Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang

Ivan Juan Alfreda, Rika Ratna Permata, Tasya Safiranita Ramli

Fakultas Hukum, Universitas Padjadjaran, Bandung, Indonesia

Email: ivanjuanal@gmail.com; tasyasafiranita@yahoo.com

ABSTRAK

Perkembangan teknologi informasi dan komunikasi yang pesat serta penemuan internet telah mendisrupsi berbagai aktivitas kehidupan manusia yang menyebabkan tingginya urgensi pelindungan informasi dalam platform digital sebagai akibat maraknya tindakan kejahatan siber. Salah satu aspek yang dipengaruhi oleh hal tersebut adalah pelindungan terhadap informasi Rahasia Dagang pada platform digital. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengetahui pelindungan hukum atas informasi Rahasia Dagang pada platform digital serta mengidentifikasi pertanggungjawaban hukum atas kebocoran informasi Rahasia Dagang pada platform digital. Penelitian ini akan menggunakan metode pendekatan yuridis normatif dan yuridis komparatif, yakni dengan menelusuri dan menjelaskan substansi dalam suatu peraturan perundang-undangan yang berlaku dan membandingkan hukum suatu negara dengan negara lainnya. Penelitian ini menunjukkan bahwa, pertama, belum adanya pelindungan informasi Rahasia Dagang elektronik pada platform digital yang secara khusus diatur dalam Undang-Undang Rahasia Dagang, melainkan pengaturan pelindungan informasi Rahasia Dagang elektronik dalam platform digital masih terpecah dalam berbagai peraturan perundang-undangan yang berlaku. Kedua, Undang-Undang Rahasia Dagang belum mencakup pertanggungjawaban hukum atas kebocoran informasi Rahasia Dagang elektronik dalam platform digital sehingga diperlukan adanya suatu pembaharuan hukum untuk menjamin pelindungan Rahasia Dagang di era digital. Diperlukan adanya kerja sama antara pemangku kepentingan dalam platform digital dan pemerintah untuk menjaga keamanan informasi Rahasia Dagang dalam platform digital dari perbuatan melawan hukum yang dilakukan secara elektronik untuk menjaga kepentingan warga negara dan badan hukum Indonesia.

Kata kunci: Rahasia Dagang, Platform Digital, Pelindungan Hukum, Tanggung Jawab.

PENDAHULUAN

Revolusi Industri yang terjadi sepanjang sejarah dimulai dari Revolusi Industri 1.0 hingga Revolusi Industri 3.0 telah menghasilkan banyak kemajuan yang signifikan pada sektor teknologi informasi dan komunikasi yang juga memicu perubahan besar pada sistem ekonomi dan struktur sosial. Perkembangan teknologi informasi dan komunikasi mengubah pola pikir tentang batas wilayah, wujud suatu benda, waktu, nilai-nilai, dan batas perilaku sosial dari yang bersifat manual menjadi bersifat digital (Ekawati, 2018, p. 158). Penemuan internet merupakan titik tolak kemajuan peradaban manusia yang menciptakan ruang interaksi antar manusia dalam dunia maya atau *cyberspace*. Dengan berbagai inovasi dan kecepatan perkembangan teknologi informasi dan komunikasi, kita telah masuk kedalam era Revolusi Industri 4.0 yang ditandai dengan munculnya interaksi tanpa batas (*borderless*) melalui internet dan teknologi yang mendisrupsi berbagai bidang kehidupan manusia (Schwab, 2016, p. 12).

Era disrupsi digital yang timbul akibat kemajuan teknologi informasi dan komunikasi merupakan era dimana masyarakat merelokasi aktivitas yang semula dilakukan dalam dunia nyata ke dunia maya, dengan hadirnya *e-commerce* untuk menggantikan toko fisik, munculnya

taksi online untuk menggantikan taksi konvensional serta aplikasi *virtual meeting* yang memungkinkan pertemuan dilakukan secara jarak jauh untuk memberikan kemudahan bagi manusia tanpa mengenal batas ruang dan waktu (Ayu Astuti, 2020, p. 2). Hal tersebut juga dibarengi dengan ditemukannya *artificial intelligence*, *drone*, aplikasi sosial media yang kemudian menimbulkan perubahan mendasar pada pola hidup manusia dan akan terus membawa perubahan untuk memenuhi kebutuhan manusia di era disrupsi digital.

Penemuan teknologi digital memicu terjadinya perpindahan informasi dari fisik ke digital, sehingga dengan kemajuan teknologi digital terdapat tantangan yaitu keamanan penyimpanan informasi berupa data dalam dunia maya atau *cyberspace*. Keberadaan suatu informasi memiliki peranan sebagai '*power*' yang berarti informasi berfungsi sebagai kekuatan dan kekuasaan yang dapat menentukan nasib peradaban manusia (Rumulus & Hartadi, 2020, p. 286). Perpindahan informasi yang berbentuk fisik menjadi bentuk digital memunculkan resiko baru dalam penyimpanan data informasi tersebut yaitu adanya potensi kebocoran informasi dalam platform digital yang dapat menyebabkan kerugian kepada pihak yang memiliki informasi tersebut. Kebocoran informasi merupakan suatu keadaan dimana suatu informasi rahasia, secara sengaja maupun tidak sengaja diakses oleh pihak yang tidak sah. Kebocoran tersebut dapat disebabkan oleh peretasan dari pihak eksternal (*malicious outsider*) dan peretasan dari pihak internal (*malicious insider*), kebocoran data secara tidak sengaja sebagai akibat dari sistem informasi yang tidak aman (*accidental loss*), *ransomware*, serta sumber-sumber kebocoran lainnya yang menyebabkan kerusakan data (Aswandi et al., 2020, p. 174).

Keberadaan informasi rahasia yang berupa data tersebut dalam platform digital memiliki keterkaitan erat dengan Rahasia Dagang (*trade secret*) sebagai bagian dari Kekayaan Intelektual. Rahasia Dagang merupakan salah satu rezim Kekayaan Intelektual yang melindungi informasi rahasia dimana pelindungannya telah diatur dalam Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang sebagai implikasi dari ratifikasi persetujuan pembentukan organisasi perdagangan dunia melalui Undang-Undang Nomor 7 Tahun 1994 yang menganut prinsip *full compliance* dalam Pasal 16 ayat (5) dan persetujuan tersebut juga mencakup perjanjian *Trade Related Aspects of Intellectual Property Rights including Trade in Counterfeit Goods* (TRIPs). Namun yang menjadi pertanyaan adalah apakah perlindungan Rahasia Dagang yang berbentuk elektronik dalam platform digital telah tercakup dalam Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang. Dalam dunia bisnis yang terus berkembang dewasa ini, perlindungan Rahasia Dagang merupakan sesuatu yang mutlak diperlukan, karena ketidakpastian rahasia dagang dapat memunculkan praktik persaingan tidak sehat dan pada akhirnya mengacaukan seluruh dunia usaha (Gerungan, 2016, p. 70).

Selain dari dampak positif yang dihasilkan bersamaan dengan kemajuan teknologi informasi dan komunikasi, terdapat dampak negatif dari perkembangan teknologi komunikasi dan informasi tersebut yakni munculnya kejahatan yang berkaitan atau menggunakan media internet yang kemudian dikenal dengan *cybercrime*. *Cybercrime* adalah bentuk kejahatan baru yang berbeda dengan kejahatan konvensional. Secara ringkas *cybercrime* dapat didefinisikan sebagai setiap tindakan seseorang, kelompok orang atau badan hukum yang menggunakan komputer sebagai alat untuk melakukan kejahatan dan komputer sebagai target (Fitriani & Pakpahan, 2020, p. 22), sehingga tidak seperti kejahatan konvensional, kejahatan ini dapat dilakukan tanpa batas wilayah bahkan negara. Salah satu bentuk praktik *cybercrime* yang timbul akibat kemajuan teknologi informasi dan komunikasi adalah pada kasus kebocoran data nasabah Tokopedia, dimana pada tanggal 2 Mei 2020 Tokopedia mengalami kebocoran data nasabahnya yang diunggah oleh akun *whysodank* dalam situs *darkweb* *raidforums.com* dan kemudian 91 (Sembilan puluh satu) juta data nasabah Tokopedia tersebut dijual seharga US \$5000 di situs *darkweb* *Empire Market* oleh akun *ShinyHunters* (Wicaksono, 2020). Dimana

dalam kasus tersebut, data nasabah Tokopedia dicuri oleh seorang peretas dan menjual data tersebut pada situs Empire Market.

Kasus diatas berkaitan dengan beberapa informasi yang dilindungi dalam rezim Rahasia Dagang yaitu sebagai berikut (Santiago, 2017, pp. 69, 72):

1. Daftar Pelanggan;
2. Formula Senyawa Kimia;
3. Proses Manufaktur;
4. Metode Pemasaran;
5. Sebuah cara untuk menjaga atau memperlakukan bahan tertentu;
6. Resep Makanan atau ramuan yang digunakan untuk menghasilkan sebuah produk tertentu;
7. Sebuah cara untuk menggunakan mesin atau alat tertentu.

Berdasarkan hal tersebut, maka kebocoran informasi data nasabah Tokopedia yang dilakukan oleh peretas dari luar (*malicious outsider*) tersebut merupakan informasi yang dilindungi dalam rezim Rahasia Dagang dimana pada masa sekarang informasi nasabah (daftar nasabah dan semua data mengenai nasabah) bersifat fundamental bagi setiap bisnis karena memiliki nilai komersial sebagai bentuk perlindungan terhadap *customer base* bisnis tersebut dan sebagai dasar untuk perencanaan marketing, kebijakan bisnis, dan lain sebagainya. (Malgieri, 2016, p. 102) Sehingga dalam penelitian ini penulis akan menganalisis mengenai bagaimana perlindungan hukum atas kebocoran informasi Rahasia Dagang pada penyedia platform digital berdasarkan hukum positif di Indonesia dan bagaimana pertanggungjawaban hukum atas kebocoran informasi Rahasia Dagang pada penyedia platform digital berdasarkan hukum positif di Indonesia. Perlu digaris bawahi bahwa terdapat keterkaitan erat antara informasi Rahasia Dagang dengan informasi Data Pribadi, dimana dalam kasus tersebut data nasabah Tokopedia yang mengalami kebocoran juga mencakup Data Pribadi dari nasabah Tokopedia.

METODE PENELITIAN

Metode Penelitian yang akan digunakan dalam penelitian ini adalah metode penelitian normatif (*normative legal research*) dengan mengumpulkan dan menganalisis data sekunder. Sehingga pendekatan yang akan digunakan dalam penelitian ini adalah yuridis normatif (*statute approach*) dan yuridis komparatif (*comparative approach*) yang bersifat deskriptif analitis. Dimana dalam penelitian ini penulis akan menelusuri dan menganalisis ketentuan-ketentuan hukum yang berkaitan dengan permasalahan yang diteliti yakni Rahasia Dagang (Soekanto & Mamudji, 2011, p. 23). Kemudian, penulis juga akan melakukan perbandingan pengaturan Rahasia Dagang di Indonesia dengan pengaturan dan putusan pengadilan berkaitan dengan Rahasia Dagang di Amerika Serikat (Zaini, 2011, p. 129).

Kemudian dalam penelitian ini penulis akan menggunakan data sekunder yang berupa bahan hukum primer yakni Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang (UU Rahasia Dagang), *Uniform Trade Secret Act of 1985*, *Economic Espionage Act of 1996* jo. *Defend Trade Secret Act of 2016*, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik (PM PDPSE), Surat Edaran Menteri Komunikasi dan Informasi Nomor 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia Platform dan Pedagang (*Merchant*) Perdagangan melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk

User Generated Content (SE Safe Harbour). Lalu bahan hukum sekunder yang digunakan berupa literatur hukum serta KBBI dan sumber bacaan lain sebagai bahan hukum tersier. Lalu, teknik pengumpulan data yang akan peneliti gunakan dalam penelitian ini adalah pengumpulan data dengan cara studi dokumen secara daring dengan teknik analisis data dengan mengkaji dan menganalisis norma hukum dalam suatu peraturan perundang-undangan dan dikaitkan dengan kasus yang berkaitan dengan Rahasia Dagang dan untuk menjawab permasalahan dalam penelitian ini.

HASIL DAN PEMBAHASAN

Perbandingan Pengaturan Rahasia Dagang di Indonesia dan Amerika Serikat

Salah satu masalah yang dihadapi Indonesia sebagai negara berkembang adalah terkait dengan perlindungan hukum dan kepastian hukum. Pembangunan hukum di Indonesia harus segera dioptimalkan secara realistis dan konsisten dengan menjalankan ketentuan dalam peraturan perundang-undangan yang mendukung iklim hukum untuk mencapai kepastian, ketertiban, dan supremasi hukum (Ramli, 2000, p. 9). Salah satu pengoptimalan hukum yang harus dilakukan di Indonesia adalah terkait dengan perlindungan hukum terhadap Kekayaan Intelektual yang salah satunya mencakup Rahasia Dagang yang melindungi informasi teknologi atau bisnis yang memiliki nilai ekonomi. Pelindungan terhadap informasi rahasia tersebut dilakukan untuk melindungi hak pemilik informasi rahasia agar informasi tersebut tidak diketahui orang lain (Salmon, 2019, p. 89).

Pengaturan hukum terhadap Rahasia Dagang di Indonesia telah tercantum dalam Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang (untuk selanjutnya disebut dengan UU Rahasia Dagang). Sementara itu, pengaturan hukum Rahasia Dagang di Amerika Serikat tercantum dalam *Uniform Trade Secret Act of 1985* (untuk selanjutnya disebut sebagai UTSA) yang mengatur aspek perdata dalam Rahasia Dagang. (Dole Jr, 2018, p. 364) Sedangkan aspek pidana Rahasia Dagang Amerika Serikat diatur dalam *Economic Espionage Act of 1996* (untuk selanjutnya disebut EEA) yang merupakan undang-undang federal pertama yang mengatur mengenai kriminalisasi pencurian Rahasia Dagang dan telah diamandemen dengan *Defend Trade Secret Act of 2016* (untuk selanjutnya disebut DTSA) yang dibentuk oleh pemerintah federal pada 11 Mei 2016. (Dole Jr, 2018, p. 380)

Berkaitan dengan definisi Rahasia Dagang, dalam pasal 1 ayat (1) UU Rahasia Dagang menjelaskan bahwa Rahasia Dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang. Sehingga berdasarkan definisi tersebut dapat diidentifikasi unsur-unsur dalam Rahasia Dagang yakni informasi yang tidak diketahui oleh umum, informasi tersebut berada di bidang teknologi dan/atau bisnis, informasi tersebut memiliki nilai ekonomi dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang. Sementara itu, dalam pengaturan Rahasia Dagang di Amerika Serikat, UTSA mendefinisikan Rahasia Dagang sebagai berikut:

“Trade secret means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

Kemudian, DTSA memberikan definisi Rahasia Dagang yang hampir sama dengan UTSA namun memiliki muatan yang lebih kompleks dimana Rahasia Dagang didefinisikan sebagai berikut:

“The term ‘trade secret’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if - (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.”

Sehingga berdasarkan definisi Rahasia Dagang dalam UTSA dan DTSA tersebut maka dapat diidentifikasi bahwa kedua aturan tersebut tidak memberikan limitasi terhadap informasi rahasia yang dapat dilindungi dalam Rahasia Dagang selama informasi tersebut dijaga kerahasiaannya dengan tindakan wajar oleh pemilik Rahasia Dagang dan memiliki nilai ekonomi, baik secara aktual maupun potensial, dari tidak diketahuinya informasi tersebut dan tidak dapat dipastikan melalui cara yang layak oleh, orang lain yang dapat memperoleh nilai ekonomis dari pengungkapan atau penggunaan informasi tersebut. Namun DTSA memberikan definisi yang lebih kompleks dibandingkan definisi Rahasia Dagang dalam UTSA dimana DTSA memberikan bentuk-bentuk Rahasia Dagang yang lebih beragam serta memberikan penjelasan mengenai cara penyimpanan dari informasi Rahasia Dagang tersebut yaitu informasi rahasia yang berbentuk berwujud maupun tidak berwujud dan disimpan, dikompilasi, atau dimemorialisasi dalam bentuk fisik, elektronik, grafik, foto, atau tulisan. Perbedaan yang dapat dilihat dalam definisi Rahasia Dagang menurut UU Rahasia Dagang dan UTSA serta DTSA adalah bahwa definisi Rahasia Dagang di Indonesia tidak menjelaskan mengenai bentuk informasi yang dapat dilindungi dalam Rahasia Dagang dimana bentuk-bentuk informasi tersebut tercantum dalam Pasal 2 UU Rahasia Dagang yang berisi mengenai ruang lingkup perlindungan Rahasia Dagang.

Berkaitan dengan pelanggaran terhadap Rahasia Dagang, UU Rahasia Dagang mengatur hal tersebut dalam pasal 13 dimana pelanggaran Rahasia Dagang terjadi apabila seseorang dengan sengaja mengungkapkan Rahasia Dagang, mengingkari kesepakatan atau mengingkari kewajiban tertulis atau tidak tertulis untuk menjaga Rahasia Dagang yang bersangkutan dan pasal 14 yang menyatakan bahwa pelanggaran Rahasia Dagang terjadi apabila pihak lain memperoleh atau menguasai Rahasia Dagang milik orang lain dengan cara yang bertentangan dengan ketentuan peraturan perundang-undangan yang berlaku. Hal tersebut berbeda dengan ketentuan pelanggaran Rahasia Dagang dalam DTSA dimana DTSA memberikan definisi mengenai *misappropriation* atau penyalahgunaan yang diatur dalam *section 1839 paragraph (5)* yaitu:

“The term ‘misappropriation’ means— (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent by a person who— (i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was— (I) derived from or through a person who had used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had

reason to know that— “(I) the trade secret was a trade secret; and “(II) knowledge of the trade secret had been acquired by accident or mistake.”

Dapat dilihat berdasarkan ketentuan diatas bahwa DTSA memberikan penjelasan yang luas terhadap penyalahgunaan informasi Rahasia Dagang dimana penyalahgunaan tersebut bukan hanya berlaku terhadap pihak yang mendapatkan atau menguasai informasi Rahasia Dagang dengan cara yang tidak sah atau melawan hukum namun penyalahgunaan juga dapat dilakukan oleh pihak yang mengungkapkan atau menggunakan informasi Rahasia Dagang yang didapatkan dengan cara yang tidak sah oleh orang lain. Kemudian DTSA juga memberikan definisi mengenai *improper means* atau cara yang tidak layak yang diatur dalam *section 1839 paragraph (6)* yaitu pencurian, penyuapan, misrepresentasi, pelanggaran atau bujukan pelanggaran kewajiban untuk menjaga kerahasiaan, atau spionase melalui elektronik atau cara lain. Cara lain sebagaimana dimaksud tersebut merupakan sebuah metode yang digunakan legislator DTSA untuk tidak memberikan limitasi terhadap tindakan yang dianggap tidak layak sebagaimana definisi *improper means* diatas, sehingga tindakan apapun yang tidak disebutkan dalam definisi tersebut namun dianggap sebagai tindakan yang tidak layak dapat masuk kedalam definisi *improper means* dalam DTSA.

Pelindungan Hukum atas Kebocoran Informasi Rahasia Dagang pada penyedia platform digital di Indonesia

Pelindungan hukum dalam bahasa Belanda disebut dengan *rechtsbecherming* sedangkan dalam bahasa Inggris dikenal dengan *legal protection*. Pelindungan yang diberikan oleh hukum memberikan hak dan kewajiban kepada subjek hukum dalam kehidupan bermasyarakat. Perlindungan hukum merupakan salah satu upaya menata berbagai kepentingan dalam masyarakat, sehingga mencegah adanya benturan kepentingan dan dapat menikmati semua hak yang diberikan hukum (Budi Asri, 2020, p. 137). Pelindungan hukum pada dasarnya dapat dibagi menjadi 2 (dua) yaitu pelindungan hukum preventif dan represif. Pelindungan hukum preventif merupakan pelindungan yang diberikan oleh pemerintah yang bertujuan untuk mencegah timbulnya permasalahan di masa mendatang, sedangkan pelindungan hukum represif merupakan pelindungan hukum yang ditujukan untuk menyelesaikan sengketa dan diberikan kepada masyarakat yang dirugikan sehingga dapat mencari keadilan dalam proses penegakan hukum melalui lembaga peradilan (Sakti & Budhisulistyawati, 2020, p. 148).

Kemajuan teknologi informasi dan komunikasi telah menyebabkan munculnya disrupsi digital yang menyebabkan terjadinya perubahan mendasar dalam masyarakat dengan mengganggu dan menyapu pola-pola lama untuk menciptakan pola baru (Ramli, 2018, p. 88). Beberapa perubahan yang dapat dilihat sebagai akibat dari perkembangan teknologi informasi adalah perilaku manusia dalam mewujudkan hasil Kekayaan Intelektualnya yang dapat dilihat secara digital melalui platform digital dengan mudah (Aulia, 2020, p. 1689).

Rahasia Dagang sebagai salah satu bagian dari Kekayaan Intelektual merupakan suatu informasi yang dimiliki oleh individu atau badan hukum yang bersifat rahasia atau tidak diketahui oleh umum di bidang teknologi dan/atau bisnis. Informasi rahasia tersebut merupakan suatu informasi yang berharga karena sifat informasi tersebut dapat mendatangkan keuntungan bagi pemiliknya dalam menjalankan usaha dan perlunya upaya untuk menjaga kerahasiaan informasi tersebut yang dilakukan oleh pemiliknya (Atmadjaja, 2016, p. 244). Informasi rahasia yang dimiliki oleh suatu badan hukum merupakan informasi berharga yang tidak boleh diketahui oleh umum terutama kompetitor khususnya informasi rahasia yang dimiliki badan hukum di bidang bisnis. Secara garis besar informasi dapat dibagi menjadi 2 (dua) jenis, yaitu: (Muhammad, 2001, p. 245)

1. Informasi Terbuka (*diclosed information*)

Merupakan suatu informasi yang dapat diketahui oleh umum sebagai bagian dari masyarakat karena informasi tersebut bermanfaat. Informasi terbuka dapat dipublikasikan secara luas agar dapat diketahui oleh masyarakat.

2. Informasi Rahasia (*undisclosed information*)

Merupakan suatu informasi yang tidak boleh diketahui oleh umum, kecuali oleh pihak yang memiliki wewenang untuk mengetahui, melaksanakan, dan menyimpan informasi rahasia tersebut.

Berkaitan dengan informasi Rahasia Dagang pada penyedia platform digital sebagaimana dalam kasus Tokopedia dimana pada tanggal 2 Mei 2020, 91 (sembilan puluh satu) juta data nasabah Tokopedia telah diakses secara melawan hukum oleh *hacker* dengan nama akun whysodank dan kemudian informasi tersebut dijual dalam situs *darkweb* Empire Market oleh akun Shiny Hunters seharga US \$5000 dimana informasi rahasia yang mengalami kebocoran tersebut mencakup nama lengkap, username, jenis kelamin, alamat, nomor telepon, *e-mail*, dan password yang terenkripsi (Waqas, 2020).

Informasi data nasabah Tokopedia dalam kasus tersebut merupakan salah satu informasi daftar pelanggan yang dilindungi dalam rezim Rahasia Dagang, dimana informasi tersebut memenuhi unsur-unsur Rahasia Dagang berdasarkan pasal 1 ayat (1) UU Rahasia Dagang. Berdasarkan hal tersebut maka perlu dianalisis mengenai unsur-unsur Rahasia Dagang dengan informasi data nasabah Tokopedia tersebut sebagaimana berikut (Faramukti, 2019, p. 43):

1. Adanya pengertian mengenai informasi;

Definisi informasi Rahasia Dagang dalam UU Rahasia Dagang tidak dijelaskan secara terperinci. Namun dalam pasal 2 UU Rahasia Dagang dijelaskan mengenai ruang lingkup perlindungan Rahasia Dagang yang meliputi metode produksi, metode pengolahan, metode penjualan, dan informasi lain di bidang teknologi dan/atau bisnis. *Oxford English Dictionary* menjelaskan bahwa informasi adalah sesuatu yang dapat diberitahukan atau dijelaskan (*that of which is apprised or told*), keterangan (*intelligence*), dan berita (*news*) (Zorkoczy, 1990, p. 9). Dalam kasus kebocoran data nasabah Tokopedia, data tersebut merupakan informasi mengenai pihak-pihak yang pernah melakukan transaksi pada platform Tokopedia dimana informasi tersebut mencakup nama, alamat, nomor telepon, *e-mail*, dan lain sebagainya. Sehingga dapat disimpulkan bahwa data nasabah tersebut merupakan keterangan mengenai nasabah Tokopedia sebagaimana definisi informasi diatas.

2. Informasi tersebut merupakan informasi rahasia atau tidak diketahui oleh umum;

Dalam UU Rahasia Dagang tidak dijelaskan pula mengenai pengertian informasi yang tidak diketahui oleh umum. Namun, apabila dilihat pada pasal 3 ayat (2) UU Rahasia Dagang, dijelaskan mengenai informasi rahasia, dimana dalam pasal tersebut disebutkan bahwa informasi dianggap bersifat rahasia apabila informasi tersebut hanya diketahui oleh pihak tertentu atau tidak diketahui secara umum. Menurut Abdulkadir Muhammad informasi rahasia adalah suatu informasi yang tidak boleh diketahui oleh umum, kecuali oleh pihak yang memiliki wewenang untuk mengetahui, melaksanakan, dan menyimpan informasi rahasia tersebut. Informasi data nasabah Tokopedia merupakan informasi yang hanya diketahui oleh pihak Tokopedia dan nasabahnya yang memberikan informasi tersebut kepada pihak Tokopedia karena data tersebut mencakup Data Pribadi nasabah Tokopedia sehingga informasi tersebut bersifat rahasia karena hanya diketahui oleh Tokopedia dan nasabahnya atau dengan kata lain tidak diketahui oleh umum kecuali oleh pihak Tokopedia yang memiliki wewenang atas informasi tersebut dan nasabah Tokopedia yang merupakan subjek data tersebut.

3. Informasi tersebut merupakan informasi dalam bidang teknologi dan/atau bisnis;

Berkaitan dengan unsur ini, UU Rahasia Dagang tidak memberikan penjelasan mengenai bidang teknologi dan bisnis yang dimaksud dalam UU Rahasia Dagang tersebut. Dalam kasus ini, Tokopedia merupakan salah satu perusahaan *start-up* yang bergerak di bidang *marketplace* sebagai penyedia platform digital untuk penyelenggaraan *e-commerce* atau kegiatan perdagangan secara elektronik. Informasi di bidang bisnis dapat berupa informasi yang berkaitan dengan penjualan dan pemasaran suatu produk, informasi yang berkaitan dengan para pelanggan dan supplier, perencanaan bisnis atau penelitian dan strategi pasar (Lie, 2016, p. 3). Sehingga berdasarkan hal tersebut informasi data nasabah Tokopedia merupakan informasi yang berkaitan dengan nasabah Tokopedia yang pernah melakukan transaksi perdagangan di platform *marketplace* Tokopedia dimana data nasabah tersebut merupakan informasi di bidang bisnis yang berpengaruh terhadap kegiatan bisnis Tokopedia.

4. Informasi tersebut harus memiliki nilai ekonomi;

Pasal 3 ayat (3) UU Rahasia Dagang menjelaskan bahwa suatu informasi yang dapat dilindungi oleh Rahasia Dagang haruslah informasi yang memiliki nilai ekonomi. Suatu informasi dianggap memiliki nilai ekonomi apabila kerahasiaan informasi tersebut digunakan untuk menjalankan kegiatan atau usaha yang bersifat komersial. Dimana berdasarkan KBBI, komersial merupakan sesuatu yang berhubungan dengan niaga atau perdagangan (Badan Pengembangan dan Pembinaan Bahasa Kementerian Pendidikan dan Kebudayaan Republik Indonesia, n.d.). Dalam hal ini Tokopedia merupakan penyelenggara sistem elektronik di bidang *marketplace* yang menyediakan platform untuk melakukan transaksi *e-commerce*. Sehingga, informasi data nasabah Tokopedia merupakan informasi yang memiliki nilai ekonomi dikarenakan informasi tersebut dapat digunakan oleh Tokopedia untuk melakukan penawaran layanan *marketplace* seperti rekomendasi produk-produk dalam platform Tokopedia sehingga akan memberikan keuntungan bagi pihak Tokopedia.

5. Informasi tersebut dijaga kerahasiaannya oleh pemiliknya.

Dalam pasal 3 ayat (4) UU Rahasia Dagang dijelaskan bahwa informasi dianggap dijaga kerahasiaannya apabila pemilik atau para pihak yang menguasainya telah melakukan langkah-langkah yang layak dan patut. Langkah-langkah yang layak dan patut tersebut merupakan semua langkah yang memuat ukuran kewajaran, kelayakan, dan kepatutan yang harus dilakukan. Informasi data nasabah Tokopedia merupakan informasi yang juga mencakup Data Pribadi nasabahnya, sehingga Tokopedia sebagai pengelola data memiliki kewajiban untuk menjaga kerahasiaan informasi tersebut dari pengungkapan yang dilakukan tanpa hak atau melawan hukum. Sehingga Tokopedia terikat kepada ketentuan Pelindungan Data Pribadi untuk menjaga kerahasiaan data tersebut dari pihak yang tidak memiliki wewenang atas data tersebut.

Perlu digarisbawahi bahwa terdapat keterkaitan yang erat antara objek perlindungan dalam Rahasia Dagang dan Data Pribadi, dimana Data Pribadi nasabah Tokopedia dapat menjadi objek perlindungan dalam Rahasia Dagang dikarenakan informasi tersebut juga memenuhi unsur-unsur Rahasia Dagang sehingga dapat diperlakukan seperti Kekayaan Intelektual dengan catatan bahwa Tokopedia sebagai pengguna Data Pribadi nasabahnya juga harus memperhatikan ketentuan-ketentuan mengenai Pelindungan Data Pribadi sebelum menggunakan data tersebut secara komersial sebagai Rahasia Dagang Tokopedia. Untuk memperkuat argumentasi bahwa daftar pelanggan atau nasabah dapat masuk kedalam perlindungan Rahasia Dagang, maka dapat dilihat berdasarkan pertimbangan hakim Amerika Serikat dalam kasus *Chartwell Staffing Servs. Inc. v. Atl. Sols. Grp. Inc.*, yang memberikan

pelindungan Rahasia Dagang pada informasi daftar pelanggan atau nasabah dengan alasan sebagai berikut:

“allows a competitor to direct its sales efforts to reach those potential customers that are already doing business with the trade secret holder.”

Berdasarkan pertimbangan hakim tersebut maka daftar pelanggan yang dapat mencakup informasi Data Pribadi dapat dilindungi oleh rezim Rahasia Dagang dan diperlakukan sebagai Kekayaan Intelektual karena informasi tersebut dapat digunakan oleh kompetitor untuk melakukan penawaran penjualan secara langsung terhadap pelanggan potensial yang telah melakukan bisnis dengan pemilik Rahasia Dagang (*Chartwell Staffing Servs. Inc. v. Atl. Sols. Grp. Inc.*, 2019, pp. 5–8)

Berdasarkan pemaparan diatas dapat dilihat bahwa data nasabah Tokopedia merupakan informasi yang dilindungi dalam rezim Rahasia Dagang. Namun dapat dilihat dalam perbandingan pengaturan Rahasia Dagang antara Indonesia dan Amerika Serikat, UU Rahasia Dagang belum mencakup pelindungan informasi Rahasia Dagang yang berbentuk elektronik secara khusus sebagaimana pelindungan Rahasia Dagang dalam UTSA dan DTSA. Dimana pengaturan mengenai pelindungan informasi Rahasia Dagang yang berbentuk elektronik dalam platform digital di Indonesia terpecah dalam peraturan perundang-undangan lainnya seperti UU ITE. Kemudian pelindungan terhadap informasi rahasia yang berbentuk data pribadi tercantum dalam PP PSTE, PP PMSE, PM PDPSE. Rahasia Dagang sebagai bagian dari rezim Kekayaan Intelektual yang berbentuk elektronik dilindungi oleh UU ITE sebagaimana tercantum dalam pasal 25 UU ITE yang menyatakan bahwa:

“Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.”

Secara lebih spesifik berkaitan dengan pelindungan informasi rahasia yang berbentuk elektronik diatur dalam pasal 32 ayat (3) UU ITE yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Maka berdasarkan ketentuan pasal 14 UU Rahasia Dagang, peretas tersebut menguasai informasi Rahasia Dagang dengan cara yang bertentangan dengan ketentuan peraturan perundang-undangan yang berlaku dalam hal ini bertentangan dengan UU ITE, sehingga peretas tersebut dapat dikenakan sanksi pidana berdasarkan pasal 17 UU Rahasia Dagang.

Apabila dilihat dari pemaparan beberapa pasal diatas maka dapat disimpulkan bahwa informasi Rahasia Dagang yang berbentuk elektronik dilindungi oleh UU ITE sebagaimana Rahasia Dagang dilindungi oleh UU Rahasia Dagang sehingga apabila terdapat perbuatan pelanggaran Rahasia Dagang yang dilakukan secara elektronik sebagaimana perbuatan yang dilakukan peretas yang melakukan penerobosan terhadap sistem pengamanan Tokopedia, peretas tersebut dapat dimintakan pertanggungjawaban atas perbuatannya karena bertentangan dengan aturan dalam UU ITE sehingga perbuatan peretas tersebut memenuhi muatan pasal 14 UU Rahasia Dagang mengenai pelanggaran Rahasia Dagang dan peretas tersebut dapat dimintakan pertanggungjawaban hukum berdasarkan UU Rahasia Dagang.

Sehingga dapat ditarik kesimpulan bahwa pelindungan informasi Rahasia Dagang yang berbentuk elektronik seperti data nasabah Tokopedia dalam kasus Tokopedia belum tercakup dalam UU Rahasia Dagang secara khusus seperti dalam pengaturan Rahasia Dagang pada

negara Amerika melalui UTSA dan DTSA, namun pengaturan atas informasi Rahasia Dagang yang berbentuk elektronik dalam platform digital masih terpengaruh dalam peraturan perundang-undangan yang berbeda seperti UU ITE. Kekayaan Intelektual memberikan perlindungan atas informasi atau konsep dalam wujud nyata sehingga tidak ada kewajiban bagi suatu informasi rahasia untuk dituangkan dalam bentuk tulisan, maka dari itu produk Kekayaan Intelektual yang berupa Rahasia Dagang memiliki perbedaan dengan rezim Kekayaan Intelektual lainnya (Safiranita et al., 2020, p. 8), sehingga dibutuhkan pembaharuan hukum UU Rahasia Dagang dalam rangka menjamin kepastian hukum untuk memberikan perlindungan terhadap informasi Rahasia Dagang yang berbentuk elektronik pada penyedia platform digital yang dimiliki oleh individu maupun badan hukum Indonesia dari adanya tindakan persaingan curang dan/atau *cybercrime* yang berpotensi dilakukan dengan kecepatan perkembangan teknologi informasi dan komunikasi serta memajukan industri yang dapat bersaing dalam ruang lingkup perdagangan nasional maupun internasional sebagaimana landasan yuridis dibentuknya UU Rahasia Dagang. Yakni sebagai suatu upaya untuk memajukan industri yang mampu bersaing dalam lingkup perdagangan nasional dan internasional sehingga diperlukan adanya jaminan perlindungan hukum terhadap Rahasia Dagang, terutama dari tindakan persaingan curang (*unfair competition*).

Pertanggungjawaban Hukum atas Kebocoran Informasi Rahasia Dagang pada Penyedia Platform Digital di Indonesia

Menurut KBBI, tanggung jawab merupakan keadaan wajib menanggung segala sesuatunya (jika terjadi sesuatu dapat dituntut, dipersalahkan, diperkarakan dan sebagainya) atau fungsi menerima beban, sebagai akibat sikap pihak sendiri atau pihak lain. Tanggung jawab dalam hukum dapat dibagi menjadi 3 (tiga), yaitu *accountability*, *responsibility*, dan *liability*. Konsep tanggung jawab hukum memiliki keterkaitan yang erat dengan hak dan kewajiban yaitu bahwa hak pada suatu individu berhubungan dengan kewajiban individu lain. Seseorang juga dianggap bertanggungjawab secara hukum apabila perbuatannya bertentangan dengan peraturan yang berlaku (Sitepu, 2020, p. 121). Hans Kelsen dalam teori tanggung jawab hukum menyatakan bahwa seseorang bertanggungjawab secara hukum apabila ia tidak melaksanakan kewajiban sebagai bentuk perintah dari aturan hukum atau dengan kata lain orang tersebut bertanggungjawab atas pelanggaran yang dilakukannya (Dyani, 2017, p. 166).

Kekayaan Intelektual merupakan kekayaan yang tidak berwujud (*intangible*) sebagai hasil dari pola pikir atau kreativitas manusia yang menghasilkan karya intelektual dan memiliki manfaat ekonomi (Darwance et al., 2020, p. 194). Rahasia Dagang sebagai salah satu bagian dari Kekayaan Intelektual merupakan suatu informasi yang dimiliki oleh individu atau badan hukum yang bersifat rahasia atau tidak diketahui oleh umum di bidang teknologi dan/atau bisnis. Informasi rahasia tersebut merupakan suatu informasi yang berharga karena sifat informasi tersebut dapat mendatangkan keuntungan bagi pemiliknya dalam menjalankan usaha dan perlunya upaya untuk menjaga kerahasiaan informasi tersebut yang dilakukan oleh pemiliknya (Atmadjaja, 2016, p. 244).

Ruang lingkup perlindungan Rahasia Dagang sangatlah luas yang mencakup hampir semua jenis informasi rahasia yang memiliki nilai ekonomi dan dijaga dengan tindakan wajar untuk melindungi kerahasiaan informasi tersebut (Linton, 2016, p. 2). Beberapa bentuk informasi yang dilindungi dalam Rahasia Dagang dapat berupa informasi bisnis yang dirahasiakan yaitu daftar pelanggan, daftar harga, atau strategi marketing; suatu ide atau konsep seperti informasi tentang metode manufaktur atau proses untuk mencapai hasil tertentu; dan informasi teknis, seperti cetakan biru (*blueprints*), algoritme, dan rumus kimia (Lippoldt & Schultz, 2014, pp. 8, 12–13). Hal tersebut berkaitan dengan informasi Rahasia Dagang yaitu daftar pelanggan yang mana informasi tersebut sangat beririsan dengan Pelindungan Data Pribadi dikarenakan daftar pelanggan dapat berupa informasi yang mencakup Data Pribadi dan

kedua hal tersebut merupakan informasi yang bersifat rahasia. Informasi daftar pelanggan dapat menjadi aset yang krusial untuk menjaga hubungan dengan pelanggan atau nasabah dan melakukan penawaran hubungan bisnis prospektif (Fish & Richardson, 2019).

Dalam kaitannya dengan kebocoran informasi Rahasia Dagang dalam platform digital sebagaimana kasus Tokopedia, data nasabah Tokopedia tersebut merupakan informasi yang dilindungi dalam Rahasia Dagang dikarenakan informasi tersebut bersifat rahasia yang dijaga kerahasiaannya oleh Tokopedia dan dapat memberikan keuntungan ekonomi bagi Tokopedia. Di sisi lain, data nasabah tersebut juga mencakup informasi yang dilindungi dalam Pelindungan Data Pribadi sebagai informasi pribadi yang dimiliki nasabah Tokopedia. Sehingga dalam pembahasan ini dapat diidentifikasi adanya pertanggungjawaban peretas yang melakukan penetrasi terhadap sistem keamanan Tokopedia serta melakukan pencurian terhadap informasi Rahasia Dagang Tokopedia dan pertanggungjawaban Tokopedia sebagai penyelenggara sistem elektronik (penyedia platform digital) kepada nasabah yang informasi pribadinya dicuri oleh peretas tersebut.

Berkaitan dengan pertanggungjawaban peretas atas informasi Rahasia Dagang Tokopedia, pasal 13 dan 14 UU Rahasia Dagang mencantumkan mengenai pelanggaran Rahasia Dagang dimana UU Rahasia Dagang melarang seseorang yang dengan sengaja mengungkapkan Rahasia Dagang, mengingkari kesepakatan, atau mengingkari kewajiban tertulis atau tidak tertulis untuk menjaga Rahasia Dagang yang bersangkutan dan melarang seseorang memperoleh atau menguasai Rahasia Dagang dengan cara yang bertentangan dengan peraturan perundang-undangan yang berlaku. Subjek hukum yang melakukan pelanggaran Rahasia Dagang dapat dimintakan pertanggungjawaban pidana sebagaimana pasal 17 UU Rahasia Dagang yang menyatakan bahwa pihak yang dengan sengaja dan tanpa hak menggunakan Rahasia Dagang milik orang lain atau melakukan perbuatan sebagaimana pasal 13 atau 14 UU Rahasia Dagang diancam pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp 300.000.000,00 (tiga ratus juta rupiah).

Perbuatan peretas sebagaimana kasus Tokopedia yang secara melawan hukum menerobos sistem keamanan dan mengambil data nasabah Tokopedia dapat dimintakan pertanggungjawaban hukum karena terdapat unsur kesalahan dalam perbuatan yang dilakukan oleh peretas tersebut sebagaimana prinsip *liability based on fault*. Perbuatan sebagaimana dimaksud memenuhi unsur-unsur dalam pasal 14 UU Rahasia Dagang karena peretas tersebut memperoleh informasi Rahasia Dagang Tokopedia dengan cara yang bertentangan dengan peraturan perundang-undangan yang berlaku dalam hal ini bertentangan dengan ketentuan dalam UU ITE karena informasi Rahasia Dagang yang diperoleh peretas tersebut berupa informasi data nasabah yang berbentuk elektronik pada platform digital.

Sebagai salah satu perusahaan *start-up* yang melakukan bisnis melalui *online service*, Tokopedia merupakan penyelenggara sistem elektronik yang memiliki kewajiban dan tanggung jawab dalam pengelolaan sistem elektroniknya. Salah satu tantangan yang dihadapi Tokopedia sebagai perusahaan *start-up* adalah Pelindungan Data Pribadi dan perlindungan data. Dikarenakan data merupakan aset yang penting bagi perusahaan *start-up* yang dikumpulkan dari waktu ke waktu, maka Tokopedia harus memperhatikan regulasi mengenai perlindungan data sebelum menggunakan data tersebut secara komersial dan mengklaim hak Kekayaan Intelektual atas data yang dikumpulkan tersebut (Malhotra & Punia, 2018). Tokopedia sebagai penyelenggara sistem elektronik di bidang *marketplace* yang berbentuk *user generated content* memiliki kewajiban dan tanggung jawab yang tercantum dalam UU ITE, PP PSTE, PP PSME, dan SE Safe Harbour. Pasal 3 PP PSTE memuat kewajiban bagi setiap penyelenggara sistem elektronik untuk menyelenggarakan sistem elektronik yang dikelolanya secara andal dan aman serta bertanggung jawab terhadap beroperasinya dan penyelenggaraan sistem elektronik sebagaimana mestinya. Penyelenggara sistem elektronik juga harus memenuhi persyaratan

minimum sebagaimana ketentuan dalam pasal 4 PP PSTE. Ketentuan tersebut juga terdapat dalam pasal 24 PP PMSE dimana Tokopedia merupakan penyelenggara perdagangan melalui sistem elektronik yang memiliki kewajiban untuk menyediakan pengamanan sistem elektronik yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.

Berkaitan dengan pertanggungjawaban Tokopedia sebagai penyelenggara sistem elektronik yang menghimpun Data Pribadi milik nasabahnya dan digunakan untuk kepentingan komersial, Tokopedia harus tunduk terhadap regulasi yang mengatur Pelindungan Data Pribadi dalam platform digital karena Tokopedia merupakan salah satu penyelenggara sistem elektronik. Ketentuan mengenai Pelindungan Data Pribadi pada penyedia platform digital diatur dalam UU ITE, PP PSTE, PP PMSE, dan PM PDPSE. Penyelenggara sistem elektronik kewajiban untuk melaksanakan prinsip Pelindungan Data Pribadi dalam melakukan pemrosesan data pribadi sebagaimana pasal 14 PP PSTE yang salah satunya adalah melakukan pemrosesan Data Pribadi dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan Data Pribadi. Kemudian dalam hal terjadinya kegagalan dalam Pelindungan Data Pribadi yang dikelolanya, penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik Data Pribadi tersebut berdasarkan pasal 14 ayat (5) PP PSTE. Lebih lanjut bahwa ketentuan pasal 59 ayat (1) PP PMSE mewajibkan Tokopedia sebagai pihak yang menyimpan Data Pribadi untuk memiliki sistem pengamanan yang patut untuk mencegah kebocoran atau mencegah setiap kegiatan pemrosesan atau pemanfaatan Data Pribadi secara melawan hukum serta bertanggung jawab atas kerugian yang tidak terduga atau kerusakan yang terjadi terhadap data pribadi tersebut. Tokopedia sebagai pengguna Data Pribadi dan penyelenggara sistem elektronik yang menyimpan data pribadi memiliki tanggung jawab atas Data Pribadi yang terdapat dalam penguasaannya apabila terjadi tindakan penyalahgunaan dan memiliki kewajiban untuk menjaga kerahasiaan dan penyimpanan Data Pribadi.

Berdasarkan beberapa ketentuan diatas maka dapat diidentifikasi bahwa Tokopedia sebagai penyelenggara sistem elektronik memiliki kewajiban berdasarkan ketentuan peraturan perundang-undangan untuk menyelenggarakan sistem elektroniknya secara aman dan andal yang mencakup keamanan dalam pengelolaan Data Pribadi nasabahnya. Apabila Tokopedia sebagai penyelenggara sistem elektronik gagal melakukan kewajiban tersebut, maka Tokopedia dapat dikenakan sanksi administratif sehingga dapat dilihat bahwa ketentuan diatas menganut prinsip *presumption of liability* yang mana prinsip tanggung jawab tersebut menempatkan Tokopedia sebagai pihak yang dianggap selalu bertanggungjawab apabila terjadi kegagalan dalam menjaga keamanan dan keandalan sistem elektronik yang dikelolanya serta beban pembuktian untuk membuktikan bahwa telah terjadinya keadaan memaksa untuk melepaskan Tokopedia dari tanggung jawab tersebut harus dibuktikan sendiri oleh pihak Tokopedia (Purwadi, 2017, pp. 115–116). Sementara itu, dalam kaitannya dengan kewajiban Tokopedia untuk melindungi Data Pribadi nasabahnya, sanksi administratif dapat diberikan kepada Tokopedia apabila terjadi kegagalan dalam melindungi Data Pribadi nasabahnya dimana hal tersebut memperlihatkan adanya prinsip *strict liability* yang menyatakan bahwa Tokopedia akan selalu bertanggungjawab apabila terjadi kegagalan dalam melindungi keamanan Data Pribadi nasabahnya tanpa perlu melihat adanya unsur kesalahan (Muthiah, 2017, p. 10).

Tokopedia sebagai pengguna Data Pribadi dan penyelenggara sistem elektronik yang melakukan penyimpanan Data Pribadi nasabahnya memiliki kewajiban untuk melakukan pemberitahuan secara tertulis kepada pemilik Data Pribadi yang menjadi nasabah Tokopedia dikarenakan terjadinya kegagalan dalam pelindungan rahasia Data Pribadi paling lambat 14 (empat belas) hari setelah terjadinya kegagalan pelindungan disertai dengan alasan atau

penyebab terjadinya kegagalan perlindungan kerahasiaan Data Pribadi tersebut dan Tokopedia harus memastikan pemberitahuan tersebut diterima oleh pemilik Data Pribadi apabila terdapat potensi kerugian yang ditimbulkan akibat kegagalan Pelindungan Data Pribadi tersebut sebagaimana ketentuan dalam pasal 28 huruf (c) PM PDPSE. Kemudian sebagai pertanggungjawaban Tokopedia yang merupakan penyelenggara sistem yang mengalami kegagalan dalam menjalani kewajibannya untuk menyelenggarakan sistem elektronik yang dikelolanya secara andal dan aman, maka Tokopedia dapat dikenakan sanksi administratif berdasarkan pasal 100 PP PSTE berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan akses dan/atau dikeluarkan dari daftar. Namun berdasarkan pasal 3 ayat (3) PP PSTE sanksi administratif tersebut dapat dikesampingkan apabila Tokopedia dapat membuktikan bahwa telah terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak Pengguna Sistem Elektronik. Ketentuan sanksi administratif pada pasal 80 PP PMSE juga dapat diberikan kepada Tokopedia sebagai bentuk pertanggungjawaban Tokopedia yang merupakan pelaku usaha dan penyelenggara perdagangan melalui sistem elektronik yang dapat berupa peringatan tertulis, dimasukkan dalam prioritas pengawasan, dimasukkan dalam daftar hitam, pemblokiran sementara layanan PPMSE dan/atau pencabutan izin usaha.

KESIMPULAN DAN SARAN

Kesimpulan

1. Kekayaan Intelektual sebagai sebuah penghargaan terhadap penemuan karya intelektual oleh seseorang atau badan hukum yang memberikan hak moral dan hak ekonomi harus mendapatkan kepastian dalam perlindungan hukum. Terlebih dengan kemajuan teknologi informasi dan komunikasi yang berkembang pesat, sehingga berimplikasi terhadap perubahan aktivitas dan pola pikir manusia secara fundamental dimana hal tersebut juga menyebabkan perlunya pembaharuan perlindungan Kekayaan Intelektual. Kemunculan era digital juga menyebabkan terjadinya persinggungan antara aspek hukum Kekayaan Intelektual, dalam hal ini Rahasia Dagang dan aspek hukum privasi. Sehingga perlindungan Rahasia Dagang sebagai salah satu rezim Kekayaan Intelektual yang berkaitan erat dengan teknologi dan bisnis perlu diperhatikan guna menjamin hak pemilik Rahasia Dagang khususnya pada era kemajuan teknologi informasi dan komunikasi.
2. Pelindungan informasi Rahasia Dagang di Indonesia yang tercakup dalam UU Rahasia Dagang, atas ratifikasi persetujuan pembentukan organisasi perdagangan dunia belum memadai. Pelindungan informasi Rahasia Dagang yang berbasis penyelenggara sistem elektronik pada platform digital belum tercakup didalam UU Rahasia Dagang dimana pelindungan terhadap informasi rahasia pada platform digital masih tersebar dalam berbagai peraturan perundang-undangan yaitu UU ITE, PP PSTE, dan PP PMSE. Sehingga perlu dibuat pengaturan secara khusus untuk mencapai fungsi hukum yang prediktif dan antisipatif.
3. Berdasarkan teori tanggung jawab Hans Kelsen, pihak yang melakukan peretasan terhadap data nasabah Tokopedia wajib bertanggungjawab karena tindakan peretasan yang dilakukannya bertentangan dengan ketentuan UU ITE yang berlaku secara ekstra territorial, sedangkan Tokopedia sebagai penyelenggara sistem elektronik di bidang *marketplace* yang berbentuk *user generated content* harus bertanggungjawab terhadap para nasabahnya atas kegagalan melaksanakan kewajibannya sebagai penyelenggara sistem elektronik dan melakukan pelindungan terhadap informasi Data Pribadi nasabahnya tersebut berdasarkan PP PSTE, PP PMSE, PM PDPSE serta SE Safe Harbour.

Saran

1. Sebagai payung hukum terhadap keberadaan Rahasia Dagang di Indonesia, UU Rahasia Dagang dirasa perlu untuk memberikan pengaturan secara khusus mengenai perlindungan informasi Rahasia Dagang secara elektronik sehingga menjamin kepastian hukum atas perlindungan informasi rahasia tersebut dan dapat mengidentifikasi akibat hukum dari pelanggaran Rahasia Dagang sebagai bentuk pertanggungjawaban hukum bagi pihak yang melakukan pelanggaran atas informasi Rahasia Dagang tersebut. Selain itu, dalam pembaharuan UU Rahasia Dagang, legislator juga harus mempertimbangkan konvergensi antara aspek Rahasia Dagang dan aspek Data Pribadi yang bersinggungan sebagai implikasi dari kemajuan teknologi, sehingga dapat menyeimbangkan dan menjamin kepentingan pemilik Rahasia Dagang dan kepentingan subjek data.
2. Kemajuan teknologi informasi dan komunikasi yang mengakibatkan informasi menjadi sesuatu yang sangat berharga (*data as a new oil*) sehingga perlu adanya kerja sama antara para pemangku kepentingan dalam platform digital khususnya *e-commerce* dan pemerintah untuk menjaga keamanan informasi terutama informasi rahasia dalam platform digital dari perbuatan melawan hukum yang dapat dilakukan secara elektronik oleh siapapun untuk menjamin kepentingan warga negara, badan hukum, dan Negara Kesatuan Republik Indonesia.

DAFTAR PUSTAKA

- Aswandi, R., Muchsin, P. R. N., & Sultan, M. (2020). Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *LEGISLATIF*.
- Atmadjaja, D. I. (2016). *Hukum Dagang Indonesia (Sejarah, Pengertian, dan Prinsip Hukum Dagang)*. Setara Press.
- Aulia, K. P. (2020). Pelindungan Hukum Terhadap Merek Terkenal (Well-Known Mark) Atas Passing Off Pada Digital Platform Marketplace. *Kertha Semaya: Journal Ilmu Hukum*, 8(20), 1688–1706.
- Ayu Astuti, S. (2020). Era Disrupsi Teknologi 4.0 Dan Aspek Hukum Perlindungan Data Hak Pribadi. *PAJOUL (Pakuan Justice Journal Of Law)*.
- Badan Pengembangan dan Pembinaan Bahasa Kementerian Pendidikan dan Kebudayaan Republik Indonesia. (n.d.). *Komersial*. Retrieved March 12, 2021, from <https://kbbi.web.id/komersial>
- Budi Asri, D. P. (2020). Perlindungan Hukum Hak Kekayaan Intelektual Bagi Produk Kreatif Usaha Kecil Menengah Di Yogyakarta. *Jurnal Hukum Ius Quia Iustum*, 27(1), 130–150. <https://doi.org/10.20885/iustum.vol27.iss1.art7>
- Chartwell Staffing Servs. Inc. v. Atl. Sols. Grp. Inc., (2019).
- Darwance, D., Yokotani, Y., & Anggita, W. (2020). Dasar-Dasar Pemikiran Perlindungan Hak Kekayaan Intelektual. *PROGRESIF: Jurnal Hukum*. <https://doi.org/10.33019/progresif.v15i2.1998>
- Dole Jr, R. (2018). The Contract Exception to the Uniform Trade Secrets Act and Its Implications for the Federal Defend Trade Secrets Act. *Santa Clara Computer and High-Technology Law Journal*, 34(4), 362.
- Dyani, V. A. (2017). Pertanggungjawaban Hukum dan Perlindungan Hukum bagi Notaris dalam Membuat Party Acte. *Jurnal Lex Renaissance*, 2(1), 162–176. <https://doi.org/10.20885/jlr.vol2.iss1.art11>
- Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan. *UNES Law Review*. <https://doi.org/10.31933/law.v1i2.24>

- Faramukti, T. S. (2019). *Perlindungan Hukum Rahasia Dagang atas Informasi Bisnis dalam Perjanjian Kerja di Kabupaten Sleman*. Universitas Islam Indonesia.
- Fish & Richardson. (2019). *Trade Secret Protection for Customer Lists: A Checklist*. <https://www.jdsupra.com/legalnews/trade-secret-protection-for-customer-29052/>
- Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *CAKRAWALA: Jurnal Humaniora Bina Sarana Informatika*, 20(1).
- Gerungan, A. E. (2016). Perlindungan Hukum Terhadap Rahasia Dagang Ditinjau Dari Aspek Hukum Perdata Dan Pidana Di Indonesia. *Jurnal Hukum Unsrat*, 22(5), 69–84.
- Lie, H. T. (2016). Introduction to Current Trade Secret Management Research. *SSRN Electronic Journal, March*. <https://doi.org/10.2139/ssrn.2869296>
- Linton, K. (2016). The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research. *Journal of International Commerce and Economics*.
- Lippoldt, D. C., & Schultz, M. F. (2014). Uncovering Trade Secrets-An Empirical Assessment of Economic Implications of Protection for Undisclosed Data. *OECD Trade Policy Papers*.
- Malgieri, G. (2016). Trade secrets v personal data: A possible solution for balancing rights. In *International Data Privacy Law*. <https://doi.org/10.1093/idpl/ipv030>
- Malhotra, T., & Punia, R. (2018). *Start-ups, Data Privacy and Trade Secrets*. <https://www.iam-media.com/strategy/start-ups-data-privacy-and-trade-secrets#>.
- Muhammad, A. (2001). *Kajian Hukum Ekonomi Hak Kekayaan Intelektual*. PT. Citra Aditya Bakti.
- Muthiah, A. (2017). Tanggung Jawab Pelaku Usaha kepada Konsumen tentang Keamanan Pangan dalam Perspektif Hukum Perlindungan Konsumen. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*. <https://doi.org/10.28932/di.v7i2.712>
- Purwadi, A. (2017). Prinsip Praduga Selalu Bertanggung-gugat dalam Sengketa Medik. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, 4(1), 104–121. <https://doi.org/10.22304/pjih.v4n1.a6>
- Ramli, A. M. (2000). *H.A.K.I Hak Atas Kepemilikan Intelektual: Teori Dasar Pelindungan Rahasia Dagang*. CV. Mandar Maju.
- Ramli, A. M. (2018). *Hak Cipta, Disrupsi Digital Ekonomi Kreatif*. Alumni.
- Republik Indonesia. Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang.
- Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik.
- Republik Indonesia. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
- Republik Indonesia. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
- Republik Indonesia. Surat Edaran Menteri Komunikasi dan Informasi Nomor 5 Tahun 2016 tentang Batasan dan Tanggung Jawab Penyedia Platform dan Pedagang (*Merchant*) Perdagangan melalui Sistem Elektronik (*Electronic Commerce*) yang Berbentuk User Generated Content.
- Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*. <https://doi.org/10.30641/ham.2020.11.285-299>

- Safiranita, T., Yasmine, M. A., Putri, S. A., & Ramli, A. M. (2020). Rahasia Dagang: Informasi Dan Hukum Positif Pada Jasa Telekomunikasi Indonesia. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*, 12(1), 001–010. <https://doi.org/10.28932/di.v12i1.2851>
- Sakti, S. T. I., & Budhisulistiyawati, A. (2020). Perlindungan Hukum Bagi Para Pihak Dalam Perjanjian Jual Beli Tanah Letter C di Bawah Tangan. *Jurnal Privat Law*, 8(1), 145.
- Salmon, M. F. G. (2019). Perlindungan Hukum Terhadap Rahasia Perusahaan Dalam Menghadapi Persaingan Bisnis Di Indonesia. *LEX PRIVATUM*.
- Santiago, F. (2017). Trade secret protection on globalization era. *European Research Studies Journal*, 20(4), 66–76. <https://doi.org/10.35808/ersj/820>
- Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.
- Sitepu, N. W. (2020). Analisa Perlindungan Konsumen Sebagai Pengguna Information Technology And Communication. *Jurnal Ius Civile*, 4(2), 117–133.
- Soekanto, S., & Mamudji, S. (2011). Penelitian Hukum Normatif, Suatu Tinjauan Singkat. In *Jakarta : Raja Grafindo Persada*.
- Waqas. (2020). *Tokopedia hacked – Login details of 91 million users sold on dark web*. <https://www.hackread.com/tokopedia-hacked-login-details-sold-on-dark-web/>
- Wicaksono, A. (2020). *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*. <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>
- Zaini, Z. D. (2011). Implementasi pendekatan yuridis normatif dan pendekatan normatif sosiologis dalam penelitian ilmu hukum. *Pranata Hukum*.
- Zorkoczy, P. (1990). *Information Technology: An Introduction*. Pittman Publishing.