848, juga KUHP di th 1915, oleh pemerintah kolonial Hindia Belanda. Hal itu salah satunya bisa dimaknai menjadi awal kemunculan konsepsi pelanggaran guna masuk dalam rumah orang lain dengan tak izin terlebih dahulu, atau munculnya larangan dalam membuka surat tanpa ijin dari Ketua Pengadilan, yang dituliskan dalam *Postordonnantie* 1935.

Dalam perjalanannya, terkhusus setelah amandemen UUD 1945, hak atas privasi yang di dalamnya juga mencakup perlindungan data pribadi dibenarkan menjadi sebuah hak konstitusional masyarakat Indonesia. Hal ini senada dengan masuknya bab khusus mengenai HAM dalam konstitusi output amandemen. Aturan tentang jaminan perlindungan data pribadi bisa ditemui pada Pasal 28G ayat (1) UUD 1945 yang menguraikan bahwasanya masing-masing orang mempunyai hak atas perlindungan diri pribadi, keluarga, martabat, dan kekayaan yang di bawah kekuasaannya, juga punya hak atas keamanan dan perlindungan dari adanya ancaman ketakutan dalam bertindak sesuatu yang menjadi hak asasi.

Keikutsertaan Indonesia menjadi negara pihak dari *International Covenant on Civil and Political Rights* yang dituliskan dalam UU No. 12 th 2005, juga mempertegas bahwasanya tugas tanggung jawab pemerintah Indonesia guna memberikan perlindungan privasi dan data personal warganya. Hal itu senada dengan UU No. 39 th 1999 mengenai HAM, yang dalam pasalnya juga memberikan jaminan atas perlindungan hak atas privasi warga, contohnya pada Pasal 14 (2), 29 (1) juga 31. Pasal 29 ayat (1) menguraikan pengakuan dari hak masing-masing orang atas perlindungan diri. Perlindungan itu tak cuma pada bahasan keterkaitan secara langsung, namun juga atas sebuah informasi atau data pribadi.

Di sisi lain, pada Pasal 14 ayat (2) diuraikan bahwasanya salah satu hak pengembangan diri yakni hak dalam mencari, mendapatkan, memelihara, menyimpan, menyunting, memanfaatkan informasi dengan memakai semua macam fasilitas yang ada. Hal ini berkaitan dengan Pasal 31 UU HAM yang juga memberikan aturan atas merdeka nya rahasia dalam keterkaitan jaminan komunikasi lewat media elektronik, terkecuali atas suruhan hakim atau kekuasaan yang lain yang sah sejalan dengan aturan UU.

Pada tahapan yang lebih rinci, juga muncul beberapa aturan UU yang dijalankan dan sah saat ini, yang punya keterkaitan atau dalamnya muncul bahasan yang terkait dengan data pribadi. Beberapa aturan UU itu bisa digolongkan jadi beberapa sektor, yakni: (1) telekomunikasi dan informatika; (2) kependudukan dan kearsipan; (3) keuangan, perbankan, dan perpajakan; (4) perdagangan dan industri; (5) layanan kesehatan; dan (6) keamanan dan penegakan hukum. (Febriana & Geraldo, 2021).

### **(1) Telekomunikasi dan Informatika**

Dalam segi ini, awalnya aturan tentang perlindungan hak atas privasi cuma mengenai atas rahasianya keterangan dan interaksi secara personal, yang dicerminkan lewat aturan larangan penyadapan, pada UU No. 36 th 1999 mengenai Telekomunikasi. Tetapi dalam kebijakan ini juga, operator telekomunikasi diberi sebuah kedudukan dalam melaksanakan upaya merekan percakapan, dengan maksud membuktikan keabsahan pemanfaatan sarana telekomunikasi atas keinginan dari pemakai atau konsumen jasa telekomunikasi. Aturan terkait dengan perlindungan data pribadi pada bagian IT atau

lebih lebarnya dalam implementasi sistem elektronik baru ada sejalan dengan munculnya UU No. 11/2008 mengenai ITE

Mengutip pada aturan Pasal 26 ayat (1) UU ITE, masing-masing pergantian tangan atas data pribadi orang harus lebih dulu memperoleh perizinan dari yang memiliki data. Jikalau data personal seseorang dipindah tangankan dengan semena-mena, yang punya data pribadi itu bisa melakukan penggugatan ganti rugi ke peradilan sesuai Pasal 26 ayat (2). Namun, susah nya upaya pembuktian dalam pengadilan perdata di negeri ini, mempersulit si pemilik data guna mengurus permasalahan secara hukum atas praduga bocornya data diri nya.

Ada satu golongan warga yang menggugat Facebook atas dugaan bocornya data pribadi user Facebook di Indonesia, pada kasus Cambridge Analytica. Dalam perjalanannya, setelah keputusan oleh CJEU di th 2014, yang mengeluarkan klausa *right to be forgotten*, juga sudah memberikan pengaruh atas berubahnya UU ITE pada 2016. Pada upaya amandemen UU ini, DPR memberikan usulan supaya Indonesia juga memakai sebuah konsepsi *right to be forgotten*. Usulan ini lalu dimasukkan pada Pasal 26 ayat (3) UU No. 19 th 2016 mengenai Perubahan UU No. 11 th 2008 terkait dengan ITE, yang menjelaskan bahwasanya masing-masing PSE harus menghilangkan Informasi Elektronik dan/ atau Dokumen Elektronik yang tak relevan yang ada di bawah kontrol nya atas keinginan orang yang berketerikatan berdasar atas aturan dari pengadilan. (Rumulus & Hartadi, 2020).

Aturan lebih dalam terkait dengan penghilangan atau penghapusan informasi yang tak berketerikatan itu kemudian akan dikelola pada PP Pasal 26 ayat (4). Aturan di atas terlalu umum, dengan hanya menguraikan penghilangan atau penghapusan Informasi Elektronik yang tak berketerikatan atau tak relevan. Tak ada uraian lebih lengkap terkait dengan yang dijelaskan sebagai informasi yang tak relevan. Hal ini mengakibatkan adanya potensi tabrakan dengan banyak kebijakan UU lainnya dalam pelaksanaannya, terkhusus pada beberapa kebijakan yang memberikan jaminan atas hak publik informasi dan bebas dalam berekspresi. Contohnya yakni potensi tabrakannya dengan UU No. 40 Th 1999 mengenai Pers, juga UU No. 14 Th 2008 mengenai Keterbukaan Informasi Publik.

Di sisi lain, di UU No. 14 th 2008 mengenai Keterbukaan Informasi Publik, perlindungan kepada data informasi publik yang dipayungi oleh badan publik yang tercantum dalam Pasal 6 ayat (3) huruf (c) UU KIP yang menguraikan pada badan publik guna tak menyebarkan informasi publik yang berketerikatan dengan hak pribadi. Hal itu pula tercantum pada penjelasan Pasal 17 huruf (g) dan (h) yang menguraikan bahwasanya akta otentik yang sifatnya pribadi dan wasiat orang serta keterangan yang berketerikatan dengan sifat rahasia atas personal diuraikan menjadi sebuah informasi yang dikhususkan.

Beberapa informasi yang bisa membuka rahasia pribadi yakni berketerikatan dengan latar belakang keluarga, latar belakang kesehatan, keadaan finansial, perolehan atau pemasukan dan rekening bank, sampai latar belakang pendidikan seseorang. Dalam kenyataannya, kebijakan atas perlindungan data pribadi yang beketerikatan dengan implementasi sistem elektronik, juga aturan IPTEK lalu disusunlah kedalam PP No. 82/2012, lalu juga dukungan dari beberapa aturan menkominfo,

Beberapa aturan dari menkominfo yang terhubung contohnya yakni di No. 20 th 2016 mengenai Perlindungan Data Pribadi dalam SE, juga aturan menkominfo Nomor 21/2017 mengenai Perubahan Kedua Atas Peraturan menkominfo No. 12 th 2016 mengenai Pendaftaran Pelanggan Jasa Telekomunikasi. Pelindungan data pribadi yang

diungkapkan oleh aturan menkominfo PDPSE terdiri atas perlindungan pada upaya pencarian dan penyatuan; pemanfaatan dan penganalisaan; peng-unggahan, pengumuman, pentransmisi, dan/atau membuka akses; dan pemusnahan data pribadi. Selain bahasan perlindungan data pribadi, yang terdiri atas seluruh segi dan upaya tahap pemrosesan data personal, dalam aturan menkominfo juga dituliskan atas hak-hak dari pemilik data pribadi, tanggung jawab pengguna data pribadi, juga tanggung jawab dari implementor sistem elektronik dalam seluruh upaya pemrosesan tersebut. (Salsabila, 2022).

Menjelaskan ulang atas amanat dari PP PSTE, dalam aturan menkominfo ini juga dikelola terkait dengan tanggung jawabnya di dalam memposisikan pusat data pada area atau wilayah di Indonesia (data lokal), teruntuk implementor dari sistem elektronik dalam layanan publik. Data center di wilayah Indonesia ini ditunjukan supaya menjadikan sarana guna memposisikan Sistem Elektronik dan elemen di dalamnya guna kepentingan pemposisian, penyimpanan, dan tata kelola data. (Salsabila, 2022).

Apabila muncul adanya sengketa dalam tata kelola data pribadi muncul adanya kekeliruan di saat proses melindungi kerahasiaan data pribadi, kebijakan menkominfo ini dapat meluaskan ruang aduan kepada Kominfo, agar dijalankan upaya penuntasan kasus secara aturan yang berlaku dengan berbagai jenis pilihan penyelesaian sengketa lain, atau apabila semua cara itu tak bisa menuntaskan kasus, bisa memakai metode gugatan perdata di peradilan. Peraturan menkominfo ini memberi sebuah batasan transisi dalam waktu 2 th untuk implementor sistem elektronik, agar menjalankan pencocokan seluruh kewajibannya dalam perlindungan data pribadi.

Namun, dalam kenyataannya setelah beberapa th berlakunya Permenkominfo, masih banyak implementor dari sistem elektronik di Indonesia yang belum menjalankan tugasnya yakni mencocokkan dengan aturan kewajiban perlindungan data pribadi yang dikelola dalam Peraturan menkominfo. Hal ini mengindikasikan bahwa kebijakan yang cuma se-level aturan menteri, dengan ancaman sanksi yang cuma berwujud sanksi administratif, dirasa kurang punya ikatan memaksa untuk implementor sistem elektronik (Ichsan, Dkk 2020).

## **(2) Kependudukan dan Kearsipan**

Berdasar atas UU Adminduk UU No. 23 th 2006 bahwasanya negarapunya tugas dan tanggung jawab guna mempersimpan dan memberi sebuah perlindungan atas data pribadi masyarakatnya. Oleh sebab itu, hak akses dari pengelola Penyelenggara dan Instansi Pelaksana pengatur data pribadi warga punya tugas guna melindungi informasi dan sifat rahasia dari data itu, yang aturannya secara lengkap dituliskan pada PP No. 67 Th 2011 mengenai KTP Berbasis NIK Secara Nasional. Namun, kebijakan ini juga masih belum mengakomodir perlindungan data pribadi masyarakat, keterikatannya dengan setelah pencarian dan menyalin data yang mengikutsertakan tindakan scan sidik jari dan retina mata warga.

Di sisi lain, pada Pasal 1 no 22 UU No. 23 th 2014, menjelaskan bahwa data pribadi menjadi data individu waga yang wajib di beri perlindungan, disimpan, dan di jaga keabsahan dan rahasianya. Lalu, pada Pasal 85 UU Adminduk, diuraikan bahwasanya negara punya tugas guna mengelola dan memberi sebuah perlindungan data pribadi warga masyarakat tersebut. Hal itu pula diatur pada Pasal 79 yang mengharuskan negara agar memberi sebuah perlindungan dan mengangkat menteri menjadi pelaksana atas hak akses data pribadi masyarakat. Persoalannya ada saat munculnya ketidak-samaan golongan data penduduk yang wajib di beri perlindungan atau dirahasiakan. Ada ketidak

samaan yang jauh diantara UU No 23 th 2006 dan amandemen nya, yakni UU No 24/2013. Keadaan seperti itu, muncul karena tak adanya kecermatan dan penjelasan atas pengelompokan data pribadi di Indonesia.

Kemudian pada cakupan kearsipan, berketerikatan dekat dengan upaya aktivitas administrasi negara yang satu diantaranya yakni berkaitan dengan implementasi sistem kearsipan oleh pemerintah, dan sering juga mencakup data dan informasi personal seseorang, contohnya data penduduk, juga data siswa dan guru di sekolah, juga mahasiswa dan dosen di kampus. Pada Pasal 3 huruf (f) No. 43 th 2009 mengenai Kearsipan diungkapkan bahwasanya salah satu misi dari kearsipan yakni guna memberikan jaminan atas menjamin aman-nya arsip menjadi bukti selesainya tugas dalam hidup di dalam sebuah negara. Di samping itu, pada UU ini juga dituliskan terkait periode retensi dari sebuah data, yang masanya mulai dari 10-25 th. Se-usai periode retensi selesai, maka arsip itu bisa ditambah masa retensi nya, bisa pula dihapus, atau bisa juga diunggah ke publik, dengan syaratnya yakni tak membocorkan rahasia atau data personal. (Husein, 2010).

### **(3) Keuangan, Perbankan, dan Perpajakan**

UU Perbankan yakni No. 10 th 1998, mengelola atas persoalan yang berketerikatan atas kerahasiaan bank dengan berasaskan prinsip rahasia, yang mengharuskan bank agar menjamin rahasia dari semua hal yang berkaitan dengan data dan keterangan terkait nasabah, mulai dari kondisi keuangannya juga keterangan yang punya sifat personal. Pada Pasal 1 ayat (28) UU Perbankan, rahasia bank diartikan menjadi semua hal yang berkaitan dengan uraian terkait nasabah penyimpanan dan simpanannya. Dengan begitu, asas percaya dan kerahasiaan menjadi pedoman kinerja lembaga keuangan, ikut dijalankan dalam kaitannya antara sisi nasabah dan bank. (Sartika, 2019).

Nasabah saat menjalankan penyimpanan atau memanfaatkan produk bank lain nya wajib menyodorkan data pribadi yang dinilai penting untuk keperluan bank. Keterkaitan itu wajib didorong dengan kecerdasan dari pihak bank dalam mengelola dan bertanggung jawab atas rasa percaya dari nasabah juga memberikan perlindungan privasi dari nasabah yang sudah rela memberi data diri nya. Hal itu tertulis pada Pasal 40 UU Perbankan dan Pasal 41 UU No. 21 th 2008 mengenai Perbankan Syariah, yang menjelaskan bahwasanya bank punya kewajiban melindungi dan menjaga rahasia informasi terkait nasabah penyimpanan dan simpanannya, terkecuali dalam bahasan tertentu yang diizinkan.

Kebijakan itu mengindikasikan perlindungan privasi nasabah tak cuma berkaitan dengan data keuangan kepunyaannya, namun juga terkait dengan data personal nasabah yang sifatnya informasi juga keterangan yang menjelaskan identitas pribadi lain slain atas keuangan. Transformasi cukup ekstrim muncul sejalan dengan adanya UU No. 21 th 2011 mengenai OJK, yang punya kedudukan dalam pengawasan kepada semua implementor jasa keuangan, di dalamnya juga ada perbankan yang awalnya diberi pengawasan oleh bank sentral.

Pengawasan ini juga terdiri atas sifat rahasia nya data pribadi nasabah. Aturan ini lalu diricuhi lagi atas Peraturan OJK No. 1/POJK.07 th 2013 mengenai Pelindungan Konsumen Sektor Jasa Keuangan, yang dalam poin Pasal 2 (d) menjelaskan bahwasanya prinsip dasar perlindungan konsumen yang wajib OJK kelola yakni berdasar pada prinsip rahasia dan aman nya data dari konsumen. Terlebih, POJK ini termuat juga bahasan

khusus yang mengelola terkait pengawasan perlindungan konsumen bagian jasa keuangan semuanya ada di kewenangan OJK.

OJK malah secara lebih mendalam mengatur atas daftar data juga informasi personal konsumen yang wajib di rahasiakan lewat SE OJK Nomor 14/SEOJK.07/ th 2014 mengenai Kerahasiaan dan Keamanan Data Informasi Pribadi Konsumen, berwujud sata diri pribadi, sampai dengan tatanan direksi dan komisaris juga berkas identitas berwujud KTP/Paspor/ dan yang serupa atau yang bisa menggantikannya.

Kemudian, menanggapi majunya layanan digitalisasi finansial, yang juga dibarengi dengan implementasi penyatuan dan permintaan data pribadi pengguna nya, OJK juga suah menerbitkan 2 kebijakan: (i) POJK terkait dengan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (LPMUBTI); juga (ii) POJK mengenai Inovasi Keuangan Digital di Sektor Jasa Keuangan. Kemudian, pada cakupan perpajakan, muncul tumpang tindih pendapat sejalan dengan adanya UU No. 11 th 2016 mengenai Pengampunan Pajak, dan adanya juga Peraturan Pengganti UU No. 1 th 2017 mengenai Akses Informasi Keuangan untuk Kepentingan Perpajakan (UU No. 9/2017). Tumbang tindih pendapat ini ada khususnya berketerikatan dengan cakupan informasi perpajakan, juga kewenangan otoritas pajak dalam memasuki dan memanfaatkan keterangan rekening wajib pajak.

#### **(4) Perdagangan dan Perindustrian**

Pada cakupan perdagangan, selain mengupas persoalan transaksi elektronik, yang sudah dikelola di UU ITE dan PP PSTE, perlindungan data pribadi juga dekat keterikatannya dengan UU No. 8/1997 mengenai Dokumen Perusahaan, UU No. 8/1999 mengenai Perlindungan Konsumen, dan UU No. 7/2014 mengenai Perdagangan. Namun, UU Perlindungan Konsumen belum dengan menyeluruh atau mendetail menuliskan perlindungan data pribadi, menjadi elemen dari hak-hak dari konsumen, yang wajib disodorkan perlindungan oleh pengusaha atau produsen. UU Pelindungan Konsumen malah lebih memfokuskan pada adanya keterangan yang jelas untuk konsumen, yang dipaparkan oleh produsen. Juga pada UU Perdagangan tak dengan tegas memberikan aturan tentang tanggung jawab perlindungan data pribadi (konsumen). (Kristiyanti, 2022).

Meskipun begitu, pada aturan Pasal 65 ayat (3) UU dijelaskan bahwasanya dalam perdagangan yang memakai sistem digital, masing-masing pihak yang melakukan transaksi wajib berpedoman pada aturan yang sah dalam UU ITE. Maksudnya, aturan terkait perlindungan data pribadi juga mejerat semuanya dalam perdagangan yang memakai sistem digital. Oleh sebab itu, penyusunan peraturan pemerintah terkait dengan perdagangan lewat sistem elektronik yang diamaantkan oleh Pasal 66 UU Perdagangan, seharusnya juga mengelola terkait perlindungan data pribadi konsumen, dengan berlandaskan pada aturan UU yang ada, terkhusus pada UU ITE dan UU Perlindungan Konsumen.

#### **(5) Layanan Kesehatan**

Perlindungan data pribadi dalam implementasi layanan kesehatan, di tingkatan aturannya bisa dibilang telah menyeluruh. Perlindungan ini khususnya berkaitan dengan data rekam medis pasien, yang dari mulanya dikatakan oleh UU No. 29 th 2004 mengenai Praktik Kedokteran, sudah dikelompokkan menjadi data yang wajib disodorkan perlindungan atas kerahasiaan nya. Pun juga pada UU No. 36 th 2009 mengenai Kesehatan, juga sudah dikelola tentang tanggung jawab guna memberikan perlindungan data pribadi seseorang. Penegasan itu pula dikelola pada UU Rumah Sakit yakni UU No.

44 th 2009, UU Kesehatan Jiwa yakni UU Nomor 18 th 2014, UU Tenaga Kesehatan yakni UU Nomor 36 th 2014, UU Keperawatan yakni UU Nomor 38 th 2014. Serta pada UU Nomor 35 th 2009 mengenai Narkotika sudah memberikan jaminan atas perlindungan data pribadi.

Secara teknis guna menjalankan sejumlah UU tersebut, Kemenkes juga sudah membentuk banyak kebijakan, terkhusus mengenai rekam medis, sistem informasi RS, tanggung jawab RS dan pasien, juga sebagainya. Berdasar atas aturan Pasal 52 ayat (2) UU Kesehatan, tenkes dalam menjalankan kewajibannya harus patuh pada standar profesi dan memberikan penghormatan atas hak pasien. Salah satu wujud hormat itu ditujukan pada hak atas informasi kesehatan personal nya.

Hal itu dituliskan pada Pasal 57 ayat (1) UU tersebut menyatakan bahwasanya hak orang atas rahasia keadaan fisik pribadinya yang sudah dijelaskan kepada implementor atau tenaga pelayanan kesehatan. Walau muncul pengakuan hak pasien menjadi jaminan perlindungan atas data personalnya yang berujud riwayat kesehatan, akan tetapi UU Kesehatan ini tak mengelola sepenuhnya terkait dengan tata cara e pemulihan untuk pemegang hak atas penyelewengan tindakan kepada perlindungan data pribadi pasien itu. Pada UU ini tak ditemui aturan sanksi atau vonis, baik secara administrasi ataupun pidana, teruntuk pengingkaran privasi atas riwayat kesehatan pasien tersebut.. (Fakih & Yulia, 2018).

#### **(6) Keamanan dan Penegakan Hukum**

Dalam cakupan pertahanan dan keamanan, pembahasan terkait dengan perlindungan data pribadi lebih berketerikatan dengan dispensasi dari aparat penegak hukum, guna menyalin interaksi personal seseorang, melihat dan menyebarkan data pribadi seseorang, juga dalam menjalankan tindakan profiling, dan membuka rekening seseorang. Dispensasi dan wewenang dari penegak hukum/intelijen guna menjalankan beberapa upaya di atas bisa ditemui di dalam UU No. 8 th 1981 mengenai KUHAP, UU No. 31 th 1999 mengenai Pemberantasan Tipikor, UU No. 30 th 2002 mengenai KPK, UU No. 21 th 2007 mengenai Pemberantasan Tindak Pidana Perdagangan Orang, UU No. 8 th 2010 mengenai Pemberantasan Tindak Pidana Pencucian Uang, UU Nomor 17 th 2011 tentang BIN, UU No. 18 th 2011 mengenai KY, UU No. 9 th 2013 mengenai Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, UU Nomor 5 th 2018 mengenai Pemberantasan Tindak Pidana Terorisme

### **KESIMPULAN**

Sebuah konsepsi hukum perlindungan kepada privasi orang memang baru muncul berbarengan dengan kemunculan aturan UU kolonial, terkhusus se-usai diberlakukannya KUHPerdara pada 1848, juga KUHP di th 1915, oleh pemerintah kolonial Hindia Belanda. Dalam perjalanannya, terkhusus setelah amandemen UUD 1945, hak atas privasi yang di dalamnya juga mencakup perlindungan data pribadi dibenarkan menjadi sebuah hak konstitusional masyarakat Indonesia. Hal ini senada dengan masuknya bab khusus mengenai HAM dalam konstitusi *output* amandemen.

Keikutsertaan Indonesia menjadi negara pihak dari *International Covenant on Civil and Political Rights* yang dituliskan dalam UU No. 12 th 2005, juga mempertegas bahwasanya tugas tanggung jawab pemerintah Indonesia guna memberikan perlindungan privasi dan data personal warganya. Pada tahapan yang lebih rinci, juga muncul beberapa aturan UU yang dijalankan dan sah saat ini, yang punya keterikatan atau dalamnya muncul bahasan yang terkait dengan data pribadi. Beberapa aturan UU itu bisa

digolongkan jadi beberapa sektor, yakni: (1) telekomunikasi dan informatika; (2) kependudukan dan kearsipan; (3) keuangan, perbankan, dan perpajakan; (4) perdagangan dan industri; (5) layanan kesehatan; dan (6) keamanan dan penegakan hukum.

#### DAFTAR PUSTAKA

- Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, S. (2015). *Application of big data for national security: a practitioner's guide to emerging technologies*. Butterworth-Heinemann.
- Fakih, M., & Yulia KM, Y. (2018). Tanggung Jawab Dokter Dan Tenaga Kesehatan dalam Pelayanan pasien Hemodialisis. *Pactum Law Journal*, 1(04), 419-433.
- Febriana, B., & Geraldo, M. (2021). Urgensi Perlindungan Hukum bagi Konsumen Peer to Peer (P2P) Lending di Indonesia. *Jurnal Education and Development*, 9(4), 197-204.
- Gärtner, B., & Hiebl, M. R. (2017). Issues with big data. In *The Routledge companion to accounting information systems* (pp. 161-172). Routledge.
- Goes, P. B. (2014). Big Data and IS Research, *MIS Quarterly* Vol. 38 No. 3 pp. iii-viii
- Hadi, S. (1995) *Metodologi Research Jilid 3. Metodologi Research Jilid 3*. Yogyakarta: Andi Offset
- Husein, Y. (2010). *Rahasia Bank dan Penegakan Hukum*. Pustaka Juanda Tigalima.
- Ichsan, R. N., SE, M., Sarman Sinaga, S. E., & Lukman Nasution, S. E. I. (2020). *Penyelesaian Masalah Bisnis Dalam Transaksi Elektronik (E-Commerce)*. CV. Sentosa Deli Mandiri.
- Inness, J. C. (1996). *Privacy, intimacy, and isolation*. Oxford University Press on Demand.
- Khairani, A., & Irwansyah, I. (2018). Pemanfaatan Big Data Untuk Percepatan Proses Underwriting Sebagai Strategi Komunikasi Marketing Terpadu Perusahaan Asuransi Jiwa. *Jurnal Nomosleca*, 4(2).
- Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big data & society*, 1(1), 2053951714528481.
- Kristiyanti, C. T. S. (2022). *Hukum perlindungan konsumen*. Sinar Grafika.
- Lukács, A. (2016). What is privacy? The history and definition of privacy.
- Mantra, I, B (2008). *Filsafat Penelitian dan Metode Penelitian Sosial*. Yogyakarta: Pustaka Pelajar.
- Manovich, L. (2011). Trending: The promises and the challenges of big social data. *Debates in the digital humanities*, 2(1), 460-475.
- Mcafee, A., & Brynjolfsson, E. (2012). Big Data: The management revolution. *Harvard Business Review*, 90(10), 60-6, 68, 128.
- Prosser, W. L. (1960). Privacy, 48 Calif. L. Rev, 383(10.2307), 3478805383.
- Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, 11(2), 285-299.
- Salsabila, R., Hosen, M., & Manik, H. (2022). Perlindungan Hukum Kerahasiaan Data Pribadi Konsumen Pengguna Produk Provider Telekomunikasi di Indonesia. *Zaaken: Journal of Civil and Business Law*, 3(1), 65-75.
- Sartika, I. K. (2019). Perbandingan Pengaturan Rahasia Bank antara Indonesia dan Singapura. *Acta Comitas: Jurnal Hukum Kenotariatan*, 4(3), 409-420.
- Schwab, Klaus (2017) *The Fourth Industrial Revolution*, Redfem: Currency Press

- Warren, S. (1890). Louis Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.
- Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10(9), 533-537.