PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI KONSUMEN YANG DIRETAS BERDASARKAN PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA NOMOR 20 TAHUN 2016 TENTANG PERLINDUNGAN DATA PRIBADI DALAM SISTEM ELEKTRONIK[1]

Oleh: Refaldy Braif Carundeng[2]
Anna S. Wahongan[3]
Presly Prayogo[4]

ABSTRAK

Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimana perlindungan hukum terhadap konsumen yang data pribadinya diretas dan bagaimana sanksi hukum terhadap pelaku kejahatan peretasan data pribadi yang mana dengn metode penelitian hukum normatif disimpulkan: 1. Dengan perkembangan zaman, kemajuan dari teknologi merupakan hal yang sangat berguna bagi manusia. Namum dalam perkembangannya teknologi memiliki kekurangan, seperti kejahatan dunia maya (Cyber Crime) salah satunya peretasan data pribadi. Macam-macam peraturan perundang–undangan yang ada di Indonesia, yang mengatur mengenai perlindungan data pribadi tidak mampu memberikan perlindungan yang cukup terhadap data pribadi. Perlindungan terhadap data pribadi telah diatur secara khusus pada Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016, namun perlindungan hukum yang sifatnya represif pada peraturan tersebut belum bisa memberikan perlindungan yang cukup karena disana tidak memiliki sanksi yang cukup untuk menghentikan atau mengurangi pelaku pelanggar data pribadi. Bentuk-bentuk perlindungan hukum terhadap data pribadi konsumen. Perlindungan hukum preventif, perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Perlindunga hukum represif**,** merupakan perlindungan hukum yang dilakukan berdasarkan keputusan yang ditetapkan badan hukum yang bersifat mengikat yang bertujuan untuk menyelesaikan suatu sengketa. Tanggung jawab perusahaan penyelenggara sistem elektronik jika terjadi peretasan data pribadi terhadap konsumenya. Munculnya hak dan kewajiban antara perusahaan penyelenggara sistem elektronik dengan konsumen ialah saat konsumen menyetujui *term of Service* (ketentuan layanan) yang di berikan oleh perusahaan penyelenggara sistem elektronik. Dengan begitu telah terjadi perikatan yang terjadi antar para pihak. 2. sanksi hukum terhadap pelaku kejahatan peretasan data pribadi menggunkan Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transksi Elektronik. Dan dirumuskan dalam Pasal 30 Tentang Ilegal Akses dan dalam Pasal 32 Tentang Pencurian Data. Pada Pasal 30 Tentang Ilegal Akses terdapat 3 ayat yang berbunyi sebagai berikut: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan.

Kata kunci: data pribadi; sistem elektronik;

PENDAHULUAN

A. Latar Belakang Masalah

Perbuatan melawan hukum di dunia maya merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan carding, penipuan, peretasan data pribadi, terorisme, dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan di dunia maya.[5] Sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan

[1] Artikel Skripsi
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM : 17071101405
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] DR. Siswanto Sunarso, SH, MH, M.Kn, Hukum Informasi dan Transaksi Elektronik, Jakarta, 2009,hlm 39.

perbuatan melawan hukum [6]. Tidak dapat disangkal bahwa perkembangan teknologi yang demikian pesat ikut mengubah sikap dan perilaku masyarakat dalam komunikasi dan interaksi. Hampir seluruh aspek kehidupan masyarakat selalu bersentuhan langsung dengan teknologi dan terbukti mendatangkan manfaat bagi perkembangan dan peradaban manusia. Kemajuan teknologi menghasilkan sejumlah situasi yang tak pernah terpikirkan sebelumnya oleh manusia.[7]

B. Rumusan Masalah

1. Bagaimana perlindungan hukum terhadap konsumen yang data pribadinya diretas ?
2. Bagaimana sanksi hukum terhadap pelaku kejahatan peretasan data pribadi ?

C. Metode Penelitian

Jenis penelitian yang digunakan ialah penelitian hukum normative.

PEMBAHASAN

A. Bagaimana Perlindungan Hukum Terhadap Konsumen Yang Data Pribadinya Diretas

Indonesia adalah negara hukum dan sudah jelas termasuk dalam Pasal 1 ayat (3) UUD Tahun 1945. Asas perlindungan dalam Negara hukum tampak antara lain dalam *declaration of independent*, deklarasi tersebut mengandung asas bahwa orang yang hidup di dunia ini, sebenarnya telah diciptakan merdeka oleh Tuhan, dengan dikaruniai beberapa hak yang tidak dapat dirampas atau dimusnahkan, hak tersebut mendapat perlindungan secara tegas dalam Negara hukum.

Hak pribadi sebagai hak asasi manusia dijelaskan Danrivanto Budhijanto bahwa "Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah."

Perlindungan hukum merupakan suatu hal yang melindungi subjek-subjek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan menggunakan suatu sanksi. Yang dimaksud dengan subjek hukum adalah orang dan badan hukum. Perlindungan hukum dibedakan menjadi dua yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif diberikan oleh pemerintah dengan tujuan mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu dalam melakukan kewajiban. Perlindungan hukum represif merupakan perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran[8]

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi, seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai 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[9] Alasan-Alasan privasi harus dilindungi yaitu :

1. Dalam membina hubungan dengan orang lain, sesorang harus menutup sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu.
2. Seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*) sehingga privasi sangat diperlukan oleh seseorang.
3. Privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hal lain tetapi hak ini hilang apabila orang tersebut

[6] Maskun, "Kejahatan Siber *Cyber Crime*", (Jakarta: Kencana Prenada Media Grup, 2013), hlm 29.

[7] Edmon Makarin, Tanggung Jawab Hukum penyelenggaraan Sistem Elektronik, Jakarta, 2010 hlm 2.

[8] Moh Kusnardi dan Harmaily Ibrahim, Hukum Tata Negara Indonesia, Jakarta: Sinar Bakti, 1998, hal 102.

[9] Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, "Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia", Jurnal ilmu Hukum, Vol.3 No.2, April, 2019, hal 155.

mempublikasikan hal-hal yang bersifat pribadi kepada umum.

4. Privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai *the right against the word*.
5. Alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai dimana kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapat kompensasi.[10]

Perlindungan terhadap Data Pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri.[11]

Pengaturan perlindungan Data Pribadi dimaksudkan untuk melindungi kepentingan kosumen dan memberikan manfaat ekonomi bagi Indonesia. Konsumen yang dimaksud pada penelitian ini ialah konsumen akhir. Pengaturan ini akan melindungi data pribadi konsumen terhadap penyalahgunaan pada saat data tersebut memiliki nilai tinggi untuk kepentingan bisnis, yang pengumpulan serta pengolahannya menjadi kian mudah dengan perkembangan teknologi informasi dan komunikasi. Perkembangan pengaturan terhadap perlindungan data pribadi secara umum akan menempatkan Indonesia sejajar dengan dengan negara negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai perlindungan data pribadi. Bagi kepentingan konsumen, kebutuhan akan perlindungan data pribadi konsumen terutama di era di mana Data Pribadi menjadi lebih sangat berharga bagi kepentingan bisnis, menimbulkan kekhawatiran bahwa data pribadi konsumen dijual atau digunakan tanpa persetujuan konsumen. Untuk itu, terlihat kebutuhan akan suatu perundang-undangan mengenai perlindungan Data Pribadi yang bersifat khusus untuk memastikan bahwa data pribadi konsumen dilindungi dengan baik.

Pengaturan tentang Data Pribadi sangat diperlukan karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman dan keamanan data pribadi individu dengan kebutuhan pemerintah dan pelaku bisnis untuk memperoleh dan memproses data pribadi untuk keperluan yang wajar dan sah.[12]

1. Bentuk-Bentuk Perlindungan Hukum Terhadap Data Pribadi Konsumen :

a. Perlindungan Hukum Preventif

Perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban.

Peraturan Menteri Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Untuk pencegahan dari adanya *cyber hacking* diperlukan peraturan internal atau *self-regulation* oleh setiap penyelenggara sistem elektronik. Dalam praktiknya *self-regulation* tidak bisa berjalan sendiri tanpa intervensi dari negara yang memberikan pengaturan dan informasi bagi konsumen terhadap pelaku usaha (penyelenggara sistem elektronik) yang aman untuk bertransaksi. Oleh sebab itu negara mengatur dalam Pasal 5 (1) Peraturan Menteri Nomor 20 Tahun 2016 tentang perlindungan data pribadi dalam system elektronik

[10] Andrew pelealu, Tesis :" Perlindungan Hukum Atas Data Pribadi Konsumen Dalam Transaksi E-Commerce", (Yogyakarta : Universitas AtmaJaya Yogyakarta, 2018), hal 18-19.

[11] Lia Sautunnida, "Urgensi Undang - Undang Perlindunngan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia", Kanun Jurnal Ilmu Hukum , Vol.20, No.2, Agustus, 2018, hal 374.

[12] Shinta Dewi Rosadi, Cyber Law : Aspek Data Privasi Menurut Hukum Internasional,
Regional, dan Nasional, Refika Aditama, Bandung, 2015, hal 15.

penyelenggara sistem elektronik, yang mengharuskan penyelenggara sistem elektronik mempunyai aturan internal mengenai perlindungan data pribadi konsumennya. Dengan adanya aturan tentang standar *self-regulation* yang di berikan oleh pemerintah diharapkan keamanan data pribadi konsumen dapat di jaga dengan baik oleh penyelenggara sistem elektronik, dan dapat mencegah terjadinya tindakan peretasan atau hacking yang mengincar data pribadi konsumen.

b. Perlindungan Hukum Represif

Perlindungan hukum represif merupakan perlindungan hukum yang dilakukan berdasarkan keputusan yang ditetapkan badan hukum yang bersifat mengikat yang bertujuan untuk menyelesaikan suatu sengketa. [13] Ketentuan-ketentuan mengenai data pribadi sebegaimana telah di kemukakan sebelumnya merupakan suatu ketentuan yang menempatkan perusahaan penyedia sistem elektronik sebagai pihak yang berkewajiban untuk selalu menjaga segala data pribadi para konsumennya. Pelanggaran terhadap ketentuan data pribadi telah diatur oleh Undang-Undang Nomor 19 tahun 2016 tentang perubahan Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE). Dalam Pasal 30 UU ITE menitik beratkan kepada para pelaku peretasan (Hacker). Sebagai upaya perlindungan hukum represif yang di tujukan untuk para konsumen agar ada kepastian hukum ketika data pribadi yang mereka miliki di gunakan secara melawan hukum demi kepentingan-kepentingan tertentu. Adapun dalam ketentuan Pasal 36 (1) Peraturan Menteri Nomor 20 tahun 2016 tentang data pribadi dalam sistem elektronik memberikan sanksi administratif kepada setiap orang yang menyalahgunakan data pribadi seseorang.

2. Tanggung Jawab Perusahaan Penyelenggara Sistem Elektronik Jika Terjadi Peretasan Data Pribadi Terhadap Konsumenya.

Munculnya hak dan kewajiban antara perusahaan penyelenggara sistem elektronik dengan konsumen ialah saat konsumen menyetujui *term of Service* (ketentuan layanan) yang di berikan oleh perusahaan penyelenggara sistem elektronik. Dengan begitu telah terjadi perikatan yang terjadi antar para pihak. *Term of Service* tersebut merupakan suatu kontrak elektronik yang di berikan oleh perusahaan penyelengara sistem eleketronik kepada konsumen untuk memenuhi atau mengikuti peraturan yang telah di buat oleh perusahaan penyelenggara sistem elektronik. Dalam hal ini, konsumen mempercayakan data pribadi yang mereka miliki untuk di proses kepada perusahaan penyelenggara sistem elektronik.

Kitab Undang-Undang Hukum Perdata membedakan dengan jelas antara perikatan yang timbul dari perjanjian dan perikatan yang timbul dari Undang- Undang. Akibat hukum suatu perikatan yang lahir dari perjanjian memang dikehendaki oleh para pihak, karena memang perjanjian didasarkan atas kesepakatan yaitu persesuaian kehendak antara para pihak yang membuat perjanjian. Adapun akibat hukum suatu perikatan yang lahir dari undang-undang mungkin tidak dikehendaki oleh para pihak tetapi hubungan hukum dan akibat hukumnya ditentukan oleh undang-undang. Apabila atas perjanjian yang disepakati terjadi pelanggaran maka dapat diajukan gugatan wanprestasi, karena ada hubungan kontraktual antara pihak yang menimbulkan kerugian dan pihak yang menderita kerugian. Apabila tidak ada hubungan kontraktual antara pihak yang menimbulkan kerugian dan pihak yang menerima kerugian, maka dapat diajukan gugatan perbuatan melawan hukum.

3. Penyelesaian Sengketa Bagi Konsumen Yang Dirugikan Dari Peretasan Data Pribadi Menurut Hukum di Indonesia.

Penyelesaian sengketa ada dua jalur yang dapat di gunakan oleh konsumen untuk menyelesaikan sengketa data pribadi yaitu litigasi (melalui pengadilan) dengan cara melakukan gugatan perdata kepada pihak penyelenggara sistem elektronik sesuai dengan prosedur yang telah di tetapkan oleh perundang-undangan. Langkah selanjutnya yaitu penyelesaian sengketa diluar pengadilan (non- litigasi) dapat ditempuh melalui BPSK (Badan Penyelesaian Sengketa Konsumen) yang tugas dan wewenangnya anatara lain meliputi pelaksanaan penanganan dan penyelesaian sengketa konsumen, dengan cara melalui mediasi atau arbitrase atau konsiliasi, yang

[13] Phillipus M. Hadjon, Perlindungan Hukum Bagi Rakyat Indonesia, PT. Bina Ilmu, Surabaya: 1987. Hal 29.

selain sebagai media penyelesaian sengketa juga dapat menjatuhkan sanksi administratif bagi pelaku usaha (penyelenggara sistem elektronik) yang melanggar larangan-larangan tertentu yang dikenakan bagi pelaku usaha.[14] Hal tersebut seperti yang telah diatur dalam Pasal 52 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Dalam Perturan Menteri Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi juga mengatur tentang tata cara penyelesaian sengketa yang terjadi, hal tersebut di atur dalam Pasal 29 hingga Pasal 33. Dalam ketentuannya konsumen dapat melakukan pengaduan bahwa telah terjadinya kegagalan perlindungan Data Pribadi kepada kementrian komunikasi dan informatika. Konsumen paling lambat melakukan pengaduan kepada kementrian komunikasi dan informatika yaitu selama 30 hari setelah konsumen mengetahui terjadinya kegagalan perlindungan terhadap data pribadinya. Dalam laporannya konsumen harus membawa bukti bukti pendukung. Apabila pengaduan telah diterima oleh kementrian komunikasi dan informatika maka lembaga penyelesaian sengketa Data Pribadi harus menanggapi pengaduan tersebut paling lama 14 hari kerja sejak pengaduan diterima. Penyelesaian sengketa Data Pribadi ini di lakukan secara musyawarah atau melalui penyelesaian alternatif lainnya. Apabila dalam permusyawarahan tersebut tidak di temukan kesepakatan maka konsumen dapat melakukan gugatan perdata sesuai dengan ketentuan perundang-undangan.

Pasal 28 Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa: Setiap Penyelenggara Sistem Elektronik wajib:

a. Melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan;
b. Menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi;
c. Memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut:
    1. Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi;
    2. Dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya;
    3. Harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan
    4. Pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut;
d. Memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan;
e. Menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya;
f. Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi;
g. Memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa menganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
h. Memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-

[14] Abdul Halim Barkatullah, Abdul Halim Barkatullah, Hukum Transaksi Elektronik, Nusa Media, Bandung, 2017, hal 138.

masing Instansi Pengawas dan Pengatur Sektor untuk itu; dan

i. Menyediakan narahubung (*contact person*) yang mudah dihubungi oleh pemilik data pribadi terkait pengelolaan data pribadinya

Kasus pencurian data pribadi pengguna tokopedia oleh pihak ketiga atau *hacker* dapat disimpulkan bahwa perlindungan sistem data tokopedia tidak aman. Pelanggaran yang dilakukan tokopedia dengan membiarkan data pribadi penggunanya jatuh kepada pihak ketiga merupakan pelanggaran hak pengguna, yang dilindungi oleh hukum atas dasar perjanjian dan atas dasar tokopedia sebagai penyelenggara sistem elektronik.

Tertulis dalam kebijakan privasi bahwa tokopedia menjamin tidak ada penjualan, pengalihan, distribusi atau meminjamkan data pribadi pengguna kepada pihak ketiga lain, tanpa terdapat izin kecuali dalam hal mematuhi kewajiban hukum dan/atau adanya permintaan yang sah dari aparat penegak hukum dan membagikan data atau informasi pengguna yang diperlukan dalam rangka kelayakan kredit kepada lembaga atau biro pemeringkat kredit atau lembaga pengelolaan informasi perkreditan (LPIP).

Tokopedia dapat dikenakan sanksi atas kelalaiannya, karena setiap penyelenggara sistem elektronik harus mempertanggungjawabkan bahwa sistemnya andal, aman dan beroperasi sebagaimana semestinya, kewajiban lain yang tidak dipenuhi oleh Tokopedia adalah Pasal 24 ayat 3 Peraturan Pemerintah Nomor 71 Tahun 2019, yaitu untuk melakukan pengamanan terhadap komponen sistem elektronik dalam hal terjadi kegagalan atau gangguan sistem yang berdampak serius sebagai akibat perbuatan pihak lain terhadap sistem elektronik. Penyelenggara sistem elektronik wajib mengamankan informasi elektronik dan atau dokumen elektronik dan segera melaporkan dalam kesempatan pertama kepada aparat penegak hukum dan kementerian atau lembaga terkait. Penegak hukum yang dimaksud ialah polisi siber dan kementerian komunikasi dan informatika Republik Indonesia.

Tokopedia sebagai penyelenggara sistem elektronik dapat dikenai sanksi dalam Pasal 100 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggara sistem dan transaksi elektronik. Sanksi yang dapat diberikan terhadap tokopedia sebagai penyelenggara sistem elektronik yang melanggar kewajiban tersebut dapat dikenakan sanksi administrastif, berupa:

a. Teguran tertulis.
b. Denda administratif.
c. Penghentian sementara.
d. Pemutusan Akses.
e. Dikeluarkan dari daftar.

Pengguna yang mengalami kerugian karena bocornya data pribadi, difasilitasi pengaduan kepada Badan Perlindungan Konsumen Nasional. Kerugian yang dialami 91.000.000 (sembilan puluh satu juta) pengguna Tokopedia karena data pribadinya "bocor" ialah kerugian imateriil karena rentan mengalami kejahatan *carding*, *phising*, *profiling*, serta *scamming*. Pengguna merasa tidak aman karena seseorang mengetahui dengan detail alamat rumah, nomor telfon maupun alamat emailnya dan juga kerugian materiil apabila *hacker* tersebut mengetahui data kartu kredit yang terdaftar dalam akun pengguna Tokopedia. Kejahatan *carding* bukan hal yang mustahil dilakukan apabila *hacker* tersebut mempunyai data-data pribadi pengguna. *Scamming* bisa terjadi akibat data personal pengguna tokopedia tersebar, data personal tersebut digunakan untuk *profiling* dan mengetahui daftar kontak orang lain yang dapat dikirimkan SMS berupa scam maupun *phising*. Data nomor telepon yang tersebar dapat diperjualbelikan untuk kepentingan telemarketing, meskipun kita tidak pernah berafiliasi dengan perusahaan penawar jasa dan produk tersebut namun penelepon telah mengetahui nama lengkap kita.

PT Tokopedia adalah suatu perseroan terbatas yang menjalankan kegiatan usaha jasa web portal www.tokopedia.com, yakni situs pencarian toko dan barang yang dijual serta terdaftar. Dan selanjutnya disebut dengan tokopedia, pengguna adalah pihak yang menggunakan layanan tokopedia, namun pengguna tidak terbatas pada pembeli, penjual maupun pihak lain yang sekedar berkunjung ke situs tokopedia. Pembeli adalah pengguna terdaftar yang melakukan permintaan atas barang yang dijual oleh penjual di situs tokopedia. Penjual adalah pengguna terdaftar yang melakukan tindakan buka toko dan/atau

melakukan penawaran atas suatu barang kepada para pengguna situs tokopedia.

Tokopedia merupakan penyedia jasa, penyelenggara sistem elektronik yang terdaftar dengan tanda daftar 00315/DJAI.PSE/07/2017. Tokopedia mengumpulkan data-data pengguna sebagai berikut, nama pengguna, alamat *email*, nomor telepon, *password*, alamat, foto, interaksi dengan pengguna lain menggunakan fitur pesan, alamat pengiriman, detil transaksi, data-data pembayaran berupa data rekening bank, kartu kredit, alamat IP, lokasi *Wi-Fi*, aktivitas pengguna, data perangkat termasuk nomor imei dan data catatan (log). Data-data berikut dapat dikatakan data pribadi dan privasi yang wajib dijaga kerahasiaannya oleh tokopedia sebagai pengumpul data dan tertuang perlindungan hak pengguna tokopedia sesuai dengan pandangan John Locke bahwa semua orang memiliki hak-hak alamiah yang harus dipertahankan dalam tatanan negara.

Hak pengguna tersebut berhubungan dengan kewajiban tokopedia untuk melindungi data pribadi penggunanya didasari dengan alasan bahwa hak setiap orang untuk tidak dicampuri atas masalah bersifat pribadi (*personal privacy*). Kewajiban tokopedia untuk melindungi data pribadi pengguna merupakan perwujudan hak pengguna agar data tersebut tidak jatuh kepada pihak ketiga yang berniat tidak baik.

B. Bagaimana Sanksi Hukum Terhadap Pelaku Kejahatan Peretasan Data Pribadi

Telah disebutkan dalam Undang-Undang Dasar 1945 dengan segala amandemennya menjelaskan bahwa salah satu bentuk hak asasi manusia harus dijaga dan dilindungi oleh negara adalah perlindungan diri seseorang terhadap hal yang bersifat public, kedalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

Hacking (peretasan) merupakan suatu proses menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan. *Hacker* sebutan bagi seorang yang melakukan aktifitas ini berupayah mencari celah komputer atau jaringan komputer guna mencari keuntungan tertentu. Dalam Undang-Undang Informasi dan Transaksi Elektronik seorang *hacker* telah diatur dalam Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transksi Elektronik. Dan dirumuskan dalam Pasal 30 Tentang Ilegal Akses dan dalam Pasal 32 Tentang Pencurian Data. Pada Pasal 30 Tentang Ilegal Akses terdapat 3 ayat yang berbunyi sebagai berikut:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun". Penjelelasan mengenai ayat (1) ini bahwa komputer dan/atau sistem elektronik merupakan privasi orang yang dilindungi keberadaannya. Perumusan Hacking sebagai tindak pidana dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik pasal 30 Ayat (1) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana pasal 46 Ayat (1) yaitu "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1), dipidana dengan pidana penjara paling lam 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)".
>
> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Sama halnya seperti pada Ayat (1) namun dalam Ayat (2) ini ditambahkan unsur "dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Perumusan Hacking sebagai tindak pidana dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Pasal 30 Ayat (2) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana Pasal 46 Ayat (2) yaitu "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah)".

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan". Penjelesan mengenai ayat di atas adalah Unsur yang "dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan". Dalam unsur ini berarti bahwa pelaku *Hacking* melakukan kejahatannya dengan menerobos sistem keamanan atau dalam ilmu komputer disebut firewall. Para hacker menggunakan berbagai aplikasi tool hacking dalam melakukan kejahatannya. Dimana aplikasi tersebut berguna untuk menerobos atau menjebol sistem keamanan suatu sistem elektronik. Hal ini dapat dianalogikan dengan memasuki rumah orang lain tanpa ijin dengan menjebol engsel pintu/jendela yang ketentuan pidananya diatur dalam Pasal 167 ayat (2) Kitab Undang-Undang Hukum Pidana. Unsur "dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan" menjadi menonjol dalam ayat ini karena memang cara-cara tersebut sering dipakai oleh hacker dapat melakukan kejahatannya.

Perumusan Hacking sebagai tindak pidana dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Pasal 30 Ayat (3) diatas diancam dengan sanksi pidana yang terdapat dalam ketentuan pidana Pasal 46 Ayat (3) yaitu "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)". Sedangkan dalam pasal 32 Tentang pencurian data terdapat pada Ayat (2) : yang berbunyi sebagai berikut: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik kepada Orang yang tidak berhak".

Tindak pidana yang dimaksud dengan ayat (2) adalah tindak pidana formil atau tindak pidana dengan perumusan formil, yaitu yang dianggap telah sepenuhnya terlaksana, dengan dilakukannya suatu perbuatan yang dilarang oleh undang-undang. Perbuatan yang dilarang oleh undang-undang adalah memindahkan atau mentrasfer informasi dan/atau dokumen elektronik milik orang lain atau milik publik dan tidak perlu dibuktikan akibat dari perbuatan yang dilarang tersebut.

Mengacu pada Pasal 32 ayat (2), maka ancaman sanksi pidana diatur dalam undang-undang, sebagaimana diatur dalam Pasal 48 ayat (2) Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik yaitu: Pasal 48 ayat (2) : "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan penjara paling lama 9 (sembilan) tahun dan/atau dengan paling banyak Rp3.000.000.000,00 (tiga miliar rupiah)". Jadi telah jelas kejahatan hacking ini telah di atur dalam Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transksi Elektronik. Dalam pasal 30 ayat (1), (2), dan (3) tentang ilegal akses dan dalam pasal 32 ayat 2 tentang pencurian data. Dengan adanya aturan tersebut merupakan wujud dari tanggung jawab yang harus diberikan oleh negara, untuk memberikan perlindungan maksimal pada seluruh aktivitas pemanfaatan teknologi informasi dan komunikasi di dalam negara Indonesia agar terlindung dari dari potensi kejahatan dan penyalahgunaan teknologi. Lebih lanjut lagi Undang-Undangi ni mengatur tindak pidana *hacking* sebagai bagian dari *Cyber Crime*, dimana terdapat pengaturan mengenai perumusan tindak pidana *hacking* dan ancaman sanksi pidana bagi para pelaku tindak pidana *hacking*. Sebab dalam perkembangannya tindak pidana *hacking* digunakan oleh para pelaku *cyber crime* sebagai tindakan awal untuk melakukan tindak pidana *cyber crime* yang lain.[15]

Kesimpulan Dan Saran

A. Kesimpulan

1. Dengan perkembangan zaman, kemajuan dari teknologi merupakan hal yang sangat berguna bagi manusia. Namum dalam perkembangannya teknologi

[15] Undang-Undang 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

memiliki kekurangan, seperti kejahatan dunia maya (Cyber Crime) salah satunya peretasan data pribadi.

Macam-macam peraturan perundang–undangan yang ada di Indonesia, yang mengatur mengenai perlindungan data pribadi tidak mampu memberikan perlindungan yang cukup terhadap data pribadi. Perlindungan terhadap data pribadi telah diatur secara khusus pada Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016, namun perlindungan hukum yang sifatnya represif pada peraturan tersebut belum bisa memberikan perlindungan yang cukup karena disana tidak memiliki sanksi yang cukup untuk menghentikan atau mengurangi pelaku pelanggar data pribadi.

Bentuk-bentuk perlindungan hukum terhadap data pribadi konsumen. Perlindungan hukum preventif, perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Perlindunga hukum represif**,** merupakan perlindungan hukum yang dilakukan berdasarkan keputusan yang ditetapkan badan hukum yang bersifat mengikat yang bertujuan untuk menyelesaikan suatu sengketa.

Tanggung jawab perusahaan penyelenggara sistem elektronik jika terjadi peretasan data pribadi terhadap konsumenya. Munculnya hak dan kewajiban antara perusahaan penyelenggara sistem elektronik dengan konsumen ialah saat konsumen menyetujui *term of Service* (ketentuan layanan) yang di berikan oleh perusahaan penyelenggara sistem elektronik. Dengan begitu telah terjadi perikatan yang terjadi antar para pihak.

Penyelesaian sengketa bagi konsumen yang dirugikan dari peretasan data pribadi menurut hukum di indonesia. Penyelesaian sengketa ada dua jalur yang dapat di gunakan oleh konsumen untuk menyelesaikan sengketa data pribadi yaitu litigasi (melalui pengadilan) dengan cara melakukan gugatan perdata kepada pihak penyelenggara sistem elektronik sesuai dengan prosedur yang telah di tetapkan oleh perundang-undangan. Langkah selanjutnya yaitu penyelesaian sengketa diluar pengadilan (non- litigasi) dapat ditempuh melalui BPSK (Badan Penyelesaian Sengketa Konsumen) yang tugas dan wewenangnya anatara lain meliputi pelaksanaan penanganan dan penyelesaian sengketa konsumen, dengan cara melalui mediasi atau arbitrase atau konsiliasi.

2. Sanksi hukum terhadap pelaku kejahatan peretasan data pribadi menggunkan Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transksi Elektronik. Dan dirumuskan dalam Pasal 30 Tentang Ilegal Akses dan dalam Pasal 32 Tentang Pencurian Data. Pada Pasal 30 Tentang Ilegal Akses terdapat 3 ayat yang berbunyi sebagai berikut

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan.

B. Saran

Sebagai konsumen, seharusnya pada zaman sekarang kita harus dapat bertindak untuk lebih teliti dan hati-hati terutama saat berbelanja. Banyaknya berbagai macam informasi yang kita lepaskan saat akan bertransaksi secara online, yang awalnya hal tersebut merupakan hal yang sangat privasi tetapi setelah berada di tangan yang salah hal tersebut bisa saja menjadi sesuatu hal yang tidak bisa lagi disebut sebagai privasi dan buruknya hal tersebut dapat menjadi sangat merugikan bagi konsumen. Oleh karena itu ketelitian dan kehati-hatian

sangatlah penting untuk menjaga privasi data pribadi sebagai konsumen online.

DAFTAR PUSTAKA

Abdurrahman, A. 1986. "*Kamus Ekonomi – Perdagangan*", Gramedia.

Barkatullah A.H. 2017. "*Hukum Transaksi Elektronik*", Nusa Media, Bandung.

Daniel J. Solove, 2008. "*Understanding Privacy*", MA: Harvard University Press, Cambridge.

Febrian, J. 2003. "*Menggunakan Internet, Informatika*", Bandung.

Fuady, M. 2005. "*Pengantar Hukum Bisnis: Menata Bisnis Era Global*", Citra Aditya Bakti, Bandung.

Hadjon P.M.1987. "*Perlindungan Hukum Bagi Rakyat Indonesia*", PT. Bina Ilmu, Surabaya.

Hadjon, P.M. 1987. "*Perlindungan Bagi Rakyat di Indonesia*", PT. Bina Ilmu, Surabaya.

Inness, J.C. 1992 "*Privacy, Intimacy, and Isolation*", Oxford University Press, New York.

Kotler, P. 2000. "*Prinsiples Of Marketing*", Rajawali Pers, Jakarta.

Kristiyanti, C.T.S. 2008. "*Hukum Perlindungan Konsumen*", Sinar Grafik, Jakarta.

Kusnardi M. & Harmaily Ibrahim, 1998. "*Hukum Tata Negara Indonesia*", Sinar Bakti, Jakarta.

Makarin, E. 2010. "*Tanggung Jawab Hukum penyelenggaraan Sistem Elektronik*", Jakarta.

Mamudji, S.S.S. 2003. "*Penelitian Hukum Normatif*", PT Raja Grafindo, Jakarta.

Maskun. 2013. "*Kejahatan Siber Cyber Crime*", Kencana Prenada Media Grup, Jakarta.

Miller, A. R. 1971. "*The Assault on Privacy: Computers, Data Banks, and Dossiers*", Ann Arbor: University of Michigan Press.

Nazution, Az. 1995. "*Konsumen dan Hukum*", Pustaka Sinar Harapan, Jakarta.

Pelealu, A. 2018. "*Perlindungan Hukum Atas Data Pribadi Konsumen Dalam Transaksi E-Commerce*", Yogyakarta: Universitas Atma Jaya Yogyakarta.

Prabowo, M.S. 2010. "*Perlindungan Hukum Jamaah Haji Indonesia*", Rangkang, Yogyakarta.

Prosser, W. L. 1960. "*Privacy: A Legal Analysis*", California Law Review

Rosadi, S.D. 2015.*Cyber Law* "*Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*" Refika Aditama, Bandung.

Sahputra, I. 2010. "*Perlindungan Konsumen Dalam Transaksi Elektronik*", PT. Alumni, Bandung.

Shidarta, 2000. "*Hukum Perlindungan Konsumen Indonesia*", PT. Grasindo, Jakarta.

Shidarta.2004 "*Hukum Perlindungan Konsumen Indonesia*", Edisi Revisi, Grasindo Jakarta.

Soekanto, S. 1984. "*Pengantar Penelitian Hukum*", Ui Press. Jakarta.

Sunarso, S. 2009. "*Hukum Informasi dan Transaksi Elektronik*", Jakarta.

Sunggono, B. 2011. "*Metodelogi Penelitian Hukum*", Raja Grafindo persada, Jakarta.

Syah, M.I. 2018 "*Hukum Bisnis Online Era Digital*", Cv. Campustaka, Jakarta.

Westin, A.F. 1967. "*Privacy and Freedom*", Atheneum, New York.

Zulham, 2013. "*Hukum Perlindungan Konsumen*", Kencana, Jakarta.

Jurnal

E. Bloustein.1964. *Privacy as An Aspect of Human Dignity*: an *Answer to Dean Prosser*, dalam New York University Law Review Vol. 39.

Jerry Kang, 1998, "*Information Privacy in Cyberspace Transaction*", Stanford Law Review Vol. 50 Issue 4, Standford.

Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, "Perlindungan hukum terhadap Keamanan Data Konsumen *Financial Technology* di Indonesia", Jurnal ilmu Hukum, Vol.3 No.2, April, 2019, hal 155

Lia Sautunnida, "Urgensi Undang - Undang Perlindunngan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia", Kanun Jurnal Ilmu Hukum, Vol.20, No.2, Agustus, 2018, hal 374.

Ririn Aswandi, Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data *Protection System* (Idps), Jurnal Legislatif Vol.3 No.2 Juni 2020, hal 175.

Rosalinda Elsina Latumahina, Aspek Hukum Perlindungan Data Pribadi di Dunia Maya, Jurnal Gema Aktualita, Vol. 3 No. 2, Desember 2014, hal 17.

Ruth Gavison, 1980 *Privacy and the Limits of Law*, dalam Yale Law Journal 89: 421-71.

Samuel Warren & Louis Brandeis, 1890. *The Right to Privacy*, dalam Harvard Law Review Vol. IV No. 5, 15 Desember 1890, tersedia di http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Gagasan dua orang pengacara Boston ini sebenarnya berangkat dari ide yang dicetuskan oleh hakim Thomas Cooley, yang menulis *Treatise on the Law of Torts* (1880), yang memperkenalkan pertama kali mengenai istilah 'hak untuk dibiarkan sendiri'.