# BAB IX
# PERLINDUNGAN DATA PENGGUNA INTERNET: MENELAAH GDPR UNI EROPA

**Agus Sudibyo**[1]

Pernahkah membayangkan fungsi penerangan, pendingin ruangan, ventilasi, mesin cuci, penyedot debu, penyaring udara, alat pemasak dan perangkat lain di rumah anda dapat dikendalikan dengan telephon-pintar yang anda genggam? Pernahkah membayangkan dengan jaringan Wi-Fi yang memadai, semua fungsi tersebut bahkan dapat diatur secara jarak jauh dari tempat kerja anda? Teknologi yang disebut *home automation* ini perlahan akan sampai ke Indonesia. Perusahaan digital semacam *Microsoft, Cisco* dan *Schneider Electric* sedang dan terus mengembangkannya hingga skala industrial dan akan dipasarkan secara global.

Kita sedang berada pada fase sejarah di mana digitalisasi menyentuh hampir semua aspek kehidupan. Pengembangan teknologi komputasi telah mencapai tahap di mana internet mampu menyambungkan hampir semua perangkat fisik dan non-fisik dalam suatu jaringan terintegrasi sehingga memudahkan pengoperasiannya. Dalam hidup masyarakat urban saat ini, internet adalah segala sesuatu dan segala sesuatu adalah internet. Tepat sekali ketika tahun 1999, Kevin Ashton, pendiri Auto-ID Center Massachusetts Institutes of Technology memperkenalkan istilah *Internet of Things* (*IoT*) untuk memprediksi apa yang akan terjadi kemudian.

Seluruh perangkat atau obyek yang berdimensi fisik maupun non fisik dalam hidup kita semakin terintegrasi ke dalam jaringan informasi digital pada skala rumah-tangga, organisasi, perusahaan, nasional maupun global. Sejauh terhubung dengan internet, peralatan maupun aktivitas kita dapat dikendalikan dari jarak jauh melalui jaringan informasi yang disediakan perusahaan-perusahaan digital. Dalam konteks inilah terbentuk sistem siber-fisik yang mencakup aplikasi serentak teknologi digital dalam wujud instalasi listrik cerdas *(smartgrid*), rumah cerdas (*home automation*), mobil pintar (*smartcar*) hingga kota cerdas (*smartcity*).

Apa yang ditawarkan *IoT* di sini jelas sekali efektivitas dan efisiensi. ABI Research memperkirakan jaringan *IoT* sudah menyambungkan 30 milyar perangkat keras dan perangkat lunak di seluruh dunia pada 2020. Ketika otomatisasi dan integrasi digital dapat diwujudkan pada hampir seluruh bidang kehidupan, yang kita dapatkan adalah kemudahan dan kepraktisan. Semakin banyak waktu yang dapat dihemat untuk menjalankan berbagai aktivitas dan semakin sedikit tenaga dan biaya yang dikeluarkan. Terjadi alih-daya digital secara massif dan banyak jenis pekerjaan yang semula dikerjakan manusia perlahan diambil-alih oleh mesin, komputer atau aplikasi digital. Semakin berkurang biaya yang kita keluarkan untuk membayar pembantu rumah tangga, sopir, teknisi listrik, teller bank, pegawai kebersihan dan lain-lain.

[1] Anggota Dewan Pers 2019-2020; Tulisan ini merupakan Bab IX dari buku Agus Sudibyo, *Jagat Digital, Pembebasan dan Penguasaan*, Sambutan: Rudiantara, Kata Pengantar: Sony Subrata, Kepustakaan Populer Gramedia, Jakarta, 2019.

Salah satu kunci dalam *IoT* adalah kapasitas penyimpanan data. Keberhasilan menghubungkan sekian banyak perangkat lunak dan keras di seluruh dunia ditentukan oleh kapasitas penyimpanan dan pengolahan data yang dimiliki perusahaan-perusahaan digital. Konsep *IoT* di sini berkaitan erat dengan konsep *cloud of thing*. *Cloud* adalah metafor baru untuk menggambarkan semakin canggihnya proses pengumpulan, penataan, penyimpanan dan pengolahan data yang dihasilkan dari rekayasa teknologi computer. Dalam konteks ini, semakin kurang dibutuhkan instrumen fisik penyimpan data seperti *harddisk, flashdisk* atau *server* pribadi. Layanan internet populer seperti *Facebook, Google, Twitter* menerapkan sistem baru yang memungkinkan penggunanya menyimpan data secara nir-ruang-fisikal. Perusahaan digital itu "meminjamkan" *server* raksasa untuk digunakan secara kolektif sehingga pengguna aplikasi digital tak lagi direpotkan untuk menyimpan data dan informasi dalam disk atau server pribadi.

Namun server raksasa ini sesungguhnya tidak disediakan secara cuma-cuma. Ketika telah tersimpan dalam server raksasa, data dan informasi pribadi tidak lagi sepenuhnya merupakan properti pribadi, tetapi telah menjadi properti umum, katakanlah dengan nama *big-data*. Istilah *cloud* merujuk pada kumpulan data digital yang besarannya hampir tak terhingga dan dapat dimanfaatkan siapa saja. Secara faktual yang pertama-tama memanfaatkannya bahkan melakukan rekayasa atasnya adalah perusahaan pemilik "server raksasa" itu: *Amazon, Google, Facebook, Twitter, Alibaba, Yahoo*.

### IX.1. Pengendalian Arus Data Digital

Masalah yang mengemuka kemudian adalah perlindungan privasi. Apakah data pribadi para pengguna internet merupakan privasi yang dilindungi? Jangan-jangan ada pihak yang diam-diam memanfaatkannya, seperti perusahaan penyedia layanan digital yang mengembangkan dan mengomodifikasi *IoT* dan teknologi *cloud*? Jangan-jangan pemanfaatan itu terjadi dalam konteks mobilisasi, komodifikasi, manipulasi bahkan kejahatan digital? Telah disinggung dalam **"Bab Surveillance Capitalism"**, Philip N. Howard, guru besar Universitas Oxford, mengingatkan *IoT* menawarkan potensi besar pemberdayaan masyarakat, transparansi dan akuntabilitas penyelenggaraan kekuasaan serta partisipasi politik, tetapi juga membawa masalah serius penerabasan privasi, rekayasa sosial serta manipulasi perilaku masyarakat.[2]

Howard mengingatkan fenomena digitalisasi global ditandai dengan munculnya koalisi antara kekuatan negara dan perusahaan-perusahaan teknologi untuk menguasai jaringan infrastruktur informasi global berikut pemanfaatannya pada berbagai bidang. Howard menggunakan istilah *pax technical* untuk menjelaskan keadaan digitalisasi global di mana sedikit aktor dominan -- pemerintah dan perusahaan platform digital Amerika Serikat seperti direpresentasikan oleh Sillicon Valey-- berkolaborasi dan saling menyokong kekuatan dan kepentingan masing-masing melalui konsensus berskala dunia sebagaimana termaktup dalam konsep seperti "*defense pacts, design collaborations, standards setting, data mining*."[3]

Digitalisasi global yang menyentuh semua aspek kehidupan masyarakat seperti terangkum dalam istilah "*internet interregnum*" membawa kabar baik sekaligus kabar buruk. Masyarakat di satu sisi memiliki sarana baru yang dapat membuat hidup menjadi lebih produktif, efisien dan

[2] Philip N. Howard, *Pax Technica: How the Internet of Things May Lock Us Up or Set Us Free*, 2015, Yale University Press, hlm. 32.

[3] Howard, "Pax Technica…". hlm. xx. Pembahasan yang sama dapat ditemukan dalam "**Bab Geopolitik Digitalisasi"**.

kreatif. Internet, khususnya media-sosial, juga telah terbukti menjadi sarana yang efektif untuk melawan rejim represif atau untuk berbagi informasi kritis tentang penyelenggaraan kekuasaan. Para aktivis demokrasi menggunakan telephon-pintar untuk mengorganisir kekuatan melawan rezim otoriter selama periode Arab Spring. Howard menunjukkan bagaimana penerapan *big-data analysis* juga sangat membantu kebutuhan pemetaan bahaya gempa bumi dan proses penanganannya di Haiti, pemetaan masalah perkampungan miskin perkotaan di Kenya, sarana berbagi informasi tentang secara *real time* tentang persebaran obat-terlarang di Meksiko, serta sarana investigasi korupsi gaji pegawai negeri di Afghanistan.

Namun, Howard mengingatkan sisi yang sebaliknya. Rezim otoriter maupun rezim demokratik sama-sama menggunakan teknologi berbasis internet untuk kebutuhan *surveillance* dan propaganda. Mereka menggunakan produk kecerdasan-buatan dan media-sosial untuk mengawasi, menghalangi atau mendinginkan wacana publik yang bersifat kritis. Rezim Bashar al-Assad di Suriah menggunakan perangkat *counterinsurgency* (yang antara lain diproduksi oleh perusahaan teknologi Barat) untuk mematai-matai pergerakan kelompok anti pemerintah, menggunakan robot Twitter otomatif untuk mendelegitimasi kelompok anti pemerintah, serta membanjiri *newsfeeds* tentang Suriah dengan pesan-pesan pro Rezim Bashar al-Assad. Selain itu, meskipun bekerja-sama dalam beberapa hal, tidak seterusnya pemerintah Amerika Serikat dan perusahaan teknologi Amerika Serikat berjalan seiring. *Apple* berselisih dengan FBI tentang proses enskripsi pada perangkat iPhone. *Facebook* diadili Senat Amerika Serikat karena dianggap membiarkan infiltrasi Russia dalam Pilpres 2016 melalui platform media-sosial yang dioperasikan *Facebook*.

Howard mengingatkan, aliran data pribadi pengguna internet terus terjadi ke perusahaan-perusahaan penyedia layanan digital (media-sosial, mesin-pencari, *ecommerce* dan lain-lain) -- sejauh pengguna internet aktif menggunakan layanan-layanan itu. Hal semestinya membuat masyarakat semakin hati-hati dan membatasi diri dalam konsumsi internet. *IoT* tanpa banyak disadari telah memberikan peluang –dalam skala yang belum pernah terjadi sebelumnya-- pengawasan dan pengendalian terhadap masyarakat kepada pemerintah, lembaga intelijen negara atau swasta dan tentu saja perusahaan-perusahaan platform digital. Howard sangat menyarankan agar masyarakat lebih berhati-hati dan waspada dalam mengonsumsi layanan-layanan internet.

Bagaimana *IoT* dan *cloud* of things memberi dampak eksesif untuk kehidupan publik juga dibahas dalam kaitannya dengan konsep *panopticon society.* Dalam buku *Discipline and Punish: The Birth of the Prison* (1975), Foucault menjelaskan bagaimana berbagai teknologi yang lahir sejak era industri dan yang secara kasat-mata mempermudah kehidupan manusia, sebenarnya juga menjadi sarana untuk mengontrol dan mengendalikan masyarakat. Esensi kekuasaan menurut Foucault bukan hanya kemampuan memaksakan kekerasan, tetapi juga kemampuan untuk mengawasi masyarakat tanpa diawasi masyarakat (*to-see-without-being-seen*), untuk memantau gerak-gerik masyarakat tanpa hal yang sebaliknya (*to have knowledge of the others that the others could never obtain*). Seperti telah dibahas dalam **"Bab Surveillance Capitalism",** masyarakat sebagai obyek pengawasan terus-menerus itu disebut –menggunakan istilah Jeremy Bentham-- sebagai *panopticon society*.

Perkembangan teknologi internet sebagaimana terangkum dalam istilah *internet of things* dalam beberapa aspek dianggap meradikalkan konsep *panopticon society* ini. Ketika hampir semua bagian dari hidup kita terhubung dengan jaringan internet, sesungguhnya internet itu juga

merupakan sarana bagi perusahaan-perusahaan digital dan agen-agen intelijen untuk mengawasi dan mencatat gerak-gerik kita. Ketika menceburkan diri dalam lanskap komunikasi-informasi digital, sesungguhnya kita sedang hidup dalam situasi *panopticon*. Hidup dalam sistem pengawasan dan kendali perusahaan penyedia layanan *IoT* atau *cloud*. Hidup yang menjadi obyek *surveillance capitalism* sedemikian rupa sehingga kita harus berpikir ulang tentang privasi. Bagaimana berbicara tentang privasi ketika tiba-tiba iklan digital memasuki email pribadi atau telephon-pintar kita tanpa permisi? Bagaimana berbicara tentang privasi jika *Facebook* dan *Google* mengetahui siapa diri kita, dengan siapa kita berteman, sedang butuh apa kita, bagaimana pandangan politik kita dan seterusnya?

Dalam konteks inilah para ahli komunikasi merisaukan potensi *IoT* dalam mengikis kendali manusia atas dirinya sendiri. Kendali itu dengan cepat dan tanpa disadari telah beralih ke tangan perusahaan-perusahaan digital beserta lembaga pemerintah dan perusahaan lain yang memanfaatkan layanan perusahaan digital itu. Seperti diuraikan Geoff Webb dalam artikelnya berjudul "Say Goodbye to Privacy", penerapan *IoT* dan analisis *big data* membuat masyarakat semakin sulit mengendalikan kehidupannya sendiri seiring dengan semakin terbukanya akses perusahaan-perusahaan digital ke kehidupan setiap orang secara langsung dan *real time*.[4]

## IX.2. GDPR Uni Eropa

Dalam konteks yang sama lahir *General Data Protection Regulation* (GDPR). Disepakati Parlemen Uni Eropa 27 April 2016, GDPR adalah undang-undang yang mengatur perlindungan data pribadi penduduk atau warga Uni Eropa yang berada di dalam maupun di luar Uni Eropa, serta yang dikelola pihak mana pun di dalam maupun di luar teritori Uni Eropa. Berlandaskan pada Piagam Hak Asasi Uni Eropa yang menetapkan "warga Uni Eropa memiliki hak untuk melindungi data pribadi masing-masing", GDPR menjadi instrumen utama harmonisasi hukum perlindungan data di seluruh negara anggota Uni Eropa. Hal yang mesti digarisbawahi, regulasi ini juga mengikat semua pihak di mana saja yang mengumpulkan, memproses dan memanfaatkan data pribadi penduduk atau warga Uni Eropa. Melalui pengaturan yang ketat dan ketentuan denda yang besar, GDPR dengan tegas menyatakan setiap orang berdaulat atas perlindungan data pribadi masing-masing di hadapan pihak mana pun. Setiap orang di sini mencakup setiap orang yang bertempat tinggal di Uni Eropa, baik yang berstatus warga negara atau bukan. Obyek pengaturan GDPR mencakup orang, perusahaan, organisasi dan lembaga pemerintah Eropa di seluruh dunia yang memproses dan memanfaatkan data pribadi semua orang yang bertempat tinggal di Uni Eropa. Berfungsi menggantikan Undang-Undang Perlindungan Data Uni Eropa (*EU Data Protection Directive*) Tahun 1995, GDPR mulai berlaku 25 Mei 2018.

GDPR dilatarbelakangi perkembangan digitalisasi global yang telah melahirkan persoalan serius bagi perlindungan privasi dan keamanan diri pengguna internet sebagaimana telah dijelaskan di atas. Proses pengumpulan, pengolahan dan pemanfaatan data pribadi pengguna internet oleh perusahaan-perusahaan penyedia berbagai layanan digital telah meningkat tajam dan mencapai skala yang nyaris tak terhingga. Perusahaan tersebut dan juga lembaga-lembaga

[4] Geoff Webb, "Say Goodbye to Privacy", 15/02/2015, *https://www.wired.com/insights/2015/02/say-goodbye-to-privacy/,* diakses 04/05/2017.

intelijen memiliki teknologi untuk memanfaatkan dan merekayasa data pribadi pengguna internet untuk berbagai kebutuhan. Di sisi lain, pemahaman masyarakat pengguna internet terhadap proses yang terjadi antara dirinya dengan perusahaan-perusahaan penyedia layanan internet tidak berjalan seiring dengan derasnya arus data yang berhasil ditambang dari layanan-layanan itu.

Ketika layanan teknologi *cloud* dan *internet of things* semakin populer dan merambah aspek-aspek kehidupan yang lebih luas dan dalam, masyarakat tetap saja tidak mengetahui secara persis bagaimana persisnya teknologi itu bekerja dan apa konsekuensinya. Tak ada lagi garis demarkasi antara yang berada dalam genggaman (komputer desktop, laptop, telephon-pintar) dengan yang jauh dan laten (*cloud system, machine learning*). Keduanya menempel satu sama lain membuat buram batas antara yang bersifat privat dalam diri pengguna layanan digital dan yang bersifat publik sebagaimana diolah para operator layanan tersebut.[5] Dalam konteks inilah, kewaspadaan pada setiap penjelasan, pemberitahuan, permintaan persetujuan, boks verifikasi dan tombol-tombol "otomatis" yang mesti kita klik sebelum kita menggunakan layanan atau fitur digital tertentu sangat menentukan sejauhmana kita dapat menjaga privasi kita.

Dalam rangka merespon perkembangan tersebut, dilakukan upaya terus-menerus memperbarui hukum perlindungan data pribadi. Hal ini mencakup pengaturan tentang proses pengumpulan, kepemilikan, pengolahan, pemanfaatan dan pemindahan informasi pribadi baik secara *offline* dan terutama sekali secara *online*. Dasar acuannya adalah perlindungan individu atas privasi dan keselamatan diri seperti termaktub dalam Konvensi Eropa untuk Hak Asasi Manusia dan Piagam Hak Asasi Uni Eropa. Negara-negara anggota Uni Eropa, pada skala yang berbeda, juga telah melembagakan GDPR. GDPR menjadi sarana pembaharuan dan harmonisasi kerangka kerja dalam melindungi data pribadi di seluruh Uni Eropa.

GDPR secara rinci merumuskan beberapa kewajiban baru yang lebih ketat dan penuh konsekuensi untuk pihak-pihak yang mengelola data pribadi penduduk atau warga Uni Eropa dan sebaliknya menyematkan hak-hak baru bagi penduduk atau warga Uni Eropa sebagai pemilik data pribadi. Salah satu prinsip yang digunakan di sini adalah --sebagaimana telah dibahas dalam Bab *Data As Labor*-- data-perilaku-pengguna-internet (*user-behavior-data*) pada dasarnya adalah milik individu pengguna internet. Bagaimana dan sejauhmana pemanfaatan data itu, mesti senantiasa pertama-tama merujuk pada kepentingan pengguna internet dan tidak sebaliknya, justru berada di luar pengetahuan pengguna internet bahkan merugikan mereka.

GDPR diproyeksikan sebagai model regulasi perlindungan data pribadi pengguna internet di tengah-tengah trend semakin besarnya kendali perusahaan platform digital (media-sosial, mesin pencari, *ecommerce* dan lain-lain) terhadap data tersebut untuk kebutuhan iklan digital tertarget, pengembangan produk kecerdasan-buatan dan proses *machine learning*. Sejak Mei 2018, setiap orang, lembaga, perusahaan, organisasi yang melakukan proses pengumpulan, analisis dan komodifikasi –sebagian atau seluruhnya-- atas data-perilaku-pengguna-internet penduduk atau warga Uni Eropa terikat untuk menaati batasan-batasan dalam GDPR.

[5] Wawancara Lukasz Olejnik, peneliti tentang *cybersecurity* dan perlindungan privasi yang menggeluti permasalahan GDPR, Jenewa, 22/12/2018.

GDPR memiliki kedudukan strategis dalam upaya pengarusutamaan (*mainstreaming*) hukum perlindungan data pribadi secara global. Tak lama setelah GDPR diundangkan, banyak organisasi atau perusahaan mulai memperbaiki sistem pengolahan data yang mereka miliki. Tidak sedikit dari mereka yang membayar jasa *Data Protection Officers* untuk memastikan ketaatan dan kesesuaian proses penyimpanan dan pelayanan data yang mereka kelola terhadap standar-standar GDPR. Untuk urusan ini, GDPR telah mempublikasikan dokumen resmi tentang panduan pelaksanaan GDPR untuk sektor bisnis. Hal ini dimaksudkan sebagai solusi atas masalah bahwa entitas yang berbeda (bisnis, sosial, pemerintahan) akan melahirkan standard yang berbeda lupa dalam pengolahan data, tujuan dan problem yang muncul dalam pengolahan data, serta proses audit yang dibutuhkan. Berbeda negara dapat berbeda pula regulasi yang mengatur standard dan model pengolahan data, berikut proses audit, pengawasan dan bentuk penegakan hukumnya.[6]

Meskipun pada awalnya cenderung menolak atau keberatan, perusahaan seperti *Google, Amazon, Facebook, Apple* dan *Microsoft* pada akhirnya juga tidak memiliki opsi lain selain melaksanakan GDPR. Bahkan muncul indikasi mereka justru hendak mengadopsi GDRP Uni Eropa sebagai standar perlindungan data-perilaku-pengguna-internet secara lebih luas. Paling tidak dua pertimbangan mendasari langkah ini. *Pertama*, Uni Eropa bagaimana pun adalah pasar utama mereka perusahaan raksasa digital itu. Menolak GDPR dalam hal ini akan mengoreksi pendapatan atau potensi pendapatan yang signifikan dari perusahaan-perusahaan tersebut. *Kedua*, akan sangat merepotkan jika perusahaan-perusahaan berskala global mesti menghadapi standar perlindungan data pribadi yang berbeda-beda di setiap negara. Lebih efektif dan efisien jika ada standar global tertentu dalam perlindungan data pribadi, betapa pun standar tersebut memberikan tanggung-jawab lebih besar pada perusahaan-perusahaan penyedia layanan digital.

## IX.3. Lingkup Pengaturan GDPR

Selanjutnya akan coba dipaparkan lingkup, isi dan bentuk pengaturan dalam GDPR. Pemaparan berikut ini didasarkan pada tinjauan berjudul "Preparing for the General Data Protection Regulation*"* yang disusun oleh Allen & Overy dan diterbitkan pada Januari 2018.[7]

### *IX.3.i. Siapa dan Apa Yang Harus Tunduk Pada GDPR?*

GDPR memiliki jangkauan yang lebih luas dibandingkan undang-undang perlindungan privasi atau perlindungan data yang ada sebelumnya, misalnya saja Undang-Undang Perlindungan Data Uni Eropa (*EU Data Protection Directive)* Tahun 1995. GDPR berlaku untuk organisasi atau perusahaan (baik sebagai Pengendali Data atau Pengolah Data) yang mengelola data pribadi (p*ersonal data*) dan yang dibentuk di Uni Eropa (Pasal 3 dan 4). Dalam beberapa

[6] Howard, "Pax Technica…". hlm. xxi.

[7] Allen & Overy, "Preparing for the General Data Protection Regulation*"*, Januari 2018, *http://www.allenovery.com/SiteCollectionDocuments/Preparing%20for%20GDPR%20compliance%20March%202018.PDF,* diakses 02/02/2019. Allen & Overy adalah lembaga konsultasi hukum internasional yang bekerja dan memiliki afiliasi di 44 negara di dunia. GDPR adalah salah sati focus kajian dan perhatian Allen & Overy.

keadaan, GDPR juga berlaku pada organisasi yang mengelola data pribadi dan dibentuk secara eksklusif di luar Uni Eropa. Ada tiga alasan utama penerapan GDPR yang dapat ditemukan dengan melakukan tiga uji berikut.

### *a. Uji Kedudukan Teritorial*

Jika sebuah perusahaan atau organisasi berkedudukan di teritori Uni Eropa dan mengelola data pribadi dalam konteks kegiatan atau operasional perusahaan atau organisasi tersebut, maka mereka harus tunduk pada GDPR. Tidak peduli di mana pengolahan data dilakukan (di Uni Eropa atau di luar Uni Eropa), apakah pengolahan dilakukan sendiri atau oleh pihak ketiga (seperti subkontraktor) atau apakah data pribadi yang diolah berkaitan dengan **Subyek Data** yang merupakan warga Uni Eropa atau yang "hanya" tinggal di Uni Eropa. Uji ini berfokus pada konsep *establishment* di Uni Eropa serta pengolahan yang dilakukan "dalam konteks kegiatan atau operasionalisasi" suatu organisasi atau perusahaan. Konsep *establishment* di sini diartikan secara luas oleh pengadilan dan merujuk pada entitas hukum yang menjalankan kegiatan yang nyata dan efektif secara langsung atau tidak langsung melalui pengaturan yang stabil, tanpa mempedulikan bentuk badan hukumnya. Dengan demikian, organisasi atau perusahaan yang memiliki perwakilan lokal, situs web atau alamat lokal di Uni Eropa mesti tunduk pada rezim GDPR.

### *b. Uji Penawaran Barang dan Jasa*

Apabila perangkat pengendali atau pengolah data tidak ditempatkan di Uni Eropa, GDPR juga akan berlaku jika sebuah organisasi atau perusahaan mengendalikan dan mengolah data terkait individu-individu yang berada di Uni Eropa (warga negara atau non warga negara) dan pengolahan ini terkait dengan salah satu dari dua hal berikut:

- Menawarkan barang atau jasa terhadap Subyek Data yang berada di Uni Eropa
- Memantau perilaku Subyek warga negara atau penduduk Uni Eropa.

Lokasi Subyek Data menjadi pertimbangan utama dalam GDPR, bukan status kewarganegaraan Subyek. Perlindungan data pribadi dalam GDPR tidak mengikat untuk pengolahan data warga negara Uni Eropa yang sedang berpergian ke luar Uni Eropa.

"Menawarkan barang dan jasa" di sini berlaku untuk pihak Pengendali Data atau Pengolah data yang terbukti menawarkan layanan barang atau jasa kepada Subyek Data di satu atau lebih dari negara anggota Uni Eropa. Dengan demikian, perusahaan *ecommerce* yang hanya menyediakan situs web yang dapat diakses dari dalam Uni Eropa saja belum terikat untuk mematuhi GDPR karena belum masuk dalam kategori "menawarkan barang atau jasa". Namun perlu diperhatikan, penggunaan bahasa atau mata uang lokal yang lazim digunakan di teritori Uni Eropa atau menyinggung konsumen yang bertempat tinggal di Uni Eropa, dapat memberi kesan bahwa barang atau jasa telah "ditawarkan" ke orang-orang di Uni Eropa oleh situs *ecommerce* tertentu. Dengan demikian, menghasilkan alasan untuk memberlakukan ketentuan dalam GDPR.

### *c. Uji Pemantauan Perilaku Digital*

Uji Pemantauan Perilaku Digital di sini mencakup uji untuk mengetahui apakah organisasi atau perusahaan penyedia layanan digital melakukan proses pemantauan (*surveillance*) atas perilaku dan sikap orang-orang melalui teknik pelacakan digital serta teknik *profiling* tertentu guna menghasilkan prediksi preferensi atau perilaku pribadi dari Subyek sebagai pengguna layanan internet.

Organisasi atau perusahaan yang tidak memiliki kedudukan di Uni Eropa, tetapi terjaring oleh uji-uji di atas diwajibkan menunjuk perwakilan di salah satu negara anggota Uni Eropa terkait. Mereka juga mesti menjelaskan langkah-langkah yang akan mereka lakukan untuk memenuhi standar GDPR terkait dengan kegiatan operasional mereka yang menghasilkan dampak sebagaimana terbukti dalam uji yang telah dilakukan.

GDPR menekankan posisi dan perbedaan antara Pengendali Data (*data controller)* dan Pengolah Data *(data processor)*. Tidak seperti Undang-Undang Perlindungan Data Uni Eropa (*EU Data Protection Directive*), GDPR berlaku baik untuk pihak Pengendali Data maupun Pengolah Data. Meskipun begitu, hanya sedikit ketentuan GDPR yang berlaku secara langsung kepada Pengolah Data. Sejumlah ketentuan berdampak secara tidak langsung pada posisi Pengolah data, yakni ketika Pengendali Data melalui mekanisme legal tertentu membagikan atau mendelegasikan tanggung jawab pengendalian data ke pihak Pengolah data.

GDPR juga menekankan pentingnya pengaturan soal **Pengolahan Data** (*data processing*). Sesuai dengan legislasi yang berlaku sebelum GDPR, Pengolahan data didefinisikan dengan sangat luas mencakup tindakan mengumpulkan, mengatur, menyimpan, mengubah, mengambil, menggunakan, memberitahukan dan menghapus data pribadi, di samping kegiatan-kegiatan lainnya. **Data Pribadi** (*personal data*) adalah semua informasi yang terkait dengan orang per orang yang dikenali atau dapat dikenali. Data ini dapat dikenali melalui rujukan pengenal seperti nama, nomor tanda pengenal, data lokasi atau pengenal daring, atau melalui faktor-faktor khas tentang diri pribadi seperti identitas fisik, data genetik, data biometrik, status ekonomi atau status sosial. GDPR juga memasukkan alamat IP serta informasi yang dapat diambil dari alamat IP sebagai data pribadi. GDPR sangat ketat dalam mendefinisikan dan mengatur perlindungan privasi ini, meskipun sanksi denda yang dapat diterapkan GDPR untuk pelanggarannya menurut beberapa pihak masih rendah dan dikhawatirkan belum menghasilkan efek jera.[8]

**Apa dampak dari Lingkup Pengaturan GDPR di atas?** Organisasi atau perusahaan di luar Uni Eropa harus memastikan keberadaan mereka berdasarkan Tiga Uji di atas, terutama "**Uji Penawaran Barang dan Jasa**" dan "**Uji Pemantauan Perilaku Digital**". Jika tidak lolos dari uji tersebut, mereka mesti segera mempertimbangkan beberapa solusi struktural. Misalnya dengan melarang pengunjung berdomisili di Uni Eropa untuk mengakses web atau layanan digital yang disediakan, menghindari penempatan *cookie* pada perangkat yang dioperasikan pengguna berdomisili di Uni Eropa. Hal ini untuk menghindari kewajiban memenuhi syarat-syarat GDPR terhadap entitas non Uni Eropa atau menghindari perluasan pemberlakuan standar GDPR ke luar teritori Uni Eropa. Organisasi atau perusahaan Pengolah Data mesti meninjau bagaimana mereka akan terdampak pemberlakuan GDPR serta memahami kewajiban hukum baru sekaligus perubahan sifat hubungan mereka dengan pihak Pengendali Data sebagai konsekuensi dari pemberlakuan GDPR.

[8] Wawancara Lukasz Olejnik……

### *IX.3.ii. Syarat Pengolahan Data (data processing)*

Pasal 6 GDPR menegaskan semua praktek pengolahan data pribadi mesti berdasarkan syarat yang sah. Meskipun bukan hal yang baru, di bawah GDPR hal ini lebih ditekankan dan menjadi lebih penting bagi Pengolah Data untuk memahami dan mencatat dasar-dasar pengolahan data. Untuk mengolah data pribadi secara hukum, Pengendali Data (dalam hal ini pihak yang menentukan tujuan dan cara pengolahan data pribadi) atau Pengolah Data harus memiliki setidaknya satu dari syarat sah berikut:

- ✓ Subyek Data telah memberikan persetujuan untuk pengolahan data dengan satu tujuan spesifik atau lebih (Pasal 7 dan 8)
- ✓ Pengolahan Data dilakukan dalam konteks menjalankan kontrak di mana Subyek Data adalah salah-satu pihak terkait atau dengan tujuan mengambil langkah-langkah pengolahan data sesuai permintaan Subyek Data sebelum memasuki sebuah kontrak.
- ✓ Pengolahan Data diperlukan untuk memenuhi kewajiban hukum tertentu di mana pihak Pengendali Data harus tunduk kepadanya.
- ✓ Pengolahan Data diperlukan untuk melindungi kepentingan utama Subyek Data.
- ✓ Pengolahan Data diperlukan untuk misi menjalankan kepentingan publik atau menjalankan otoritas resmi yang berada di tangan Pengendali Data.
- ✓ Pengolahan Data diperlukan untuk mewujudkan kepentingan yang sah Subyek Data atau pihak ketiga, kecuali jika kepentingan ini mengesampingkan hak fundamental dan kebebasan Subyek Data yang dilindungi menurut prinsip perlindungan data pribadi, terutama sekali jika Subyek Data adalah anak-anak.

Pihak Pengendali Data juga diwajibkan menyediakan catatan resmi terkait dengan pemenuhan syarat-syarat di atas. ***Apa konsekuensi Syarat Pengolahan Data di atas?*** Syarat pengolahan data untuk pihak Pengendali Data atau Pengolah Data di atas menjadi dasar perumusan hak Subyek Data. Berdasarkan syarat di atas, GDPR dapat menentukan apakah seorang individu memiliki hak keberatan terhadap pengolahan data pribadi atau terhadap pemanfaatan atau pemindahtanganan data tersebut, atau apakah keputusan dapat diambil secara arbitrer oleh pihak Pengendali Data terkait Subyek Data yang datanya ditambang melalui proses pengolahan pemrofilan otomatis yang sejauh ini lazim terjadi tanpa diketahui Subyek Data.

Syarat pengolahan data juga berdampak pada **Pengertian Persetujuan Subyek Data**. Kesalahpahaman umum yang sering muncul adalah persetujuan individu pemilik data mesti diperoleh untuk mengolah data individu secara sah berdasarkan hukum. Padahal, persetujuan umumnya bukanlah prasyarat untuk pengolahan, atau bukan pula alasan pembenar untuk kegiatan-kegiatan semacamnya yang dalam keadaan lain dianggap tidak sah. Persetujuan dibutuhkan untuk keperluan lain yang areanya lebih pada pemanfaatan data. Misalnya, di bawah Undang-Undang E-Privasi Uni Eropa, pengiriman pesan penjualan elektronik yang tidak diminta (melalui e-mail, media-sosial atau *whatsapp*) kepada seorang pengguna layanan internet memerlukan persetujuan khusus dari pengguna tersebut sebelumnya.

Syarat Pengolahan data juga berkaitan dengan pengertian **Kepentingan Yang Sah (*legitimate interests*)** untuk pengolahan data. **Kepentingan Yang Sah** khususnya dalam konteks

penggunaan data untuk kepentingan bisnis, di mana sebuah perusahaan wajib menjalankan kontrak kerja-sama tertentu atau memiliki hak menjalankan bisnis yang sah berdasarkan undang-undang tertentu. Perusahaan Pengendali Data perlu melakukan *assessment* apakah kepentingan mereka yang sah itu ternomorduakan oleh kepentingan, hak dan kebebasan individu yang di saat yang sama juga dilindungi oleh regulasi perlindungan data pribadi. Dengan demikian, aspek proporsionalitas dalam pengumpulan dan pengolahan data, ekspektasi individu pemilik data yang masuk akal dan hubungan mereka dengan pihak Pengendali Data mesti dipertimbangkan. Perusahaan atau organisasi Pengendali Data mesti menjalankan "penilaian seksama" terhadap pengolahan data yang mereka lakukan demi memastikan adanya keseimbangan yang semestinya antara **Kepentingan Yang Sah** dan **Hak Subyek Data.**

Perubahan yang signifikan dalam GDPR adalah jika Pengendali Data menggunakan argumentasi kepentingan yang sah untuk melandasi tindakan pengolahan data, hal ini mesti diungkapkan dan dijelaskan kepada Subyek Data, sebagai bagian dari informasi pengolahan yang adil dan transparan yang diberikan kepada individu dalam sebuah **Pemberitahuan Tentang Privasi.** Dalam melakukan ini, organisasi mesti melihat rentang kegiatan yang dilakukan dengan dasar kepentingan sah serta memastikan bahwa hal ini dimasukkan ke dalam "Pemberitahuan Tentang Privasi" tersebut. Apabila Pengendali Data ingin menggunakan data untuk tujuan lain, mereka mesti memastikan tujuan baru tersebut "sesuai" dengan tujuan awal pengolahan data, serta perlu melihat benar kaitan antara tujuan, kemungkinan konsekuensi dan keberadaan jaminan perlindungan privasi.

### *IX.3.iii. Persetujuan Subyek Data*

Persetujuan Subyek pemilik data seperti diatur dalam Pasal 4, 6, 7 GDPR memiliki berbagai tujuan. Persetujuan itu memberi dasar yang sah bagi Pengendali Data untuk melakukan pengolahan data pribadi, melakukan pengolahan kategori-kategori data khusus, serta memberikan dasar atau koreksi atas pelarangan memindahkan data ke luar wilayah ekonomi Uni Eropa. Persetujuan juga penting sebagai syarat atas praktek pengiriman pesan pemasaran elektronik atau penempatan *cookies*. Namun, harus diakui lingkup dan kedalaman pengaturan **Persetujuan Subyek Data** dalam GDPR semakin sulit dilaksanakan dan dikhawatirkan beberapa pihak berdampak kontraproduktif terhadap bisnis digital jika mesti berpegang padanya sebagai dasar pegolahan data.

Meskipun **Persetujuan Subyek Data** dapat digunakan untuk mencapai tujuan-tujuan partikular pihak Pengendali Data sejauh diperoleh secara sah, berbagai syarat untuk memperoleh persetujuan itu telah diperketat sedemikian rupa di dalam GDPR. Bagi perusahaan penambang dan pengolah data-perilaku-pengguna-internet (*user behavior*), dengan demikian masalahnya bukan hanya bahwa mereka harus mendapatkan persetujuan dari pengguna untuk mengelola data pengguna, melainkan juga bagaimana cara mereka memperoleh persetujuan tersebut harus sesuai dengan syarat-syarat dalam GDPR.

Pada prinsipnya, perusahaan Pengendali Data harus menyediakan mekanisme yang memungkinkan penggunanya untuk dapat memberikan persetujuan penggunaan data secara bebas, sadar, transparan dan spesifik dalam tujuan dan konteks penggunaan.[9] Hal ini membuat

[9] Wawancara Lukasz Olejnik…….

persetujuan lebih sulit didapatkan dan dipertahankan, serta membutuhkan pendekatan yang berbeda bagi praktek penambangan data yang telah berlangsung. Apa saja syarat-syarat bagi persetujuan yang sah di bawah GDPR? Persetujuan harus mengindikasikan keinginan –bukan keterpaksaan-- Subyek Data, diberikan secara bebas dan sadar, terjadi dalam konteks yang spesifik dan diberitahukan dengan jelas. Persetujuan harus memenuhi syarat berikut:

- ✓ Permintaan Persetujuan Subyek Data yang diajukan pihak Pengendali Data harus dalam bentuk yang mudah dimengerti dan diakses, menggunakan bahasa yang jelas dan lugas.
- ✓ Permintaan persetujuan harus dibedakan secara jelas dan rinci dari urusan-urusan lain dalam hubungan antara Pengendali Data atau Pengolah Data dengan Subyek Data.
- ✓ Persetujuan yang diberikan Subyek Data harus mencerminkan tindakan afirmatif yang jelas.
- ✓ Jika data pribadi akan diproses untuk berbagai tujuan, persetujuan harus diberikan terpisah untuk setiap tujuan.
- ✓ Persetujuan tidak akan sah jika individu Subyek Data tidak memiliki pilihan bebas yang nyata atau jika ada halangan bagi Subyek Data untuk menolak atau mencabut persetujuan.
- ✓ Persetujuan dapat menjadi tidak sah jika ada masalah ketidakseimbangan relasi-kuasa yang nyata antara Pengendali Data atau Pengolah Data dengan Subyek Data.
- ✓ Persetujuan akan dianggap tidak sah jika menjadi syarat pelaksanaan sebuah kontrak tetapi sebenarnya tidak benar-benar dibutuhkan untuk pelaksanaan kontrak tersebut.
- ✓ Persetujuan harus dapat dicabut kapan pun dan harus mudah dicabut sebagaimana mudah diberikan.
- ✓ Individu Subyek Data harus mengetahui dengan sadar bahwa mereka memiliki hak mencabut persetujuan ketika mereka memberikan persetujuan itu pada awalnya.

Karena persetujuan harus diperoleh melalui tindakan yang nyata dan afirmatif, Pengendali Data tidak dapat lagi “bermain-main” dengan persetujuan yang diandaikan dan bersifat otomatis diberikan Subyek Data ketika mengakses layanan digital tertentu. Ketidakaktifan atau kediaman Subyek, adanya kotak persetujuan yang sudah atau tinggal dicentang (*pre-ticked box*) tidaklah memadai. Persetujuan mesti diperoleh melalui serangkaian tindakan yang sadar, bebas dan afirmatif. GDPR menyatakan bahwa tindakan yang nyata dan afirmatif Subyek Data mencakup tindakan mencentang kotak persetujuan secara langsung untuk menandakan persetujuan ketika mengunjungi situs web atau memilih pengaturan teknis tertentu.

***Persetujuan Subyek Data Dapat Dicabut.*** Persetujuan Subyek Data untuk proses pengendalian atau pengolahan data dapat dicabut setiap saat oleh Subyek Data. Setelah pencabutan ini, pihak Pengendali Data wajib menghentikan proses pengolahan data yang mungkin saja mencakup keharusan pembersihan data-data terkait, kecuali jika Pengendali Data memiliki dasar hukum lain untuk melanjutkan pengendalian atau pengolahan data. Menerapkan sistem dan proses untuk mengatur pencabutan persetujuan ini dengan semua konsekuensi yang mengikutinya membutuhkan investasi yang signifikan pada pihak perusahaan atau organisasi Pengendali Data.

***Persetujuan Subyek Data Tidak Dapat “Dianakcucukkan”.*** Persetujuan yang telah diberikan Subyek Data hanya berlaku untuk proses pengendalian atau pengolahan data yang

telah disepakati dan tidak untuk tujuan-tujuan berikutnya. Dengan demikian, persetujuan baru dari Subyek Data perlu diperoleh kembali apabila ada kebutuhan atau tujuan baru dalam pengolahan dan pengendalian data. *There is no 'grandfathering' of consents obtained before the GDPR applies.* Misalnya, dikarenakan banyak data pemasaran diperoleh dengan menerapkan kotak-kotak persetujuan yang sudah dicentang dan persetujuan yang bersifat implisit lainnya untuk melakukan pengolahan data di masa lalu, maka perusahaan perlu meminta persetujuan lagi dari Subyek Data jika ingin memanfaatkan data pemasaran itu. Jika permintaan persetujuan ditolak, data terkait dengan Subyek Data dalam gugus data pemasaran itu mesti dihapuskan.

Persetujuan senantiasa dibutuhkan untuk praktek mengirimkan pemasaran langsung kepada konsumen melalui e-mail atau SMS, kecuali jika pihak perusahaan telah memiliki hubungan atau perjanjian dengan Subyek Data sehingga perusahaan memiliki legitimasi untuk menerapkan apa yang disebut sebagai pengecualian "kontak lunak (*soft opt-in*)".

***Apa dampak dari pengaturan Persetujuan Subyek Data dalam GDPR?***

- Perusahaan pengendali atau pengolah pribadi harus memahami benar kapan dan dalam konteks apa mereka membutuhkan Persetujuan Subyek Data untuk mengelola data pribadi mereka.
- Perusahaan tersebut wajib menyediakan mekanisme yang memungkinkan Subyek Data memberikan persetujuan secara bebas, sadar, transparan, dalam maksud dan konteks yang spesifik. Mekanisme itu harus memungkinkan Subyek Data untuk bertanya atau membatalkan persetujuan. Pembatalan ini memiliki konsekuensi bahwa data tentang atau terkait dengan Subyek Data juga harus dihapuskan oleh pihak pengendali atau pengolah data.
- Pihak pengendali atau pengolah data wajib memastikan bahwa "form" persetujuan yang mereka sediakan telah memenuhi standar GDPR. Tidak standarnya form ini, dapat membatalkan hak pengolahan data secara otomatis, tanpa permintaan Subyek Data. Hal ini berarti menghadapkan pihak pengolah atau pengendali data pada sanksi denda yang berat untuk kesalahan yang tidak mereka sengaja atau tidak mereka sadari.
- Pihak pengendali atau pengolah data perlu melakukan audit untuk menentukan sejauhmana persetujuan yang sah telah mereka peroleh dari Subyek Data untuk pemanfaatan data untuk tujuan baru tertentu. Jangan-jangan diperlukan persetujuan baru demi terpenuhinya syarat-syarat GDPR! Namun, perusahaan perlu mempertimbangkan apakah memungkinkan untuk memperoleh persetujuan baru tersebut. Jangan-jangan secara teknis sulit dilakukan dan membutuhkan biaya besar dan tidak realistis untuk membangun sistem pendukungnya?
- Pihak pengendali atau pengolah data wajib memastikan: 1) Subyek Data diberi pilihan yang jelas untuk memberikan persetujuan dan kebebasan untuk mencabut persetujuan tanpa kerugian; 2) Persetujuan dibedakan dari hal-hal lain dan tidak dimasukkan ke dalam dokumen lain (misalnya dimasukkan dalam syarat dan ketentuan atau dalam kontrak karyawan); 3) Subyek Data mengetahui setidaknya identitas Pengendali Data dan tujuan pengolahan sebelum mereka diminta untuk memberikan persetujuan; 4) Persetujuan yang dimaksud diberitahukan terlebih dahulu kepada Subyek Data, misalnya dijadikan satu dengan **Boks Pemberitahuan Privasi**; 5) Persetujuan ditulis dalam bahasa yang jelas

dan lugas sehingga ada transparansi tentang untuk urusan apa pengolahan data dilakukan, seberapa lama, apa saja konsekuensinya dan lain-lain; 6) Persetujuan diberikan melalui tindakan afirmatif yang jelas (misalnya dengan mencentang kotak), dengan istilah yang gamblang (misalnya secara eksplisit menggunakan istilah "persetujuan" dalam form persetujuan).

### *IX.3.iv. Pemberitahuan Privasi*

Berdasarkan pasal 12, 13, 14 GDPR, Pengendali Data harus lebih transparan terhadap Subyek Data tentang kegiatan pengolahan data yang mereka lakukan. Subyek Data harus mendapatkan informasi tentang cara dan tujuan pengolahan data pribadi mereka. Informasi tersebut harus ringkas, transparan, jelas dan mudah diakses. Di saat yang sama, "daftar belanja" informasi yang dikelola Pengendali Data harus dimuat dalam pemberitahuan privasi, yang lingkupnya telah diperluas secara signifikan dalam GDPR. Pengendali Data harus senantiasa memeriksa kembali **Form Persetujuan** dan **Boks Pemberitahuan Privasi** yang mereka berlakukan untuk memastikan terpenuhinya syarat-syarat GDPR yang lebih terperinci.

***Bagaimana memberikan Pemberitahuan Privasi yang sah?*** Baik data diperoleh langsung dari Subyek Data atau secara tidak langsung melalui pihak ketiga, Pemberitahuan Privasi harus menyatakan:

- ✓ Rincian identitas dan kontak pihak Pengendali Data atau perwakilannya.
- ✓ Rincian kontak petugas perlindungan data yang ditunjuk pihak Pengendali Data.
- ✓ Tujuan dan dasar hukum pengolahan data, serta kepentingan yang melatarbelakanginya.
- ✓ Hak Subyek untuk mencabut persetujuan.
- ✓ Kategori-kategori data pribadi yang diproses dan sumbernya (jika data diambil dari pihak ketiga dan tidak ditambang langsung dari Subyek Data).
- ✓ Kategori-kategori penerima data pribadi (misalnya mitra atau vendor pihak ketiga).
- ✓ Rincian pemindahan data ke luar Uni Eropa, termasuk rincian mekanisme perlindungan yang digunakan.
- ✓ Periode penyimpanan data atau penggunaan kriteria untuk menentukan periode tersebut.
- ✓ Rincian hak-hak individu, termasuk hak mengadu kepada Lembaga Pengawas Perlindungan Data.
- ✓ Rincian pembuatan keputusan otomatis.

Ada tantangan mendasar dalam masalah **Pemberitahuan Privasi**. Di satu sisi, Pengendali Data harus berkomunikasi dengan individu Subyek Data dengan cara yang jelas dan dapat dimengerti. Di sisi lain, mereka harus mengomunikasikan informasi yang cukup terperinci dan berpandangan ke depan tentang kegiatan pengolahan data yang mereka lakukan. Perlu ada keseimbangan antara menjelaskan aktivitas pengolahan secara akurat dan memastikan keberlanjutan proses pemberitahuan privasi. Memastikan keberlanjutan ini termasuk misalnya menulis pemberitahuan privasi sedemikian rupa sehingga memungkinkan adanya fleksibilitas bagi Pengendali Data untuk menggunakan data pribadi seperti yang dipersyaratkan, termasuk untuk tujuan yang tidak diketahui secara khusus pada saat pengumpulan data, sementara tetap tunduk pada syarat-syarat GDPR. Ada kemungkinan sistem pengoperasian bisnis yang kompleks

akan kesulitan memuat semua informasi yang dipersyaratkan dalam pemberitahuan privasi, tanpa melakukan perubahan pada pengaturan yang berlaku. Beberapa syarat juga cukup sulit dipenuhi.

### *IX.3.v. Pembatasan Konteks dan Tujuan Penggunaan Data*

GDPR sangat menekankan prinsip pembatasan konteks dan tujuan penggunaan data pribadi oleh pihak Pengendali dan rekanannya (Pasal 6). GDPR menegaskan, data pribadi dapat dikumpulkan dan dikelola hanya untuk tujuan yang sudah ditetapkan atau disepakati secara gamblang dan sah dan tidak dapat diproses lebih lanjut dengan cara yang tidak kompatibel dengan tujuan tersebut. Memang ada peluang untuk memperluas tujuan tersebut di luar batas-batas yang telah disetujui antara Subyek Data dan Pengendali Data, tetapi penggunaan lebih lanjut data untuk tujuan lain secara arbitrer dan tanpa pemberitahuan yang memadai dianggap pelanggaran oleh GDPR. GDPR menyatakan bahwa Pengendali Data harus mempertimbangkan apakah tujuan lebih lanjut kompatibel dengan tujuan awal data dikumpulkan. Jika Pengendali Data menemukan bahwa tujuannya tidak kompatibel, ia harus meminta persetujuan atau tidak melakukan pengolahan secara arbitrer. Hal-hal yang perlu dipertimbangkan termasuk kaitan antara tujuan awal dan tujuan berikutnya, ekspektasi Subyek Data yang masuk akal berdasarkan hubungan mereka dengan Pengendali Data, sifat pribadi dari data yang dikelola, konsekuensi yang mungkin muncul dari pengolahan yang dimaksud terhadap subyek data.

Banyak sistem manajemen data akan mempergunakan serangkaian sumber data pribadi untuk tujuan-tujuan yang diperluas atau tujuan lain yang berbeda dengan tujuan awal. GDPR berkepentingan untuk memastikan keberadaan tujuan baru membutuhkan persetujuan baru dari Subyek Data, serta untuk membatasi atau meminimalisir penggunaan data pribadi Subyek yang dalam perkembangannya cenderung semakin tak terbatas dan tak terkontrol.

***Apa dampak pemberlakuan prinsip pembatasan konteks dan tujuan penggunaan data?***

- Jika perusahaan ingin menggunakan data pribadi untuk tujuan baru, perlu dipastikan tujuan baru ini kompatibel dengan tujuan awal pengumpulan data.
- Perusahaan perlu meninjau Pemberitahuan Privasi dan Form Persetujuan untuk memastikan tujuan pengolahan digambarkan secara akurat, gamblang dan tidak membuka kemungkinan bagi penggunaan data yang menyimpang dari persetujuan awal antara Pengendali Data dan Subyek Data.
- Perusahaan harus menerapkan mekanisme yang baku dan pengawasan tertulis untuk memastikan pengawasan pengolahan data yang tepat dan sesuai dengan tujuan awal untuk kemungkinan-kemungkinan tujuan yang lain berikutnya.

### *IX.3.vi. Hak Subyek Data*

GDPR telah meningkatkan dan memperluas hak-hak Subyek Data. GDPR memperkenalkan beberapa hak baru seperti hak portabilitas, kodifikasi atas “hak untuk dilupakan” serta membuat perubahan terhadap hak-hak yang berada di bawah Undang-Undang Perlindungan Data Uni Eropa (*EU Data Protection Directive*) Tahun 1995. Hanya tersedia waktu yang singkat bagi perusahaan atau organisasi Pengendali Data dan Pengolah Data untuk melakukan penyesuaian diri di sini. Perluasan hal Subyek Data tersebut adalah sebagai berikut:

### *a. Hak Akses (Pasal 15)*

Hak Subyek Data untuk memperoleh konfirmasi dari Pengendali Data tentang apakah data pribadi mereka sedang dikumpulkan dan dikelola, dari mana data pribadi itu diambil dan bagaimana data tersebut diproses? Sekaligus hak untuk memperoleh salinan data pribadi tersebut. Apakah Pengendali Data menggunakannya untuk tujuan pemrofilan? Hak ini harus dapat dengan mudah digunakan dalam interval waktu yang masuk akal. Hak-hak ini sebelumnya (di bawah Undang-Undang Perlindungan Data Uni Eropa) telah terbukti memberatkan perusahaan layanan digital di berbagai kawasan dan kerap dikritik karena acapkali digunakan untuk kebutuhan pencarian informasi atau taktik penyingkapan pra-litigasi. Ada beberapa langkah untuk membatasi lingkup pembatasan ini, misalnya dengan mengecualikan data non pribadi, menggunakan pengecualian sempit yang berlaku pada materi yang diberi hak istimewa. Namun hal ini berisiko dan tidak didukung oleh regulator Uni Eropa.

### *b. Hak Pembetulan (Pasal 16)*

Hak Subyek Data untuk memperoleh, tanpa keterlambatan yang tidak semestinya, pembetulan data pribadi yang tidak akurat tentang diri mereka. Tergantung pada tujuan pemrosesan, Subyek Data juga memiliki hak untuk melengkapi data yang belum lengkap.

### *c. Hak Penghapusan (Pasal 17)*

Juga disebut “hak untuk dilupakan”, ini adalah hak Subyek Data untuk menghapus data pribadi mereka tanpa keterlambatan yang tidak semestinya. Setelah keputusan Mahkamah Hukum Uni Eropa (CJEU) yang dikenal luas dalam kasus Google Spanyol di mana Google harus menghapuskan tautan-tautan ke beberapa artikel di media siber hasil pencarian Google tentang nama seorang warga Spanyol (artikel-artikel tersebut merujuk kepada sejarah masalah keuangannya), beberapa perusahaan dibanjiri dengan permintaan agar data-data pelanggan yang tidak menyenangkan segera dihapuskan. Meskipun menerima permintaan penghapusan berdasarkan hak tersebut, Pengendali Data tetap dapat menyimpan atau memroses data itu jika masih memiliki dasar alasan yang sah (berdasarkan hukum) lainnya untuk mengumpulkan dan mengelola data pribadi. Permintaan penghapusan data itu juga dapat dikesampingkan untuk alasan-alasan kepentingan publik seperti masalah kesehatan publik, riset ilmiah, riset sejarah dan lain-lain.

### *d. Hak Membatasi Pengolahan Data (Pasal 18)*

Subyek Data memiliki hak untuk memperoleh pembatasan pengolahan data dalam keadaan-keadaan tertentu. Jika Subyek Data menggugat keakuratan data pribadi, pengolahan dapat dibatasi sejauh terbukti ada masalah dalam keakuratan itu. Hak ini juga berlaku saat pengolahan data terjadi secara tidak sah tetapi Subyek Data tidak ingin data tersebut dihapus, atau pada saat Pengendali Data tidak memerlukan data tetapi diperlukan oleh Subyek Data untuk pengerjaan atau pembelaan klaim hukum.

### *e. Hak Mengajukan Keberatan (Pasal 21)*

Hak Subyek untuk mengajukan keberatan atas pengolahan data karena keadaan mereka di satu waktu tertentu. Hak ini berlaku pada saat alasan untuk pengolahan data adalah menjalankan

kepentingan publik atau pelaksanaan otoritas resmi yang diberikan kepada Pengendali Data. Hak ini juga berlaku pada konteks pemrofilan yang didasarkan pada alasan tersebut. Pengendali Data harus berhenti mengelola dan memanfaatkan data kecuali dapat menunjukkan dasar yang lebih kuat untuk melanjutkan pengelolaan atau pemanfaatan data.

### *f. Hak Portabilitas Data (Pasal 20)*

Hak Subyek Data untuk menerima data pribadi dari Pengendali Data dalam format yang terstruktur, dapat digunakan, dapat dibaca perangkat teknologi yang standar sehingga dapat dipindahkan dengan mudah ke pihak lain. Idenya adalah memberikan kepada Subyek Data lebih banyak kendali atas data dirinya. Agar berada di bawah cakupan portabilitas data, proses pengolahan mesti berdasarkan pada persetujuan Subyek Data atau berdasarkan kontrak di mana Subyek Data adalah menjadi salah satu.

## *3.vii. Akuntabilitas Pengendali Data*

GDPR (Pasal 30, 35) mensyaratkan akuntabilitas dan tanggung-jawab Pengendali Data untuk:

- ✓ Membuat catatan tentang semua kegiatan pengumpulan dan pengolahan data yang dilakukannya. Ini adalah tanggung-jawab yang sulit dan tidak boleh diremehkan, tetapi tidak semestinya dibuat terlalu sulit.
- ✓ Melakukan penilaian dampak terhadap perlindungan data untuk pengolahan data yang lebih beresiko, termasuk mengidentifikasi di mana saja perlindungan tersebut dibutuhkan.
- ✓ Menerapkan perlindungan data berdasarkan tujuan dan standar GDPR.
- ✓ Melaporkan pelanggaran data tertentu yang terjadi.
- ✓ Menunjuk petugas perlindungan data.

Dengan demikian, menjadi penting bagi pihak Pengendali Data untuk sewaktu-waktu dapat menunjukkan dasar pengolahan data pribadi Subyek Data, bagaimana pengolahan dilakukan dan untuk tujuan apa. Apakah semua ini telah dilakukan dengan memenuhi syarat-syarat GDPR? GDPR menegaskan pentingnya pihak Pengendali Data untuk menyusun dan menjaga laporan kinerja pengolahan dan pengendalian secara terdokumentasi.[10] Suatu hal yang tidak mudah untuk dilakukan. Catatan-catatan ini perlu disediakan dan dilaporkan kepada Lembaga Pengawas Perlindungan Data (*The Supervisory Authority*) kapan pun diminta. Transparansi dan akuntabilitas pengolahan dan pengendalian data ini menjadi isu yang dibahas secara khusus belakangan dan memicu upaya pengembangan teknologi yang kompatibel. Perusahaan-perusahaan digital besar terus bergulat untuk mendapatkan solusi teknologis yang memadai untuk hal tersebut.

Pihak Pengendali Data harus memiliki catatan informasi tentang: nama dan rincian kontak perwakilan Pengendali Data dan petugas Lembaga Pengawasan Perlindungan Data di suatu negara, tujuan pemrosesan data, deskripsi kategori-kategori data pribadi Subyek yang diproses, kategori-kategori penerima olahan data termasuk penerima di negara ketiga atau organisasi internasional, rincian pemindahan data pribadi ke negara ketiga, periode penyimpanan yang

[10] Wawancara Peter Van Dyck, anggota dari dari Allen & Overy LLP cabang Brussels Belgia, 21/12/2018.

dipertimbangkan untuk berbagai kategori data pribadi, deskripsi umum tindakan pengamanan data untuk situasi darurat tertentu. Dalam konteks yang sama, Pihak Pengolah Data juga diwajibkan memiliki catatan semua kategori kegiatan pengolahan yang dilakukan atas nama pihak Pengendali Data, rincian tentang proses pemindahan data ke negara ketiga, serta antisipasi tindakan pengamanan data dalam keadaan darurat tertentu.

GDPR menekankan kewajiban Pengendali Data atau Pengolah data untuk melakukan penilaian *(assessment*) dampak perlindungan data untuk pengolahan data yang beresiko tinggi. Hal ini misalnya untuk pengolahan data pribadi berkategori khusus dalam skala besar, penggunaan teknologi baru yang belum diketahui benar dampak-dampaknya, atau proses pemrofilan pengguna internet secara sistematis dan ekstensif (Pasal 29). Hal ini memberikan beban sekaligus tantangan baru bagi perusahaan-perusahaan penyedia layanan digital. Atas teknologi dan inovasi baru penambangan dan pengolahan data pengguna yang akan mereka terapkan, perlu dipastikan antisipasi dampaknya terhadap prinsip perlindungan data pengguna. *Assessment* atas dampak ini perlu diberitahukan kepada Lembaga Pengawas Perlindungan Data, atau setidak-tidaknya harus tersedia setiap saat jika sewaktu-waktu diminta (lihat Pasal 36).

### *IX.3.viii. Pengaturan Privacy by Design*

*Privacy by Design* adalah sebuah pendekatan untuk melindungi privasi dalam proses pembangunan sistem digital (teknologi, praktek bisnis dan rancangan fisik infrastruktur berjaringan) yang berfokus pada pengutamaan atau pengintegrasian perlindungan privasi ke dalam sistem secara keseluruhan. Dengan demikian, prinsip perlindungan privasi mutlak dimasukkan dalam arsitektur sistem digital sedari awal. Perlindungan privasi adalah sesuatu yang direncanakan, bukan sesuatu yang muncul setelah terjadinya insiden atau kecelakaan. Konsep *Privacy by Design* menempatkan prinsip perlindungan privasi sejak proses perancangan sistem pengolahan data hingga pelaksanaan pengolahan data (GDPR Pasal 36). Saat berpikir tentang pengaturan privasi, sebuah organisasi mesti mempertimbangkan bahwa privasi mesti tercermin atau terintegrasikan dalam kecanggihan teknologi yang digunakan, biaya implementasi teknologi, sifat, cakupan, konteks dan tujuan pemrosesan data, sekaligus perhitungan resiko-resiko terhadap individu Subyek Data. Kewajiban ini mensyaratkan pernyataan perlindungan privasi pada setiap awal kegiatan atau proyek baru yang melibatkan proses pengolahan data pribadi atau ketika menerapkan sistem manajemen baru atau modifikasi manajemen pengolahan data.

Konsep *Privacy by Design* dalam GDPR juga mewajibkan Pengendali Data menerapkan prinsip minimalisasi pengambilan dan pemanfaatan data pribadi (*data minimisation*). GDPR juga mewajibkan Pengendali Data untuk menerapkan *privacy by default* berdasarkan prinsip minimisasi data itu. Dengan demikian, organisasi atau perusahaan harus memastikan data pribadi bukanlah sesuatu yang secara tak sengaja, lalai atau tanpa persetujuan Subyek Data (*by default*) digunakan untuk pihak atau orang yang tak terbatas jumlahnya. Dengan demikian, perusahaan penyedia layanan media-sosial tidak diizinkan untuk secara lalai atau otomatis menampilkan profil pribadi penggunanya untuk publik tanpa izin yang bersangkutan.

***Apa dampak penerapan Privacy by Design dalam GDPR?*** Perusahaan penyedia layanan digital harus memikirkan privasi ketika:

- Menciptakan produk, aplikasi dan layanan digital baru.
- Membangun situs web (bagaimana anda mengumpulkan data, informasi apa saja yang anda kumpulkan, kepada siapa informasi itu anda berikan atau kerjasamakan, apakah anda menggunakan produk dari pihak ketiga misalnya untuk tombol media-sosial, aplikasi iklan atau *platform* komentar yang juga berfungsi untuk mengumpulkan data tambahan atau mengatur *cookies*?)
- Menunjuk pihak ketiga untuk mengolah data (apakah mereka memiliki reputasi bagus soal keamanan perlindungan data, apakah mereka bersedia membantu Anda melaksanakan kewajiban perlindungan data?)
- Mengembangkan strategi bisnis baru (apakah strategi yang anda gunakan selaras dengan kebijakan perlindungan privasi, apakah anda mengumpulkan terlalu banyak data, apakah anda menggunakan data untuk tujuan yang tepat?)

### *IX.3.ix. Pengolahan Data dan Pemrofilan Otomatis (Automated Processing And Profiling)*

Subyek Data memiliki hak untuk tidak terikat pada keputusan-otomatis (*automated decisions*) termasuk yang bertolak dari proses pemrofilan pengguna internet jika keputusan tersebut menghasilkan dampak hukum yang berhubungan dengan Subyek Data atau jika memiliki dampak yang signifikan terhadap Subyek Data. **Pemrofilan** didefinisikan GDPR (Pasal 4 dan 22) sebagai semua bentuk pengolahan otomatis data pribadi yang mencakup penggunaan data pribadi untuk mengevaluasi aspek-aspek pribadi tertentu dari setiap pengguna internet, terutama untuk menganalisis atau memprediksikan aspek-aspek kinerja seseorang (pekerjaan, situasi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi dan mobilitas). Contoh penggunaan pemrofilan dalam konteks keputusan-otomatis misalnya saja penerapan aplikasi kredit online atau praktik perekrutan online tanpa campur-tangan manusia. Berdasarkan GDPR, individu pemilik data memiliki hak untuk menolak proses pengolahan dan pemrofilan otomatis berikut pemanfaatannya. Dalam proses pengolahan dan pemrofilan data otomatis, keputusan-keputusan dipaksakan secara arbiter dan otomatis oleh pihak Pengendali Data. Subyek Data memiliki hak untuk menolak keputusan-keputusan itu. Pengecualian terhadap aturan ini terjadi jika individu Subyek Data sudah memberikan persetujuan yang gamblang untuk proses pengolahan data dan pemrofilan, jika pembuatan keputusan otomatis telah disahkan oleh hukum Uni Eropa atau negara anggota Uni Eropa, atau jika keputusan otomatis merupakan bagian dari pelaksanaan kontrak antara Subyek Data dan Pengendali Data.

Perlu diperhatikan, bahkan dalam kasus pengecualian itu pun, pihak Pengendali Data tetap diharuskan memberikan perlindungan atas data Subyek guna mendukung kebebasan dan hak mereka untuk terbebas dari intervensi orang lain, untuk mengekspresikan pandangan diri-sendiri dan untuk mempersoalkan keputusan-otomatis. Seperti yang telah dibahas, GDPR menuntut Pengendali Data untuk memberitahu Subyek Data bahwa mereka sedang atau telah melakukan pemrofilan dan pembuatan keputusan otomatis sebagai bagian dari proses pengolahan data yang mereka lakukan. Pihak Pengendali Data harus menjelaskan logika kerja dan konsekuensi

dari proses pemrofilan otomatis yang mereka lakukan. Hal ini juga berlaku untuk perusahaan yang berusaha memperoleh keuntungan ekonomi dari pemanfaatan *big-data analysis* dan produk kecerdasan buatan untuk sektor bisnis, misalnya dengan mengevaluasi resiko untuk harga asuransi mobil, penilaian kredit atau perekrutan tenaga kerja berdasarkan data-perilaku-pengguna-internet yang mereka tambang dan kumpulkan.

***Apa dampak Pembatasan Pengolahan Data dan Pemrofilan Otomatis?***

- Pengendali Data harus mengidentifikasi terus-menerus apakah pihaknya telah membuat keputusan otomatis-arbitrer yang menghasilkan dampak terhadap Subyek Data atau memiliki konsekuensi hukum tertentu bagi Pengendali Data atau Subyek Data.
- Pengendali Data harus menyediakan mekanisme yang memungkinkan subyek untuk: menuntut campur tangan manusia dalam keputusan-keputusan yang berdasarkan pengolahan data otomatis, mengekspresikan pandangan dan kepentingan mereka, menggugat keputusan otomatis dengan beberapa pengecualian konteks dan alasan.
- Pengendali Data harus menjelaskan dalam istilah-istilah yang jelas dan logis tentang signifikansi dan konsekuensi pengolahan data dan pemrofilan otomatis kepada Subyek Data.
- Pengendali Data harus menerapkan pendekatan teknis dan organisatoris untuk menjelaskan dan melaksanakan transparansi sistem algoritma yang digunakan dalam pengolahan data Subyek Data.

### *IX.3.x. Keamanan Data dan Transparansi Tentang Pembobolan Data (data breach notification)*

Pengendali Data atau Pengolah Data diwajibkan memberitahukan pembobolan atau pengambilan data secara diam-diam yang telah mereka lakukan (Pasal 30 dan 32). Apabila terjadi pembobolan data pribadi Subyek Data, seperti akses tanpa izin ke akun pribadi atau pengambilan data yang berefek penghapusan data, ada beberapa kewajiban pemberitahuan yang mesti dilaksanakan Pengendali Data atau Pengolah Data sebagai berikut.

***a. Pemberitahuan Kepada Lembaga Pengawas Keamanan Data (Pasal 33)***

Pemberitahuan ini harus dilakukan tanpa keterlambatan yang tidak semestinya – setidak-tidaknya dalam waktu maksimal 72 jam-- setelah diketahui adanya pembobolan data. Namun, kewajiban ini tidak berlaku apabila pelanggaran tidak menghasilkan resiko terhadap hak dan kebebasan individu Subyek Data. Jika Pengendali Data atau Pengolah Data tidak memberitahukan selama periode waktu ini, harus ada penjelasan tentang alasan keterlambatan. Pemberitahuan itu harus setidaknya menjelaskan sifat pelanggaran, kategori data, jumlah subyek data yang terbobol datanya, pihak-pihak yang kira-kira terlibat, penjelasan petugas perlindungan data yang berkompeten dan ditunjuk Pengendali Data atau Pengolah Data, konsekuensi yang mungkin muncul serta tindakan yang sedang dilakukan atau diusulkan agar dilakukan segera. Semua

pembobolan data harus didokumentasikan termasuk dampak serta tindakan perbaikan yang dibutuhkan.

***b. Pemberitahuan Kepada Subyek Data (Pasal 34)***

Pemberitahuan ini harus dilakukan tanpa keterlambatan yang tidak semestinya apabila pelanggaran data dapat berujung pada resiko serius terhadap hak dan kebebasan Subyek Data. Pemberitahuan ini harus menjelaskan konteks pembobolan data yang terjadi secara jelas serta memberikan informasi lain yang terkait. Pemberitahuan dapat diabaikan, misalnya jika data telah dienkripsi dengan aman serta akses ke kunci enkripsi belum dibuka untuk pihak lain. Pemberitahuan yang bersifat publik dimungkinkan jika pemberitahuan yang bersifat individu (orang per orang) dianggap memerlukan usaha dan biaya yang tidak sepadan.

### *IX.3.xi. Sanksi*

Sebelum pemberlakuan GDPR, negara anggota Uni Eropa telah menerapkan sanksi denda untuk perusahaan atau organisasi yang melakukan pelanggaran pembobolan data (*data breach*) atau penyalahgunaan data. Sanksi denda ini pada umumnya tidak terlalu memberatkan, misalnya 500.000 pounds di Inggris. Namun, beberapa negara belakangan telah meningkatkan denda tersebut, yakni 3 juta Euro di Prancis dan 820,000 Euro atau hingga 10% dari pendapatan bersih tahunan perusahaan di Belanda. GDPR (Pasal 84) kemudian mengatur denda yang lebih berat, dapat mencapai 20 juta Euro atau 4% pendapatan global tahunan perusahaan untuk jenis-jenis pelanggaran tertentu. Pemberlakuan denda ini bersifat berjenjang tergantung pada sifat spesifik pelanggaran pembobolan data yang terjadi dan perkiraan kerugian yang ditimbulkan. Dengan demikian, denda dapat digolongkan denda hingga 2% (atau 10 juta Euro) atau denda hingga 4% (atau 20 juta Euro).

Untuk memutuskan denda administratif dan berapa jumlahnya, Lembaga Pengawas Perlindungan Data (*The Supervisory Authority*) mempertimbangkan beberapa hal berikut (Pasal 82 dan 83):

- Bentuk, tingkat kegawatan dan durasi pembobolan data yang terjadi dengan mempertimbangkan sifat, cakupan atau tujuan pengolahan data yang menyertainya, jumlah Subyek Data yang terdampak dan tingkat kerusakan yang mereka alami
- Apakah pelanggaran pembobolan data bersifat sengaja atau lalai?
- Tindakan mitigasi yang dilakukan perusahaan atau organisasi untuk mengatasi pembobolan data
- Rekam jejak sebelumnya dari perusahaan atau organisasi yang melakukan pelanggaran
- Apakah perusahaan atau organisasi tersebut kooperatif terhadap lembaga pengawas perlindungan data?
- Apakah mereka dengan inisiatif sendiri menyampaikan pemberitahuan atau laporan kepada lembaga pengawas perlindungan data ketika menemukan indikasi pembobolan data?

Sebagai contoh pendekatan berjenjang untuk penerapan denda, denda maksimal atau denda yang mendekati maksimal terutama sekali diberlakukan untuk pelanggaran pasal-pasal:

pemindahan data antar-bangsa, transparansi dan akuntabilitas pemberlakuan syarat-syarat persetujuan untuk Subyek Data, serta perlindungan hak-hak Subyek Data. GDPR membuka peluang bagi negara anggota Uni Eropa untuk menerapkan sanksi-sanksi tambahan di luar sanksi denda administratif. Hal ini dapat berupa sanksi pidana untuk pelanggaran yang serius terhadap prinsip perlindungan data. Dalam rangka pelaksanaan sanksi, Lembaga Pengawas Perlindungan Data memiliki wewenang untuk: melakukan audit, meminta perbaikan sistem pengolahan data dalam kurun waktu tertentu, meminta penghapusan data atau menangguhkan pemindahan data ke penerima di negara ketiga.

Di bawah GDPR, Subyek Data memiliki dasar hukum lebih kuat untuk meminta tanggung-jawab lebih dari pihak Pengolah Data atau Pengendali Data, termasuk meminta kompensasi untuk kerugian yang diderita Subyek Data.[11] Klaim kompensasi dapat berkaitan dengan pelanggaran GDPR atau kegagalan Pengendali Data atau Pengolah data dalam mengikuti instruksi Lembaga Pengawas Perlindungan Data. Secara umum, Subyek Data dimungkinkan untuk meminta kompensasi dari Pengendali Data dan Pengolah Data untuk kerusakan material atau non material, termasuk kerugian non finansial yang diderita Subyek Data. Subyek Data dapat memperjuangkan aspirasi dan tuntutannya secara pribadi maupun secara kelompok sehingga dimungkinkan dibentuknya badan-badan perwakilan Subyek Data untuk membawa aspirasi dan tuntutan mereka ke hadapan Lembaga Pengawas Perlindungan Data atau secara langsung ke pihak Pengendali Data atau Pengolah Data.

GDPR secara gamblang memberikan kemungkinan tanggung jawab bersama untuk Pengendali Data dan Pengolah Data jika mereka sama-sama dianggap bertanggung jawab untuk pelanggaran pembobolan data atau penyalahgunaan data. Tuntutan dapat dibawa baik ke pengadilan negara anggota Uni Eropa di mana pihak Pengendali Data atau Pengolah data berkedudukan maupun ke pengadilan negara anggota Uni Eropa di mana Subyek Data berdomisili.

### *IX.4. Data As Labor*

Terlepas dari kritik dan keberatan yang disampaikan berbagai pihak, GDPR diakui sebagai pioneer pelembagaan perlindungan data pribadi. GDPR memberikan model sekaligus fondasi untuk pelembagaan perlindungan data di seluruh dunia. Standar perlindungan data konsumen atau pengguna layanan digital yang dikembangkan perusahaan platform global seperti *Google, Amazon* dan *Facebook* pun juga menjadikan GDPR sebagai acuan. Bukan hanya kalangan korporasi yang menjadikan GDPR sebagai barometer pengelolaan dan pengendalian data, melainkan juga institusi resmi negara, lembaga intelijen, organisasi non pemerintah dan lain-lain. Bagi individu sebagai Subyek Data, GDPR adalah upaya untuk mengembalikan kekuasaan individu atas data dan informasi yang mereka miliki tetapi selama ini kendalinya berada di tangan pihak lain. GDPR mengatur syarat perlindungan data berikut sanksi denda yang berat untuk organisasi atau perusahaan yang gagal memenuhi syarat tersebut. Dengan kebijakan perlindungan data

[11] Wawancara Peter Van Dyck……..

yang sangat ketat, Uni Eropa berharap akan terwujud sistem perlindungan yang memadai atas penyimpanan data dan privasi.[12]

Dalam konteks inilah GDPR dapat diletakkan dalam perdebatan tentang *data as labor*. Pertanyaannya adalah apakah data-perilaku-pengguna-internet (*user behavior data*) merupakan aset milik perusahaan penyedia layanan digital (*data-as-capital*) atau merupakan hak milik setiap orang pengguna layanan tersebut (*data-as-labor*)? Seperti dijelaskan dalam **"Bab *Data As Labor*"**, perdebatan ini dilatarbelakangi fakta yang telah sedemikian jauh berlangsung, bahwa data-perilaku-pengguna-internet diperlakukan sebagai semata-mata aset perusahaan penyedia layanan digital (*capital*) daripada sebagai jerih-payah atau aset dari pengguna layanan-layanan itu (*labor*). Sebagai pengguna telephon-pintar, masyarakat terus-menerus didorong untuk membelanjakan lebih banyak waktu, tenaga dan biaya untuk mengakses berbagai layanan dan aplikasi digital. Dengan cara yang sama, mereka sesungguhnya didorong untuk menghasilkan data-perilaku-pengguna-internet sebanyak-banyaknya. Dalam prakteknya, data tersebut hanya dimanfaatkan untuk pengembangan produk dan operasionalisasi bisnis perusahaan platform digital.

GDPR ingin mengoreksi praktek semacam ini. GDPR adalah suatu antitesa dari perspektif *data-as-capital* yang melihat data-perilaku-pengguna-internet sebagai properti perusahaan platform digital yang merasa telah memberikan layanan digital cuma-cuma kepada masyarakat. Di tangan pengguna internet, data tersebut memang hanya merupakan sampah konsumsi digital yang tak termanfaatkan. Di tangan perusahaan digital, sampah itu dikumpulkan dan diolah kembali untuk memiliki nilai ekonomi tertentu. Perspektif *data-as-capital* mengafirmasi upaya perusahaan layanan digital untuk memberi nilai-tambah ekonomis atas sampah digital itu untuk pengembangan kecerdasan-buatan dan iklan digital tertarget. Sementara GDPR –paralel dengan perspektif *data-as-labor*-- menempatkan data-perilaku-pengguna-internet sebagai hak milik pribadi para pengguna layanan digital. Pemanfaatan data tersebut mesti atas sepengetahuan dan seizin pengguna. Pemanfaatan data itu mesti memberikan keuntungan –alih-alih membahayakan keselamatan—pengguna layanan internet. GDPR memberikan kekuasaan yang besar kepada pengguna layanan internet atas pemanfaatan data-perilaku-pengguna-internet dan melindungi mereka dari pemanfaatan yang merugikan atau mengancam keselamatan.

Dalam perspektif *data-as-capital*, pengelolaan data-perilaku-pengguna-internet oleh perusahaan digital adalah sesuatu yang legal karena dilakukan atas persetujuan pengguna. Persetujuan itu merupakan sebentuk perjanjian antara pengguna internet dan penyedia layanan-layanan digital untuk melakukan barter yang sepadan antara layanan digital gratis (*free services*) dengan pengambilan data yang gratis (*free data*). Dalam kaitan ini, GDPR ingin memastikan persetujuan itu terjadi dengan pengetahuan, kesadaran dan kebebasan pengguna. GDPR ingin memastikan persetujuan itu tidak dipaksakan atau tidak memanfaatkan ketidaktahuan pengguna tentang transfer otomatis data pribadi yang terjadi berikut konsekuensi-konsekuensinya ketika mereka memanfaatkan layanan digital gratis tersebut. Paralel dengan perspektif *data-as-labor*,

[12] Mcgavisk, Taylor. "The Positive And Negative Implications Of GDPR", *https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr*, diakses 09/01/2019.

GDPR beranggapan masyarakat sebagai pengguna internet membutuhkan kehadiran lembaga resmi baru yang berfungsi mengawasi dan mengendalikan kemampuan perusahaan digital dalam mengambil dan mengelola data penggunanya dan memaksimalkan kekuatan monopsoni atau monopoli atas industri digital yang berbasis pada komodifikasi data-perilaku-pengguna-internet. Tujuannya adalah mewujudkan sistem pasar informasi dan data yang adil dan transparan berlandaskan prinsip *data-as-labor*.

Monopsoni adalah keadaan di mana satu pelaku usaha menguasai penerimaan pasokan yang tersedia atau menjadi pembeli atau penguasa tunggal atas suatu produk dalam suatu pasar. Pasar monopsoni atau oligopsoni merujuk pada jenis pasar di mana satu atau sedikit pelaku usaha menguasai penyerapan produk di pasar tersebut. Pengertian monopsoni atau oligopsoni dengan demikian merupakan kebalikan dari pengertian monopoli atau oligopoli di mana satu atau beberapa pelaku usaha menguasai penjualan produk di suatu pasar. Monopsoni itulah yang terjadi dalam dunia digital. Data-perilaku-pengguna-internet (*user behavior data*) yang besarannya berskala global hanya dikuasai segelintir perusahaan raksasa yang memiliki kapasitas untuk memonetisasi data tersebut: *Amazon, Google, Facebook, Uber, Microsoft* dan lain-lain. Kapitalisasi dan penetrasi perusahaan-perusahaan ini terjadi sedemikian pesat sehingga tak bisa lagi ditandingi oleh pemain yang lain. Terciptalah kemudian iklim, struktur dan sistem digital yang sedemikian rupa memusatkan perhatian pengguna internet dan pasokan data-perilaku-pengguna-internet untuk menopang pengembangan *big-data, cloud*, iklan digital tertarget dan kecerdasan-buatan hanya pada sedikit perusahaan digital saja. GDPR juga perlu diletakkan dalam konteks ini. GDPR dapat dilihat sebagai instrumen legal untuk mengurai lanskap monopsonistik industri pemanfaatan data pribadi (*personal data*) atau data-perilaku-pengguna-internet (*user behavior data*) secara global. Intervensi yang dilakukan tidak secara langsung menukik pada dimensi-dimensi ekonomi atau ekonomi-politik lanskap digitalisasi secara langsung, tetapi dalam konteks perlindungan data pribadi.

GDPR pada konteks yang kurang-lebih sama juga merupakan sebuah koreksi atas *surveillance capitalism*. Jenis kapitalisme baru yang mendasarkan diri pada tindakan pengawasan terhadap hidup semua orang melalui berbagai layanan atau aplikasi digital yang diproduksi dan dipasarkan secara global. Tanpa banyak disadari, penyedia layanan mesin-pencari, *ecommerce* dan media-sosial, seperti *Google, Amazon, Facebook, Twiter* sebenarnya selalu memata-matai penggunanya. Melalui sistem algoritma yang semakin lama semakin canggih, raksasa teknologi digital itu mampu melacak dan merekam identitas diri, kebiasaan dan perilaku para penggunanya. Mereka menyediakan berbagai layanan atau aplikasi digital yang diberikan secara cuma-cuma kepada penggunanya. Namun dengan layanan yang sama, mereka mampu melacak di mana kita berada, kendaraan yang kita gunakan atau yang sedang kita cari, restauran seperti apa yang sering kita kunjungi, barang apa yang kita koleksi atau ingin koleksi, liburan ke mana yang kita dambakan, gangguan kesehatan yang sedang kita hadapi dan seterusnya. Data perilaku itu kemudian diolah untuk menghasilkan surplus-perilaku (*behavioral surplus),* yakni ketika perusahaan media-sosial, mesin-pencari atau situs *ecommerce* mampu mengolah data perilaku penggunanya untuk menghasilkan prediksi pola konsumsi, keputusan dan interaksi sosial pengguna tersebut. Surplus-perilaku inilah sebenarnya instrumen utama bisnis perusahaan-perusahaan digital. Menguasai

dan mengelola data prediksi pola konsumsi dan interaksi sosial pengguna internet di seluruh dunia tentu saja menghasilkan kekuasaan ekonomi yang sangat besar. Secara faktual terlihat, surplus-perilaku ini pada tataran global dikuasai hanya sedikit perusahaan raksasa seperti *Google, Amazon* dan *Facebook*.

Hidup di bawah bayang-bayang *surveillance-capitalism* dalam konteks ini adalah hidup yang menegasikan privasi. Semakin banyak aspek dalam hidup kita menjadi obyek pengawasan dan pengendalian. Pengawasan dan pengendalian itu terakumulasi ke tangan perusahaan-perusahaan digital serta ke pihak ketiga (perusahaan, lembaga pemerintah, pribadi) yang memanfaatkan layanan perusahaan digital itu. *Internet of things, big-data* dan teknologi *cloud* membuat masyarakat semakin sulit mengendalikan kehidupannya sendiri seiring dengan semakin terbukanya akses perusahaan-perusahaan digital ke kehidupan setiap orang secara langsung dan *real time*.[13] Dalam konteks inilah kita menemukan relevansi GDPR. Sebagaimana telah dijelaskan di atas, GDPR secara ketat dan komprehensif mengatur prinsip-prinsip perlindungan data pribadi para pengguna internet atau layanan digital. Sebaliknya, GDPR membebani pihak Pengendali Data atau Pengolah Data dengan berbagai kewajiban –berikut sanksi yang memberatkan-- untuk mewujudkan perlindungan privasi dan keselamatan para pengguna internet atau layanan digital itu sebagai Subyek Data.

**1. Kritik**

Benar dalam maksud dan tujuan tetapi berlebihan dalam pengaturan. Sangat kontekstual dan dibutuhkan tetapi berpotensi melenceng dari tujuan awal. Dua kalimat ini barangkali tepat untuk menggambarkan posisi GDPR. GDPR dianggap sebagai pengaturan yang berlebihan (*overregulation*) tentang perlindungan data pribadi. GDPR membebani organisasi atau perusahaan penyedia layanan digital dengan kewajiban membangun sistem perlindungan data pribadi yang sangat kompleks, menyeluruh dan dalam beberapa hal kurang realistis untuk dilaksanakan. Sebagai konsekuensinya, organisasi atau perusahaan penyedia layanan digital harus menginvestasikan lebih banyak dana untuk memperbarui sistem perlindungan data pribadi, mengembangkan teknologi perlindungan data yang lebih sempurna, merekrut lebih banyak orang untuk menjalankan syarat dan standar GDPR. Bahkan mereka juga mesti mengevaluasi kembali proyeksi-proyeksi ke depan. Sanksi denda yang diterapkan GDPR juga sangat signifikan dan memberatkan.

Pertanyaannya kemudian, siapakah yang kira-kira yang memiliki kemampuan untuk memenuhi syarat dan standar GDPR? Siapa yang memiliki dana besar untuk berinvestasi membangun sistem pengelolaan data yang ramah privasi? Siapa yang memiliki kemampuan finansial untuk menebus denda yang ditetapkan GDPR? Pada titik ini, kita dihadapkan pada suatu kemungkinan bahwa GDPR “salah sasaran”. Pada awalnya GDPR sebenarnya dimaksudkan untuk mengurai dominasi atau monopsoni perusahaan raksasa digital seperti *Google (Alphabet), Amazon, Facebook, Microsoft, Apple* dalam pengendalian data-pribadi pengguna internet di

[13] Geoff Webb, "Say Goodbye to Privacy", 15/02/2015, *https://www.wired.com/insights/2015/02/say-goodbye-to-privacy/,* diakses 04/05/2017.

seluruh dunia. Namun dalam kenyataan, sangat mungkin justru perusahaan-perusahaan ini yang memiliki kekuatan finansial, SDM dan teknologi untuk menghadapi situasi pasca GDPR. Bisa jadi mereka yang memiliki kemampuan untuk secara cepat menyesuaikan diri standar baru perlindungan privasi. Karena khawatir menderita kerugian yang signifikan, mereka pada awalnya memang menolak GDPR. Namun, penolakan ini sepertinya hanya merupakan strategi untuk mengulur-ulur waktu agar mereka dapat mempersiapkan diri dengan lebih baik. Pada akhirnya, justru merekalah yang paling siap memenuhi syarat dan standar GDPR.

Lalu bagaimana dengan perusahaan digital berskala menengah atau kecil? Bagaimana nasib perusahaan digital nasional atau lokal? GDPR tidak mengenal pandang bulu. GDPR berlaku sama untuk semua perusahaan atau organisasi, baik yang besar maupun yang kecil, baik yang nasional maupun yang internasional. Dalam konteks ini, jangan-jangan justru perusahaan digital yang kecil, menegah, nasional atau lokal yang akan berguguran lebih dulu karena tidak mampu memenuhi syarat dan standar GDPR? Mereka tidak memiliki ketangguhan finansial, teknologi, jaringan dan SDM yang memadai untuk bertransformasi ke era pasca GDPR di mana standar perlindungan data pribadi menjadi sedemikian tinggi. Sementara perusahaan platform seperti seperti *Google, Facebook, Amazon, Alibaba* dan lain-lain sekali lagi --meskipun menderita kerugian signifikan sebagai dampak pemberlakuan GDPR-- tetap mampu bertahan dan menjaga dominasi dalam lanskap digital global.

Hal ini yang perlu dipertimbangkan jika Indonesia hendak melembagakan GDPR. Kita perlu menimbang benar dampaknya terhadap industri digital nasional. Mesti dipastikan bahwa regulasi semacam GDPR memberikan afirmasi yang tegas terhadap pembangunan lanskap digital nasional. Berbicara tentang lanskap digital nasional, berarti kita sekaligus berbicara tentang nasib media (jurnalistik) online, perusahaan *ecommerce*, perusahaan-perusahaan lain yang berdasar pada pemanfaatan teknologi internet, serta lingkup industri kreatif secara keseluruhan. Jangan sampai yang terjadi adalah peraturan yang dikeluarkan pemerintah atau DPR justru menghambat perusahaan-perusahaan rintisan digital nasional, tetapi hanya memberikan “sedikit goncangan” untuk perusahaan raksasa digital global yang beroperasi di Indonesia. Meskipun di sisi lain juga perlu diakui, keberadaan GDPR sangat mendesak untuk melindungi privasi dan keselamatan setiap orang dari berbagai bentuk kejahatan digital, serta untuk mengoreksi hegemoni perusahaan raksasa digital global di Indonesia. Operasi perusahaan-perusahaan ini perlu untuk secara sah dan transparan segera dikendalikan demi melindungi kepentingan nasional Indonesia yang warganya sedang bereuforia dengan media-media baru berbasis teknologi internet dan telephon-pintar.