WIDYA YURIDIKA: JURNAL HUKUM
P-ISSN: 2615-7586, E-ISSN: 2620-5556
Volume 3, Nomor 2, Desember 2020

PERBANDINGAN KEBIJAKAN SISTEM *BIG DATA* DI INDONESIA DAN UNI EROPA

Tanzil Kurmiawan[1], Anang Setiyawan[2], Woro Winandi[3]

[1]Program Pascasarjana, Magister Hukum, Universitas Wiraraja. Email: tanzilkurnain@gmail.com
[2]Program Pascasarjana, Magister Hukum, Universitas Wiraraja
[3]Program Pascasarjana, Magister Hukum, Universitas Wiraraja

ABSTRAK

Hak asasi manusia merupakan privasi individu yang harus atau wajib dilindungi oleh negara dan diakui secara internasional. Perlindungan privasi diatur dalam pasal 28 G ayat (1) Undang-Undang Dasar 1945. Peraturan pemerintah di Indonesia cukup banyak dalam mengatur privasi individu pada data pribadi namun belum cukup tegas dan jelas dalam mengatur perlindungan dan kerahasiaan privasi individu khususnya yang tersimpan dalam *big data*. Perkembangan big data di Indonesia sangat pesat sehingga telah banyak pihak yang mengambil keuntungan bisnis dengan mengelola data warga negara Indonesia dalam sistem yang dibuatnya. Namun hal tersebut tidak diimbangi dengan adanya pembaruan regulasi dan adanya kepastian hukum atas standar keamanan informasi yang diterapkan dalam sistem big data tersebut sehingga pemilik data mengalami kerugian jika terjadi pelanggaran atas data pribadinya. Hasil penelitian ini adalah membandingkan dan menganalisis peraturan yang berlaku di Indonesia dengan *General Data Protection Regulation* yang secara efektif berlaku di Uni Eropa sejak 2018.

ARTICLE INFO

Kata Kunci:
Perlindungan hukum, privasi individu, big data.

Cite this paper:
Tanzil Kurmiawan, A. S. W. W., 2020. Perbandingan Kebijakan Sistem Big Data Di Indonesia dan Uni Eropa. *Widya Yuridika: Jurnal Hukum,* 3(2).

PENDAHULUAN

Perkembangan teknologi informasi semakin maju seiring dengan perkembangan zaman. Perkembangan teknologi ini menjadi peluang dan tantangan bagi masyarakat. Berbagai pengembangan baik secara *software* maupun *hardware* terus dilakukan. Perkembangan teknologi informasi merupakan adanya interaksi aktif baik antara individu dengan pihak peneyedia jasa dan informasi.[1] Informasi dan data memiliki keterkaitan yang erat. Informasi merupakan data yang memiliki makna dan dapat diolah menjadi bentuk yang lebih berarti. Sementara data adalah kumpulan fakta-fakta yang

[1] Sinta Dewi, *Konsep perlindungan hukum atas privasi dan data pribadi dikaitkan dengan pengguanaan cloud computing di Indonesia*,Yustisia Vol.5 no.1. 2016

menggambarkan suatu kejadian pada saat tertentu.[2] Dengan kemajuan teknologi terkini, data dengan ukuran kecil dapat dengan mudah dibagikan melalui berbagai perangkat dan aplikasi. Misalnya melalui media sosial, *e-mail*, blog/web, dan sebagainya. Sementara untuk data dengan jumlah banyak dan ukuran yang lebih besar, disimpan dan dibagikan dengan bantuan sistem *cloud*.

Konsep sistem *cloud* inilah yang menjadi dasar pengembangan sebuah *big data*. dalam *big data* berbagai macam bentuk dan ukuran data akan tersimpan dalam satu wadah yang disebut dengan Pusat Data / *Data Center*. Saat ini implementasi *big data* dan analisis data diperlukan oleh berbagai perusahaan untuk mengumpulkan data pengguna bagi kepentingan kemajuan bisnis perusahaan. Sebagai contoh penerapan sebuah sistem *big data* adalah penyimpanan dan pemrosesan data pengguna aplikasi *facebook* dan perusahaan *starup*, GOJEK dan perusahaan lainya. Hasil analis *big data* sangat menguntungkan bisnis perusahaan. Sementara bagi pengguna, manfaatnya tergantung dari jenis layanan yang didapatkan. Data pengguna tersimpan dan diproses tanpa diketahui maksud dan tujuannya bahkan tidak tahu sampai kapan data tersebut dipergunakan. Bisa saja data-data disalahgunakan oleh perusahaan pemilik dengan tujuan lain atau bahkan diperjualbelikan kepada pihak lain tanpa sepengetahuan pemilik data. Itulah pentingnya sebuah regulasi yang mampu mengatur secara jelas dan tegas tentang implementasi analisis sistem *big data.*

Istilah *big data* pertama kali muncul sekitar tahun 2005-an yang diperkenalkan oleh O'Reilly Media. Sejak saat itu berbagai perusahaan berusaha untuk mempelajari konsep *big data* dan berupaya menemukan sistem yang tepat sebagai cara untuk memanfaatkan *big data* untuk pengembangan bisnisnya. Salah satu pihak yang sukses dalam mengembangkan teknologi *big data* adalah perusahaan Google dan Facebook. Sejak saat itu istilah *big data* menjadi pusat perhatian dalam perkembangan dunia teknologi. Secara sederhana, *big data* terdiri atas tiga V, yaitu *volume*, *variety*, dan *velocity*[3]. *Volume* berupa kapasitas atau ukuran media penyimpanan data dalam skala besar bahkan mungkin tidak terbatas. *Variety* adalah keragaman data berupa tipe atau jenis data yang dapat diolah, baik yang terstruktur maupun tidak terstruktur. Sementara *velocity* adalah kecepatan memproses data yang tersimpan. Pemanfaatan *big data* di berbagai sektor, organisasi dan perusahaan di Indonesia tetap memperhatikan aspek keamanan siber dan infrastruktur jaringan yang tersedia, sehingga bisa diimplementasikan secara efektif dan tepat sasaran. Namun demikian, setiap konsep teknologi yang canggih tetap memiliki celah, khususnya masalah privasi dan keamanan informasi. Sistem *big data* yang menyimpan data dalam ukuran besar, harus selalu dipastikan keamanannya khususnya di sisi infrastrukturnya. Sehingga tidak terjadi kebocoran di dalamnya. Keamanan siber juga bisa dijamin jika ada keterlibatan dan sinergitas antar berbagai pihak yang terkait. Pemerintah memiliki kewajiban dalam hal menyiapkan regulasi atau aturan-aturan yang bisa menjamin keamanan data tersebut.

Information Security atau keamanan informasi adalah bagaimana memahami dan mengontrol ancaman terhadap aset yang kita miliki dan lindungi. Keamanan informasi juga bisa berarti tindakan pencegahan dari serangan pengguna atau pengakses sebuah sistem yang tidak bertanggung jawab. Hal ini sangat penting untuk dipahami dalam hal

[2] Nafiudin, *Sistem informasi manajemen*, Qiara Media, Pasuruan, 2019, hlm. 24.

[3] Wijaya, W. M, Teknologi Big Data: Sistem Canggih di Balik Google, Yahoo!, Facebook, IBM (Vol. 1), Deepublish, Yogyakarta, hlm 8.

membuat sebuah kebijakan kaitannya dengan data pribadi yang disimpan dalam sebuah sistem *Big Data*. Prinsip dasar keamanan informasi adalah :

1. *Confidentiality* (kerahasiaan). Artinya informasi yang kita miliki pada sistem kita, adalah bersifat rahasia dan pengguna/orang lain yang tidak berkepentingan tidak dapat melihat/mengaksesnya.
2. *Integrity* (integritas). Artinya informasi sesuai dengan aslinya, tidak diubah oleh pihak yang tidak berwenang, sehingga konsistensi, akurasi, dan validitas informasi tersebut tetap terjaga.
3. *Availability* (ketersediaan). Artinya dipastikan bahwa informasi selalu tersedia dan dapat diakses oleh pihak yang membutuhkan dan berwenang atas informasi tersebut.

Penyalahgunaan data dapat merugikan pihak pemilik sistem dan pemilik data. Beberapa hal yang dapat menjadi ancaman keamanan informasi yaitu:

1. *Interruption*. Yaitu suatu ancaman terhadap ketersediaan data, dengan cara data yang ada dalam sistem dirusak atau dihapus sehingga informasi yang tersedia dalam data tersebut sudah tidak ada lagi.
2. *Interception*. Yaitu ancaman terhadap kerahasiaan isi data. Informasi yang ada dalam data tersebut disadap atau dapat diketahui oleh orang yang tidak berhak atas data tersebut.
3. *Modification*. Yaitu ancaman terhadap integritas data, dengan cara mengakses jalur lalu lintas informasi yang sedang dikirim kemudian merubahnya sesuai dengan keinginan orang tersebut.
4. *Fabrication*. Yaitu dengan cara memalsukan isi informasi suatu data sehingga membuat orang yang menerima data tersebut menganggap informasi itu berasal dari orang yang dapat dipercaya.

Pada tahun 2019, *facebook* menghapus *backup* data pengguna yang tersimpan di server *cloud* Amazon menyusul adanya laporan terekseposnya 540 juta data pengguna *facebook*. Sama halnya dengan *facebook*, aplikasi lain yang menerapkan sistem *big data* adalah aplikasi *marketplace* atau belanja secara daring. Contoh implementasi analis *big data* oleh lembaga pemerintah adalah program *Horizon Scanning Center* di United Kingdom (Inggris). Dilansir ec.europe.eu, program *Foresight dan Horizon Scanning* yang diterapkan di Uni Eropa berhasil merekomendasikan kebijakan jangka panjang di bidang teknologi guna mengantisipasi tantangan yang muncul dalam masyarakat. Studi *foresight* tersebut bahkan mampu menganalisis tantangan sosial berdasarkan penelitian dan kebijakan Uni Eropa yang telah dilakukan selama kurun waktu lima hingga tiga puluh tahun.

Seiring perkembangan sistem *big data* yang telah banyak dimanfaatkan baik oleh lembaga pemerintah maupun perusahaan swasta di Uni Eropa, *Big data* tidak akan ada artinya jika tidak ada proses pengumpulan data dari masyarakat. Oleh karena itu, masyarakat sangat berperan dalam memberikan data yang tepat dan akurat. Masyarakat perlu jaminan data yang diberikan dapat digunakan dengan semestinya. Tidak adanya jaminan perlindungan keamanan dan kerahasiaan data, akan menyebabkan data di dalamnya mudah dicuri dan disalahgunakan. Data sensitif seperti privasi individu yang dikumpulkan dan disimpan dalam sebuah *big data*, seharusnya telah diatur sebuah mekanisme yang menjamin bagaimana data tersebut dilindungi, dibagi, dipelihara dan dimusnahkan. Salah satu isu bobolnya *big data* di Indonesia adalah klaim seorang peretas dari akun twitter @underthebreach, yang mengklaim telah membobol data 2,3 juta warga Indonesia dari sistem KPU.

Menurut Undang-Undang Dasar Negara Republik Indonesia, negara Indonesia adalah negara hukum yaitu negara yang menegakkan supremasi hukum untuk menegakkan kebenaran dan keadilan. Negara Indonesia merupakan penganut sistem hukum Eropa Kontinental sejak era penjajahan, yang sangat kental dengan unsur kepastian hukum. Salah satu aspek asas kepastian hukum adalah penegakan hukum. Pelanggaran atau tindak kejahatan dapat dipidana apabila telah ada undang-undang atau hukum tertulis yang mengaturnya. Unsur-unsur utama dalam sistem Eropa Kontinental yang dikemukakan Julius Stahl sebagaimana dikutip Azhary, yaitu:[4]

1. Mengakui dan melindungi hak-hak asasi manusia;
2. Untuk melindungi hak asasi tersebut maka penyelenggaraan negara harus berdasarkan pada teori trias politika (pemisahan);
3. Di saat menjalankan tugasnya, pemerintah berdasarkan undang-undang (welmatigh bestuur); dan
4. Apabila dalam menjalankan tugasnya berdasarkan undang-undang pemerintah masih melanggar hak asasi (campur tangan pemerintah dalam kehidupan pribadi seseorang), maka akan ada pengadilan yang akan menyelesaikannya.

Data privasi individu merupakan hak asasi yang dilindungi oleh negara. Sebagaimana diatur dalam Undang-Undang Dasar 1945 Pasal 28 G ayat(1). Sementara berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, perlindungan data pribadi yang juga merupakan privasi individu yang bukan untuk dibuka dan dipublikasikan. Pemerintah wajib menjamin dan memastikan privasi individu yang dikumpulkan dan disimpan dalam bentuk data-data di sistem *big data* harus berada dalam kondisi aman dan terlindungi. Salah satunya penggunaan *General Data Protection Regulation* (GDPR). Wilayah Uni Eropa secara efektif memperlakukakan GDPR dan mengikat masalah perlindungan privasi warga negara anggotanya. Masyarakat memerlukan kepastian hukum mengenai data yang diberikan. Bentuk perlindungan subjek hukum tersebut termasuk di dalamnya yaitu keamanan dan kerahasiaan data pribadi masyarakat dalam sebuah sistem *big data.* Hal ini sama artinya dengan melindungi privasi individu masyarakat tersebut. Melindungi privasi menjadi sebuah tuntutan bagi negara sebagai bentuk penghargaan atas hak seseorang sehingga masyarakatnya dapat lebih menikmati kehidupannya. Dengan demikian diperlukan adanya pengetahuan mengenai perbandingan kebijakan sistem big data di Indonesia dan Uni Eropa agar dapat memberikan manfaat terhadap perusahaan dan masyarakat.

Artikel ini ditulis berpedoman pada penelitian hukum normatif dengan pendekatan *statuta* dan *comparative approach*. Penelitian hukum dilakukan dengan maksud untuk menemukan kebenaran koherensi, yaitu adakah aturan hukum yang sesuai dengan norma hukum, kemudian adakah norma yang berupa perintah atau larangan itu sesuai dengan prinsip hukum, serta apakah tindakan yang dilakukan seseorang telah sesuai dengan norma hukum atau prinsip hukum yang ada, yaitu kaitannya dengan kebijakan sistem *big data* di Indonesia dan bagaimana perbandingan perlindungan hukum atas privasi individu dalam kebijakan tersebut dengan yang diatur di Uni Eropa. Pendekatan *statute approach* dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi di Indonesia yang berkaitan dengan perlindungan hukum atas privasi individu, khususnya yang diatur dalam kebijakan sistem *big data* di Indonesia, apakah ada konsistensi dan kesesuaian antara undang-undang atau aturan-aturan yang satu dengan

[4] Miriam Budiarjo, *Dasar-Dasar Ilmu Politik*, Gramedia, Jakarta, 1993, hlm 57.

undang-undang atau aturan-aturan yang lainnya. Sedangkan pendekatan komparatif (*comparative approach*) dilakukan dengan cara membandingkan undang-undang yang berlaku di Indonesia dengan undang-undang di negara lain, dengan tujuan memperoleh hasil tentang persamaan dan perbedaan di antara keduanya. Peraturan perundang-undangan yang digunakan sebagai pembanding adalah peraturan perundang-undangan yang berlaku di Uni Eropa, seperti *General Data Protection Regulation* (GDPR) atau peraturan lain mengenai sistem *big data* dan perlindungan privasi individu.

HASIL DAN PEMBAHASAN

Privasi individu sebagai hak asasi diakui secara internasional sebagaimana tercantum dalam *Universal Declaration of Human Rights* atau Deklarasi Universal Hak-Hak Asasi Manusia (UDHR) oleh Perserikatan Bangsa-Bangsa pada tanggal 10 Desember 1948. Adanya perbedaan dan persamaan mengenai peraturan sistem *big data* di Indonesia dan Uni Eropa menjadi tantangan sendiri untuk memberikan pengetahuan mendalam mengenai peraturan hukum yang ada.

A. Persamaan Dan Perbedaan Kebijakan Sistem *Big Data* Di Indonesia Dan Uni Eropa

1. Definisi dan Jenis Data Pribadi yang Disimpan dalam Sistem *Big Data*

Persamaannya adalah privasi individu merupakan hak asasi manusia yang wajib dilindungi oleh negara dan telah diakui secara internasional. Definisi privasi yang diatur dalam peraturan perundang-undangan di Indonesia secara garis besar sama dengan yang diatur di Uni Eropa, namun tetap butuh penegasan secara khusus di UU ITE. Pengaturan tentang penyelenggaraan sistem elektronik yang memproses data pribadi di dalamnya sudah sama-sama ada baik di Indonesia maupun di Uni Eropa. Hanya saja di Indonesia pengaturan secara rinci, jelas dan tegas bukan diatur dalam Undang-undang, melainkan Peraturan Pemerintah. Perbedaan sistem *big data* dapat terlihat dari perbedaan peraturan di Indonesia dan Uni Eropa dimana dalam Undang-Undang ITE yang mengatur secara khusus tentang sistem elektronik, tidak menjelaskan secara tegas apa yang termasuk dalam kriteria data pribadi. Penegasan tentang data pribadi justru dijelaskan di Undang-Undang lain, yaitu Undang-Undang Nomor 24 tahun 2013 tentang Administrasi Kependudukan. Hal ini menyebabkan penanganan kasus hukum kaitannya dengan pelrindungan data pribadi yang diproses dalam sebuah sistem elektronik menjadi sulit diselesaikan. Berbeda dengan yang dijelaskan dalam GDPR Uni Eropa, yang dengan tegas mendeskripsikan kriteria data pribadi yang dilindungi. Dalam pasal 4 GDPR, data pribadi diartikan sebagai segala informasi yang berkaitan dengan seseorang yang dapat diidentifikasi baik secara langsung maupun tidak langsung, khususnya yang merujuk pada identitas orang tersebut, seperti nama, nomor identifikasi, data lokasi, *userid/username*, kondisi fisik, fisiologis, genetik, mental, ekonomi, kesehatan, budaya atau kehidupan sosial orang tersebut.

Pengaturan definisi dan jenis data pribadi juga disebutkan dengan jelas dan tegas dalam *Data Protection Act 2018 (DPA)*. DPA merupakan undang-undang di negara Inggris yang merupakan implementasi GDPR. Data pribadi yang diatur di dalam DPA termasuk di antaranya adalah merupakan data sensitif, seperti ras, latar belakang etnis, opini politik, keyakinan agama, keanggotaan serikat pekerja, genetika, biometrik, informasi kesehatan dan kehidupan seksual. Pengaturan definisi dan jenis data pribadi dalam sebuah peraturan perundang-undangan sangatlah penting, terutama yang berkaitan dengan pengelolaan data dalam sebuah sistem elektronik. Dengan menegaskan definisi dan jenis data pribadi, maka baik pihak pemilik data maupun pengelola data akan lebih berhati-hati dan bertanggung jawab atas data-data tersebut. Pengeloa data hanya akan meminta data

sesuai dengan tujuan pengelolaan data. Dengan demikian prinsip *minimitation* dan *storage limited* bisa diterapkan dan penyalahgunaan data bisa diantisipasi.

Perlindungan hukum atas data pribadi yang diatur di dalam GDPR adalah kepastian hukum atas perlindungan beberapa hak pemilik data. Di antaranya adalah hak agar data miliknya disediakan dan dibuka aksesnya untuk pemilik data. Pemilik data juga berhak memiliki salinan data miliknya yang disimpan dan diolah dalam sebuah sistem, serta informasi mengenai tujuan pengolahan data, kategori data apa saja yang diolah, siapa saja yang dapat melihat data tersebut, serta berapa lama data tersebut disimpan dan diolah dalam sistem. GDPR menjamin jika terjadi kerusakan atau perubahan data, maka pemilik data dapat meminta pengelola data agar memperbaiki atau menghapus data tersebut, serta menyampaikan keluhannya kepada otoritas pengawas perlindungan data yang berwenang.

2. Pihak yang Bertanggung Jawab

Undang-Undang Informasi dan Teknologi Informasi di Indonesia sebagaimana telah dijelaskan sebelumnya, pihak yang bertanggung jawab atas perlindungan data pribadi disebut Penyelenggara Sistem Elektronik (PSE). PSE yang dimaksud adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. Di dalam PP Nomor 71 Tahun 2019, PSE dibagi menjadi dua, yaitu PSE lingkup publik dan PSE lingkup privat. Lingkup publik artinya penyelenggara tersebut berbentuk institusi penyelenggara negara atau yang ditunjuk oleh institusi penyelenggara negara, sementara lingkup privat diselenggarakan oleh orang, badan usaha dan masyarakat. Selain PSE, dijelaskan pula pengguna sistem elektronik yaitu setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh penyelenggara sistem elektonik.

Penyelenggara sistem elektronik wajib melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik yang dikelolanya, serta wajib menyediakan prosedur mengenai tata cara sistem yang mudah dipahami oleh pengguna atau pemilik data. Kaitannya dengan perlindungan data pribadi, penyelenggara sistem elektronik wajib melaksanakan prinsip-prinsip perlindungan data pribadi dalam melakukan pemrosesan data pribadi, seperti melakukan pengumpulan data secara sah dan adil secara hukum sesuai dengan tujuan yang ingin dicapai setelah mendapatkan persetujuan dari pemilik data, kemudian melakukan pemrosesan secara akurat dan dapat dipertanggungjawabkan. Apabila tujuan utama telah tercapai, penyelenggara sistem elektronik wajib menghapus data penggunanya kecuali masih dibutuhkan sesuai dengan ketentuan peraturan perundang-undangan.

Sementara di Uni Eropa, sebagaimana diatur dalam *General Data Protection Regulation (GDPR)*, pihak yang bertanggung jawab dalam pengelolaan sebuah sistem dibagi menjadi dua, yaitu *controllers* (pengendali) dan *processors* (pengelola) data. Pengendali adalah orang atau badan hukum, otoritas publik atau badan lain, sendiri atau bersama-sama yang menentukan tujuan dan cara pemrosesan data pribadi. Sementara pengelola data adalah orang atau badan hukum, otoritas publik atau badan lain yang memproses data pribadi dan bertanggung jawab kepada pengendali data. Pengendali harus memastikan bahwa pemrosesan data pribadi telah sesuai dengan yang diatur di dalam GDPR sebelum pengelola data mulai mengumpulkan dan memproses data pribadi. Pengendali menerapkan tahapan-tahapan guna memastikan bahwa hanya data pribadi

yang diperlukan saja yang akan diproses sesuai dengan tujuan, termasuk jumlah dan tipe data serta berapa lama data tersebut akan disimpan dalam sistem.

Berbeda dengan yang diatur dalam PP Nomor 71 Tahun 2019, di dalam GDPR diatur lebih detil kewajiban pengendali dan pengelola data kaitannya dengan perlindungan data pribadi. Misalnya, pengendali maupun pengelola data wajib memberitahukan otoritas pengawas perlindungan data dan juga kepada pemilik data apabila terjadi pelanggaran. Di pasal 37 GDPR juga diatur yang disebut dengan *The Data Protection Officer (DPO)* atau petugas perlindungan data. DPO ditunjuk oleh pengendali dan pengelola data jika terjadi kasus hukum pelanggaran perlindungan data pribadi. DPO merupakan tenaga profesional yang memiliki keahlian khusus yang memiliki tugas memberitahu dan mengingatkan pihak pengendali dan pengelola data agar selalu melaksanakan kewajibannya sesuai dengan ketentuan GDPR. DPO bekerja sama dengan otoritas pengawas perlindungan data dalam memberikan saran jika diminta oleh pengendali dan pengelola data kaitannya dengan dampak pemrosesan data dan/atau kinerja mereka.

3. Pihak yang Mengawasi

Terdapat tiga pengawas perlindungan data di Uni Eropa yaitu *Independent Supervisors*, *European Data Protection Board*, dan *European Data Protection Supervisors*. *Independent Supervisors* diatur dalam pasal 51 s.d. 59. Tugas utama *Independent Supervisors* adalah secara khusus memantau dan menegakkan penerapan peraturan perlindungan data (GDPR); mensosialisasikan pemahaman publik tentang pentingnya perlindungan dan hak atas pemrosesan data pribadi; melayani, menyelidiki dan menangani pengaduan yang diajukan oleh pemilik data serta bekerja sama dengan otoritas pengawas lainnya untuk memastikan konsistensi penerapan dan penegakan hukum atas peraturan ini. *European Data Protection Board (EDPB)* diatur dalam pasal 68 s.d. 70. EDPB atau Dewan Perlindungan Data Eropa dibentuk sebagai badan perhimpunan dan memiliki kepribadian hukum. Dewan ini terdiri atas perwakilan dari masing-masing negara di Uni Eropa ditambah dengan *The European Data Protection Supervisor (EDPS)* atau Pengawas Perlindungan Data Eropa. EDPS adalah otoritas pengawas independen yang memastikan lembaga-lembaga dan badan-badan Eropa untuk menghormati hak privasi individu dan perlindungan atas data ketika diproses untuk kemudian digunakan sebagai rekomendasi mengambil kebijakan. Dasar hukum pembentukan otoritas perlindungan data Uni Eropa ini adalah *Regulation (EC) No. 45/2001 of European Parliement and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data* yang kemudian diubah menjadi *Regulation (EU) 2018/1725 of the European Parliement and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institution, bodies, offices, and agencies and on the free movement of such data*. Dengan dasar hukum ini, maka tugas dan fungsi EDPS sebagai otoritas perlindungan data di Uni Eropa akan sejalan dengan Undang-undang perlindungan data yang telah dikeluarkan sebelumnya, yaitu *The General Data Protection Regulation (GDPR).* Pembentukan otoritas pengawas perlindungan data sangat bermanfaat jika terjadi pelanggaran perlindungan data pribadi lintas negara namun masih dalam satu teritorial. Adanya otoritas pengawas ini diharapkan dapat menyelesaikan kasus hukum pelanggaran perlindungan data pribadi dengan cepat.

4. Penetapan Sanksi Ketika Terjadi Pelanggaran

Persamaan lainnya antara peraturan perundang-undangan di Indonesia dan Uni Eropa adalah sama-sama telah menetapkan sanksi administratif apabila terjadi

pelanggaran terhadap perlindungan data pribadi. Penetapan sanksi dalam ketentuan pidana sebagaimana diatur pada UU ITE disesuaikan dengan pelanggaran yang dilakukan. Kaitannya dengan perlindungan privasi individu dalam sebuah sistem *big data*, sebagaimana disebut dalam pasal 30, yaitu "*(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."* Pelanggaran atas pasal 30 ayat(1) akan dikenakan sanksi pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,- (enam ratus juta rupiah), pelanggaran atas pasal 30 ayat(2) akan dikenakan sanksi pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,- (tujuh ratus juta rupiah), dan pelanggaran atas pasal 30 ayat(3) akan dikenakan sanksi pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,- (delapan ratus juta rupiah). Sementara bagi penyelenggara sistem elektronik yang lalai atas keamanan perlindungan data pribadi hanya akan dikenasi sanksi adminstratif berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan akses dan/atau dikeluarkan dari daftar.

Penetapan sanksi kaitannya dengan pelanggaran atas perlindungan data pribadi di Indonesia sangat berbeda dengan yang ditetapkan di dalam GDPR. Ketentuan umum mengenai penetapan sanksi ada dalam pasal 83 GDPR. Penetapan sanksi berbeda-beda sesuai dengan pelanggaran yang terjadi. Beberapa hal yang berbeda dengan yang ada di Indonesia, yaitu :

a) Penetapan sanksi bergantung pada jenis data pribadi dan dampak yang diderita pemilik data akibat pelanggaran yang terjadi
b) Pelanggaran yang terjadi akibat disengaja atau karena kelalaian pengendali dan pengelola data
c) Penetapan sanksi bergantung pada tingkat tanggung jawab dan kerja sama pengendali dan pengelola data
d) Peran otoritas pengawas perlindungan data sangat berperan sebagai bahan pertimbangan dalam menetapkan sanksi
e) Jika pelanggaran terjadi akibat kelalaian pengendali dan pengelola data, maka jumlah denda administratif tidak akan melebihi jumlah yang ditentukan untuk pelanggaran paling berat
f) Denda yang dikenakan sebagai sanksi adminisrtrasi sebesar 10.000.000 (sepuluh juta) s.d. 20.000.000 (dua puluh juta) EUR atau 2 s.d. 4 % dari total perputaran kas di seluruh dunia selama setahun, tergantung prinsip perlindungan data pribadi mana yang dilanggar.
g) Denda yang dikenakan akibat ketidakpatuhan terhadap perintah otoritas pengawas perlindungan data pribadi adalah paling banyak 20.000.000 (dua puluh juta) EUR atau maksimal 4% dari total perputaran kas di seluruh dunia selama setahun, tergantung prinsip perlindungan data pribadi mana yang dilanggar.

B. Tabel perbandingan kebijakan sistem *big data* di indonesia dan uni eropa

Perbandingan antara kebijakan yang ada dalam peraturan perundang-undangan kaitannya dengan implementasi sistem *big data* di Indonesia dan Uni Eropa dapat dilihat pada tabel berikut.

No	Pembanding	Indonesia	Uni Eropa
1	Pengakuan privasi individu sebagai hak asasi manusia	√	√
2	Definisi dan jenis data pribadi	√ UU ITE tidak detil, ada di UU Administrasi Kependudukan	√ Lengkap dari definisi hingga jenis data sensitif
3	Ketentuan mengenai sistem elektronik	√	√
4	Pihak penyelenggara sistem elektronik	√ Masih terlalu umum dan kabur	√ Detil, dibagi menjadi pengendali dan pengelola data, serta petugas perlindungan data
5	Otoritas pengawas perlindungan data pribadi	Tidak jelas / kabur	√ Detil, dibagi menjadi *Independent Supervisors*, *European Data Protection Board*, dan *European Data Protection Supervisors*
6	Hak dan kewajiban penyelenggara sistem elektronik dan pemilik data	√ Kurang jelas dan tegas	√ Detil sesuai dengan tahapan-tahapan berdasarkan prinsip perlindungan data pribadi
7	Standar Keamanan Informasi	√	√ Detil sesuai risiko pelanggaran
8	Ketentuan pidana dan penetapan sanksi	√ Jumlah denda kecil dan tidak jelas penentuan dasar pengenaannya	√ Jelas dasar pengenaan sanksinya dan jumlah denda yang sangat besar akan menekan pengendali dan pengelola data lebih bertanggung jawab atas perlindungan data pribadi yang diprosesnya

PENUTUP

Peraturan perundang-undangan antara Indonesia dan Uni Eropa terdapat persamaan dan perbedaan diantara keduanya. Persamaan tersebut mengenai privasi individu, Sistem elektronik dan Sanksi Administratif. Privasi Individu dimana hak asasi manusia yang wajib dilindungi oleh negara telah diakui secara internasional. Peraturan perundang undangan di Indonesia secara garis besar memiliki kesamaan dengan aturan di Uni Eropa, akan tetapi butuh penegasan secara khusus di UU ITE. Keduanya dalam penyelenggaraan sistem elektronik baik. Peraturan di Indonesia dipaparkan secara rinci, jelas dan tegas dalam aturan Peraturan Pemerintah. Perbedaan peraturan terdapat pada kebijakan sistem *big data* pada lingkup definisi data pribadi. Indonesia masih tidak ditetapkan dengan jelas dan tegas mengenai perlindungan data pribadi. Perbedaan lain

terlihat dari penetapan denda pelanggaran data pribadi serta jumlah denda yang dikenakan.

DAFTAR PUSTAKA

Buku Literatur.

Dewi, S. 2009. *Cyber Law: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran.

Miriam B. 1993. *Dasar-Dasar Ilmu Politik*. Jakarta: Gramedia

Nafiudin. 2019. *Sistem informasi manajemen*. Pasuruan : Qiara Media.

Wijaya, W. M. 2019. *Teknologi Big Data: Sistem Canggih di Balik Google, Yahoo!, Facebook, IBM (Vol. 1)*. Yogyakarta : Deepublish

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Perdata (KUH Perdata)

Undang-Undang Republik Indonesia Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

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

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Universal Declaration of Human Rights oleh Perserikatan Bangsa-Bangsa pada tanggal 10 Desember 1948

European Treaty Series No. 108 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* pada tanggal 28 Januari 1981

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 *on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data*

Jurnal

Dewi, Sinta. 2016. *Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Pengguanaan Cloud Computing di Indonesia,*Yustisia. 5.1

Demchenko, Y & Laat, Cees & Membrey, Peter, 2014, *Defining Architecture Components of the Big Data Ecosystem*. International Conference on Collaboration Technologies and Systems (CTS), IEEE (p. 104-112). https://www.researchgate.net/publication/269272409_Defining_architecture_components_of_the_Big_Data_Ecosystem/citation/download

Kim, Gang-Hoon & Trimi, Silvana & Chung, Ji-Hyong. 2014. *Big Data Applications in the Government Sector: A Comparative Analysis among Leading Countries*. Communications of The ACM (p. 78-85). https://www.researchgate.net/publication/260865566_Big_Data_Applications_in_the_Government_Sector_A_Comparative_Analysis_among_Leading_Countries

Kuner, Christopher, et al. 2012. *The Challenge of 'Big Data' for Data Protection*. International Data Privacy Law, Volume 2, Issue 2, May 2012, Pages 47–49. https://doi.org/10.1093/idpl/ips003

McDermott, Yvonne. 2017. *Conceptualising the Right to Data Protection in an Era of Big Data."*. Big Data & Society 4.1: 2053951716686994. https://journals.sagepub.com/doi/full/10.1177/2053951716686994

Nugroho, FP, Abdullah, RW, Wulandari, S & Hanafi, H. 2019. *Keamanan Big Data di Era Digital di Indonesia*. Jurnal Informa 5.1 (hlm. 28-34)

Warren, Samuel D and Louis D Brandeis. 1890. *The Right to Privacy*. Harvard Law Review Vol. 4 (p. 193-220)

Zarsky, Tal Z. 2016. *Incompatible : The GDPR in the Age of Big Data*. Seton Hall L. Rev. 47 : 995.

Internet

Act, *Data Protection 1998, London Station Off*, diakses pada tanggal 30 Januari 2020 : http://www.legislation.gov.uk/ukpga/1998/29/contents

BBC, *Data on 540 million Facebook Users Exposed*, diakses pada tanggal 2 Pebruari 2020 : https://www.bbc.com/news/technology-47812470

Europa.eu, *Foresight and Horizon Scanning*, diakses pada 13 Mei 2020 : https://ec.europa.eu/jrc/en/research/crosscutting-activities/foresight

Fyk, *Hacker Diduga Jebol Jutaan Data Penduduk di KPU*, diakses pada tanggal 30 Mei 2020 : https://inet.detik.com/security/d-5024151/hacker-diduga-jebol-jutaan-data-penduduk-di-kpu

Gov.uk, *Horizon Scanning Programme Team*, diakses pada tanggal 13 Mei 2020 : https://www.gov.uk/government/groups/horizon-scanning-programme-team

Josh Constine, *How Big is Facebook's Data? 2.5 Billion Pieces of Content and 500+ Terabytes Ingested Every Day*, diakses pada tanggal 20 Juni 2020 : https://techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day/

OECD, *OECD Privacy Guidelines*, diakses pada tanggal 20 Mei 2020 : https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

Wahyunanda KP, *Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web*, diakses pada tanggal 13 Mei 2020 : https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark

Wan Ulfa NZ, *Bagaimana Data Pengguna Memberi Untung bagi Go-Jek*, diakses pada tanggal 2 Pebruari 2020 : https://tirto.id/bagaimana-data-pengguna-memberi-untung-bagi-go-jek-cukG