

SANKSI TERHADAP KORPORASI SEBAGAI PENYELENGGARA SISTEM ELEKTRONIK AKIBAT KEBOCORAN DAN PENYALAHGUNAAN DATA PRIBADI

**RINA RAHMA ORNELLA ANGELIA¹, RAHMI ERWIN², ANDI DESMON³
ZENNIS HELEN⁴**

Fakultas Hukum, Universitas Ekasakti, Padang, Indonesia
rinarahmaornella@unespadang.ac.id

Abstrat: *This research focuses on imposing sanctions on Corporations as Electronic System Operators (PSE) if the Corporation fails to carry out its obligations and misuses User's Personal Data improperly based on Law Number 27 of 2022 concerning Protection of Personal Data. The method used in this research is normative-descriptive legal research and normative-juridical research. Normative Descriptive is research that aims to find correlation, which relates to legal rules in accordance with legal norms and whether there are legal norms in the form of orders and prohibitions that are in accordance with legal principles and whether there are actions (acts) in accordance with legal norms and legal principles. Normative Juridical, namely conducting research with an approach, examining, concepts, and related theories to study existing regulations to obtain answers to legal issues in this writing. This type of research is research on legal systematics by conducting research that has the aim of identifying the understanding and legal basis that exists. The results of this study indicate that in Law No. 27 of 2022 concerning Protection of Personal Data there are strict sanctions for Corporations as Electronic System Operators (PSE) if the Corporation leaks or misuses its Users' Personal Data.*

Keywords: *Personal Data, Corporations, Sanctions.*

Abstrak: Penelitian ini berfokus pada pemberian sanksi terhadap Korporasi sebagai Penyelenggara Sistem Elektronik (PSE) apabila Korporasi tersebut gagal dalam menjalankan kewajibannya serta menyalahgunakan Data Pribadi Penggunanya dengan tidak semestinya yang berdasarkan pada Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi. Metode yang dipergunakan dalam penelitian ini adalah penelitian hukum (*legal research*) yang bersifat Normatif Deskriptif dan penelitian Yuridis Normatif. Normatif Deskriptif merupakan penelitian yang bertujuan untuk menemukan korehensi, yang berhubungan dengan aturan hukum sesuai dengan norma hukum dan apakah ada norma hukum yang berupa perintah dan larangan yang sesuai dengan prinsip hukum dan apakah ada perbuatan (*act*) sesuai dengan norma hukum dan prinsip hukum. Yuridis Normatif yaitu melakukan penelitian dengan pendekatan, menelaah, konsep-konsep, serta teori-teori yang berkaitan untuk mengkaji peraturan-peraturan yang ada untuk memperoleh jawaban atas isu hukum dalam penulisan ini. Jenis penelitian ini merupakan penelitian terhadap sistematika hukum dengan cara melakukan penelitian yang mempunyai tujuan mengidentifikasi pengertian dan dasar hukum yang ada. Hasil dari penelitian ini menunjukkan bahwa dalam Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi terdapat sanksi yang tegas bagi Korporasi sebagai Penyelenggara Sistem Elektronik (PSE) apabila Korporasi tersebut membocorkan atau menyalahgunakan Data Pribadi Penggunanya.

Kata Kunci: Data Pribadi, Korporasi, Sanksi

A.Pendahuluan

Perkembangan zaman yang semakin modern menghasilkan Teknologi Informasi sehingga mengubah pola kehidupan masyarakat secara global. Globalisasi berdampak pada kehidupan masyarakat sehari-hari, dimana globalisasi tersebut tidak dapat dihindarkan atau diberhentikan. Dukungan terhadap Kemajuan teknologi dan informasi memberikan dampak positif dan negatif bagi kemajuan kehidupan manusia untuk terselenggaranya globalisasi. Perubahan itu dapat kita lihat dan rasakan di era sekarang ini dalam berbagai bidang misalnya perubahan dalam bidang sosil budaya, ekonomi, pendidikan, kesehatan, hukum yang berlangsung secara signifikan. Perkembangan teknologi Informasi dan Komunikasi (TIK) yang

kita rasakan semakin baik dari hari-hari sebelumnya sehingga membuat kehidupan manusia lebih dinamis dan fleksibel dibandingkan sebelumnya.

Pengaruh globalisasi dalam bidang teknologi memberikan kemudahan terhadap aspek kegiatan yang dilakukan manusia saat ini. Dibalik kemudahan tersebut juga memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Perkembangan teknologi informasi mengubah pola pemikiran manusia dari yang bersifat manual menjadi komputerisasi/ digital. Informasi sudah dianggap sebagai “*power*” yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia itu sendiri (Simatupang, 2018).

Internet merupakan salah satu hasil dari perkembangan Teknologi Informasi dan Komunikasi dapat menjadi pedang bermata dua karena selain memiliki kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia disisi lain internet juga memiliki dampak negatif salah satunya yakni menjadi sarana efektif perbuatan melawan hukum seperti tindak pidana kejahatan. Berbagai bentuk tindak pidana kejahatan dalam internet ini yang kemudian lebih dikenal dengan nama *cybercrime* (Riskawati, 2016). Dengan Kehadiran internet memudahkan manusia untuk menjangkau segala aspek informasi, mengalami peningkatan cara berkomunikasi serta mengalami peningkatan cara beraktivitas. Aktivitas manusia yang dahulu dilakukan secara konvensional, saat ini dapat dilakukan melalui suatu sistem internet atau media elektronik lain yang kemudian diselenggarakan oleh penyelenggara sistem elektronik.

Saat ini banyak korporasi yang berperan sebagai penyelenggara sistem elektronik. Korporasi tersebut tidak hanya dikelola oleh pihak pemerintah melainkan juga pihak swasta. Keberadaan korporasi tersebut sebagai penyelenggara sistem elektronik menjadi penting karena hampir semua aspek kehidupan sosial masyarakat menggunakan sistem layanan elektronik. Bukti nyata saat ini yang dapat kita lihat adalah bermunculan berbagai sistem pembayaran yang menggunakan media elektronik, sistem perbankan elektronik, akses kesehatan secara elektronik, pendidikan, serta perkembangan industri. Dalam menyelenggarakan pelayanan elektronik kebanyakan korporasi saat ini meminta data informasi elektronik yang dimiliki oleh pengguna sistem elektronik yang masuk untuk diproses dan dikelola oleh korporasi sebagai penyelenggara sistem elektronik tersebut. Informasi elektronik dianggap suatu aset yang sangat penting bagi suatu korporasi.

Informasi elektronik merupakan elemen penting dalam sebuah sistem elektronik karena proses verifikasi (*verification*) atau autentikasi (*authentication*) terhadap seseorang di sebuah sistem elektronik dilakukan melalui dokumen atau informasi elektronik. Masyarakat sebagai subjek perlindungan data pribadi apabila menggunakan jasa Korporasi sebagai penyelenggara sistem elektronik harus memperhatikan beberapa ketentuan karena dalam sistem tersebut terdapat informasi pribadi pengguna, data pribadi, preferensi pribadi, hingga tanda tangan digital yang masuk kedalam sistem yang diselenggarakan oleh penyelenggara sistem elektronik. Dengan sistem tersebut membuat adanya berbagai bentuk tindak kejahatan dimana kejahatan tersebut dapat dilakukan dengan cara membobol terhadap sistem penyimpanan data pribadi pengguna yang dikelola korporasi. Dengan terjadinya tindak kejahatan yang seperti itu, korporasi selaku penyelenggara sistem elektronik dituntut untuk memberikan jaminan terhadap keamanan data pribadi pengguna yang telah disimpannya, apabila data pribadi pengguna yang telah disimpan tersebut bocor atau disebarluaskan maka korporasi dapat dimintai pertanggung jawaban terhadap tindak kejahatan tersebut (Rosadi, 2017). Keberadaan informasi elektronik berupa data pribadi pengguna layanan yang dikelola oleh penyelenggara sistem elektronik perlu mendapatkan perhatian serius dari semua pihak.

Kebocoran data pribadi di Indonesia sudah berulang kali terjadi. Pada tahun 2020 sebanyak 91 juta data pengguna dan 7 juta data merchant perusahaan e-commerce terbesar di Indonesia, Tokopedia juga mengalami kebocoran dan disebar secara gratis di forum internet serta ditahun yang sama sebanyak 2,3 juta Data Pemilih Komisi Pemilihan Umum dan sebanyak 230 ribu data pasien covid -19 diretas dan dijual di situs dan forum online Pada Mei 2021, Indonesia dihebohkan dengan dugaan kebocoran data pengguna BPJS Kesehatan. Terdapat 279 juta data pribadi diperjual belikan di Raid Forum dengan harga 80 juta rupiah

(Lidwina, 2013). Sepanjang tahun 2022 setidaknya ada 10 kasus kebocoran data pribadi dengan jumlah yang fantastis. Kebocoran data tersebut diduga berasal dari aplikasi yang dimiliki oleh pihak pemerintah atau institusi negara. Kebocoran data pribadi tersebut berupa nomor ponsel hingga Nomor Induk Kependudukan (NIK) yang dapat membahayakan karena jadi kunci beragam layanan keuangan.

Sebelum di sah kannya Undang-Undang No. 27 tahun 2022 tentang Pelindungan Data Pribadi oleh Pemerintah, Indonesia memiliki 30 ketentuan Perpu yang mengatur kewajiban negara dalam memberikan suatu bentuk perlindungan terhadap data pribadi warga negaranya (Djafar, 2019). Undang-Undang No 23 tahun 2006 tentang Administrasi Kependudukan Junto Undang-Undang Nomor 24 tahun 2014 tentang Pemerintah Daerah tidak memberikan perincian terkait perolehan, pengolahan, dan penyimpanan data pribadi tersebut. Dalam Permrnkoinfo Nomor 20 tahun 2016 mengatur mengani perlindungan data pribadi yang meliputi perlindungan terhadap perolehan, pengumpulan, penyimpanan, pengiriman, penganalisaan, penyebarluasan, penampilan, pemusnahan terhadap data pribadi.

Pengguna layanan elektronik sebagai subjek data pribadi mempunyai hak untuk menggugat korporasi yang menyelenggarakan kegiatan elektronik apabila terjadi kebocoran data terhadap data pribadinya tetapi hal tersebut tidak serta merta dapat membuka jalan pemilik untuk mempertahankan hak pribadinya. Berbagai bukti harus dipersiapkan oleh pengguna sebagai pemilik data pribadi karena terjadinya kebocoran hingga penyalahgunaan data pribadinya sebelum adanya peraturan yang secara khusus mengatur mengenai perlindungan data pribadi sehingga membuat pengguna merasa kesulitan untuk mendapatkan haknya serta meminta pertanggung jawaban korporasi sebagai Penyelenggara Sistem Elektronik (PSE) atas kebocoran dan penyalahgunaan data yang terjadi. Dengan di sahkannya oleh Pemerintah Undang-Undang No. 27 tahun 2022 tentang Pelindungan data pribadi memberikan kepastian dan perlindungan terhadap data pribadi warganya. Sesuai dengan asas Perlindungan data Pribadi yang terdapat dalam Pasal 3 UU perlindungan data Pribadi yakni berasaskan pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.

Undang-Undang No. 27 tahun 2022 ini merupakan bukti kongkret dari keseriusan pemerintah untuk melindungi data pribadi warganya, karena mengatur tentang kewajiban-kewajiban yang harus dipenuhi oleh orang perorangan maupun korporasi yang bertindak sebagai Penyelenggara Sistem Elektronik (PSE) serta sanksi yang tegas baik bagi para pelaku yang membocorkan serta penyalahgunaan data pribadi baik itu orang perorangan maupun korporasi yang melakukan kegiatan pemrosesan data pribadi. Dengan Adanya Undang-Undang ini diharapkan baik orang perorangan maupun korporasi sebagai pemroses dan pengendali data pribadi agar berhati-hati dalam melakukan pemrosesan serta mengelola data pribadi masyarakat serta melakukan upaya preventif dalam sistem keamanan data yang dimiliki sehingga dapat meminimalisir kasus kebocoran serta penyalahgunaan data pribadi yang tidak bertanggung jawab yang dapat merugikan masyarakat. Berdasarkan latar belakang masalah yang disampaikan diatas, maka permasalahan yang akan dibahas dalam penulisan ini adalah apa saja sanksi yang diberikan oleh pemerintah terhadap korporasi sebagai penyelnggaras sistem elektronik akibat kebocoran dan penyalahgunaan data pribadi pengguna berdasarkan Undang-Undang Perlindungan data Pribadi.

B. Metodologi Penelitian

Dalam penelitian ini penulis menggunakan metode penelitian hukum (*legal research*) yang bersifat normatif deskriptif (Marzuki, 2015) dan penelitain yuridis normatif. Normatif Deskriptif merupakan penelitian yang bertujuan untuk menemukan korehensi, yang berhubungan dengan aturan hukum sesuai dengan norma hukum dan apakah ada norma hukum yang berupa perintah atau larangan yang sesuai dengan prinsip hukum dan apakah perbuatan (act) seseorang sesuai dengan norma hukum dan prinsip hukum. Yuridis normatif yaitu metode penelitian yang dilakukan dengan menggunakan pendekatan, menelaah, konsep-konsep serta teori-teori yang berkaitan untuk mengkaji peraturan-peraturan yang ada untuk menjawab isu hukum dalam penulisan ini. Pengumpulan data dilakukan melalui studi literatur untuk mencari

data sekunder dengan menggunakan bahan hukum primer, sekunder, dan tertier (Marzuki, 2015).

C.Hasil dan Pembahasan

Indonesia sudah mengenal Hak Pribadi sejak zaman Hindia Belanda. Hal ini dapat dilihat dengan diberlakukannya KUHPdata oleh pemerintahan Hindia Belanda yaitu terdapatnya konsep larangan memasuki rumah atau perkarangan orang lain tanpa adanya izin terlebih dahulu. Data Pribadi merupakan Hak Konstitusional bagi setiap warga negara hal ini diatur dalam Undang-Undang Dasar 1945 Pasal 28 G. Dalam Pasal 28 G UU 1945 berisi “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang ada dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan diri dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Perlindungan yang terdapat dalam Pasal 28 UUD 1945 ini dapat memiliki arti yang sangat luas tidak hanya untuk perlindungan terhadap diri sendiri melainkan juga untuk melindungi privasi setiap warga negaranya. Dalam Pasal tersebut juga menjelaskan bahwa perlindungan data pribadi merupakan suatu bentuk dari perlindungan yang diberikan oleh negara terhadap hak privasi warga negaranya untuk dapat menikmati hidup tanpa adanya ancaman dari pihak lain.

Hak privasi melalui perlindungan data merupakan elemen penting bagi kebebasan serta harga diri individu. Pelindungan data menjadi pendorong untuk mewujudkan kebebasan politik, spiritual, keagamaan, bahkan kegiatan yang sifatnya pribadi (privat). Hak untuk menentukan nasib terhadap dirinya sendiri, kebebasan untuk berkespresi, dan privasi adalah hak-hak penting bagi kita sebagai manusia. Hak Privasi juga terdapat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM) / *Universal Declaration of Human Rights* (UDHR) Pasal 12 yaitu : “ *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks*”

Deklarasi HAM merupakan salah satu instrument internasional yang sangat penting karena telah berhasil menyatukan kesepakatan dari hampir seluruh negara (Starkey, 2017). Potensi pelanggaran privasi atas data pribadi secara online misalnya dapat dilihat dalam kegiatan pengumpulan data pribadi secara massal (*digital dossier*), pemasaran langsung (*direct selling*), media sosial, pelaksanaan program e-KTP, pelaksanaan program *e-health* dan kegiatan komputasi awan (*cloud computing*). Khusus di bidang big data, pengumpulan data dilakukan secara masif, yang dilakukan tidak hanya oleh pemerintah saja, tetapi juga dilakukan oleh entitas bisnis atau korporasi. Jenis data yang dikumpulkannya beragam diantaranya *personally identifiable information* (PII) hingga *sessitive personal information* (SPI).

Korporasimemiliki peranan yang cukup berpengaruh pada suatu negara baik itu terhadap kepentingan orang perorangan maupun kepentingan negara itu sendiri. Peranan korporasi bagi kehidupan manusia diantaranya korporasi dapat memberikan kehidupan manusia saat ini. Bagi negara Korporasi mempunyai peranan untuk meningkatkan pendapatan yang diterima oleh negara melalui pajak yang dibebankan, membuka lapangan pekerjaan, serta pemanfaatan teknologi. Bentuk pemanfaatan teknologi yang dilakukan oleh korporasi salah satunya yakni pemanfaatan dan pengolahan data, seperti terdapatnya kartu credit, cek elektronik, hingga dompet digital (e-wallet), yang kesemuanya merupakan hasil produk ciptakaan korporasi yang memanfaatkan data sebagai inti (core) dalam menjalankan usahanya.

Pada saat ini dengan era digital semua data dapat disimpan secara online (Marc, 2004) Informasi atau data dikumpulkan oleh situs dan / atau aplikasi yang dimiliki pemerintah dan korporasi swasta dengan tujuan tertentu. Pemerintah melakukan pengumpulan dan pengelolaan data dengan tujuan untuk mendukung kegiatan publik. Sedangkan bagi korporasi sebagai penyelenggara sistem elektronik, data atau informasi pribadi yang dimiliki oleh pengguna sistem elektronik dipergunakan untuk verifikasi data dan autentikasi atas pelayanan yang diberikan oleh penyelenggara. Korporasi yang bergerak dibidang penyelenggara sistem elektronik memiliki tanggung jawab untuk menjaga data pengguna sistem elektronik yang menggunakan sistem elektronik yang dimiliki oleh korporasi tersebut dari kebocoran serta

penyalahgunaan data. Bocornya serta penyalahgunaan data pribadi pengguna sistem elektronik merupakan suatu bentuk pelanggaran terhadap hak privasi . Korporasi dapat menjadi pihak pertama yang dapat diidentifikasi atas kebocoran serta penyalahgunaan data pribadi.

Perlindungan data merupakan bagian dari perlindungan privasi. Allan Westin mendefinisikan bahwa privasi merupakan hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi. Perlindungan data merupakan hak asasi manusia yang fundamental, beberapa negara seperti Albania, Armenia, Philipina, timur Leste, Kolombia, dan Argentina sudah mengakui perlindungan data sebagai hak konstitusional atau dalam bentuk “habeas data” yaitu hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk membenarkan ketika ditemukan kesalahan terhadap datanya serta mengakui peran dari perlindungan data yang dapat memfasilitasi proses demokrasi dan menjamin perlindungannya dalam konstitusi mereka (Greenleaf, 2011). Dalam Pasal 1 angka (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dijelaskan bahwa data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik maupun nonelektronik.

Pelindungan data Pribadi sendiri dalam UU Pelindungan Data Pribadi memiliki arti yakni “keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak Konstitusional subjek Data Pribadi”. Negara berkewajiban untuk melindungi data pribadi warganya. Tetapi, negara juga tidak dapat bekerja dengan sendiri. Semua pihak harus turut berpartisipasi dalam upaya pelindungan data pribadi tersebut. Para pihak tersebut diantaranya pemerintah, selaku penyelenggara negara, *data controller* atau pengendali data pribadi baik itu pemerintah ataupun swasta. Pengendali data pribadi pemerintah misalnya Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Ditjen Dukcapil) Kementerian Dalam Negeri (Kemedagri) yang mencatat data pribadi penduduk untuk kepentingan negara maupun publik. Dari Pihak swasta misalnya Korporasi yang membuat layanan marketplace karena untuk dapat menggunakan layanan marketplace tersebut masyarakat harus memasukkan data pribadinya. Pemilik data itu sendiri (*data owner*) masyarakat harus memiliki pengetahuan bahwa data pribadi merupakan sesuatu yang penting dan harus dijaga kerahasiannya sehingga tidak mudah untuk mengumbar ke publik. Terakhir adalah penegak hukum karena apabila terjadi tindak pidana kebocoran hingga penyalahgunaan data pribadi seseorang, maka penegak hukum berkewajiban untuk melindungi hak pemilik data yang dilanggar oleh pengendali data.

Ketentuan yang mengatur tentang kewajiban korporasi sebagai penyelenggara sistem elektronik untuk melindungi dan mengamankan data pribadi ketentuan tersebut diatur dalam Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi yang mensyaratkan bahwa baik orang perorangan maupun badan hukum sebagai pengendali data pribadi dalam melakukan Pemrosesan Data Pribadi harus berdasarkan persetujuan subjek data pribadi. Pengendali data pribadi wajib menyampaikan kepada subjek data pribadi terkait legalitas dari pemrosesan data pribadi, tujuan pemrosesan data pribadi yang akan dilakukan, jenis dan relevansi Data Pribadi yang akan di proses, jangka waktu retensi dokumen yang memuat Data Pribadi, rincian mengenai Informasi yang dikumpulkan, jangka waktu pemrosesan Data Pribadi dilakukan, serta hak subjek Data Pribadi. Apabila dikemudian hari terdapat perubahan Data Pribadi milik subjek data pribadi, maka Pengendali Data Pribadi wajib memberitahukan kepada Subjek Data Pribadi sebelum data sebelumnya / data sebelum terjadi perubahan informasi.

Untuk keaman serta melindungi subjek Pelindungan data pribadi dalam Pasal 22 Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi dijelaskan bahwa pengendali data pribadi dalam melakukan pemrosesan data pribadi Subjek Pelindungan data pribadi wajib memperoleh persetujuan Pemrosesan Data Pribadi yang dilakukan melalui persetujuan secara tertulis atau terekam yang dapat dilakukan melalui sarana media elektronik atau non elektronik. Selain itu juga terdapat dalam Pasal 32 ayat (1) Undang-Undang Nomor 27

tahun 2022 tentang Pelindungan Data Pribadi yang menyebutkan bahwa kewajiban Pengendali Data Pribadi untuk memberikan akses kepada Subjek Data Pribadi yang diproses beserta rekam jejak pemrosesan data pribadi sesuai dengan jangka waktu penyimpanan data pribadi. Sesuai hak subjek data pribadi yang diatur dalam Undang-Undang Pelindungan data pribadi, Subjek data pribadi juga dapat menarik menarik pemrosesan data pribadinya sehingga berdasarkan pasal 40 Undang-Undang Perlindungan data Pribadi pengendali data pribadi wajib menghentikan pemrosesan data jika subjek data pribadi menarik pemrosesan data. Serta penghentian paling lama dilakukan 3x24 jam (tiga kali dua puluh empat) jam terhitung sejak pengendali data pribadi menerima permintaan penarikan kembali persetujuan pemrosesan Data Pribadi.

Korporasi yang bergerak dibidang Penyelenggaraan Sistem Elektronik sebagai Pengendali Data berbadan hukum apabila melakukan penggabungan, pemisahan, pengambilalihan, peleburan atau pembubaran badan hukum berdasarkan Pasal 48 ayat Undang-Undang Nomor 27 tahun 2022 berkewajiban menyampaikan / memberitahukan pengalihan data kepada Subjek Data Pribadi sebelum dan sesudah penggabungan pemisahan atau peleburan korporasi tersebut. Pemerintah juga dalam Undang-Undang Pelindungan Data Pribadi ini secara tegas mewajibkan dalam sebuah korporasi yang bergerak dibidang Penyelenggara Sistem Elektronik wajib memiliki Pejabat atau Petugas yang melaksanakan Fungsi Pelindungan Data Pribadi. Pejabat atau Petugas yang melaksanakan Fungsi Pelindungan Data Pribadi ini berdasarkan Pasal 53 ayat (2) dan ayat (3) UU Pelindungan Data Pribadi adalah seseorang yang memiliki profesionalitas, pengetahuan di bidang hukum terutama praktik-praktik pelindungan data pribadi dan mampu mengamban tugas-tugasnya dengan sebaik mungkin serta dapat berasal dari dalam dan / atau luar Pengendali Data Pribadi atau Prosesor Data Pribadi.

Dalam pasal 54 ayat (1) Undang-Undang pelindungan data pribadi disebutkan tugas yang harus dilaksanakan oleh Pejabat atau Petugas yang melaksanakan fungsi Pelindungan Data Pribadi yaitu: 1) Menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau prosesor data pribadi agar mematuhi ketentuan dalam peraturan perundang-undangan; 2) Memantau dan memastikan kepatuhan terhadap peraturan perundang-undangan dan kebijakan Pengendali Data Pribadi atau Prosesor Data Pribadi; 3) Memberikan saran mengenai penilaian dampak Pelindungan Data Pribadi dan Prosesor Data Pribadi; dan 4) Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi.

Dalam hal terjadi kebocoran dan atau pelanggaran Data Pribadi Undang-Undang Pelindungan Data Pribadi (UUPDP) mengatur secara tegas terkait sanksi untuk pelanggaran data pribadi baik yang dilakukan oleh orang-perorangan maupun korporasi yang menyelenggarakan kegiatan elektronik. Sanksi tersebut dapat berupa sanksi pidana dan juga sanksi administratif. Sanksi yang dapat dibebankan bagi koroprasi sebagai Penyelenggara Sistem Elektronik (PSE) apabila terjadi kelalaian baik itu berupa kebocoran dan / atau penyalahgunaan Data Pribadi korporasi tersbut dapat dikenakan sanksi administratif yang ditetapkan oleh lmebaga peraturan tersebut terdapa dalam Pasal 57 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi berupa: a) Peringatan tertulis; b) Penghentian sementara kegiatan pemrosesan Data Pribadi; c) Penghapusan dan / atau pemusnahan Data Pribadi; dan d) Denda Administratif.

Denda Administratif yang diberikan oleh lembaga jumlahnya paling tinggi 2% (dua persen) dari seluruh pendapatan tahunan terhadap variabel pelanggaran. Denda tersebut dikenakan terhadap Pengendali atau Prosesor Data Pribadi jika melanggar ketentuan Undang-Undang Pelindungan Data Pribadi. Pelanggaran tersebut diantaranya Prosesor Data Pribadi melakukan pemrosesan Data Pribadi diluar perintah dan tujuan yang telah ditetapkan oleh Pengendali Data Pribadi serta baik Pengendali Data Pribadi maupun Prosesor Data Pribadi tidak melakukan pencegahan terhadap akses yang tidak sah. Ketentuan sanksi pidana terhadap kebocoran serta penyalahgunaan Data Pribadi diatur dalam Pasal 67 sampai dengan 73 Undang-Undang Pelindungan Data Pribadi (UUPDP). Pelanggar yang secara sah dan terbukti bersalah melakukan pelanggaran baik berupa perbuatan melawan hukum dengan cara

memperoleh dan mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain sehingga dapat mengakibatkan kerugian Subjek Data Pribadi berdasarkan Pasal 67 ayat (1) UU Pelindungan Data Pribadi dikenakan ancaman pidana berupa pidana penjara paling lama 5 (lima) tahun dan / atau pidana denda paling banyak sebesar Rp. 5.000.000.000,- (lima milyar rupiah). Bagi orang atau korporasi yang mengungkapkankan Data Pribadi bukan miliknya dapat dikenakan sanksi pidana berupa pidana penjara dengan kurun waktu maksimal 4 tahun dan/ atau pidana denda paling banyak sebesar Rp. 4.000.000.000,- (empat milyar rupiah). Sedangkan bagi orang yang melakukan perbuatan melawan hukum berupa menggunakan Data Pribadi yang bukan miliknya dikenakan pidana berupa pidana penjara paling lama 5 tahun serta denda sebesar Rp.5.000.000.000,- (lima milyar rupiah).

Hukuman lebih tinggi dapat diberikan bagi orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan tujuan untuk memperoleh keuntungan baik untuk diri sendiri maupun orang lain sehingga mengakibatkan kerugian bagi orang lain dapat dikenakan pidana penjara paling lama 6 (enam) tahun dan / atau pidana denda paling banyak Rp.6.000.000.000,- (enam milyar rupiah). Tindak pidana yang dilakukan oleh korporasi berupa perbuatan melawan hukum dengan cara memperoleh dan mengupulkan data Pribadi dengan maksud untuk menguntungkan korporasi sehingga dapat mengakibatkan kerugian bagi Subjek Data, maka yang bertanggung jawa adalah pengurus korporasi tersebut yakni pemegang kendali, pemberi perintah, pemilik manfaat. Pidana yang dapat dikenakan kepada korporasi berdasarkan Pasal 70 Undang-Undang Pelindungan Data Pribadi hanya dapat berupa pidana denda dan pidana denda yang diterima korporasi tersebut paling banyak 10 (sepuluh) kali dari maksimal pidana yang diancamka.

Selain dapat dijatuhi pidana berupa denda dalam Pasal 70 ayat (4) Undang-Undang Pelindungan Data Pribadi Korporasi dapat dijatuhi pidana tambahan berupa: a) Perampasan keuntungan dan / atau harta kekayaan yang diperoleh atau hasil dari tindak pidana; b) Pembekuan seluruh atau sebagian usaha Korporasi; c) Pelarangan permanen melakukan perbuatan tertentu; d) Penutupan seluruh atau sebagian tempat usaha dan / atau kegiatan Korporasi; e) Melaksanakan kewajiban yang telah dilalaikan; f) Pembayaran ganti kerugian; g) Pencabutan izin; dan / atau h) Pembubaran Korporasi

D.Penutup

Berdasarkan analisis permasalahan yang dilakukan maka dapat ditarik kesimpulan bahwa terdapat beberapa jenis sanksi yang dapat dibebankan kepada Korporasi apabila Korporasi tersbut melakukan pelanggaran dan penyalahgunaan data pribadi secara elektronik dberdasarkan UU Pelindungan data Pribadi yakni: Pertama, Sanski secara Administartif yang dapat dilakukan oleh lembaga tertentu. Dimana pengaturan terkait jenis sanksi administratif itu diatur dalam Pasal 57 ayat (2) Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi yaitu dapat berupa: a) Peringatan tertulis; b) Penghentian sementara kegiatan Pemrosesan Data Pribadi; c) Penghapusan atau pemusnahan Data Pribadi dan / atau; dan d) Denda administratif. Kedua, Sanksi secara Pidana bagi Korporasi diatur dalam pasal 70 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yakni Pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemilik manfaat Korporasi tersebut. Serta pidana yang dpat dijatuhkan kepada Korporasi berupa Pidana denda. Jumlah Pidana denda yang dapat dijatuhkan kepada Korporasi sebanyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan. Korporasi dapat juga dijatuhi pidana tambahan berupa: a) Perampasan keuntungan dan / atau harta kekayaan yang diperoleh atau hasil dari tindak pidana; b) Pembekuan seluruh atau sebagian usaha Korporasi; c) Pelarangan permanen melakukan perbuatan tertentu; d) Penutupan seluruh atau sebagian tempat usaha dan / atau kegiatan Korporasi; e) Melaksanakan kewajiban yang telah dilalaikan; f) Pembayaran ganti kerugian; g) Pencabutan izin; dan / atau h) Pembubaran Korporasi

Daftar Pustaka

- Marzuki, Peter Mahmud. Penelitian Hukum, Prenada Media Grup, Jakarta, 2015
- Alan Westin : *Privacy is the claim of individuals group or institution to determine for themselves, when, how, and to what extent information about them is communicated to others* dalam Allan Westin, Alan F. Westin, *Privacy and Freedom*, London 1967
- Freeman, Marc and Van Er, Gibran. *International Human Right Law*, Irwin Law Inc, Canada, 2004.
- Aco. A. Agus dan Riskawati. “Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)”. *Jurnal Supremasi Volume 10, Nomor 5*, 2016
- Djafar Wahyudi. “Perlindungan Data Pribadi di Indonesia Lanskap Urgensi dan Kebutuhan Pembaharuan”. *Jurnal Becoss Volume 1, Nomor 1*, 2019
- Dewi Rosadi Sinta. “Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit menurut Ketentuan Nasional dan Implementasinya. *Jurnal Sosiohumariora Volume 19, Nomor 3*, 2017
- Siagian Lauder, Arief Budiarto dan Simatupang. “Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional”. *Jurnal Prodi Perang Asimetris, Volume 4, Nomor 2*, 2018.
- Starkey dan Eppel, E. “Digital Data in New Zealand School: Policy Reform and School Leadership”. *Educational Management Administration and Leadership* (2017)
- Indonesia, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251)
- Indonesia, Undang-undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 6820)
- Graham Greenleaf, 76 Global Data Protection Laws, Privacy Laws & Business Special Report, September 2011
- Lidwina, Andrea. “Kebocoran Data Pribadi yang Terus Berulang <https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang>, 24 Maret 2023
- <https://cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-domain-ramai-ramai-bantah>, 24 Maret 2023