Fakultas Hukum UPN Veteran Jakarta
Jl. Pondok Labu Raya, Pondok Labu, Cilandak
Jakarta Selatan, D.K.I. Jakarta, Indonesia 12450

E-ISSN: xxxx-xxxx
P-ISSN: xxxx-xxxx

Jurnal Hukum Statuta
Volume 1 Nomor 2, April 2022

Dampak Cyber Attack Bagi Ekonomi Perdagangan Elektronik: Studi Pada Bocornya Data di Platform Tokopedia

Fachri Fadillah[1], Adelya[2], Hagi Nur Khanif[3], Rani Shahira[4*]

[1]*Fakultas Hukum UPN Veteran Jakarta, Indonesia, fachrifadillah@upnvj.ac.id*

[2]*Fakultas Hukum UPN Veteran Jakarta, Indonesia, adelyaadelya241@upnvj.ac.id*

[3]*Fakultas Hukum UPN Veteran Jakarta, Indonesia, haginurkhanifr@upnvj.ac.id*

[4]*Fakultas Hukum UPN Veteran Jakarta, Indonesia, ranishahira@upnvj.ac.id*

Diterima: 10 Desember 2021 **Direview: 28 Desember 2021** **Disetujui: 15 Januari 2022**

Abstract

Abstract is typed in Book Antiqua font style Cyber attack is a crime or attack type of offensive maneuver that targets computer information network systems. Crime with the aim of weakening an object in cyberspace has become a crime that often occurs in our daily lives. Social media or even e-commerce is familiar, the more social media is growing, the same thing with crime that continues to follow the times. This has led to an increase in cyber attacks. One example of a cyber attack that occurred in Indonesia recently is the leak of personal data of Tokopedia users on the dark web. So we created this journal article with the aim to find out what is the basis of cyber attack law in Indonesia and how the impact of cyber attacks on e-commerce in Indonesia.

Keywords: Cyber Attack, E-commerce, Crime

Abstrak

Serangan Siber (*Cyber Attack*) merupakan kejahatan atau serangan jenis manuver ofensif yang menargetkan sistem jaringan informasi komputer. Kejahatan dengan tujuan melemahkan pada suatu objek di dunia maya ini sudah menjadi kejahatan yang sering terjadi di kehidupan sehari-hari kita. Media sosial atau bahkan *e-commerce* sudah tidak asing lagi, semakin hari media sosial semakin berkembang, sama hal dengan kejahatan yang berkemang mengikuti zaman. Hal tersebut menyebabkan adanya peningkatan *cyber attack*. Salah satu contoh *cyber attack* yang terjadi di Indonesia baru-baru ini ialah bocornya data pribadi pengguna Tokopedia di *dark web*. Sehingga kami membuat artikel jurnal ini dengan tujuan untuk mengetahui apa yang menjadi dasar hukum *cyber attack* di Indonesia dan bagaimana dampak *cyber attack* bagi *e-commerce* di Indonesia.

Kata Kunci : Cyber Attack, E-commerce, Kejahatan

1

2

PENDAHULUAN

Pada abad ke-21 dikenal sebagai era revolusi industri 4.0 dimana kehadiran komputer dan internet banyak membawa manfaat bagi manusia. Masyarakat melakukan banyak aktivitas dengan lebih mudah dan cepat menggunakan komputer dan internet. Perkembangan teknologi sekarang ini tumbuh semakin cepat, dengan kemajuan teknologi informasi dan komunikasi, jarak dan waktu bukan lagi menjadi masalah yang besar bagi setiap orang, perusahaan, dan pemerintah. Setiap orang dapat saling berhubungan satu sama lain tanpa harus bertemu di *real space*. Perusahaan dapat mengembangkan usahanya ke banyak negara hanya dengan melakukan pemasaran melalui internet dan komputer. Dengan kemajuan teknologi maka dapat digunakan sebagai sarana untuk menyediakan barang-barang yang diperlukan bagi kelangsungan dan kenyamanan hidup manusia serta memberikan kemudahan mekanisme pembayaran yang cepat dan tidak terhalang oleh waktu.

Tidak hanya membawa manfaat, tetapi teknologi juga memberikan risiko keamanan. Banyak pihak-pihak tidak bertanggung jawab yang menyalahgunakan teknologi internet untuk berbuat kejahatan. Kejahatan dalam dunia maya ini disebut dengan *cyber crime*. Terdapat empat masalah keamanan utama yang dihadapi industri *e-commerce* yaitu keamanan transaksional, privasi, keamanan sistem *commerce*, dan kejahatan dunia maya di *e-commerce*. Terkait privasi dalam transaksi online, pengguna diharuskan untuk mengungkapkan sejumlah besar informasi pribadi kepada penjual sebagai syarat utama untuk menggunakan aplikasi dimana peruntukannya memiliki berbagai tujuan tergantung kebijakan perusahaan aplikasi. Hal tersebut rentan dengan kebocoran informasi sensitif sehingga memicu terjadinya pelanggaran data dan pencurian identitas terkait data pribadi.

Data pribadi dapat dikatakan sebagai aset berharga, seperti komoditas dengan nilai ekonomi tinggi sehingga harus dijaga dan dikelola dengan baik di dunia digital saat ini. Digitalisasi di satu sisi membawa manfaat bagi peradaban, namun di sisi lain, digitalisasi membawa masalah baru sekaligus tantangan di era Revolusi Industri 4.0. Pesatnya perkembangan informasi dan komunikasi yang meliputi tahapan pengumpulan, penyimpanan, pengolahan, produksi dan pengiriman data ke dan dari industri atau masyarakat secara efektif dan efisien tidak disertai perlindungan hukum yang optimal, seperti yang diungkapkan oleh Wahyudi Djafar, "Tidak ada payung hukum yang memadai yang mengatur soal perlindungan data pribadi di Indonesia. Peraturan yang tersebar di berbagai

undang-undang belum sepenuhnya mengacu pada prinsip-prinsip perlindungan data pribadi."[3]

E-commerce merupakan teknologi yang menjadi kebutuhan mendasar setiap organisasi yang bergerak di bidang perdagangan. *E-commerce* merupakan cara bagi konsumen untuk dapat membeli barang yang diinginkan dengan memanfaatkan teknologi internet[4]. *E-commerce* yang ada di Indonesia berdasarkan pernyataan memang banyak jenisnya, dan yang akan dibahas pada penelitian ini adalah dalam bentuk aplikasi.

Aplikasi merupakan program yang secara langsung dapat melakukan proses-proses yang digunakan dalam komputer oleh pengguna. Aplikasi merupakan kumpulan dari file-file tertentu yang berisi kode program yang menghubungkan antara pengguna dan perangkat keras komputer[5].

Pada penelitian ini, penulis menjelaskan mengenai *cyber attack*, jenis-jenis pelanggaran data, pencurian identitas pada *e-commerce* di Indonesia, contoh kasus *e-commerce* di Indonesia, dan upaya perlindungan data pada *e-commerce*. Pustaka penelitian ini berdasarkan studi literatur naskah- naskah penelitian terkait pelanggaran data dan pencurian identitas pada *e-commerce*. Sehingga berdasarkan latar belakang yang penulis tulis di atas, terdapat dua permasalahan penting, antara lain : Pertama, Apa dasar hukum yang mengatur mengenai *Cyber Attack* di Indonesia dan Kedua Bagaimana dampak *Cyber Attack* bagi perekonomian yang khususnya dalam perdagangan elektronik (*e-commerce tokopedia*).

METODE PENELITIAN

Penelitian Jenis penelitian dalam penelitian ini adalah penelitian hukum normatif, dimana hukum dikonsepkan sebagai apa yang tertulis dalam peraturan Perundang-Undangan (*law in books*) atau hukum dikonsepkan sebagai kaidah atau norma yang merupakan patokan berperilaku manusia yang dianggap pantas. Oleh karena itu sifat penelitian ini adalah kepustakaan (*library research*), artinya sebuah studi dengan mengkaji buku-buku atau kitab-kitab terkait dengan artikel ini yang berasal dari perpustakaan (bahan pustaka). Semua sumber berasal dari bahan-bahan

[3] Elnizar, N. E. (2019). Perlindungan Data Pribadi Tersebar Di 32 UU, Indonesia Perlu Regulasi Khusus. *Retrieved Februari*, *5*, 2020.

[4] Mumtahana, Hani Atun, Nita and Tito, 2017

[5] Pengertian Aplikasi, 2016 (website http://edel.staff.unja.ac.id/blog/artikel/Penger tian-Aplikasi.html (Accessed: 10 June 2020).

tertulis (cetak) yang berkaitan dengan permasalahan penelitian dan literatur-literatur lainnya (elektronik). Sehubungan dengan pendekatan penelitian ini menggunakan pendekatan normatif, maka bahan hukum yang digunakan diperoleh melalui penelusuran bahan hukum atau studi pustaka terhadap bahan hukum primer, sekunder, dan tersier. Bahan hukum primer yaitu bahan hukum yang terdiri atas aturan hukum nasional yang berdasarkan hierarki peraturan Perundang-Undangan, yang dimulai dari Undang-undang dasar 1945, Undang-undang, peraturan pemerintah, dan aturan lain dibawah undang-undang. Bahan hukum sekunder adalah bahan hukum yang diperoleh dari buku teks, jurnal-jurnal asing, pendapat para sarjana. Kasus-kasus hukum, serta symposium yang dilakukan para pakar yang terkait, dengan pembahasan hukum pidana dan proses pemidanaan. Bahan hukum tersier adalah bahan hukum yang memberikan petunjuk atau penjelasan bermakna terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia, dan lain-lain.

Teknik Pengumpulan Data yaitu sumber hukum yang diperoleh dalam penelitian studi kepustakaan, undang-undang, peraturan pemerintah, serta peraturan-peraturan perundang-undangan, jurnal-jurnal hukum, pendapat para sarjana, dan kasus-kasus hukum yang digunakan. Penulis akan menguraikan dan menghubungkan sedemikian rupa, sehingga dapat disajikan dalam penulisan yang sistematis dengan harapan dapat memberikan suatu jawaban atas permasalahan yang bersifat umum terhadap permasalahan konkret yang dihadapi. Teknik analisis data dalam penelitian ini dilakukan secara kualitatif, analisa sumber hukum yang digunakan dalam penelitian ini adalah interpretasi, yaitu dengan penggunaan metode normatif dalam membahas suatu persoalan hukum. Penulis menggunakan dua metode penafsiran di antaranya, pertama Penafsiran gramatikal yaitu penafsiran menurut tata bahasa dan kata-kata yang merupakan alat bagi pembuat undang-undang untuk menyatakan maksud dan kehendaknya. Kedua, Penafsiran sistematis yaitu penafsiran yang mengaitkan pasal yang satu dengan pasal yang lain dalam suatu perundang-undangan yang bersangkutan atau pada peraturan lainnya, supaya pembaca memahami dan mengerti penjelasan suatu perundang-undangan tersebut.

HASIL DAN PEMBAHASAN

A. CYBER ATTACK DI INDONESIA

Cyber attack merupakan penyerangan yang terjadi di dunia *cyberspace*. Penyerangan di dunia siber terjadi karena adanya globalisasi yang telah mendunia. Penyerangan di dunia *cyberspace* berawal di tahun 1988 yang mana terjadi di dalam peristiwa *The Morris Worm*. *Worm* merupakan senjata *cyber* yang digunakan untuk memperlambat kinerja komputer yang terhubung pada

jaringan sampai pada titik dimana komputer tidak dapat digunakan. Cyber Attack merupakan serangan dalam dunia maya, baik yang ditujukan untuk menyerang ataupun bertahan yang diharapkan dapat sebagai penyebab kematian seseorang atau kerusakan suatu objek yang dituju.[6] Cyber Attack memiliki dampak yang dapat menimbulkan ancaman serius bagi dunia maya antara lain mampu mematikan sentrifugal nuklir, sistem pertahanan udara, dan jaringan listrik. Tujuan *cyber attack* antara lain pemusnahan integritas (*loss of integrity*), ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan pemusnahan fisik (*physical destruction*) yang dampaknya terlihat pada aktivitas korban di *real space.*[7]

Menghadapi era globalisasi yang telah membuka era borderless akibat perkembangan teknologi informasi maka jalan yang harus ditempuh oleh setiap negara yaitu dengan menerima perkembangan tersebut. Hal ini kemudian menyebabkan ketergantungan bagi setiap negara terhadap teknologi informatika, baik dalam rangka menjalankan roda pemerintahan maupun memberikan pelayanan kepada publik. Oleh sebab itu, perlindungan terhadap sarana dan prasarana infrastruktur negara yang memanfaatkan teknologi informatika sangat penting. Sebagai langkah antisipatif terhadap ancaman cyber, pemerintah Indonesia telah mengeluarkan regulasi terkait keamanan informasi dan perlindungan data pribadi konsumen yang dimana pengaturannya masih bersifat parsial contohnya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik; Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik; Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, terakhir Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOKL.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen. Walaupun dengan kehadiran regulasi sebagaimana tersebut di atas keabsenan undang-undang khusus terkait perlindungan data pribadi konsumen masih menyisakan ruang di struktur hukum perlindungan konsumen Indonesia.

Penyerangan siber dilakukan dengan meluncurkan serangan untuk mencapai tujuan baik dengan tujuan kepuasan pribadi atau kompensasi. Hal ini tentu menjadi ancaman bagi dunia digital. Mereka bisa menjadi hacker. Serangan itu sendiri mungkin datang dalam berbagai bentuk, termasuk serangan jaringan

[6] Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *5*(1).

[7] Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurisdiction*, *2*(2), 539-554.

aktif untuk memantau lalu lintas yang tidak terenkripsi untuk mencari informasi sensitif; serangan pasif seperti memantau komunikasi jaringan yang tidak terlindungi untuk mendekripsi lalu lintas terenkripsi lemah dan mendapatkan informasi otentikasi; serangan close-in; eksploitasi oleh orang dalam, dan sebagainya. Jenis serangan siber umum antara lain adalah :

- Serangan fisik: Serangan semacam ini merusak komponen perangkat keras. Karena sifat Internet of things atau yang selanjutnya disebut sebagai IoT yang tidak dijaga dan terdistribusi, sebagian besar perangkat biasanya beroperasi di lingkungan luar ruangan, yang sangat rentan terhadap serangan fisik.
- Serangan pengintaian – penemuan dan pemetaan sistem, layanan, atau kerentanan yang tidak sah. Contoh serangan pengintaian adalah memindai port jaringan, *packet sniffers*, analisis lalu lintas, dan mengirim pertanyaan tentang informasi alamat IP.
- *Denial-of-service* (DoS): Serangan semacam ini adalah upaya untuk membuat mesin atau sumber daya jaringan tidak tersedia untuk pengguna yang dituju. Karena kemampuan memori yang rendah dan sumber daya komputasi yang terbatas, sebagian besar perangkat di IoT rentan terhadap serangan enervation sumber daya.
- Serangan akses – orang yang tidak berwenang mendapatkan akses ke jaringan atau perangkat yang tidak memiliki hak untuk mengakses. Ada dua jenis serangan akses: yang pertama adalah akses fisik, di mana penyusup dapat memperoleh akses ke perangkat fisik. Yang kedua adalah akses jarak jauh, yang dilakukan ke perangkat yang terhubung dengan IP.
- Serangan terhadap privasi: Perlindungan privasi di IoT telah menjadi semakin menantang karena volume besar informasi yang mudah tersedia melalui mekanisme akses jarak jauh. Serangan yang paling umum terhadap privasi pengguna adalah *data mining*, spionase siber, menguping, pelacakan, dan *breach* pada *password*.[8]
- Kejahatan cyber: Internet dan objek pintar digunakan untuk mengeksploitasi pengguna dan data untuk keuntungan materialistis, seperti pencurian kekayaan intelektual, pencurian identitas, pencurian merek, dan penipuan . Serangan destruktif: Ruang angkasa digunakan untuk menciptakan gangguan skala besar dan penghancuran kehidupan dan properti. Contoh serangan destruktif adalah terorisme dan serangan balas dendam.

[8] I. Naumann and G. Hogben, "Privacy features of european eid card specifications," Network Security, vol. 2008, no. 8, pp. 9–13, 2008.

- Supervisory Control and Data Acquisition (SCADA) Attacks: Seperti sistem TCP /IP lainnya, sistem SCADA rentan terhadap banyak serangan cyber.

Cyber attack yang terjadi di ataupun dari Indonesia tergolong banyak, salah satunya merupakan terjadinya kebocoran data pengguna dari platform Tokopedia yang terjadi pada awal tahun 2020 kemarin. Kebocoran data pengguna tersebut termasuk kedalam jenis kejahatan siber dalam kategori serangan siber terhadap privasi yaitu *breach* pada *password* pengguna akun Tokopedia.

B. DAMPAK CYBER ATTACK TERHADAP PERDAGANGAN ELEKTRONIK

Cyber attack sendiri merupakan penyerangan yang terjadi di dunia maya atau siber, maka pemicu atau hal yang melawan hukum juga meliputi dunia maya atau siber, seperti perdagangan elektronik atau juga bisa disebut dengan ekonomi elektronik. *Cyber attack* yang dapat menyerang suatu *website* atau tempat di internet biasanya tidak pernah disangka bahwa akan menyerang. Biasanya suatu *website* sudah memberi proteksi yang cukup untuk meminimalisir adanya penyerangan tersebut, namun yang dinamakan cyber attack merupakan penyerangan internet yang bisa dimasuki dengan berbagai cara lainnya. Namun, karena kita sudah hidup di zaman di mana internet termasuk ke dalam kehidupan sehari-hari kita, kita juga tidak bisa meninggalkan perekonomian yang terjadi di dunia siber tersebut. Dikutip dari buku Ekonomi dan Bisnis Digital, bahwa aktivitas ekonomi digital dihasilkan dari miliaran koneksi daring di antara orang, bisnis, perangkat, data, dan proses. Tulang punggung ekonomi digital adalah hiper-konektivitas yang menciptakan keterkaitan orang, organisasi, dan mesin yang berbasis pada Internet, teknologi seluler, dan *Internet of Things*.[9]

Adanya dampak *cyber attack* terhadap perdagangan elektronik sebenarnya tidak selalu mengganggu konsumen maupun produsen, karena sebelumnya suatu perusahaan sudah pasti menyediakan proteksi dari kejahatan siber tersebut. Namun, yang menjadi masalah disini adalah bagaimana perusahaan tersebut menanggulangi kesalahan yang sama dan kesalahan yang akan datang nanti. Maka dari itu, perusahaan-perusahaan yang ada dan berbasis digital, biasanya sudah memiliki *cyber security industry*, yang mana merupakan

[9] Budiarta, K., Ginting, S. O., & Simarmata, J. (2020). *Ekonomi dan Bisnis Digital*. Yayasan Kita Menulis.

penggabungan komponen fisik dan jaringan digital untuk mengubah cara perusahaan manufaktur melakukan otomatisasi proses dan berbagi informasi. [10]

Perkembangan teknologi dan internet telah membawa peradaban manusia menuju apa yang disebut sebagai perdagangan bebas. Perdagangan bebas adalah situasi yang terjadi ketika proses perdagangan tidak dibatasi ruang dan waktu. Sehingga dapat dikatakan, perdagangan bebas muncul karena melihat adanya manfaat dari pengembangan arus teknologi.[11] Perkembangan teknologi inilah yang kemudian menjadi cikal bakal Electronic Commerce yang selanjutnya disebut e-commerce. Untuk menghindari dampak berkepanjangan, penyelenggaraan *cyber security* sangat dibutuhkan dalam industri ekonomi elektronik, maka dari itu penting juga untuk mengetahui apa yang menjadi komponen utama dari *cyber security*. Komponen utama tersebut antara lain[12] :

- *Confidentiality* (kerahasiaan);
- *Integrity* (integritas);
- *Availability* (ketersediaan).

C. STUDI KASUS

Pada zaman teknologi saat ini, masyarakat dihadapi oleh berbagai cara untuk berbelanja. Berbelanja dapat dilakukan secara online maupun offline. Banyaknya inovasi yang sudah dilakukan untuk dapat menarik minat beli para konsumen, maka dari itu aktivitas berbelanja bukan lagi menjadi hal yang sulit. Kegiatan belanja online merupakan alternatif untuk menghemat waktu dan energi konsumen untuk dapat membeli barang yang diperlukan tanpa harus mengunjungi toko offline.

Tokopedia memberikan konsep e-commerce baru yang inovatif dengan mengumpulkan berbagai toko di Indonesia secara online. Semua kegiatan jual beli dan transaksi melalui perantaraan Tokopedia dijamin keamanannya. Tokopedia diharapkan dapat menciptakan sebuah mall online yang mengorganisasikan sejumlah transaksi secara online. Namun pada April 2020 peretas internasional dengan nickname “Why So Dank” berhasil meretas Tokopedia. Berita terkait peretasan Tokopedia ini pada mulanya beredar di media sosial Twitter, salah satu yang memberitakan peristiwa ini adalah akun Twitter @underthebranch, menyampaikan bahwa terdapat 15 juta pengguna Tokopedia yang data nya telah

[10] Rinaldi, R., & Krisnadi, I. (2019). ANALISIS DAMPAK REVOLUSI INDUSTRI 4.0 TERHADAP KEAMANAN DATA DIGITAL.

[11] Fathur, M. (2020, November). TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN. In *National Conference on Law Studies (NCOLS)* (Vol. 2, No. 1, pp. 43-60).

[12] Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Peperangan Asimetris*, *4*(3).

diretas. Menurut @underthebranch, data yang telah diretas berisi email, password, dan nama pengguna.

Kejadian kebocoran data ini menghasilkan dampak yang besar bagi konsumen yang datanya sudah bocor ke situs dark web. Data-data konsumen mempunyai potensi adanya kejahatan siber, seperti scamming atau phishing.[13] Tokopedia sendiri memastikan, informasi berharga milik pengguna sudah berhasil terlindungi, contohnya password. Pihak Tokopedia memberikan anjuran bagi konsumen untuk merubah password akun secara terus menerus serta tidak memberi password OTP (*One Time Password*). Kejadian ini cukup menuai respon yang meresahkan pada masyarakat. Data-data pribadi yang beredar cukup memberikan kekhawatiran bagi masyarakat.

Setelah penelusuran lebih lanjut, ternyata jumlah akun pengguna Tokopedia yang berhasil diretas sebanyak 91 juta akun dan 7 juta akun Merchant. Pakar keamanan Cyber, Pratama Persadha, menceritakan peretas yang meretas Tokopedia pertama kali mempublikasikan hasil peretasannya di sebuah situs di dark web yakni Raid Forums. Dalam situs tersebut, hasil peretasan data pengguna Tokopedia dipublikasikan untuk dijual oleh pelaku sebesar US$5.000 atau sekitar Rp. 74 juta.[14]

Namun, setelah terjadi kasus tersebut, tokopedia langsung mengambil langkah untuk pertanggungjawaban yaitu mengacu pada dasar hukum yang dapat dijadikan landasan oleh konsumen dalam mengajukan gugatan kepada Tokopedia adalah Pasal 1365 Kitab Undang-Undang Hukum Perdata yang pada intinya menjelaskan bahwa tiap perbuatan hukum yang membawa kerugian kepada orang lain, orang menyebabkan kerugian tersebut harus menggantinya.[15] Terdapat pula prinsip pertanggungjawaban pelaku usaha/produsen yang disebut tanggung jawab berdasarkan kelalaian/kesalahan (*Negligence*). Tanggung jawab berdasarkan kelalaian/kesalahan adalah prinsip tanggung jawab yang sifatnya subjektif, maksudnya sifat tanggung jawab ini timbul tergantung perilaku dari pelaku usaha/produsen yang bersangkutan.[16]

Kendati konsumen memiliki hak untuk mengajukan gugatan serta adanya prinsip hukum yang mendasari gugatan tersebut, hal tersebut tidak serta merta

---

[13] Roos, A. B. E., Setyabudi, D., & Gono, J. N. S. (2021). ¬¬ Pengaruh Terpaan Berita Kebocoran Data Pengguna Tokopedia dan Terpaan E-Word of Mouth Terhadap Citra Tokopedia. *Interaksi Online*, *9*(2), 33-39.

[14] Rahmad Fauzan, (2020), "Ini Kronologis Informasi Peretasan di Tokopedia!", Teknologi.bisnis.com, https://teknologi.bisnis.com/read/20200503/266/1235699/ini- kronologisinformasi-peretasan-di-tokopedia (diakses 2 November 2021)

[15] Lihat Pasal 1365 Kitab Undang-Undang Hukum Perdata

[16] Fathur, M. (2020, November). TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN. In *National Conference on Law Studies (NCOLS)* (Vol. 2, No. 1, pp. 43-60).

memberikan jalan kepada konsumen untuk memperjuangkan haknya. Terdapat banyak proses yang harus dilakukan oleh konsumen dalam masa persidangan yaitu harus melalui proses persidangan yang panjang, proses pembuktian terhadap adanya kelalaian/kesalahan Tokopedia yang menyebabkan kebocoran data sampai pembuktian kerugian akibat peristiwa kebocoran data pribadi. Sebenarnya kasus kebocoran data pribadi ini berujung pada meja hijau. Komunitas Konsumen Indonesia (KKI) yang diekatuai oleh David Tobing mengajukan gugatan hukum kepada Menkominfo dan Tokopedia.[17] Perkara gugatan tersebut teregister di Pengadilan Negeri Jakarta Pusat dengan Nomor 235/PDT.G/2020/PN.JKT.PST. Oleh karena ketiadaan undang-undang khusus terkait perlindungan data pribadi, maka hal tersebut menyulitkan konsumen menuntut pertanggungjawaban Tokopedia terkait peristiwa kebocoran data pribadi yang terjadi.

Kejadian seperti ini bukan yang pertama kali di tanah air. Sebelumnya di platform e-commerce lain juga mengalami hal serupa. Seharusnya ini menjadi peringatan keras pada setiap penyedia layanan di Internet yang memakai banyak data masyarakat dalam kegiatan nya. Dibandingkan dengan negara-negara lain, perkembangan regulasi Indonesia masih belum cukup. Hal ini dibuktikan dengan belum adanya regulasi khusus yang mengatur terkait dengan perlindungan data pribadi di Indonesia. Sedangkan di negara-negara tetangga seperti Malaysia dan singapura sudah memiliki regulasi khusus mengenai perlindungan data pribadi. Singapura sudah memiliki regulasi khusus tentang perlindungan data pribadi, yaitu *The Personal Data Protection Act No. 26 of 2012 Singapore* (PDPA 2012 Singapura). Sedangkan perindungan data pribadi Malaysia dilakukan melalui The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia). Sebagaimana negara-negara Asia, Indonesia sulit untuk mengatur serta mendefinisikan tentang privasi.[18] kebanyakan orang Asia yang secara tradisi hidup dalam masyarakat komunal tidak memberikan perhatian serius terhadap privasi. Privasi sebagai hak asasi manusia lebih dikenal sebagai konsep dari Dunia Barat, namun pada era tekonologi informasi kini menjadi sangat penting. Sampai saat ini Indonesia masih belum memiliki undang-undang khusus, Rancangan Undang-Undang Perlindungan Data Pribadi masih dalam proses pembuatan yang pada tahun 2020 telah masuk ke dalam Program Legislasi Nasional (Prolegnas).

Penyebaran pengaturan hukum mengenai data pribadi di Indonesia hingga berbagai aturan yang tidak secara khusus mengatur perlindungan data pribadi merupakan masalah serius yang melemahkan perlindungan hukum data pribadi di Indonesia sehingga harus segera diselesaikan melalui reformasi hukum. Diseminasi

[17] Naufal, R. A. (2020). TANGGUNG JAWAB PT TOKOPEDIA DALAM KASUS KEBOCORAN DATA PRIBADI PENGGUNA.

[18] Naufal, R. A. (2020). TANGGUNG JAWAB PT TOKOPEDIA DALAM KASUS KEBOCORAN DATA PRIBADI PENGGUNA.

regulasi dalam berbagai peraturan perundang-undangan selain menunjukkan perlindungan data pribadi belum menjadi prioritas hukum nasional, juga mengakibatkan lemahnya hukum perlindungan data pribadi warga negara untuk memposisikan WNI dalam posisi rentan, yang tentunya tidak sejalan dengan tujuan hukum memberikan kepastian hukum, keadilan dan kemanfaatan. Berbagai kasus yang ada dan memperhatikan fenomena digitalisasi di era revolusi industri 4.0 dan perkembangan dunia saat ini harus menjadi perlindungan hukum terhadap data pribadi sebagai prioritas negara.

Setelah kejadian tersebut, isu Tokopedia menyebar luas di berbagai sosial media sehingga timbul berbagai cuitan tentang peretasan tersebut. Namun ditengah isu dan kasus hukum yang masih bergulir, Tokopedia langsung meluncurkan iklan promo "Bagi-Bagi Semangat Ramadhan" yang bernilai puluhan miliaran Rupiah sebagai kejutan bagi konsumen nya.[19] Hal ini tentu saja membuat minat konsumen terhadap Tokopedia kembali naik. Ketika iklan ini diluncurkan, tidak sampai sehari publik kembali *mendownload* aplikasi Tokopedia lagi. Tentunya hal ini karena paparan strategi pengalihan isu Tokopedia, dimana fokus konsumen tidak lagi kepada kasus kebocoran data yang mengecewakan konsumen, tetapi konsumen lebih tertarik dengan isi iklan tersebut. Iklan ini dinilai sebagai strategi dari pihak Tokopedia untuk membangun opini publik ke arah positif dengan strategi pengalihan isu untuk mengembalikan kepercayaan konsumen serta memperbaiki citra perusahaan. Namun pihak Tokopedia berdalih bahwa peluncuran iklan promo ini bukanlah bagian dari strategi, melainkan bahwa iklan tersebut sudah menjadi tradisi ramadhan dalam setiap perusahaan untuk meluncurkan iklan promosi di bulan ramadhan.

Citra yang didapatkan oleh Tokopedia tetap sama meski adanya isu negatif yang menerpanya. Menurut pandangan masyarakat pengguna, Tokopedia tetap memiliki nilai lebih sehingga tetap dapat dipercaya sebagai e-commerce yang memiliki kenyamanan, kemudahan, dan terpercaya bagi masyarakat yang berbelanja online berkat usaha perusahaan untuk melakukan iklan rutin serta memberikan banyak promo.[20]

Namun sudah jelas bahwa PT Tokopedia dapat dimintai tanggung jawab berdasarkan Perbuatan Melawan Hukum karena melanggar kewajiban yang lahir dari peraturan perundang-undangan. Model tanggung jawab dalam UU ITE dan

[19] Komalawati, D., MR, M. D., & Kartika, R. D. (2021). Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data. *journal of admiration*, *2*(1), 49-56.

[20] Komalawati, D., MR, M. D., & Kartika, R. D. (2021). Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data. *jurnal of admiration*, *2*(1), 49-56.

peraturan turunannya adalah *presumption liability.* Hal ini dapat dilihat dari pasal 15 UU ITE yang mencerminkan permodelan tanggung jawab tersebut. Berikut adalah pasalnya:

> *"(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinta Sistem Elektronik sebagaimana mestinya.*
>
> *(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.*
>
> *(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik."*

Pada ayat (2) dinyatakan bahwa Penyelenggaraan Sistem Elektronik diasumsikan untuk selalu bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya. Tanggung jawab tersebut hanya tidak lagi berlaku dalam hal dapat dibuktikan keadaan memaksa, kesalahan dan/atau kelalaian dari pengguna Elektronik. Model tanggung jawab presumption liability menganut asas pembuktian terbalik, yaitu pihak yang tergugat lah yang harus membuktikan bahwa dia tidak melakukan PMH. Hubungan hukum yang terjadi dalam kasus kebocoran data pribadi Tokopedia melibatkan 3 (tiga) subjek hukum, yaitu PT Tokopedia, Pengguna Tokopedia, dan Kementerian Komunikasi dan Informatika yang masing-masing memiliki hak dan kewajiban. Dalam tataran yuridis, kedudukan Tokopedia pada UU ITE adalah sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Privat yang memiliki beberapa tanggung jawab yang melekat padanya, yaitu memiliki kewajiban melakukan notifikasi kepada pengguna Tokopedia sebagaimana telah diatur dalam Pasal 14 ayat (5) PP PSTE 2019. Sedangkan pengguna Tokopedia merupakan pemilik data pribadi yang memiliki hak atas persetujuan terhadap pemrosesan data pribadi miliknya. Sementara Kementerian Komunikasi dan Informatika memiliki kewenangan untuk melakukan pengawasan terhadap penyelenggaraan sistem elektronik yang meliputi pemantauan, pengendalian, pemeriksaan, penelusuran, dan pengamanan sebagai tempat pengaduan dari terjadinya kegagalan perlindungan data pribadi dalam bentuk panel penyelesaian sengketa pribadi.

PT Tokopedia dapat dimintai tanggung jawab Perbuatan Melawan Hukum (PMH) oleh penggunanya. Adapun PMH yang terjadi didasarkan pada kelalaian PT Tokopedia dalam menjaga keamanan Sistem Elektronik yang melanggar prinsip kerahasiaan dalam perlindungan data pribadi sehingga mengakibatkan terjadinya kebocoran data dan sikap PT Tokopedia yang tidak melakukan prosedur pemberitahuan secara spesifik mengenai rincian data yang dicuri serta alasan dan penyebab terjadinya kegagalan perlindungan data pribadi sebagaimana diatur

dalam Pasal 28 huruf c. Permenkominfo 20/2016. Terjadinya kedua hal tersebut mengakibatkan kerugian pengguna PT Tokopedia berupa perasaaan khawatir serta terganggunya rasa aman karena data pribadi yang tersebar di dunia maya. Tersebarnya data pribadi tersebut memberi potensi yang sangat besar bagi pengguna menjadi kejahatan siber. Hal ini tentu merupakan pelanggaran terhadap hak privasi yang merupakan hak asasi dan dilindungi secara konstitusional. Model tanggung jawab dalam UU ITE dan turunan nya adalah presumption liability sehingga dalam hal kebocoran data pribadi ini beban pembuktian terletak pada PT Tokopedia. PT Tokopedia yang memiliki kewajiban bahwa ia tidak bersalah.[21]

KESIMPULAN DAN SARAN

KESIMPULAN

Dari paparan diatas, dapat kami simpulkan bahwa pada dasarnya telah mengeluarkan regulasi terkait keamanan informasi dan perlindungan data pribadi konsumen yang dimana pengaturannya masih bersifat parsial contohnya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik; Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik; Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, terakhir Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOKL.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.

SARAN

(1) Bahwa Tokopedia harus mampu menyeimbangkan antara strategi marketing yang baik dan juga memiliki sistem keamanan yang mumpuni.

(2) Bahwa kasus kebocoran data ini bisa saja tidak terjadi jika pihak Tokopedia Melakukan double keamanan untuk menjaga privasi para penggunanya.

[21] Naufal, R. A. (2020). TANGGUNG JAWAB PT TOKOPEDIA DALAM KASUS KEBOCORAN DATA PRIBADI PENGGUNA.

(3) Bahwa harus ada lembaga atau institusi yang dapat mengawasi e-commerce yang diduga lalai menerapkan prinsip etika dalam menjaga privasi penggunanya. Dengan demikian, lembaga tersebut dapat melakukan peneguran terhadap perusahaan yang telah melakukan kelalaian.

DAFTAR PUSTAKA

JURNAL

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *5*(1).

Elnizar, N. E. (2019). Perlindungan Data Pribadi Tersebar Di 32 UU, Indonesia Perlu Regulasi Khusus. *Retrieved Februari*, *5*, 2020.

Fathur, M. (2020, November). TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN. In *National Conference on Law Studies (NCOLS)* (Vol. 2, No. 1, pp. 43-60).

Komalawati, D., MR, M. D., & Kartika, R. D. (2021). Kejutan Puluhan Miliar Tokopedia Ditengah Kasus Kebocoran Data. *jurnal of admiration*, *2*(1), 49-56.

Roos, A. B. E., Setyabudi, D., & Gono, J. N. S. (2021). ¬¬ Pengaruh Terpaan Berita Kebocoran Data Pengguna Tokopedia dan Terpaan E-Word of Mouth Terhadap Citra Tokopedia. *Interaksi Online*, *9*(2), 33-39.

Rinaldi, R., & Krisnadi, I. (2019). ANALISIS DAMPAK REVOLUSI INDUSTRI 4.0 TERHADAP KEAMANAN DATA DIGITAL.

Naufal, R. A. (2020). TANGGUNG JAWAB PT TOKOPEDIA DALAM KASUS KEBOCORAN DATA PRIBADI PENGGUNA.

Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Peperangan Asimetris*, *4*(3).

BUKU

Budiarta, K., Ginting, S. O., & Simarmata, J. (2020). *Ekonomi dan Bisnis Digital*. Yayasan Kita Menulis.

Kitab Undang-Undang Hukum Perdata (KUHPer)

Mumtahana, Hani Atun, Nita and Tito, 2017

WEBSITE

Rahmad Fauzan, (2020), "Ini Kronologis Informasi Peretasan di Tokopedia!", Teknologi.bisnis.com, https://teknologi.bisnis.com/read/20200503/266/1235699/ini-kronologisinformasi-peretasan-di-tokopedia (diakses 2 November 2021)

Pengertian Aplikasi, 2016 (website http://edel.staff.unja.ac.id/blog/artikel/Pengertian-Aplikasi.html (Accessed: 10 June 2020).