

URGENSI PENGATURAN DATA DIGITAL/ ELEKTRONIK PRIBADI

Deny Susanto¹

¹Institut Bisnis dan Informatika Kwik Kian Gie

Email : deny.susanto@kwikkiangie.ac.id

ABSTRAK

Pengaturan Data Pribadi adalah wujud perlindungan hukum bagi individu warga masyarakat yang saat ini urgensinya dibutuhkan di Indonesia, dalam semua sektor kehidupan warga masyarakat baik dalam aktifitas bisnis atau bidang kehidupan lain, pemrosesan data terkait dengan individu yang menyangkut identitas baik rahasia ataupun tidak termasuk data-data yang sensitive dari segi ekonomis harus memperhatikan keamanan data-datanya, penelitian ini menggunakan penelitian hukum normative dengan mengkaji aturan regulasi terkait dengan perlindungan data, untuk melihat mengenai urgensi dan tata laksana yang efektif mengenai perlindungan data pribadi di Indonesia, dan diharapkan dalam penelitian ini dapat diformulasikan suatu regulasi yang komprehensif mengenai pengaturan perlindungan data pribadi di Indonesia.

Kata kunci: *Perlindungan Data, Data Elektronik, Perlindungan Hukum*

ABSTRACT

Regulation of Personal Data is a type of legal protection for individual citizens that is urgently required in Indonesia right now. This protection is needed in all spheres of community life, including business activities and other fields of life, where data processing relating to individuals concerning identity, whether confidential or not, is involved. In order to understand the urgency and effective management of personal data protection in Indonesia, this research uses normative legal research to review regulatory rules related to data protection. It is hoped that this research will result in the formulation of a comprehensive regulation on protection arrangements and private information in Indonesia.

Keyword: *Data Protection, Electronic Data, Law Protection*

PENDAHULUAN

Pencemaran udara atau polusi udara kian hari semakin meningkat, ini sangat memprihatinkan mengingat pencemaran adalah hal yang sangat membahayakan bagi kelangsungan makhluk hidup dan lingkungannya. Di Kota-Kota besar, kontribusi gas buang kendaraan bermotor sebagai sumber polusi udara mencapai 60-70%. Sedangkan kontribusi gas buang dari cerobong asap industri hanya berkisar 10-15%, sisanya berasal dari sumber pembakaran lain, misalnya dari rumah tangga, pembakaran sampah, kebakaran hutan, dll. Sebenarnya banyak polutan udara yang perlu diwaspadai, tetapi organisasi kesehatan dunia (WHO) menetapkan beberapa jenis polutan yang dianggap serius.

Beberapa waktu belakangan publik dikejutkan dengan pemberitaan di media massa mengenai kebocoran atas data-data pribadi individu yang ada di lembaga/instansi pemerintah atau negara maupun data-data pribadi yang ada pada perusahaan-perusahaan

swasta yang berbentuk *start-up fintech*. Yang terbaru adalah mengenai dugaan adanya kebocoran data pada sistem milik Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan.

Sebelumnya dilaporkan data dari sekitar 279 juta penduduk di Indonesia telah dijual dan ditawarkan pada suatu forum *online* yang bernama *Raid Forums* oleh akun bernama Kotz (Bill Clinton, 2021). Adapun data yang dijual berisi nomor kartu (noka), NIK, nomor ponsel, e-mail, alamat, dan gaji. Data tersebut termasuk data penduduk yang telah meninggal dunia. Untuk memastikan data tersebut valid, akun bernama Kotz ini membagikan sejumlah 1 juta sampel data yang dapat diunduh secara bebas oleh pengguna. Pemerintah melalui Kementerian Komunikasi dan Informatika telah mendalami kasus ini dan menemukan bahwa sampel data identik dengan data milik BPJS Kesehatan, temuan tersebut kemudian mengarah pada data yang identik dengan data pada BPJS berdasarkan pada struktur data yang terdiri dari Noka (Nomor Kartu), Kode Kantor, Data Keluarga/Data Tanggungan, dan status Pembayaran.

Kemudian kasus terkait dengan data pemilih pada Komisi Pemilihan Umum (KPU) terjadi pada sekitar Mei 2020 dimana data yang bocor adalah Nama Lengkap dan Nomor Kartu Pemilih yang diperkirakan mencapai sekitar 2,3 juta nama pemilih dimana ada klarifikasi dari KPU bahwa terbukanya data pemilih ini bukan dikarenakan kesalahan data sistem atau *human error*, melainkan mutlak karena datanya sudah terbuka dan terekspose ke publik (Tim CNN, 2020).

Kasus terbukanya data yang hingga berujung ke pengadilan adalah gugatan pengadilan yang terdaftar di Pengadilan Negeri Jakarta Pusat pada 8 Mei 2020 dengan Nomor: 235/PDT.G/2020/PN.JKT.PST dengan klasifikasi perkara Perbuatan Melawan Hukum (Tergugat I yakni Menteri Komunikasi dan Informatika (Menkominfo) serta PT Tokopedia sebagai Tergugat II). Gugatan dilakukan oleh Komunitas Konsumen Indonesia yang mewakili dan menjadi korban dalam terbukanya data pada *platform e-commerce* Tokopedia dimana data pribadi yang bocor berupa nama lengkap, nama akun, email, toko online, tanggal lahir, nomor HP, tanggal mendaftar, dan sejumlah data yang terenkripsi berbentuk *hash* dengan perkiraan data jumlah yang bocor 91 juta data pengguna dan 7 juta *merchant* (Adhi Wicaksono, 2020; Rahmad Fauzan, 2020; Wahyunanda Kusuma Pertiwi, 2020). Tokopedia ini

kemudian melakukan klarifikasi, melaporkan kepada pihak berwajib, berkoordinasi dengan pemerintah serta pihak berwenang, dan telah menerapkan langkah-langkah keamanan.

Pengaturan mendesak perihal perlindungan data pribadi yang tersedia pada media elektronik atau digital saat ini di Indonesia sangat dibutuhkan. Suatu data pribadi pada media elektronik atau digital saat ini tersedia melalui sistem internet, sebagai suatu sistem yang terbuka dan dapat siapapun melakukan akses dengan atau tanpa proteksi. Data-data pribadi dapat selalu berhubungan dengan aset lainnya baik yang memiliki nilai ekonomi maupun tidak, sehingga sangat berpotensi terjadi penyalahgunaan (Susanto, 2022).

Jika dikaitkan dengan perbuatan hukum yang bernilai ekonomis seperti misalnya transaksi digital yang dilakukan pada suatu *platform e-commerce*, maka transaksi digital tersebut selalu menggunakan "*identifier*" data pribadi sebagai *validator* untuk menguji mengenai kapasitas dari subjek hukum yang melakukan proses transaksi tersebut. Perlindungan tidak dapat hanya dilakukan dari sisi teknologinya namun yang lebih penting juga aspek hukumnya.

Berdasarkan statistik dari Bank Indonesia dan *platform statistika* (<https://www.Statista.Com/Statistics/958171/Indonesia-Online-Transaction-Value/>, 2021), periode tahun 2018 sampai dengan 2021 telah terjadi peningkatan pada aspek transaksi digital yang digambarkan pada tabel sebagai berikut:

No.	Tahun	Jumlah Transaksi (kali)	Nilai Transaksi (rupiah)
1.	2018	40 juta	47,1 Trilyun
2.	2019	80 juta	152,6 Trilyun
3.	2020	140 juta	204,9 Trilyun
4.	2021	573 juta	3114 Trilyun

dari tabel di atas terjadi peningkatan yang signifikan pada jumlah transaksi yang berbanding lurus dengan peningkatan nilai transaksi pada periode waktu 4 tahun secara berturut-turut, hal ini tentu saja mengindikasikan adanya suatu peningkatan transaksi yang mengandung aspek ekonomi dengan meningkatnya risiko atas celah keamanan yang dihubungkan dengan aspek data pribadi.

METODE PENELITIAN

Metode penelitian yang digunakan adalah menggunakan metode penelitian hukum normatif, yaitu melakukan analisis dari sumber primer peraturan atau regulasi hukum mengenai peraturan data pribadi yang saat ini tersedia pada berbagai aturan hukum di Indonesia. Selain itu dikaji juga mengenai analisis dari referensi ilmiah dan buku yang menunjang mengenai penelitian ini.

HASIL PENELITIAN DAN PEMBAHASAN

A. Perbandingan Hukum Tentang Konsep Dan Definisi Mengenai Data Digital Pribadi

GDPR

Uni Eropa (UE) membentuk Regulasi Perlindungan Data (*General Data Protection Regulation*) yakni suatu bentuk regulasi dalam hukum Uni Eropa (UE) yang mengatur mengenai perlindungan data pribadi di dalam maupun di luar UE. Regulasi perlindungan data terbaru yang diadopsi UE ini adalah Regulasi Umum Perlindungan Data (*General Data Protection Regulation/GDPR*) yakni Regulasi (EU) 2016/679 tanggal 27 April 2016 (*Official Journal of the European Union*, 2021).

Regulasi ini dilandasi oleh Piagam Hak Asasi Uni Eropa yang menetapkan bahwa warga UE memiliki hak untuk melindungi data pribadi mereka. Personal Data: Data berarti informasi yang tersimpan (secara elektronik), tanda-tanda atau indikasi-indikasi. Namun, data harus 'pribadi' (personal) agar dapat masuk dalam ruang lingkup penerapan Regulasi GDPR. Data dianggap pribadi jika informasi tersebut berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi (Pasal 4 No.1 GDPR). GDPR telah memberikan suatu standar atas undang-undang perlindungan data di semua negara anggota UE dan menerapkan aturan baru yang ketat untuk mengendalikan dan memproses informasi identitas pribadi. Regulasi ini juga telah memperluas perlindungan data pribadi dan hak perlindungan data dengan memberikan kendali kembali ke penduduk UE. GDPR mengatur perorangan, perusahaan atau organisasi yang memproses data pribadi individu di UE. GDPR menggantikan regulasi Direktif Perlindungan Data UE 1995, dan mulai berlaku pada tanggal 25 Mei 2018 (Lahiri, 2018).

GDPR mengenal sistem *active digital footprint* dan *passive digital footprint*. *Active digital footprint* adalah informasi (tentang diri mereka sendiri atau yang lain) yang

ditinggalkan oleh pengguna pada saat menggunakan internet, biasanya secara sadar, tidak terlalu dibutuhkan atau dianggap tidak dibutuhkan. Sedangkan *passive digital footprint* adalah yang secara tidak sadar ditinggalkan oleh pengguna saat menggunakan layanan internet.

UNIDROIT

UNIDROIT (secara formal, Institut Internasional untuk Penyatuan Hukum Perdata; Bahasa Prancis: Institut international pour l'unification du droit privé) adalah organisasi antar pemerintah yang memiliki tujuan untuk melakukan harmonisasi Hukum perdata internasional di seluruh negara dengan penyeragaman aturan, konvensi internasional, dan produksi model hukum, seperangkat prinsip, panduan, dan pedoman. Didirikan pada 1926 sebagai bagian dari Liga Bangsa-Bangsa, institut ini didirikan kembali pada 1940 karena pembubaran Liga Bangsa-Bangsa melalui perjanjian multilateral, menurut Statuta UNIDROIT per tahun 2019, bahwa UNIDROIT memiliki sejumlah 63 anggota negara.

Personal Data diartikan sebagai Data yang bersifat pribadi jika identifikasi seseorang dapat dilakukan berdasarkan data yang tersedia, artinya bila seseorang dapat dideteksi, secara langsung atau tidak langsung dengan mengacu pada suatu pengidentifikasi (*identifier*), merujuk ke satu atau lebih karakteristik yang merupakan ekspresi dari identitas fisik, fisiologis, psikologis, genetik, ekonomi, budaya atau sosial, misalnya: nama seseorang, nomor identifikasi, seperti nomor asuransi sosial, nomor personil atau nomor KTP, data lokasi, pengidentifikasi online (seperti alamat IP atau *cookie*).

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (PP PSTE) Dan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)

Pasal 1 angka 29 PP PSTE menjelaskan bahwa Data Pribadi adalah setiap data tentang seseorang, baik yang teridentifikasi dan dapat diidentifikasi tersendiri atau dikombinasikan dengan informasi lainnya, secara langsung maupun tidak langsung melalui sistem elektronik dan non-elektronik.

Dalam RUU PDP, terdapat hubungan hukum kontraktual bahwa pemrosesan data pribadi dilakukan melalui suatu bentuk persetujuan tertulis atau lisan terekam, dimana

dibedakan menjadi 2 (dua) jenis kategori yakni umum dan khusus, kategori umum terdiri dari nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang sedangkan kategori khusus terdiri dari data dan informasi kesehatan, data biometrik, data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

B. Ruang Lingkup Hak Pribadi (Data Pribadi) Dalam GDPR Dan UNIDROIT

Dikenal adanya suatu Hak Kontrol yang menimbulkan Hak Otonomi, dalam lingkup secara umum bahwa setiap individu berwenang penuh atas data pribadi yang dikenal dengan adanya hak control yang mencakup penghapusan data dan hak otonomi yang terkait dengan informasi *self determination* (hak apa saja yang dapat dibuka untuk umum oleh pribadi yang bersangkutan).

ruang lingkupnya terdiri dari: 1) meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, mengakses data pribadi miliknya, 2) memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi miliknya, 3) mengakhiri pemrosesan, menghapus, dan/atau memusnakan data pribadi miliknya menarik kembali persetujuan pemrosesan data pribadi miliknya, 4) mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang, 5) memilih atau tidak memilih pemrosesan data pribadi melalui mekanisme pseudonim untuk tujuan tertentu, 6) mendapatkan dan/atau menggunakan data pribadi miliknya, 7) menggunakan dan mengirimkan data pribadi miliknya ke pengendali data pribadi lainnya, 8) menuntut dan menerima ganti rugi atas pelanggaran data pribadi miliknya.

C. Perlindungan Hak

Dalam melaksanakan fungsi pengelolaan Data Pribadi Digital (Kustodian-Kurator) maka akan dikenal fungsi-fungsi antara lain yang melakat pada Pengendali Data Pribadi, Pihak Ketiga, dan Individu Pengguna.

Beberapa catatan mengenai respon dari perusahaan/instansi terhadap kasus kebocoran Data sepanjang masa Pandemi (2020-2021) berdasarkan pengamatan dari liputan berita oleh pers media massa antara lain:

- 1) Masing-masing Penyelenggara Sistem Elektronik (PSE) menggunakan *action plan* yang berbeda-beda terhadap kebocoran data yang terjadi.
- 2) Tidak semua PSE melakukan klarifikasi kepada publik secara formal terhadap potensi kebocoran data, ada PSE yang menyanggah data bocor, karena data yang bocor adalah data pengguna yang sudah lama bocor (contoh *Platform Bukalapak*).
- 3) Beberapa PSE meminta maaf secara formal kepada pengguna. PSE yang tidak melakukan klarifikasi secara formal memberikan notifikasi kepada korban terhadap kebocoran data, kecuali BPJS Kesehatan.
- 4) Ada PSE yang menyatakan data bocor adalah data terbuka, sehingga hal tersebut bukan termasuk kebocoran data (misal data KPU pada saat pemilihan umum Presiden dan Wakil Presiden).
- 5) Beberapa PSE tidak menerapkan kontrol ganda untuk mengamankan data Pribadi.
- 6) sebelum kebocoran terjadi Beberapa PSE Swasta berkoordinasi dengan BSSN terhadap kebocoran data.

Pada prinsipnya, dalam RUU PDP suatu pengelolaan data pribadi harus dilakukan dengan cara-cara sebagai berikut:

- 1) Terbatas dan spesifik, sah secara hukum, patut dan transparan
- 2) Sesuai dengan tujuan
- 3) Menjamin hak pemilik data pribadi
- 4) Akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggung jawabkan
- 5) Dilindungi keamanannya dari pengaksesan pengungkapan, dan perubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan data pribadi
- 6) Memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan perlindungan data pribadi
- 7) Dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan pemilik data pribadi sesuai peraturan perundang- undangan
- 8) Bertanggung jawab dengan memenuhi pelaksanaan prinsip perlindungan data pribadi dan dapat dibuktikan secara jelas.

Aspek hukum diperlukan untuk mengatur mengenai tata kelola dan norma agar tidak terjadi penyalahgunaan atau pelanggaran yang dikenal juga sebagai *fraud* atau *negligence*

(kelalaian). Dalam ketentuan dunia perbankan, definisi fraud diatur dalam Surat Edaran No. 13/28/ DPNP Tahun 2011 mengenai Penerapan Strategi Anti Fraud bagi Bank Umum. Fraud dikatakan sebagai tindakan penyimpangan atau pembiaran yang sengaja dilakukan untuk mengelabui, menipu, atau memanipulasi Bank, nasabah, atau pihak lain yang terjadi di lingkungan Bank dan/atau menggunakan sarana Bank sehingga mengakibatkan Bank, nasabah, atau pihak lain menderita kerugian baik secara langsung maupun tidak langsung (Kismawadi, 2021).

KESIMPULAN

Isu yang akan muncul di masa mendatang perlu diantisipasi khususnya dengan perkembangan transaksi digital dengan berbagai *platform* seperti halnya mengenai *Digital Asset*, *Cripto Asset*, *Cripto Currency*.

Indonesia belum ada pengaturan mengenai Perlindungan Data Pribadi dan/atau *Digital Asset* oleh karenanya bahwasanya pengaturan mengenai Perlindungan Data Pribadi adalah sebuah keharusan, Perlindungan Data Pribadi Elektronik/Digital tidak hanya dari aspek teknologi tapi yang lebih penting adalah aspek hukum agar keamanan data elektronik dapat dilindungi hukum. Bahwasanya Perlindungan Data Pribadi selalu terkait dengan digital aset, sehingga juga diperlukan peraturan perundang-undangan terkait dengan Digital Aset.

DAFTAR PUSTAKA

- Adhi Wicaksono. (2020, July 20). <https://www.cnnindonesia.com/teknologi/20200706104712-185-521267/91-juta-data-pengguna-bocor-di-fb-tokopedia-lapor-polisi>. CNN Indonesia.
- Bill Clinton. (2021, May 25). <https://tekno.kompas.com/read/2021/05/25/15020057/data-bpjs-kesehatan-bocor-cek-apakah-anda-terdampak-?page=all> .
- <https://www.statista.com/statistics/958171/indonesia-online-transaction-value/>. (2021, June 15).
- Kismawadi, E. R. (2021). *Fraud Pada Lembaga Keuangan Dan NonKeuangan-Rajawali Pers*. PT. RajaGrafindo Persada.
- Lahiri, K. (2018). *US Businesses Can't Hide From GDPR*.

Official Journal of the European Union. (2021, June 15). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. GDPR.

Rahmad Fauzan. (2020, June 19). <https://kabar24.bisnis.com/read/20200619/16/1254883/sidang-kasus-kebocoran-data-tokopedia-posisikan-diri-sebagai-korban>. Kabar Bisnis.

Susanto, D. (2022). Sharia-Based Legal Formula For Personal Data Protection In The Financial Services Industry Post-Covid-19 Pandemic. *BULLET: Jurnal Multidisiplin Ilmu*, 1(04), 545–552.

Tim CNN. (2020, May 21). <https://www.cnnindonesia.com/teknologi/20200521223601-185-505726/23-juta-data-kpu-diduga-bocor-dijual-di-forum-hacker>. CNN Indonesia.

Wahyunanda Kusuma Pertiwi. (2020, June 10). <https://tekno.kompas.com/read/2020/06/10/09144017/sidang-perdana-kasus-kebocoran-data-tokopedia-digelar-hari-ini?page=all>.