Transaksi Fiktif Melalui *Marketplace* Daring Memanfaatkan Promo *Cashback*

(a) Christian Tarapul Anjur Hasiholan, (b) Anton Hendrik Samudra

(a) Universitas Airlangga, christianolan98@gmail.com
(b) Universitas Surabaya, antonhendrik@staff.ubaya.ac.id

Abstract

The present development of technology, mainly with the presence of internet has presented new ways and opportunities in business, namely by electronic commerce (e-commerce). Despite having positive impact, e-commerce also has the potential to cause a negative impact, that is by cyber crime. This research is intended to analyse the possibility of a new cyber crime mode which utilizes cashback promotion in e-marketplace (mainly known as marketplace). The mode used by the perpetrators is to make fictitious transaction in order for the system of marketplace to provide many cashback promos for each transaction made. The perpetrators are allowed to do this mode because they take advantage of the flaw in the system of the marketplace due to the availability of the cashback promo for all of the consumer. The emergence of the possibility of a new cyber crime mode shows the importance of this case to be assessed based on The Law of Republic Indonesia Number 19 of 2016 Concerning Amandment to The Law of Republic Indonesia Number 11 Number 11 of 2008 concerning Electronic Information and Transactions when a transaction is considered as manipulative.

Keywords: *Cybercrime; Fictious; Marketplace; Cashback.*

Abstrak

Perkembangan teknologi pada masa kini, khususnya dengan adanya internet telah menghadirkan caradan peluang baru dalam bisnis yaitu dengan adanya jual-beli daring. Selain menimbulkan dampak positif, jual-beli daring juga berpotensi menimbulkan dampak negatif, yaitu adanya kejahatan siber. Penelitian ini dimaksudkan untuk menganalisis kemungkinan modus kejahatan siber baru yang memanfaatkan promo pengembalian dana yang ada dalam pasar daring. Modus yang dilakukan oleh para pelaku adalah membuat transaksi fiktif agar sistem dari pasar daring tersebut memberikan banyak promo pengembalian dana dari tiap transaksi yang dilakukan. Para pelaku dimungkinkan melakukan modus tersebut karena pengembalian dana dibagikan kepada setiap konsumen. Adanya kemungkan modus kejahatan siber baru tersebut, maka perlu dikaji berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik kapan suatu transaksi disebut sebagai transaksi yang memanipulasi.

Kata Kunci: Kejahatan Siber; Fiktif; Pasar Daring; Pengembalian Dana.

Jurnal
YUSTIKA
Media Hukum dan Keadilan
Fakultas Hukum Universitas Surabaya
Vol. 23 No. 02, Desember 2020
P-ISSN: 1410-7724,
E-ISSN: 2655-7479

1. Pendahuluan

Perkembangan teknologi khususnya internet telah memasuki berbagai aspek dalam kehidupan masyarakat, mulai dari untuk pekerjaan hingga kebutuhan pribadi. Menurut Rohaya (2008, p.2) "Internet *(Inter-Network)* adalah sebutan untuk sekumpulan jaringan

komputer yang menghubungkan situs akademik, pemerintahan, komersial, organisasi, maupun perorangan. Internet menyediakan akses untuk layanan telekomunikasi dan sumber daya informasi untuk jutaan pemakainya yang tersebar di seluruh dunia." Melalui internet kita dapat berhubungan dengan seluruh pemakainya, serta mendapatkan berbagai informasi dari seluruh dunia.

Kemajuan teknologi informasi dan segala bentuk manfaat yang meguntungkan masyarakat juga membawa konsekuensi negatif di dalamnya, karena setiap ada teknologi baru pasti ada kesempatan yang baru untuk mengeksploitasi teknologi tersebut. Seperti pada abad ke 19 saat teknologi pada saat itu adalah telegram banyak orang memanfaatkan kesempatan tersebut untuk mengintersepsi komunikasi antar telegram guna mendapatkan informasi yang dibutuhkan (Grabosky, 2007). Konsep kejahatan siber sendiri berkembang dari kejahatan komputer, pada tahun 1970-an komputer hanya digunakan oleh orang-orang yang bekerja di bidang keamanan. Jenis kejahatan dunia maya yang pertama adalah peretasan, pengrusakan, virus komputer, intrusi komputer, dan penipuan identitas. Kemudian pada tahun 1980 dan 1990 ketika komputer dan teknologi telah menjadi lebih utama dan karena komputer dan internet menjadi lebih banyak digunakan, kejahatan komputer menjadi lebih sering ditemui. Selama tahun 1990-an istilah kejahatan siber mulai digunakan karena penggunaan internet yang masif dan lebih luas. Saat ini, di era 2020 ketika media sosial menjadi populer dan menjadi kebutuhan sehari-hari bagi pengguna komputer dan internet, kejahatan baru akan berkembang dan menjadi lebih canggih (Prahassacitta, 2019). Menurut Pasaribu (2017, p.3) "Munculnya kejahatan baru sebagai akibat dari perkembangan arus teknologi di dunia melalui globalisasi juga berkembang pesat seperti pesatnya perkembangan teknologi itu sendiri, diantaranya kejahatan manipulasi data, spionase, sabotase, provokasi, *money laundering, hacking*, pencurian *software*, penipuan *online* dan berbagai macamnya."

Menurut data dari Pusat Operasi Keamanan Siber Nasional (Pusopkamsinas) Badan SIber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Serangan siber tersebut antara lain *Trojan Hawkeye, Reborn, Blackwater malware, BlackNET RAT, DanaBot Banking Trojan, Sypnote RAT, ransomware Netwalker, Cerberus Banking Trojan, malware Ursnif, Adobot Spyware, Trojan Downloader Metasploit, Projectspy Spyware, Metasploit, Xerses Bot, dan Covid19 Tracker Apps*. Insiden siber merupakan kejadian yang mengganggu berjalannya sistem elektronik misalnya serangan virus, pencurian data, informasi pribadi, hak kekayaan intelektual perusahaan, *web defacement* dan gangguan akses terhadap layanan elektronik.

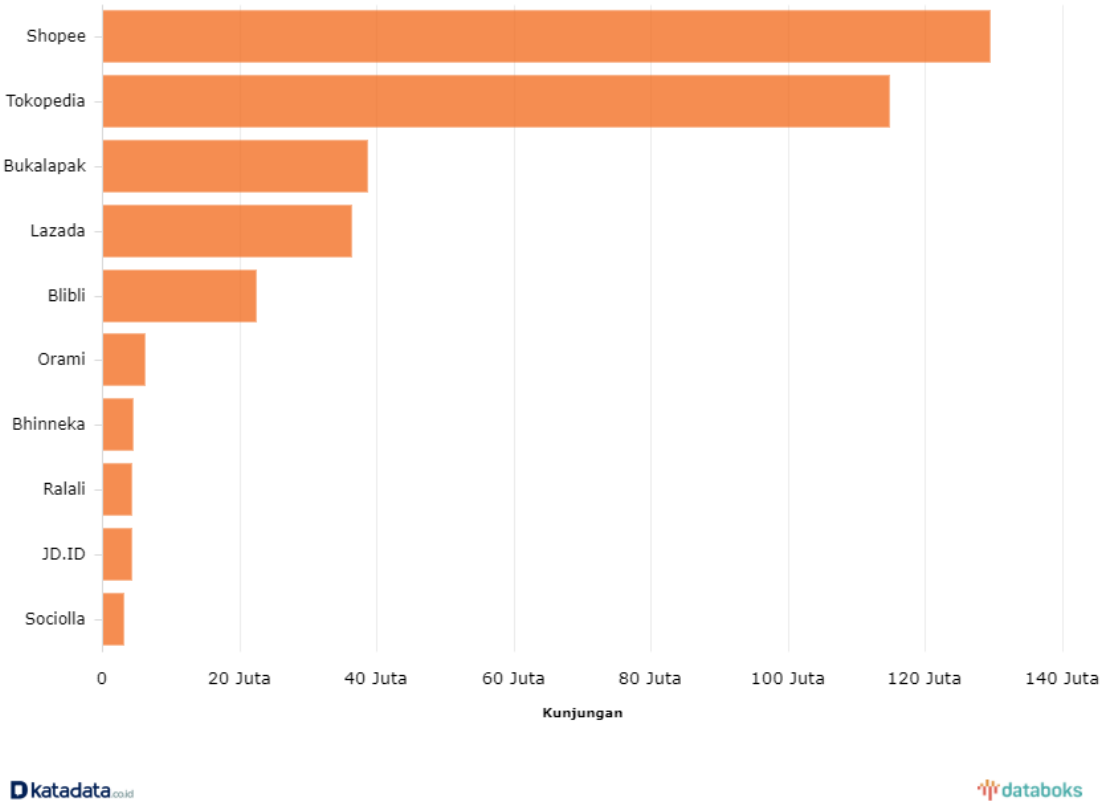
Banyak potensi-potensi terjadinya serangan siber dengan modus baru, seperti melalui *e-marketplace. E-marketplace* merupakan pasar virtual dimana bertemunya calon penjual dan pembeli untuk melakukan transaksi jual beli. Para pelaku usaha sangat diuntungkan karena dengan adanya *e-marketplace* sebagai wadah bertemunya penjual dan pembeli, maka para pelaku usaha hanya perlu memasukkan barang dagangannya ke dalam *e-marketplace* tersebut dan menunggu adanya pembeli tanpa perlu bersusah payah membangun sistem terlebih dahulu. Pembeli tidak perlu khawatir akan ditipu oleh pihak penjual karena *e-marketplace* berperan sebagai pihak ketiga dalam transaksi tersebut. Pihak ketiga yang dimaksud adalah sebagai pengawas apakah transaksi yang dilakukan oleh para pihak merupakan penipuan atau tidak. Beberapa *e-marketplace* yang dimaksud di Indonesia adalah Tokopedia, Bukalapak, Shopee, Blibli, dan sebagainya. *E-marketplace* berperan mengawasi apabila barang yang dijanjikan oleh pihak penjual telah sampai ke pihak pembeli, setelah itu sebagai pihak ketiga

barulah *e-marketplace* dapat mencairkan dana kepada penjual. Berikut merupakan data banyaknya pengguna berbagai *e-marketplac*e di Indonesia berdasarkan katadata.com.

Jurnal Yustika
Vol. 23 No. 02, Des 2020

Cristian T. A. Hasiholan
Go Lisanawati
Anton Hendrik Samudra

Grafik 1. Pengunjung Bulanan Situs E-Commerce Kuartal IV 2020



Berdasarkan data dari katadata.com dapat diketahui bahwa terdapat hampir 140 juta pengunjung tiap bulannya pada berbagai *e-marketplace* di Indonesia. Pengunjung tersebut biasanya tertarik dengan berbagai promosi yang diberikan oleh tiap *e-commerce*, seperti promo gratis ongkos kirim, *voucher* belanja, hingga adanya *cashback* atau pengembalian dana.

Terdapat modus kejahatan siber baru dimana ada sekelompok orang yang diduga melakukan transaksi fiktif yang terjadi pada salah satu *e-marketplace* di Indonesia yaitu Tokopedia. Kasus tersebut bermula dari promo yang diberikan oleh Tokopedia berupa *cashback* atau pengembalian sejumlah uang bagi tiap pengguna yang melakukan pembelian di Tokopedia. Modusnya para pelaku berperan sebagai penjual sekaligus pembeli. Bermula saat RL, HB dan KK yang merupakan warga Surabaya bergantian sebagai penjual dan pembeli. Pada saat RL menjadi penjual maka pembelinya adalah HB dan KK, dan apabila HB sebagai penjual maka RL dan KK menjadi pembeli, begitu seterusnya. RL, HB dan KK melakukan modusnya dengan akun lebih dari satu, agar setiap pihak dapat berperan sebagai penjual dan pembeli. Memanfaatkan promo *cashback* RL, HB dan KK memperoleh keuntungan, misalnya terdapat promo *cashback* sebanyak 10% (sepuluh persen) dengan maksimal *cashback* sebesar Rp.300.000 (tiga ratus ribu rupiah), maka salah satu orang yang berperan sebagai penjual

menjual barang seharga Rp.3.000.000 (tiga juta rupiah). Pelaku sebagai pembeli harus membeli barang tersebut seharga Rp.3.000.000 (tiga juta rupiah) sebagai modal agar dapat mendapatkan *cashback* yang maksimal. Setelah mendapatkan *cashback*, uang yang digunakan untuk membeli barang tersebut akan dikembalikan oleh pelaku lain yang bertindak sebagai penjual kepada pembeli sehingga pembeli memperoleh keuntungan dari *cashback* tersebut sebesar Rp.300.000 (tiga ratus ribu rupiah).

Selain itu, barang yang akan dikirimkan juga tidak sesuai dengan apa yang diiklankan di Tokopedia, jadi apabila di Tokopedia diiklankan barang berupa komputer seharga Rp.3.000.000 (tiga juta rupiah), maka untuk menghemat biaya pengiriman maka penjual hanya mengirimkan buku saja kepada pihak pengangkut agar biaya yang dikeluarkan menjadi murah, serta penjual telah mendapatkan nomor resi sebagai tanda bahwa barang yang telah dibeli telah dikirim, dan apabila barang tersebut sampai di pembeli maka uang akan masuk sejumlah Rp.3.000.000 (tiga juta rupiah) di dalam akun penjual dan *cashback* sebesar Rp.300.000 (tiga ratus ribu rupiah) akan masuk ke dalam akun pembeli, sehingga RL, HB dan KK memperoleh keuntungan sebesar Rp.300.000 (tiga ratus ribu rupiah). Adanya kemungkinan modus kejahatan siber baru tersebut, maka perlu dikaji berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik kapan suatu transaksi dapat disebut sebagai transaksi yang memanipulasi.

2. Pembahasan

Electronic Commerce (e-commerce) adalah proses jual beli produk, jasa dan informasi melalui jaringan komputer sehingga memudahkan terjadinya interaksi bisnis dalam dunia maya. Jenis-jenis interaksi dalam dunia bisnis, yaitu: B2B *(Business to Business)* yang berarti transaksi bisnis terjadi antara pelaku bisnis dengan pelaku bisnis lainnya, B2C *(Business to Consumer)* yang berarti transaksi terjadi antara produsen kepaa konsumen secara langsung, C2C *(Consumer to Consumer)* yang berarti aktivitas bisnis dilakukan antar individu, C2B *(Consumer to Business)* dimana konsumen menciptakan dan membentuk nilai akan proses bisnis, B2G *(Business to Government)* dimana terjadi transaksi antara pelaku bisnis dan instansi pemerintah, serta G2C *(Government to Consumer)* merupakan interaksi antar pemerintah dan masyarakat sehingga memperoleh kemudahan dalam pelayanan sehari-hari (Pradana, 2015).

E-marketplace merupakan salah satu bagian dari *e-commerce*, karena *e-marketplace* atau biasa dikenal sebagai *marketplace* merupakan sebuah tempat jual-beli produk atau jasa secara online yang menghubungkan para penyedia produk atau jasa (penjual) dengan para pencari produk atau jasa tersebut (pembeli). Kemudahan yang diberikan oleh *marketplace* juga menimbulkan dampak negatif yaitu dengan adanya kejahatan siber atau biasa disebut dengan *cybercrime.* Terjadinya kejahatan siber dapat disebabkan karena pengguna yang tidak jelas usulnya, sehingga untuk meminimalisir terjadinya kejahatan siber perlu dilakukan verifikasi data. Verifikasi data bertujuan untuk membuktikan siapa pengguna tersebut sebenarnya, apakah pengguna tersebut benar merupakan orang yang dia daftarkan *(who you claim to be)* (Pamungkas, 2019).

Kejahatan siber merupakan suatu aktivitas yang dilakukan dengan sebuah gawai atau *gadget,* seperti *PC, Laptop, Notebook, Handphone* yang terhubung dengan jaringan internet dan

Jurnal Yustika
Vol. 23 No. 02, Des 2020

aktivitas tersebut melanggar Undang-Undang. Kejahatan siber *(cyber crime)* secara garis besar terbagi menjadi kejahatan siber yang menggunakan teknologi sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas sebagai sasaran (Sutarman, 2007). Modus yang dilakukan oleh RL, HB dan KK merupakan kejahatan siber yang menggunakan teknologi sebagai fasilitias, karena RL, HB dan KK menggunakan *marketplace* sebagai fasilitas untuk memperoleh keuntungan.

Modus memanfaatkan promo *cashback* yang diberikan oleh *marketplace* Tokopedia dapat dengan mudah dilakukan oleh RL, HB dan KK karena Tokopedia merupakan *marketplace* yang menggunakan interaksi bisnis berbasis C2C atau *Consumer to Consumer*. Tokopedia merupakan *marketplace* yang menyediakan wadah untuk konsumen dapat melakukan transaksi secara langsung dengan konsumen lainnya, sehingga akan lebih mudah untuk bekerja sama memanfaatkan suatu celah karena transaksi dilakukan secara langsung antar individu. Apabila interaksi yang disediakan merupakan B2C atau *business to consumer* maka akan sulit untuk memanfaatkan suatu celah karena konsumen akan melakukan transaksi secara langsung dengan suatu perusahaan.

Tindakan yang dilakukan oleh RL, HB dan KK yaitu membuat akun lebih dari satu untuk mendapatkan *cashback* menyalahi ketentuan Tokopedia dalam bagian promosi yang mengatur bahwa Pengguna hanya boleh menggunakan 1 (satu) akun Tokopedia untuk mengikuti setiap promo Tokopedia. Jika ditemukan pembuatan lebih dari 1 (satu) akun oleh 1 (satu) pengguna yang mempunyai informasi akun yang sama dan/atau identitas pembayaran yang sama, maka pengguna tidak berhak mendapatkan manfaat dari promo Tokopedia. Tokopedia mengalami kerugian akibat tindakan yang dilakukan oleh RL, HB, dan KK yaitu dengan membuat berbagai akun fiktif hingga mendapatkan keuntungan dari promo *cashback* hingga Rp.300.000 (tiga ratus ribu rupiah) dalam tiap transaksi yang telah berjalan kurang lebih selama 5 bulan.

Pemerintah Indonesia menerbitkan UU ITE dan perubahan UU ITE untuk memberikan kepastian hukum dan melakukan penegakan hukum bagi pengguna dan penyelenggara Teknologi Informasi. UU ITE tersebut bersifat khusus sehingga dapat menjadi pedoman bagi masyarakat Indonesia dalam beraktivitas di dunia siber (Rahmanto, 2018). Berdasarkan kasus tersebut tindakan yang dilakukan oleh RL, HB, dan KK merupakan kejahatan siber oleh karena itu akibat dari tindakan tersebut dapat dikenakan UU ITE. Tindakan RL, HB dan KK merupakan tindak pidana yang memanipulasi dokumen elektronik. Berdasarkan Pasal 1 angka 1 UU ITE menyatakan bahwa:

> "Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik, telegram, teleks, *telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."

Pengertian dokumen elektronik berdasarkan Pasal 1 angka 4 UU ITE menyatakan bahwa:

> "Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimban dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol

> atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya."

Sedangkan, pengertian sistem elekronik berdasarkan Pasal 1 angka 5 UU ITE menyatakan bahwa:

> "Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik."

Berdasarkan penjelasan di atas dapat ditarik kesimpulan bahwa semua dokumen elektronik adalah informasi elektronik, dan semua informasi elektronik merupakan data elektronik (Jika A=B, dan B=C maka A=C) (Shidarta, 2018). Apabila dikaitkan dengan kronologi kasus, maka yang termasuk dokumen elektronik adalah akun Tokopedia yang dibuat oleh RL, HB, dan KK karena mereka menggunakan akun tersebut untuk bertransaksi di Tokopedia, sedangkan website Tokopedia merupakan sistem elektronik, sedangkan yang termasuk informasi elektronik merupakan Informasi di dalam akun Tokopedia yang berisi informasi seperti data diri pengguna dan *e-mail*, sedangkan data elektronik karena bersifat abstrak maka seluruh data yang ada dalam sistem elektronik merupakan data elektronik, termasuk informasi elektronik dan dokumen elektronik.

Tindakan yang dilakukan oleh RL, HB dan KK yang memanfaatkan promo *cashback* yang diberikan oleh Tokopedia merupakan kejahatan siber karena telah sesuai dengan Pasal 35 UU ITE yang menjelaskan bahwa "setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik."

Tindakan yang dilakukan oleh RL, HB, dan KK telah memenuhi unsur-unsur yang ada dalam Pasal 35 UU ITE. Unsur dalam Pasal 35 UU ITE adalah:

1. Setiap orang
   Berdasarkan kasus ini yang dimaksud dengan orang adalah RL, HB, dan KK.
2. Sengaja dan tanpa hak atau melawan hukum
   RL, HB dan KK melakukan perbuatannya dengan niat untuk mendapatkan keuntungan yang banyak dengan memanfaatkan adanya promo *cashback*. Sifat melawan hukum yang ada dalam Pasal 35 merupakan sifat melawan hukum khusus atau *special wederrechtelijkheid,* yang mencantumkan kata "melawan hukum" dalam rumusan deliknya, dengan demikian sifat melawan hukum merupakan syarat tertulis untuk dapat dipidananya suatu perbuatan (Hiariej, 2014)
3. Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik.
   RL, HB dan KK memanipulasi sistem Tokopedia dengan cara membuat banyak akun fiktif, yaitu tidak berisi informasi yang sebenarnya dengan cara membuat banyak *email* palsu. RL, HB, dan KK juga tidak mengirim barang yang seharusnya mereka kirim agar menghemat biaya ekspedisi, misalnya mengirimkan baju kaos atau bahkan paket kosong walaupun berbeda dengan apa yang diiklankan.
4. Dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Tujuan dari perbuatan RL, HB dan KK yaitu agar akun-akun yang telah dibuat dianggap seolah-olah akun yang otentik oleh sistem Tokopedia. Barang yang dikirim juga tidak sesuai dengan apa yang diiklankan dengan tujuan hanya untuk mendapatkan nomor resi yang akan dimasukkan kedalam *website* atau aplikasi Tokopedia agar proses transaksi dapat diselesaikan.

Tindakan yang telah dilakukan oleh RL, HB dan KK sesuai dengan ketentuan Pasal 35 UU ITE dengan sanksi pidana yang tercantum pada Pasal 51 ayat (1) UU ITE yang menentukan bahwa: "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000 (dua belas miliar rupiah)."

Tindakan yang dilakukan oleh RL, HB dan KK dapat diminimalisir dengan memperkuat kemanan *e-marketplace* khususnya pada bagian verifikasi data pengguna. Verifikasi data pengguna dapat dilakukan sama seperti verifikasi pembayaran, namun dengan tujuan untuk memverifikasi apakah akun milik pengguna adalah benar miliknya sendiri. Aplikasi verifikasi pembayaran adalah aplikasi yang akan menggantikan proses manusia dalam hal verifikasi pembayaran (Mulyana, 2015). Berdasarkan penjelasan tersebut dapat disimpulkan bahwa verifikasi data dapat memudahkan proses dalam memverifikasi data, seperti dengan cara verifikasi menggunakan kartu identitas, seperti KTP, SIM, maupun kartu identitas lainnya.

3. Kesimpulan

Berdasarkan uraian di atas dapat disimpulkan bahwa transaksi yang dilakukan oleh RL, HB, dan KK merupakan transaksi yang memanipulasi karena modus yang dilakukan telah sesuai dengan unsur-unsur yang ada dalam Pasal 35 UU ITE. Tindakan yang dilakukan oleh RL, HB dan KK sesuai dengan Pasal 35 UU ITE karena RL, HB dan KK dalam melakukan transaksi menggunakan banyak akun fiktif sehingga sistem dari *marketplace* Tokopedia dapat memberikan *cashbacknya* secara terus menerus. RL, HB dan KK juga memanipulasi pengiriman dengan tidak mengirimkan barang sesuai dengan yang diiklankan agar dapat memperoleh nomor resi tanpa biaya yang mahal. Akibat dari manipulasi akun dan pengiriman barang yang dilakukan oleh RL, HB dan KK maka sistem dari Tokopedia menganggap bahwa transaksi yang dilakukan merupakan transaksi yang otentik. Namun, tidak dapat dikatakan sebagai transaksi yang memanipulasi bilamana tindakan tersebut memenuhi unsur-unsur pada Pasal 35 UU ITE. Bilamana pelaku melakukan transaksi tanpa menggunakan akun palsu serta mengirimkan barang sesuai dengan yang diiklankan, maka transaksi tersebut tidak dapat dikatakan sebagai transaksi yang memanipulasi karena pelaku hanya memanfaatkan promo *cashback* tanpa menyalahi Pasal 35 UU ITE.

Modus yang dilakukan oleh RL, HB dan KK dapat dilakukan karena *e-mail* serta akun palsu dapat dengan mudah dibuat oleh setiap orang tanpa adanya verifikasi apakah yang membuat akun tersebut merupakan orang dengan identitas yang asli atau tidak, serta sistem dari *marketplace* juga tidak dapat memverifikasi tiap akun yang telah dibuat. Modus tersebut dapat diminimalisir dengan pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi yang akan memudahkan dalam proses verifikasi data, serta memperkuat sistem keamanan dari *marketplace* terutama dibidang verifikasi data pengguna e-*marketplace* tersebut.

Daftar Referensi

Buku:

Grabosky, Peter. (2007) *Electronic Crime*. Upper Saddle River: Pearson Education.

Marzuki, Peter Mahmud. (2005). *Penelitian Hukum*. Jakarta: Kencana

Soekanto, Soerjono dan Sri Mamudji. (2003). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo.

Sutarman, H. (2007). *Cyber Crime (Modus Operandi dan Penanggulangannya).* Yogyakarta: Laksbang.

Artikel Jurnal:

Hiariej, Eddy O.S. (2014). Prinsip-Prinsip Hukum Pidana. Cahaya Atma Pustaka.

Mulyana, Yana dan Peti Savitri. (2015*). Pembuatan Aplikasi Verifikasi Pembayaran dengan Metode Web Scraping Pada Pengembangan Aplikasi Penerimaan Mahasiswa Baru (Studi Kasus: Politeknik Manufaktur Negeri Bandung).* Jurnal Manajemen Informatika Universitas Komputer Indonesia, Vol. 5, No 2. Diunduh dari: https://ojs.unikom.ac.id/index.php/jamika/article/view/647

Pamungkas, Danar Putra. (2019). Rancang Bangun Sistem Verifikasi Data Dokumen. Jurnal Ilmiah Inovasi Teknologi Informasi. Vol 3 no. 2 Universitas Nusantara PGRI Kediri. Diunduh dari: http://ejournal.unhasy.ac.id/index.php/inovate/article/view/739

Pasaribu, Ana Maria F. (2007). *Kejahatan Siber Sebagai Dampak Negatif dari Perkembangan Teknologi dan Internet di Indonesia Berdasarkan Undang-Undang No.19 Tahun 2016 Perubahan Atas Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Perspektif Hukum Pidana.* Jurnal Hukum Universitas Sumatera Utara. Diunduh dari: https://jurnal.usu.ac.id/index.php/jmpk/article/download/19132/8068

Pradana, Mahir. (2015) *Klasifikasi Jenis-Jenis Bisnis E-Commerce di Indonesia.* Jurnal Neo-bis Universitas Telkom Bandung. Vol.9, No.2. Diunduh dari: https://journal.trunojoyo.ac.id/neo-bis/article/download/1271/1095

Prahassacitta, Vidya. (2019). *Konsep Kejahatan Siber dalam Sistem Hukum Indonesia.* Rubric of Faculty Members Binus University. Diunduh dari: https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Rahmanto, Tony Yuri. (2018). *Penegakan Hukum terhadap tindak Pidana Penipuan Berbasis Transaksi Elektronik*. Jurnal Penulisan Hukum De Jure, vol 19 no.1. Diunduh dari: https://ejournal.balitbangham.go.id/index.php/dejure/article/view/550/pdf_1

Artikel Internet:

Aturan Penggunaan Tokopedia.com. (2020) Diunduh dari: https://tokopedia.com/terms

Badan Siber dan Sandi Negara. (2020). Rekap Serangan Siber (Januari-April 2020). Diunduh dari: bssn.go.id/rekap-serangan-siber-januari-april-2020/

Grafik Pengguna *E-commerce* di Indonesia. (2020). Diunduh dari: https://databoks.katadata.co.id/datapublish/2021/02/11/10-e-commerce-dengan-pengunjung-terbesar-pada-kuartal-iv-2020

Shidarta. (2018). Data, Informasi, dan Dokumen Elektronik. Business-law Binus. Diunduh dari: https://business-law.binus.ac.id/2018/10/24/data-informasi-dan-dokumen-elektronik/

Peraturan Perundang-Undangan:

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik