

PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PERUSAHAAN AKIBAT PENYALAHGUNAAN DATA DIGITAL OLEH KARYAWAN PERUSAHAAN

Emmy Febriani Thalib¹, Ketut Laksmi Maswari²

STMIK STIKOM Indonesia, E-mail: emmy.febriani87@gmail.com

Abstrak

Salah satu contoh nyata dari implementasi transformasi digital adalah masyarakat sudah tidak asing lagi dalam mengakses sosial media dan menggunakan media penjualan elektronik untuk memenuhi kebutuhan hidup mereka. Namun, dibalik itu semua tersimpan pula dampak negatif yang jarang disadari yakni kebocoran data pribadi perusahaan dan individu. Penelitian ini menganalisis kondisi tentang masih banyak perusahaan yang belum menyadari pentingnya perlindungan data perusahaan atas penyalahgunaan data digital, penelitian ini dilakukan melalui metode kepustakaan (*library research*) dengan pendekatan kasus yang bersifat yuridis normatif. Hasil penelitian menunjukkan bahwa masih banyak bermunculan kasus penyalahgunaan dan pencurian data pribadi perusahaan oleh karyawan perusahaan yang dapat diselesaikan dengan mekanisme litigasi dan non litigasi. Ada baiknya melakukan antisipasi terlebih dahulu dengan menerapkan cara mengamankan data pribadi perusahaan. Saat ini sangat penting bagi pemerintah untuk dapat segera merampungkan Rancangan Undang-Undang Perlindungan Data Pribadi yang diharapkan dapat memberikan kepastian hukum bagi para pemangku kepentingan dalam rangka melindungi data pribadi masing-masing pihak.

Kata Kunci : Perlindungan Hukum, Data Pribadi Perusahaan, Penyalahgunaan Data.

Abstrack

One clear example of the implementation of digital transformation is that people are familiar with accessing social media and using electronic sales media to meet their daily needs. However, beyond that there is also a negative impact that is rarely realized, namely the leakage of private company and individual data. This study analyzes the condition that there are still many companies that do not realize the importance of protecting corporate data from misuse of digital data. This research was conducted through the library research method with a normative juridical case approach. The results showed that there are many cases of misused and theft of company personal data have emerged by its employee and the dispute resolution could be done through litigation and non litigation process. It is better to anticipate in advance by implementing ways to secure company personal data. Currently, it is very important for the government to immediately finalize the Draft on Regulation concerning of Personal Data Protection which is expected to provide legal certainty for stakeholders in protecting the personal data of each party.

Keywords: Legal Protection, Company Personal Data, Misuse of Data

I

. PENDAHULUAN

1.1.Latar Belakang Masalah

Tidak disangkal lagi bahwa salah satu penyebab utama terjadinya globalisasi yang datangnya lebih cepat dari dugaan semua pihak adalah karena perkembangan pesat teknologi informasi. Penggabungan antara teknologi komputer dengan telekomunikasi telah menghasilkan suatu revolusi di bidang sistem informasi yang telah menerobos batas-batas fisik antar negara. Berdasarkan hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) yang dilakukan pada 2 sampai 25 Juni 2020. Jumlah pengguna internet di Indonesia meningkat menjadi 196,7 juta jiwa hingga kuartal II 2020. Jika pada 2018 lalu, jumlah pengguna internet di Indonesia hanya sebesar 171,2 juta jiwa.¹

Maraknya penyalahgunaan data pribadi dan meningkatnya kesadaran konsumen tentang pentingnya menjaga privasi menuntut perusahaan untuk lebih sadar dan berbenah. Perusahaan perlu memahami regulasi, prinsip-prinsip, serta praktik perlindungan data pribadi. Bukan hanya untuk menghormati hak konsumen, tapi juga agar tak ditinggalkan para konsumennya tersebut.

Perkembangan teknologi dan industri bisnis menjadikan kumpulan data

sebagai salah satu hal yang paling rentan untuk disalahgunakan. Ada saja berbagai pihak yang tidak bertanggung jawab yang sengaja memberikan data pribadi perusahaan terutama klien yang mereka kelola guna kepentingan dan keuntungan pribadi.

Hal ini sangat tentu saja menyalahi kode etik bisnis serta bertentangan dengan hukum. Masih banyak perusahaan belum menyadari pentingnya perlindungan data perusahaan. Dapat dilihat dari peraturan internal perusahaan yang jarang mengatur kewajiban karyawan dan eks karyawan menjaga kerahasiaan data. Akibatnya bermunculan kasus kehilangan data dan pencurian data pribadi perusahaan.

Salah satunya adalah Kasus kebocoran data pengguna juga banyak dialami oleh *startup* unicorn Indonesia sebut saja database pengguna *e-commerce* Tokopedia yang pernah dibobol peretas. Sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopedia dilaporkan dijual di situs gelap, dengan harga 5.000 dollar AS atau sekitar Rp 75 juta.²

Sementara itu di Indonesia sendiri berdasarkan data dari Bareskrim Polri mencatat pada 2017 terdapat 47 kasus, 2018 meningkat jadi 88 kasus, dan lonjakan kasus terus terjadi pada 2019-

¹ Cited on 23 November 2020 "Pengguna Internet Indonesia hingga Kuartal II 2020 Capai 196,7 Juta Orang", <https://money.kompas.com/read/2020/11/09/213534626/pengguna-internet-indonesia-hingga-kuartal-ii-2020-capai-1967-juta-orang>.

² Cited on 23 November 2020 "Kasus Kebocoran Data di Indonesia dan Nasib UU Perlindungan Data Pribadi", <https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all>.

2020 sebanyak 140 kasus.³ Melihat jumlah kasus tersebut maka dapat dilihat bahwa kesadaran masyarakat untuk melaporkan kejahatan atas penyalahgunaan data pribadi sangat kecil persentasenya dibanding kejahatan siber lain.

Pada awal September 2019 lalu, data konsumen dari anak perusahaan Lion Air yakni Malindo Air dan Thai Lion Air mengalami kebocoran. Hal tersebut diungkapkan oleh perusahaan keamanan siber Kaspersky Lab, dan setidaknya sebanyak 21 juta data penumpang bocor dan diunggah ke forum daring.

Perlindungan data pribadi karyawan dan menjaga hak privasi klien perusahaan sudah merupakan hal yang mutlak. Data dan informasi karyawan dan klien yang disimpan harus dipastikan keamanan dan kerahasiaannya, tidak hanya dari pihak luar yang menjamah, tetapi juga dari pihak internal perusahaan yang sengaja menyebarkan data pribadi karyawan untuk kepentingan tertentu.

Secara umum, setiap negara memiliki hukum yang berbeda pula dalam pengaturan berbagai aspek. Saat ini banyak negara yang memiliki undang-undang keterbukaan informasi, undang-undang yang memungkinkan individu untuk meminta akses ke sejumlah data, terutama data pribadi, dan melakukan koreksi data jika data tersebut memiliki kesalahan. Jika secara hukum memungkinkan individu untuk meminta

akses ke semua data, maka kemungkinan data-data yang sensitif mengenai celah keamanan beresiko untuk terbuka.

1.2. Rumusan Masalah

Dari uraian latar belakang diatas, dapat dirumuskan permasalahan antara lain sebagai berikut:

1. Bagaimanakah perlindungan hukum atas penyalahgunaan penggunaan data pribadi perusahaan oleh karyawan perusahaan?
2. Bagaimanakah penyelesaian sengketa yang dapat ditempuh jika terjadi insiden penyalahgunaan penggunaan data pribadi tersebut?

1.3 Tujuan Penelitian

1. Penelitian ini bertujuan untuk memberikan gambaran serta pemahaman tentang perlindungan hukum atas penyalahgunaan penggunaan data pribadi perusahaan oleh karyawan perusahaan
2. Penelitian ini diharapkan dapat memberikan informasi atas penyelesaian sengketa yang dapat ditempuh jika terjadi insiden penyalahgunaan penggunaan data pribadi tersebut.
3. Hasil dari penelitian ini diharapkan dapat mengembangkan ilmu pengetahuan khususnya di bidang hukum siber serta memberikan masukan yang konstruktif atas kebijakan serta ketentuan pemerintah.

2. Metode Penelitian

Menurut Soerjono Soekanto, penelitian hukum adalah suatu kegiatan ilmiah yang didasarkan atas metode,

³ Cited on 20 November 2020, <https://www.alinea.id/nasional/polri-kejahatan-pencurian-data-pribadi-di-level-bahaya-b1ZQw9vR0>

sistematika dan pemikiran tertentu yang bertujuan untuk mempelajari satu atau beberapa gejala hukum tertentu, dengan jalan menganalisisnya, termasuk mengadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut untuk kemudian mengusahakan suatu pemecahan atas permasalahan yang timbul di dalam gejala yang bersangkutan.⁴ Pendekatan penelitian yang digunakan adalah *Statute Approach*, *Conceptual Approach*, serta *Case Approach*.

Tipologi penelitian ini bersifat deskriptif analisis yang bertujuan untuk menggambarkan, menginventarisir, dan menganalisis kondisi yang sebenarnya tentang perlindungan hukum terhadap data pribadi perusahaan akibat penyalahgunaan penggunaan data digital oleh karyawan perusahaan.

Melalui penelitian kepustakaan (*library research*) serta berdasarkan sifatnya penelitian ini adalah penelitian yang bersifat normatif (*legal research*) dengan menekankan pada sumber data sekunder.⁵

3. Hasil Dan Pembahasan

3.1. Perlindungan Hukum atas Penyalahgunaan Penggunaan Data Pribadi Perusahaan oleh Karyawan Perusahaan

Kemajuan teknologi informasi menciptakan evolusi perkembangan gaya

hidup manusia dari zaman ke zaman. Pada saat ini, manusia di abad ke-21 telah mencapai tahapan yang masuk dalam Revolusi Industri 4.0. Perlu diketahui bahwasanya perkembangan Revolusi Industri 4.0 menekankan pada otomatisasi kerja dan mesin tanpa intervensi manusia dengan mendasarkan pada artificial intelligence (AI) dan kecerdasan buatan yang didasarkan pada algoritma pekerjaan yang telah ditentukan.⁶

Sebelum mengurai pembahasan mengenai konsep perlu untuk dikaji terkait dengan tinjauan ruang lingkup / lapangan dari perlindungan data pribadi itu sendiri. Di beberapa negara maju, masalah perlindungan data pribadi sudah dianggap sebagai bagian dari ruang lingkup hak asasi manusia yang harus dilindungi dan oleh karena itulah disediakan peraturan yang mampu mengakomodasinya.⁷

Di wilayah Eropa misalnya, mempunyai ketentuan yang terdapat dalam GDPR yang mengakomodasi masalah perlindungan data pribadi sejak tahun 2016. Negara Inggris sendiri terlepas dari bagian Uni Eropa juga dianggap telah mempunyai peraturan

⁴ Soekanto, S. 2012. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia Press

⁵ Amirudin & Zainal Asikin, *Pengantar Metode Penelitian Hukum*, (Jakarta, Radja Grafindo Persada, 2004), hlm. 118

⁶ Klaus Schwab, 2017, *The Fourth Industrial Revolution*, cet. 1, Crown Business, New York, hlm. 177

⁷ Rosalinda E. Latumahina, 2014, ‘Aspek Hukum Perlindungan Data Pribadi di Dunia Maya’, *Jurnal GEMA AKTUALITA*, Vol. 3, No. 2, hlm. 18.

terhadap perlindungan data pribadi di dalam Data Protection Act 1998⁸

Informasi dan transaksi elektronik yang berhubungan dengan internet, aplikasi, hingga perdagangan elektronik awalnya diatur dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Seiring berkembangnya teknologi informatika dan dampak positif maupun negatif bagi masyarakat, akhirnya diubah lagi menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008. (selanjutnya disebut UU ITE)

Jika dimaknai dari Pasal 1 ayat (1) dapat disimpulkan bahwa hal yang diatur mengenai keamanan dan perlindungan informasi elektronik berupa data. Meliputi suara, foto, video, surat elektronik, *electronic data interchange*, telegram, tulisan, huruf, angka, simbol, kode akses, dan lainnya. Sementara, transaksi elektronik diartikan sebagai suatu perbuatan hukum dilakukan dengan memanfaatkan media komputer, jaringan komputer, dan media elektronik lain.

Informasi adalah kumpulan dari data yang digunakan untuk memperoleh manfaat ekonomi dan keuntungan lainnya. Bagi perusahaan yang bergerak dalam bidang Informasi dan Teknologi dan memanfaatkan teknologi, tentunya data menjadi sesuatu berharga dibanding aset tetap.

Setelah subjek dari konsep perlindungan data pribadi sudah dipahami maka yang selanjutnya harus dipahami adalah objeknya. Objek perlindungan data pribadi adalah informasi yang berdasarkan data dan data tersebut milik pihak pertama. Data dapat disebut sebagai objek perlindungan data pribadi jika data tersebut dapat digunakan untuk mengidentifikasi si pemilik data⁹

Saat ini Indonesia masih belum memiliki kebijakan atau regulasi mengenai perlindungan data pribadi dalam satu undang-undang khusus. Pengaturan tersebut masih berupa Rancangan Undang-Undang Perlindungan Data Pribadi. Sementara itu, aturan yang berlaku saat ini mengenai hal tersebut masih termuat terpisah dan tersebar di beberapa undang-undang dan hanya mencerminkan aspek perlindungan data pribadi secara umum.

UU ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Namun dalam ketentuannya, terdapat Pasal 26 ayat (1) dan penjelasannya UU 19/2016, yang berbunyi:

“Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas

⁸ Edmon Makarim, 2005, Pengantar Hukum Telematika (Suatu Kompilasi Kajian), Jakarta: RajaGrafindo Persada, hlm. 170.

⁹ European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Belgium, 2014, hlm. 36.

persetujuan Orang yang bersangkutan.”

Penjelasan Pasal 26 ayat (1) UU 19/2016:

“Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:

- a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.*
- b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.*
- c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.”*

Jika terjadi penggunaan data pribadi seseorang tanpa izin dari orang yang bersangkutan, maka orang yang dilanggar haknya itu dapat mengajukan gugatan atas kerugian yang ditimbulkan

Sedangkan, hal yang berkaitan dengan penjabaran tentang data elektronik pribadi, UU ITE mengamanatkannya lagi dalam PP No.71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik(selanjutnya disebut PP PSTE) Definisi data pribadi terdapat dalam Pasal 1 angka 29 PP PSTE:

“Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik”

Terdapat satu kasus, dimana seorang pegawai kontrak di sebuah perusahaan telekomunikasi Telkomsel, menyebarkan data pribadi seorang pelanggan hingga membuat ramai media social. Yang dialami Telkomsel adalah karyawan *customer service* tersebut yang diberikan akses terbatas tersebut melakukan tindakan ilegal dengan memfoto data pribadi korban dengan menggunakan HP. Setelah difoto, pelaku mengunggah melalui media sosial ke akun tertentu.¹⁰

Tokopedia dan Bukalapak telah diretas oleh hacker. Data pribadi pelanggan mereka diambil oleh peretas yang berhasil masuk ke server mereka. Atas kejadian peretasan tersebut, perusahaan *e-commerce* tersebut telah melaporkan kepada polisi sebagai korban.

Sebelum mengambil sejumlah langkah dalam melindungi perusahaan dari kebocoran data, pemilik perusahaan harus paham betul sudah ada di tahapan mana internal organisasi perusahaan. Apakah sudah matang dengan teknologi atau belum.

Hingga detik ini banyak orang masih bertanya-tanya mengenai data yang penting bagi perusahaan. Dalam praktiknya perusahaan menyimpan berbagai jenis data yang dikelompokkan sebagai berikut ini.

- 1) Data yang dapat dipublikasikan
- 2) Data biasa
- 3) Data rahasia

¹⁰ Cited on 19 November 2020, <https://www.tribunnews.com/nasional/2020/07/19/kebocoran-data-pelanggan-karena-akses-ilegal-karyawan>

4) Data sangat rahasia

Biasanya data-data tersebut dapat diketahui karyawan ketika melakukan operasional perusahaan. Adapun hal yang dipermasalahkan yakni sering terjadi pergantian karyawan. Sehingga, ujung-ujungnya banyak perusahaan berhadapan dengan hukum karena data rahasia dan data sangat rahasia tersebar ke luar.

Berikut ini beberapa langkah paling direkomendasikan agar data pribadi perusahaan terlindung, yakni:¹¹

- 1) Membuat klasifikasi data yang ada di perusahaan.
- 2) Mengkategorikan jenis data, hak akses, dan tanggung jawab bagi karyawan pemegang data.
- 3) Menetapkan aturan resmi cara forward email.
- 4) Membuat SOP yang mewajibkan karyawan mengembalikan laptop dan komputer dari perusahaan.
- 5) Membuat SOP terkait aturan backup data.
- 6) Membuat surat perjanjian tentang kerahasiaan data dari perusahaan yang dipegang oleh karyawan. Sehingga, ketika suatu saat karyawan sengaja atau tidak sengaja membocorkan maka dianggap melanggar perjanjian dan dapat diproses secara hukum.

2. Penyelesaian Sengketa atas insiden Penyalahgunaan Data Pribadi

Saat ini banyak perusahaan tidak mengetahui informasi perusahaan mereka telah beredar di pasaran seperti layaknya

barang dagangan. Informasi memiliki harga jual dan harga beli, menjadi objek tawar menawar di pasar gelap informasi. Penjual dapat menawarkan harga informasi tersebut tergantung dari seberapa pentingnya informasi tersebut. Semakin penting dan berharga suatu informasi, semakin mahal pula harga yang ditawarkan. Contoh : identitas pribadi, biografi para petinggi perusahaan, kartu kredit, alamat email, nomor hp, alamat rumah, alamat perusahaan, informasi database konsumen, database karyawan, database rekanan, database produk, database daftar *improvement innovation*, dan banyak lagi.

Berdasarkan survei Risiko Keamanan TI Kaspersky, informasi pribadi pelanggan lebih sering terlibat dalam pelanggaran data (*data breaches*) daripada jenis data perusahaan (korporat) lainnya.¹² Dampak dari kebocoran informasi bagi perusahaan adalah antara lain :

1. *Legal liability*. Perusahaan yang lalai dalam melindungi informasi penting miliknya (yang mengandung informasi customer didalamnya) akan berhadapan dengan UU ITE
2. *Lost productivity*. Perusahaan yang tidak menjaga dengan aman hasil-hasil penemuan baru dan pengembangan baru akan menimbulkan lost productivity, baik bagi karyawan maupun perusahaan itu sendiri karena desain produk baru sudah berpindah ke perusahaan lain

¹¹ Cited on 20 November
<https://www.dslalawfirm.com/data-pribadi-perusahaan-uu-ite/>

¹² Cited on
<https://www.katakini.com/artikel/32705/survey-kaspersky-data-pribadi-pelanggan-lebih-sering-bocor/>

3. *Business reputation.* Kejatuhan reputasi bisnis tidak serta merta akan dialami perusahaan saat itu juga bila perusahaan mengalami kebocoran informasi. Kerugian juga tidak akan bisa dihitung secara kuantitatif. Namun demikian, pelan tapi pasti perusahaan yang tidak dapat menjaga informasinya akan mengalami degradasi reputasi bisnis, baik nasional dan internasional.

Secara hukum Perusahaan yang memiliki dan mengolah data pribadi dari konsumennya disebut sebagai Penyelenggara Sistem Elektronik (selanjutnya disebut PSE). PSE wajib menyimpan dan melindungi data pribadi yang dimiliki oleh pemilik data pribadi dalam sistem elektronik. Jika diretas, sehingga semua data pribadi yang disimpan PSE diambil oleh pelaku, berarti PSE telah gagal melakukan perlindungan rahasia data pribadi dalam sistem elektronik yang dikelolanya.

Keamanan data pribadi memerlukan instrument perlindungan hukum yang memadai di era modern ini. Berkaca pada European Union General Data Protection Regulation, salah satu aspek perlindungan atas keamanan data pribadi adalah adanya tanggungjawab keamanan apabila terjadi serangan terhadap privasi data pribadi. Dalam hal ini, pihak yang bertanggungjawab atas pemrosesan data pribadi harus melaporkan pada otoritas keamanan terkait dalam waktu maksimal 72 jam.¹³

Pemilik data pribadi dapat menyelesaikan sengketa dengan cara non-litigasi dengan mengajukan pengaduan pada Menteri Komunikasi dan Informatika atau menempuh cara litigasi (mengajukan gugatan perdata). Merujuk kepada aspek pidana, setidaknya ada enam UU yang mengatur mengenai sanksi pidana bocornya kerahasiaan data pribadi, yaitu UU No. 8/1999 tentang Perlindungan Konsumen, UU No. 7/1992 jo. UU No. 10/1998 tentang Perbankan, UU No. 11/2008 jo. UU 19/2106 tentang ITE, UU No. 14/2008 tentang Keterbukaan Informasi Publik, UU No. 40/2014 tentang Asuransi, dan UU No. 23/2006 jo. UU No. 24/2013 tentang Administrasi Kependudukan. Sanksi pidana penjara paling berat ada pada UU ITE dimana sanksi pidana kebocoran data adalah maksimal 10 tahun penjara.

Sementara itu, sanksi denda paling berat ada pada UU Perbankan dimana denda maksimum yang bisa dikenakan adalah Rp10 miliar hingga Rp200 miliar. Proses penyelesaian sengketa perlu mencerminkan restorative justice agar memberikan dampak keadilan bagi subjek data yang melanggar hak privasinya.

Sebagai perbandingan Inggris telah memiliki lembaga independen yang menjalankan fungsi pengawasan terhadap perlindungan data, melalui Komisi Informasi Inggris (ICO). Lembaga inilah yang memiliki wewenang untuk menginvestigasi, dan kemudian menjatuhkan sanksi denda bagi perusahaan, sebagai pengendali data.

¹³ General Data Protection Regulation, Article 33

Pada poin 2 (f) Peraturan Menteri Kominfo No 20 Tahun 2016. Penyelenggara Sistem Elektronik harus memiliki itikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi. Dalam kasus ini, apakah pemilik sistem elektronik yang merupakan perusahaan harus sudah memberitahukan secara eksplisit bahwa terjadi kegagalan perlindungan data pribadi. Seperti pada kasus Malindo Air, Masalah kebocoran data ini pun ditindaklanjuti ke otoritas Malaysia untuk investigasi lanjutan.

Pada kasus ini, Lion Air Group berada pada posisi korban. Pasalnya, kerjasama dengan perusahaan el GoQuo tertuang dalam bentuk MoU dan *non-disclosure agreement* (NDA). Sebagai akibat dari kekosongan hukum ini, lanjutnya, Lion Air selaku pengendali data (*data controller*) terhindar dari kewajiban-kewajiban yang sepatutnya dilekatkan selaku pengendali data pribadi.

Secara umum, pengendali data memiliki kewajiban untuk menjaga infrastruktur keamanan data pribadi pengguna layanannya, yang meliputi penerapan *pseudonymization* dan enkripsi data pribadi, serta memberikan jaminan kerahasiaan, integritas, ketersediaan, dan ketahanan yang berkelanjutan dari sistem dan layanan pemrosesan.

Selain itu, Lion Air juga berkewajiban memiliki kemampuan untuk memulihkan ketersediaan dan akses ke data pribadi dalam waktu yang tepat (tidak menunda-nunda) dalam hal terjadi insiden fisik atau teknis (i.e. kebocoran data), dan menerapkan proses

pemantauan dan evaluasi secara teratur serta audit terhadap efektivitas langkah-langkah teknis dan organisasi untuk memastikan keamanan pemrosesan (termasuk menerapkan *Privacy by Design dan Data Protection Impact Assessments (DPIAs)*).¹

4.PENUTUP

4.1 Simpulan

Berdasarkan uraian pembahasan diatas, maka dapat diambil kesimpulan sebagai berikut :

- 1) Jika terjadi penggunaan data pribadi seseorang tanpa izin dari orang yang bersangkutan, maka orang yang dilanggar haknya itu dapat mengajukan gugatan atas kerugian yang ditimbulkan kepada perusahaan yang dianggap lalai dalam pengendalian data. Begitu pula perusahaan yang mempekerjakan karyawan yang sengaja atau tidak sengaja menyalahgunakan data pribadi perusahaan maka karyawan tersebut dianggap melanggar perjanjian dan dapat diproses secara hukum.
- 2) Pemilik data pribadi dapat menyelesaikan sengketa dengan cara non-litigasi dengan mengajukan pengaduan pada Menteri Komunikasi dan Informatika atau menempuh cara litigasi (mengajukan gugatan perdata) dengan harus menerapkan prinsip *restorative justice*.

1.2 Saran

¹ Cited on 21 November 2020, <https://www.hukumonline.com/berita/baca/lt5d8947d7aa783/data-penumpang-lion-air-bocor--uu-perlindungan-data-pribadi-dibutuhkan?page=all>

- 1) Sejauh ini Indonesia belum memiliki aturan yang jelas mengenai perlindungan data pribadi. Pelanggaran-pelanggaran terhadap data pribadi baru diatur sebatas Peraturan Menteri, belum setingkat Undang-Undang. Maka hal ini menjadi urgensi atas terbitnya RUU Perlindungan Data Pribadi yang sampai sekarang belum rampung.
- 2) Hukum kita belumlah menjangkau eksekusi atas pengembalian data pribadi elektronik yang bocor. Begitupun dengan konteks “pengembalian”, data yang bocor secara elektronik mudah diduplikasi secara masif dan bagaimana kemudian data ini kembali bisa menjadi “satu” agar data tidak lagi disalahgunakan oleh pihak lain yang mungkin tidak terlibat dalam kasus yang bersangkutan. Hal ini tentu masih menjadi pekerjaan rumah bagi Indonesia.
- 3) Peran Pemerintah dan Masyarakat Berupa Partisipasi dan Edukasi Masyarakat dapat dilakukan melalui pendidikan dan/atau pelatihan, advokasi, bimbingan teknis, dan sosialisasi dengan menggunakan berbagai media sangat diperlukan.

DAFTAR PUSTAKA

- Undang Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
- PP No.71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

General Data Protection Regulation

Amirudin & Zainal Asikin, *Pengantar Metode Penelitian Hukum*, (Jakarta, Radja Grafindo Persada, 2004)

Edmon Makarim, 2005, *Pengantar Hukum Telematika (Suatu Kompilasi Kajian)*, Jakarta: RajaGrafindo Persada,

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, Belgium, 2014

Klaus Schwab, 2017, *The Fourth Industrial Revolution*, cet. 1, Crown Business, New York

Rosalinda E. Latumahina, 2014, ‘*Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*’, Jurnal GEMA AKTUALITA, Vol. 3, No. 2

Soekanto, S. 2012. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia Press

Cited on 20 November ,<https://www.dslalawfirm.com/data-pribadi-perusahaan-uu-ite/>

Cited on 19 November 2020, <https://www.tribunnews.com/nasional/2020/07/19/kebocoran-data-pelanggan-karena-akses-ilegal-karyawan>

Cited on 20 November 2020, <https://www.alinea.id/nasional/polri-kejahatan-pencurian-data-pribadi-di-level-bahaya-b1ZQw9vR0>

Cited on 21 November 2020, <https://www.hukumonline.com/berita/baca/1t5d8947d7aa783/data->

penumpang-lion-air-bocor--uu-
perlindungan-data-pribadi-
dibutuhkan?page=all

kebocoran-data-di-indonesia-dan-
nasib-uu-perlindungan-data-
pribadi?page=all.

Cited on 20 November 2020,
<https://www.katakini.com/artikel/32705/survey-kaspersky-data-pribadi-pelanggan-lebih-sering-bocor/>

Cited on 23 November 2020 "Pengguna Internet Indonesia hingga Kuartal II 2020 Capai 196,7 Juta Orang", <https://money.kompas.com/read/2020/11/09/213534626/pengguna-internet-indonesia-hingga-kuartal-ii-2020-capai-1967-juta-orang>.

Cited on 23 November 2020 "Kasus Kebocoran Data di Indonesia dan Nasib UU Perlindungan Data Pribadi", <https://tekno.kompas.com/read/2020/05/05/19080067/kasus->