CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 1, Mei 2020, hlm. 7-13

PELANGGARAN DATA DAN PENCURIAN IDENTITAS PADA *E-COMMERCE*

Rahmawati Nafi'ah

Magister Informatika, Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
rahmawati.nafiah@gmail.com

Abstrak

Peningkatan belanja online membuktikan bahwa teknologi memberikan dapak positif terutama dalam aspek ekonomi dan bisnis. Tidak hanya membawa manfaat, tetapi teknologi juga memberikan risiko keamanan. Banyak pihak-pihak tidak bertanggung jawab yang menyalahgunakan teknologi internet untuk berbuat kejahatan. Terkait privasi dalam transaksi online, pengguna diharuskan untuk mengungkapkan sejumlah besar informasi pribadi kepada penjual. Hal tersebut rentan dengan kebocoran informasi sensitif sehingga memicu terjadinya pelanggaran data dan pencurian identitas. Ada banyak website dan aplikasi *e-commerce* di Indonesia yang terkenal diantaranya shopee, tokopedia, bukalapak, lazada, Blibli, JD ID, Orami, Bhinneka, Socialla, dan Zalora. *E-commerce* tersebut berasal dari dalam maupun luar Indonesia. Beberapa regulasi telah dikeluarkan oleh Pemerintah untuk mengatur transaksi di *e-commerce*. Alat keamanan seperti firewal, Infrastruktur Kunci Publik (PKI), perangkat lunak enkripsi, sertifikat digital, tanda tangan digital, biometrik, kata sandi dll digunakan untuk melindungi bisnis *e-commerce*. Pada *e-commerce* terdapat beberapa level pendekatan keamanan yaitu tingkat sistem aplikasi, protokol , autentikasi keamanan dan teknologi enkripsi.

Kata kunci: *pelanggaran data, pencurian identitas, e-commerce, pendekatan keamanan.*

DATA BREACH AND IDENTITY THEFT ON E-COMMERCE

Abstract

The increase in online shopping proves that technology provides a positive impact, especially in the economic and business aspects. Not only does it bring benefits, but technology also provides security risks. Many irresponsible parties misuse internet technology to commit crimes. Regarding privacy in online transactions, users are required to disclose large amounts of personal information to the seller. This is vulnerable to the leakage of sensitive information that triggers data breaches and identity theft. There are many well-known e-commerce websites and applications in Indonesia including shopee, tokedia, bukalapak, lazada, Blibli, JD ID, Orami, Bhinneka, Socialla, and Zalora. Several regulations have been issued by the Government to regulate transactions in e-commerce. The e-commerce originates from inside and outside Indonesia. Security tools such as firewalls, Public Key Infrastructure (PKI), encryption software, digital certificates, digital signatures, biometrics, passwords etc. are used to protect e-commerce businesses. In e-commerce there are several levels of security approach, namely the application system level, protocol, security authentication and encryption technology.

Keywords: *data breaches, identity theft, e-commerce, security approaches;*

1. PENDAHULUAN

Perkembangan teknologi sekarang ini tumbuh semakin cepat. Teknologi merupakan semua sarana untuk menyediakan barang-barang yang diperlukan bagi kelangsungan dan kenyamanan hidup manusia. Teknologi yang diawali dengan adanya pengubahan sumber daya alam menjadi berbagai macam alat-alat hingga benda yang tidak berwujud seperti software.

Hal tersebut memberikan dampak kepada manusia dalam berbagai sektor seperti pada informasi, ekonomi dan bisnis. Teknologi dari berbagai macam alat seperti handphone, televisi, komputer hingga internet. Aspek ekonomi dalam penggunaan internet akan melahirkan perdagangan secara elektronik atau lebih dikenal dengan *e-commerce*.

Sebelum adanya internet dan komputer, penjual dan pembeli harus bertemu secara langsung disuatu tempat. Namun setelah adanya teknologi, kegiatan jual beli bisa dilakukan secara digital. Dengan adanya telpon genggam proses jual beli dan

mekanisme pembayaran bisa dilakukan dengan cepat dan tidak terhalang jarak dan waktu.

Terdapat peningkatan berbelanja online yang dilakukan oleh masyarakat sejak wabah pandemi Covid-19 meluas di Indonesia dan kebijakan Pembatasan Sosial Berskala Besar (PSBB) diterapkan di berbagai daerah. Perilaku konsumen paling besar yaitu dalam hal Belanja Online, dimana menurut Analytic Data Advertising (ADA) aktivitas belanja online naik 400% sejak Maret 2020 akibat pandemi ini. Hal ini dinilai menjadi momentum yang tepat bagi pemerintah untuk mengatur keberadaannya. Bank Indonesia (BI) mencatat, transaksi pembelian lewat *e-commerce* pada bulan Maret 2020 mencapai 98,3 juta transaksi. Angka itu meningkat 18,1% dibanding dengan Februari. Tak hanya itu, total nilai transaksinya pun meningkat 9,9% menjadi Rp 20,7 triliun dari bulan Februari 2020. (Safari, 2020). Peningkatan belanja online membuktikan bahwa teknologi memberikan dapak positif terutama dalam aspek ekonomi dan bisnis.

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*. Teridentifikasi empat masalah keamanan utama yang dihadapi industri *e-commerce* berdasarkan tiga kriteria; platform elektronik, pemilik, dan pengguna menurut (Kuruwitaarachchi *et al.*, 2019). Empat masalah keamanan tersebut adalah 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. Hal tersebut rentan dengan kebocoran informasi sensitif sehingga memicu terjadinya pelanggaran data dan pencurian identitas.

Pada penelitian ini, terdapat pemahaman pelanggaran data, pencurian identitas, *e-commerce* yang ada di Indonesia, contoh kasus serta upaya perlindungan data pada *e-commerce*. Pustaka penelitian ini berdasarkan sudi literatur naskah-naskah penelitian terkait pelanggaran data dan pencurian identitas pada *e-commerce*.

2. TINJAUAN PUSTAKA

2.A. Pelanggaran Data dan Pencurian Identitas

Data merupakan keterangan yang benar dan nyata atau keterangan atau bahan nyata yang dapat dijadikan dasar kajian (analisis atau kesimpulan) (*Arti kata - Kamus Besar Bahasa Indonesia (KBBI)*). Dikutip dari Roberds and Schreft (2009, p. 920*), a data breach defined as an unauthorized access of personal data recorded by organization has promoted identity theft* (Artiningsih and Sasmita, 2016). Berdasarkan hal tersebut dapat diartikan bahwa pelanggaran data didefinisikan sebagai akses tidak sah atas data pribadi yang dicatat oleh organisasi sehingga mendorong pencurian identitas. Pelanggaran data pribadi, sebagai bagian dari risiko dunia maya, di mana sejumlah besar informasi pribadi (yaitu, nama, nomor jaminan sosial, alamat, email, tanggal lahir, nomor kartu kredit, nama pengguna dan kata sandi, dll.) dikeluarkan dari organisasi, biasanya untuk digunakan dalam penipuan identitas (Wheatley, Maillart and Sornette, 2016).

Menurut KBBI, identitas adalah ciri-ciri atau keadaan khusus seseorang; jati diri. Selain itu identitas adalah suatu entitas yang berharga bagi setiap individu yang memilikinya. Dikutip dari (Rebovich, Allen and Platt, 2015) menyatakan bahwa pencurian identitas adalah tindakan menggunakan informasi pribadi milik orang lain tanpa persetujuan dari pemilik informasi asli seperti nomor jaminan sosial, nama, alamat, nomor telepon, nomor SIM atau informasi identitas lainnya untuk menyamarkan identitas mereka dan hal tersebut dapat menimbulkan berbagai kerugian. Selama masa teknologi yang lebih mudah diakses dan permintaan informasi yang tinggi, kejahatan pencurian identitas telah menjadi kejahatan yang mudah dilakukan dengan mengurangi rasa takut tertangkap atau dituntut (Mahmud, 2019).

Pencurian identitas telah berkorelasi dengan penyalahgunaan komputer, kejahatan komputer dan kejahatan terkait komputer karena Internet memfasilitasi mereka, itu disebut pencurian identitas online, misalnya adalah kasus peretas yang mencuri informasi pribadi seseorang melalui pelanggaran data online (Artiningsih and Sasmita, 2016). Pencurian data pribadi sangat mempengaruhi konsumen dan organisasi. Pencurian data dapat mengakibatkan dampak negatif langsung pada nilai saham perusahaan yang diperdagangkan serta kepercayaan konsumen pada perusahaan tersebut.

Kejahatan lintas negara merupakan bentuk kejahatan yang menjadi ancaman serius terhadap keamanan dan kemakmuran global mengingat sifatnya yang melibatkan berbagai negara. Pada tahun 2010, *Conference of States Parties* (CoSP) UNTOC yang kelima telah mengidentifikasi beberapa Kejahatan Lintas Negara Baru dan Berkembang (*New and Emerging Crimes*), antara lain *cybercrime, identity-related crimes*, perdagangan gelap benda cagar budaya, kejahatan lingkungan, pembajakan di atas laut, dan perdagangan gelap organ tubuh (*Kejahatan Lintas Negara | Portal Kementerian Luar Negeri Republik Indonesia*, 2019).

Gambar 1. *Transnational Organized Crime*

Data breach biasanya diikuti dengan *identity theft* atau pencurian identitas. *Data breach* dan *identity theft* termasuk *Transnational Organized Crime* karena bersifat lintas negara, pelaku kejahatan berkemungkinan besar berada di negara yang berbeda dengan korban.

2.B. *E-commerce*

Menurut (Varmaat, 2007) *e-commerce* atau kependekan dari *elektronik commerce* (perdagangan secara *electronic*), merupakan transaksi bisnis yang terjadi dalam jaringan elektronik, seperti internet. Siapapun yang dapat mengakses komputer, memiliki sambungan ke internet, dan memiliki cara untuk membayar barang-barang atau jasa yang mereka beli, dapat berpartisipasi dalam *e-commerce*. *E-commerce* adalah proses transaksi jual beli yang dilakukan melalui internet dimana website digunakan sebagai wadah untuk melakukan proses tersebut (Aco and Endang, 2017).

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. Pemanfaatan teknologi *e-commerce* dapat dirasakan oleh konsumen (*business to consumer*) maupun oleh pelaku bisnis (*business to business*) (Mumtahana, Hani Atun, Nita and Tito, 2017).

Electronic Commerce (*E-Commerce*) berdasarkan OECD 2009 adalah penjualan atau pembelian barang atau jasa, yang dilakukan melalui jaringan komputer dengan metode yang secara spesifik dirancang untuk tujuan menerima atau melakukan pesanan. Barang atau jasa dipesan dengan metode tersebut, tetapi pembayaran dan pengiriman utama barang atau jasa tidak harus dilakukan secara online. Transaksi *E-Commerce* dapat terjadi antar usaha, rumah tangga, individu, pemerintah, dan organisasi swasta atau publik lainnya. Pemesanan yang termasuk *e-commerce* adalah yang melalui halaman website, ekstranet maupun EDI (Electronic Data Interchange), email, media sosial (facebook, instagram, dan lainnya), serta instant messaging (whatsapp, line, dan lainnya). Pemesanan yang tidak termasuk *e-commerce* adalah yyang dibuat melalui telepon, faksimili (Rozama; *et al.*, 2019).

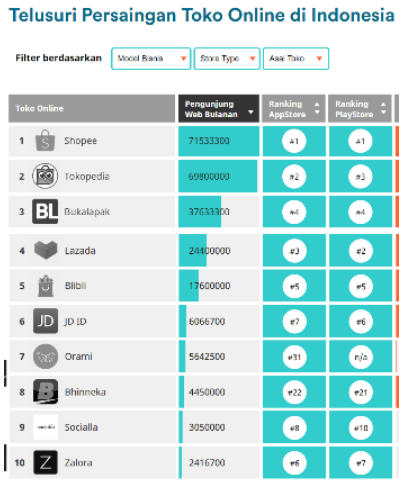
E-commerce yang ada di Indonesia berdasarkan pernyataan memang banyak jenisnya, dan yang akan dibahas pada penelitian ini adalah dalam bentuk website serta aplikasi. Menurut Badan Pusat Statistik, website adalah suatu halaman web yang saling berhubungan yang umumnya berisikan kumpulan informasi berupa data teks, gambar, animasi, audio, video maupun gabungan dari semuanya yang biasanya dibuat untuk personal, organisasi dan perusahaan (Rozama; *et al.*, 2019).

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 (*Pengertian Aplikasi*, 2016).

3. PEMBAHASAN

3.A. *E-commerce* di Indonesia

Ada banyak website dan aplikasi *e-commerce* di Indonesia. Sebagian besar usaha ecommerce menggunakan website dan aplikasi terkenal. Gambar 2 menunjukan peta *E-commerce* Indonesia mengurutkan pemain besar *e-commerce* berdasarkan rata-rata pengunjung website di setiap kuartal, ranking aplikasi, pengikut media sosial, dan jumlah karyawan (*Daftar 50 Website & Aplikasi E-Commerce di Indonesia 2019*, 2020).



Gambar 2. Peta *E-commerce* Indonesia Q1 2020

Pada halaman iprice.co.id hanya ditunjukkan website dan aplikasi ecommerce terbesar yang ada di indonesia. Selain nama-nama yang ada didaftar masih banyak lagi *e-commerce* yang ada di indonesia namun biasanya hanyak dalam bentuk website saja. Sepuluh daftar ecommerce terbaik dalam bentuk website dan aplikasi di kuartal 1 tahun 2020 yaitu shopee, tokopedia, bukalapak, lazada, Blibli, JD ID, Orami, Bhinneka, Socialla, Zalora. Toko yang berasal dari Indonesia sendiri adalah Tokopedia, Bukalapak, Blibli, Bhinneka,

Shocialla. Sedangkan yang berasal dari Internasional adalah Shopee, Lazada, JD ID, Orami, Zalora.

Pengunjung web dari Toko terpopuler yaitu Shopee mencapai 71.533.300 per bulan. Sedangkan pengunjung toko lewat aplikasi tidak terhitung, dan tingkat kepopuleran melalui media sosial juga cukup tinggi.

Gambar 3. Peta *E-commerce* Indonesia Q1 2019

Pada kuartal 1 tahun 2019 terlihat pengunjung web tokopedia mencapai 137.200.900 per bulan. Perbedaan jumlah pengunjung yang sangat jauh jika dibandingkan dengan peringkat 1 di tahun 2020. Banyaknya media komunikasi, aplikasi dan mudahnya akses internet membuat membuat konsumen *e-commerce* meningkat. Bentuk pembayaran dari *e-commerce* ini juga beragam. Model yang paling banyak digunakan adalah COD/ Cash On Delivery atau pembeli bisa membayar pesanan secara tunai pada saat pesanan tiba di tujuan. Selain COD ada pembayaran melalui transfer bank, kartu kredit, mobile money dan lain-lain.

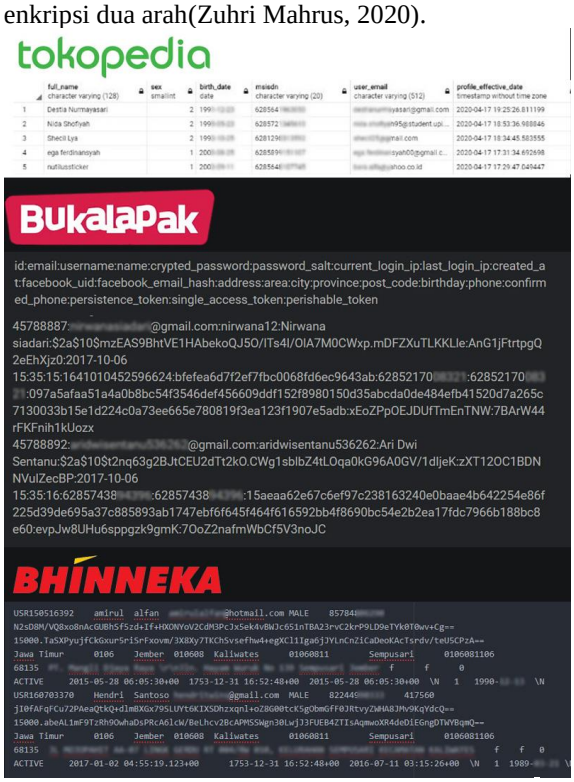
3.B. Contoh Kasus

Pada bulan Mei 2020, Indonesia dikejutkan dengan berita tentang upaya pelanggaran data dari 3 *e-commerce*. Berdasarkan (Zuhri Mahrus, 2020) kasus pelanggaran data dan pencurian identitas yang terjadi :

a. Pada tanggal 1 Mei muncul berita mengenai kebocoran data pengguna Tokopedia. Sebanyak 91 juta data yang dilaporkan sebagai data pengguna Tokopedia ditawarkan seharga US$5.000 di forum hacker. Dalam rilis resminya, Tokopedia menyatakan bahwa mereka "menemukan adanya upaya pencurian data terhadap pengguna Tokopedia."
b. Pada tanggal 6 Mei, sebanyak 12,9 juta data pengguna Bukalapak kembali diperjualbelikan. Data ini diduga merupakan data yang bocor pada Maret 2019. Sementara Bukalapak mengakui adanya akses tidak sah terhadap cold storage mereka (rilis Bukalapak).
c. Pada 10 Mei , sebanyak 1,2 juta data yang diduga data pengguna toko online Bhinneka diketahui bocor dan ditawarkan untuk dijual di forum pasar gelap online (dark web). Bhinneka menyatakan masih melakukan investigasi terhadap dugaan kebocoran tersebut.

Ketiga perusahaan ini menyatakan bahwa tidak ada data transaksi yang dibobol, data finansial tetap aman. Namun, data pribadi pengguna seperti tanggal lahir, alamat email, nomor telepon, bahkan alamat lengkap muncul sebagai teks tanpa enkripsi.

Ketiga perusahaan telah melindungi akun penggunanya dengan melakukan hashing terhadap password. Berdasarkan gambar 3, Tokopedia diduga menggunakan SHA384 sementara Bukalapak menggunakan algoritma SHA512 dan salt atau Bcrypt. Pada Bhinneka, password pengguna tampak seperti teks berformat Base64 encode atau hasil enkripsi dua arah(Zuhri Mahrus, 2020).



Gambar 4. Sampel data pengguna yang dibocorkan hacker

Ancaman utama terhadap keamanan *e-commerce* yang terlihat berpotensi menghancurkan tidak hanya bagi pelaku usaha tetapi juga konsumen. Pada contoh kasus pelaku usaha sudah cukup bagus dalam melindungi akun penggunanya namun kurang memperhatikan data pribadi penggunanya dengan tidak memberikan enkripsi.

3.C. Regulasi Pemerintah

Di Indonesia sudah ada undang-Undang perdagangan dan perlindungan konsumen. Dalam konteks hukum perlindungan konsumen yang berlaku di Indonesia, yaitu UU No 8 Tahun 1999 tentang Perlindungan Konsumen, hak dan kewajiban konsumen dan pelaku usaha telah diatur dengan jelas dan tegas. Untuk hak dan kewajiban konsumen diatur dalam Pasal 4 dan 5 UU No 8 Tahun 1999, sedangkan untuk hak dan kewajiban pelaku usaha diatur dalam Pasal 6 dan 7 UU No 8 tahun 1999. Dalam pasal-pasal tersebut diatur bagaimana proporsi atau kedudukan konsumen dan pelaku

usaha dalam suatu mekanisme transaksi bisnis atau perdagangan. Aspek tanggung jawab pelaku usaha dalam UU No 8 Tahun 1999 diatur dalam Pasal 19 sampai dengan Pasal 28. Aspek ini berlaku pada saat pelaku usaha melakukan perbuatan yang menyebabkan kerugian bagi konsumen (Paryadi, 2018).

Beberapa regulasi telah dikeluarkan oleh Pemerintah untuk mengatur transaksi di *e-commerce* dalam rangka melindungi konsumen, seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) dan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) serta peraturan turunan yang menguatkan hal-hal yang belum diatur. "Perdagangan Melalui Sistem Elektronik (*e-commerce*) yang selanjutnya disingkat PMSE adalah Perdagangan yang transaksinya dilakukan melalui serangkaian perangkat dan prosedur elektronik" merupakan bunyi dari pasal 1 ayat 2 (Republik Indonesia, 2019).

Pengaturan mengenai perlindungan terhadap data pribadi dibahas lebih lengkap dalam bab XI. Pasal 59 ayat 2 poin g menyatakan bahwa pihak yang menyimpan data pribadi harus mempunyai 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. Sehingga pelaku usaha wajib menyimpan data pribadi sesuai dengan standar perlindungan data pribadi.

3.D. Perlindungan Data

Data pribadi dapat bocor jika PSE (Penyelenggara Sistem Elektronik) tidak peduli dengan kewajiban regulasi, rendahnya awareness pimpinan organisasi tentang pentingnya pelindungan data pribadi, ketidaktahuan pegawai (internal threat) karena tidak mendapat training yang cukup, kesengajaan pengawai untuk mengumpulkan/ mencuri data untuk kepentingan pribadi dan kapasitas attacker yang melebihi kemampuan sistem pengamanan data yang diterapkan." (Safari, 2020).

Tata kelola dan manajemen berfungsi dengan baik jika didasarkan pada serangkaian kebijakan, proses, dan pelatihan yang cerdas, dikembangkan oleh empat pemangku kepentingan utama dalam bidang organisasi jaringan : TI, SDM, manajemen eksekutif, dan pengguna(Lawrence C. Miller, 2016). Pemerintah perlu menegakkan regulasi yang mengatur transaksi *e-commerce* dan bekerja sama dengan tim manajemen tersebut. Diperlukan pelatihan kepada pegawai untuk mengetahui risiko dan mewaspadai kemungkinan serangan.

Dari aspek IT, dalam keamanan front-end server *e-commerce* harus dilindungi terhadap akses yang tidak sah, sistem back-end harus dilindungi untuk memastikan privasi, kerahasiaan, integritas data dan jaringan perusahaan harus dilindungi terhadap intrusi. Alat keamanan yang berbeda seperti firewal, Infrastruktur Kunci Publik (PKI), perangkat lunak enkripsi, sertifikat digital, tanda tangan digital, biometrik, kata sandi dll digunakan untuk melindungi bisnis *e-commerce*. Berikut ini adalah berbagai pendekatan keamanan di berbagai level dalam *e-commerce* (Shaikh, Babar and Iliev, 2017) (Chaudhary, Ahmad and Rizvi, 2014):

a. Tingkat Sistem Aplikasi
   Pada tingkat aplikasi, fitur keamanan seperti kerahasiaan, integritas, ketersediaan, Non-repudiation dan anonimitas. Fitur tersebut dipertimbangkan dengan berbagai cara teknik enkripsi, tanda tangan digital dll.
b. Tingkat Protokol Keamanan
   Ada dua protokol yang terkait yaitu : Secure Socket Layer (SSL) dan Secure Electronic Transaction (SET). SSL adalah lapisan protokol yang ada antara lapisan berorientasi koneksi (TCP / IP) dan lapisan aplikasi (HTTP). TCP menyediakan layanan ujung ke ujung yang dapat diandalkan yang digunakan oleh SSL. TCP menjalin komunikasi aman antara klien dan server menggunakan enkripsi dan tanda tangan digital. SET adalah standar protokol komunikasi dan protokol spesifikasi enkripsi dan keamanan untuk mengamankan transaksi kartu kredit dalam jaringan terbuka yang disebut Internet selama transaksi *E-commerce*. SET juga menyediakan privasi dan perlindungan untuk memastikan keaslian transaksi elektronik.
c. Tingkat Autentikasi Keamanan
   Teknik digunakan ntuk menjaga keamanan pada tingkat otentikasi yaitu penggunaan intisari pesan, tanda tangan digital, dan penggunaan standar enkripsi dan dekripsi yang berbeda.
d. Tingkat Teknologi Enkripsi
   Teknologi enkripsi menyediakan komunikasi yang aman melalui jaringan yang tidak aman. Teknik enkripsi mengkodekan teks biasa ke bentuk yang tidak dapat dibaca (teks sandi) yang membantu melindungi data agar tidak dilihat oleh orang yang tidak berwenang. Enkripsi kunci simetris / pribadi menggunakan kunci yang sama untuk enkripsi dan dekripsi. Enkripsi kunci asimetris / publik menggunakan dua kunci, satu untuk metode enkripsi dan satu lagi untuk metode dekripsi. Satu kunci adalah Publik dan yang kedua adalah pribadi.

Pada transaksi *e-commerce* ada sejumlah sistem dan jaringan yang terlibat. Masing-masing memiliki beberapa masalah, prioritasnya back-end dan basis data harus memiliki keamanan yang kuat. Karena situs server dapat melemahkan jaringan

internal perusahaan. Kelemahan ini memungkinan pencurian identitas pelanggan atau data perusahaan.

4. KESIMPULAN

Berdasarkan pembahasan pustaka dari beberapa sumber, bisa disimpulkan bahwa pelanggaran data dan pencurian identitas pada *e-commerce* merupakan tantangan bersama. Berbagai teknologi alat keamanan digunakan untuk mengatasi ancaman pelanggaran data dan pencurian identitas. *E-commerce* telah berkembang selama bertahun-tahun, namun masalah keamanan data masih terjadi. Diperlukan solusi yang mampu memperkuat sistem hukum dan manajemen yang ada. Perlu ditingkatkan juga teknik kriptografi yang lebih canggih agar kemanan data bisa terjaga.

Selama data pribadi pelanggan maupun data perusahaan *e-commerce* mudah diakses maka kejahatan pelanggaran data dan pencurian identitas akan menjadi kejahatan yang mudah dilakukan. Serta lemahnya penegakan hukum akan mengurangi rasa takut tertangkap atau dituntut. Pemerintah harus menegakan peraturan yang ada dan menambahkan peraturan yang belum diatur. Pemerintah juga harus melindungi dan menjamin masyarakat dari kemungkinan yang timbul. Dengan adanya perlindungan, maka kekhawatiran akan tekanan/ancaman dari luar akan berkurang dan pertumbuhan ekonomi nasional akan semakin maju.

DAFTAR PUSTAKA

ACO, A. AND ENDANG, A. H. (2017) 'Analisis Bisnis E-Commerce pada Mahasiswa Universitas Islam Negeri Alauddin Makassar', *Jurnal Insypro*, 2, pp. 1–13. Available at: http://journal.uin-alauddin.ac.id/index.php/insypro/article/view/3246.

Arti kata - Kamus Besar Bahasa Indonesia (KBBI) Online (no date). Available at: https://kbbi.web.id/ (Accessed: 10 June 2020).

ARTININGSIH, A. AND SASMITA, A. S. (2016) 'Data Breaches and Identity Theft: A Case Study of U.S. Retailers and Banking', *Journal Paramadina*, 13, pp. 1476–1496. Available at: http://journal.paramadina.ac.id/index.php/upm/article/view/112/65.

CHAUDHARY, A., AHMAD, K. AND RIZVI, M. A. (2014) 'E-commerce security through asymmetric key algorithm', *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, (April), pp. 776–781. doi: 10.1109/CSNT.2014.163.

Daftar 50 Website & Aplikasi E-Commerce di Indonesia 2019 (2020). Available at: https://iprice.co.id/insights/mapofecommerce/ (Accessed: 10 June 2020).

Kejahatan Lintas Negara | Portal Kementerian Luar Negeri Republik Indonesia (2019). Available at: https://kemlu.go.id/portal/id/read/89/halaman_list_lainnya/kejahatan-lintas-negara (Accessed: 10 June 2020).

KURUWITAARACHCHI, N. *ET AL.* (2019) 'A Systematic Review of Security in Electronic Commerce- Threats and Frameworks', *Global Journal of Computer Science and Technology*, 19(1), pp. 33–39. doi: 10.34257/gjcstevol19is1pg33.

LAWRENCE C. MILLER, C. (2016) *Cybersecurity For Dummies®, Palo Alto Networks 2nd Edition*. John Wiley & Sons, Inc.

MAHMUD, R. (2019) 'Identity Theft Categories & Cases', 2(1), pp. 38–42. doi: http://dx.doi.org/10.14421/csecurity.2019.%25x.

MUMTAHANA, HANI ATUN, NITA, S. AND TITO, A. W. (2017) 'khazanah informatika Pemanfaatan Web E-Commerce untuk Meningkatkan Strategi Pemasaran', *Pemanfaatan Web E-Commerce untuk Meningkatkan Strategi Pemasaran*, 3(1), pp. 6–15. Available at: http://journals.ums.ac.id/index.php/khif/article/view/3309/2784.

PARYADI, D. (2018) 'Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen', *Jurnal Hukum & Pembangunan*, 48(3), p. 652. doi: 10.21143/jhp.vol48.no3.1750.

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

REBOVICH, D. J., ALLEN, K. AND PLATT, J. (2015) 'The New Face of Identity Theft'. Available at: https://www.utica.edu/academic/institutes/cimip/New_Face_of_Identity_Theft.pdf.

Republik Indonesia (2019) 'Regulation of The Government No.80 of 2019', *Government Regulation*, 80(019092), p. 61.

ROBERDS, W. AND SCHREFT, S. L. (2009) 'Data breaches and identity theft', *Journal of Monetary Economics*, 56(7), pp. 918–929. doi: https://doi.org/10.1016/j.jmoneco.2009.09.003.

ROZAMA;, N. A. *ET AL.* (2019) *Statistik E-Commerce 2019*. Jakarta: Badan Pusat Statistik.

SAFARI, A. (2020) *Aktualisasi Hak Atas Kenyamanan, Keamanan dan Keselamatan*

dalam Bertransaksi Melaluie-Commerce. Available at: https://www.bpkn.go.id/posts/show/id/1634.

SHAIKH, J. R., BABAR, S. D. AND ILIEV, G. (2017) 'E-commerce Development with Respect to its Security Issues and Solutions : A Literature Review', *ICEST*, (June 2017), pp. 165–168. Available at: http://icestconf.org/wp-content/uploads/2018/02/ICEST2017.pdf.

VARMAAT, S. C. (2007) *Discovering Computers: Menjelajah Dunia Komputer Fundamental Edisi 3*. Jakarta: Salemba Infotek.

WHEATLEY, S., MAILLART, T. AND SORNETTE, D. (2016) 'The extreme risk of personal data breaches and the erosion of privacy', *European Physical Journal B*, 89(1), pp. 1–12. doi: 10.1140/epjb/e2015-60754-4.

ZUHRI MAHRUS (2020) *OPINI : Kebocoran Data Pengguna Tokopedia, Bukalapak, dan Bhinneka: Siapa Peduli?*, *https://cyberthreat.id/*. Available at: https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli (Accessed: 17 June 2020).