

## CYBERCRIME DAN DAMPAKNYA PADA TEKNOLOGI E-COMMERCE

Siti Kurnia Rahayu<sup>1</sup>, Siti Ruqoyah<sup>2</sup>, Sanniyah Berliana<sup>3</sup>,  
Sekar Budi Pratiwi<sup>4</sup>, Herry Saputra<sup>5</sup>

Departemen Akuntansi<sup>1,2,3,4</sup> Departemen Sistem Informasi<sup>5</sup>  
Universitas Komputer Indonesia<sup>1,2,3,4,5</sup>

Siti.kurnia@email.unikom.ac.id<sup>1</sup>

Siti.21118030@mahasiswa.ac.id

Sanniy.21118011@mahasiswa.ac.id

Sekar.21118025@mahasiswa.ac.id

Correspndent Email: herryhs222@gmail.com

**Received:** June 9,2021; **Revised:** June 28, 2021; **Accepted:** July 15, 2021 **Page:** 632-637

**Abstrak:** Penelitian ini bertujuan untuk menginformasikan kepada pengguna *e-commerce* tentang keberadaan *cybercrime* dan dampak dari *cybercrime* pada aplikasi *e-commerce*. *Cybercrime* adalah kejahatan yang dilakukan secara online. Banyak contoh kasus *cybercrime* yang terjadi, salah satunya di dunia *e-commerce*. Penelitian ini menggunakan data primer. Sedangkan metode analisis data yang digunakan adalah kuantitatif dengan menggunakan skala likert. Populasi penelitian ini sebanyak 55 responden yang terdiri dari mahasiswa dan masyarakat sebagai sampel penelitian, dengan menggunakan Google Form. Hasil penelitian ini menunjukkan bahwa pengguna *e-commerce* sudah mengetahui dampak *cybercrime* pada *ecommerce*. Perilaku *cybercrime* masih sulit diantisipasi. Mengetahui dampak dari pengguna *ecommerce* sekarang lebih waspada terhadap kejahatan ini. Disarankan kepada pengguna *ecommerce* agar lebih selektif dalam menggunakan aplikasi *e-commerce* dan pihak *e-commerce* agar memiliki sistem pengamanan yang lebih tinggi untuk mencegah terjadinya *cybercrime*.

**Kata kunci:** Cybercrime, E-commerce, Penjualan, Aplikasi

**Abstract:** This study aims to inform *e-commerce* users about the existence of *cybercrime* and the impact of *cybercrime* on *e-commerce* applications. *Cybercrime* is a crime that is committed online. There are many examples of *cybercrime* cases that occur, one of which is in the world of *e-commerce*. This study used primary data. Moreover, the data analysis method used is quantitative using a Likert scale. This study population was as many as 55 respondents consisting of students and the public as research samples, using Google Form. The results of this study indicate that *e-commerce* users already know the impact of *cybercrime* on *ecommerce*. *Cybercrime* behavior is still difficult to anticipate. Knowing the impact of *ecommerce* users is now more aware of these crimes. It is suggested for *e-commerce* users to be more selective in using *e-commerce* applications and *e-commerce* parties to have more high-security systems to prevent *cybercrime* from happening.

**Keywords:** Cybercrime, E-commerce, Sales, Application



## I. PENDAHULUAN

Kemajuan dan perkembangan teknologi internet saat ini menjadi salah satu acuan dalam menilai keberhasilan atau kegagalan semua perilaku manusia modern di hampir semua bidang kehidupan. Salah satu bidang yang terkena dampak paling signifikan adalah sektor bisnis yang mulai merambah media online, dimana melalui media online penggunaannya dapat menyajikan informasi dengan mudah dan cepat. Pemanfaatan teknologi internet dalam dunia bisnis lebih dikenal dengan istilah perdagangan elektronik atau *e-commerce*. *Ecommerce* merupakan aktivitas bisnis yang memberikan akses kepada semua pengguna untuk memudahkan aktivitas jual beli [1].

Selain peningkatan teknologi dalam *e-commerce*, teknologi internet tidak lepas dari teknologi *ecommerce* yaitu teknologi internet di bidang perbankan. Teknologi di bidang ini juga mengalami perubahan yang sangat signifikan. Namun penerapan teknologi ini tidak diimbangi dengan tingkat keamanan yang tinggi. Teknologi ini masih sangat rentan terhadap aktivitas kriminal seperti skimming, hacking, dan malware. Oleh karena itu, diperlukan adanya inovasi pada tingkat keamanan sistem perbankan untuk melindungi dan mencegah terjadinya tindak pidana dalam transaksi elektronik [2].

Dengan adanya sistem transaksi dalam *e-commerce* yang digunakan pengguna aplikasi untuk mendapatkan barang yang diinginkan, pengguna juga harus menanggung banyak risiko yang ditimbulkan oleh *e-commerce* itu sendiri, salah satunya adalah *cybercrime* [3]. *Cybercrime* adalah istilah untuk kejahatan yang menggunakan komputer untuk perampokan dan tindakan kriminal. Daftar kejahatan dunia maya yang semakin meningkat mencakup kejahatan komputer, misalnya, penyebaran intrusi jaringan dan virus komputer. Selain itu, varian kejahatan yang tak terbantahkan berbasis komputer dapat berupa pencurian, penguntitan, intimidasi, dan pemaksaan. Sejak teknologi memainkan peran penting dalam kehidupan sehari-hari masyarakat dengan perkembangan teknologi, kejahatan dunia maya akan meningkat [4].

Selain itu terdapat kendala dalam penerapan *e-commerce* yaitu kurangnya sumber daya manusia dan rendahnya kepercayaan terhadap tingkat keamanan *e-commerce* [3]. Dampak besar mengintai semua orang yang menggunakan Internet, *e-commerce*, teknologi baru, dan platform seluler [5]. *Cybercrime* telah menimbulkan ketakutan di benak banyak orang yang telah aktif menggunakan *e-commerce* [6]. *Cybercrime* berdampak tidak langsung pada dunia bisnis global. Pemerintah dan organisasi juga membuat ketentuan untuk mencegah dan mengembangkan kejahatan dunia maya [7]. Tidak hanya terjadi di negara lain, *cybercrime* juga terjadi di Indonesia, bahkan sudah ada sejak masuknya teknologi internet ke Indonesia. Jumlah pengguna internet di Indonesia hanya 14,5 juta dari total penduduk yang hampir 220 juta. Meski kurang dari 10%, Indonesia menempati urutan pertama dalam kasus *cybercrime*. Meski pada 2007, posisinya turun ke urutan keempat, setelah Ukraina dan beberapa negara di Eropa Timur yang mencatat kasus *cybercrime* lebih tinggi [8].

*Cybercrime* sendiri merupakan ancaman bagi dunia yang dapat menimbulkan kerugian yang minimal. Total kerugian akibat *cybercrime* yang terjadi pada *e-commerce* di Indonesia setiap tahunnya mencapai \$ 1,5 triliun. Pemerintah Indonesia secara serius mempersiapkan hal-hal yang diperlukan untuk mencegah kejahatan tersebut, misalnya masalah ITE, sistem yang diperlukan, dan instansi terkait. Undang-undang yang mengatur hal tersebut antara lain Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Ada pula Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Menurut Kementerian Informasi dan Informasi, terdapat pula Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik di Penyelenggaraan Negara, dan Permen Kominfo Nomor 7 Tahun 2018 Pelaksanaan pemetaan manajemen dapat menggunakan indeks BSSN dan penerapan Standar, ISO 270001, IDSS, dan OSO. Meski sudah ada undang-undang seperti diuraikan di atas, penegakan hukum terhadap pelaku *cybercrime* masih minim. Hal ini membuat kejahatan dunia maya masih bebas di Indonesia. Masalah regulasi dan hukum di Indonesia harus lebih tegas untuk menyelesaikan masalah *cybercrime* di dunia bisnis digital saat ini [9].

Penelitian ini bertujuan untuk menginformasikan kepada pengguna *e-commerce* tentang keberadaan *cybercrime* dan dampak dari *cybercrime* pada aplikasi *e-commerce*. Kuesioner yang akan digunakan adalah Kuesioner Use, yang memiliki beberapa aspek yaitu efisiensi, efektivitas, dan kepuasan. Kuesioner ini dibuat dalam bentuk skor lima poin dengan menggunakan model skala likert.

## II. METODE



**2.1. Populasi dan Sampel**

Sesuai dengan tujuan penelitian, maka dalam penelitian dengan standar tertentu, populasi dalam penelitian ini sebanyak 55 responden mahasiswa dan masyarakat yang menggunakan *e-commerce*.

**2.2. Data Pengumpulan Data**

Data primer diperoleh dengan menyebarkan kuesioner melalui Google Forms untuk memperoleh data. Dalam penelitian ini digunakan metode skala likert. Skala likert merupakan alat untuk mengukur atau mengumpulkan data dengan menggunakan metode pengukuran dan balancing [10]. Pemeringkatan skala likert dimulai dari 1 sebagai peringkat terendah, yang sangat berbeda, kemudian 5 sebagai peringkat tertinggi, yang sangat setuju. Peringkat skala likert dijelaskan pada Tabel 1.

Tabel 1. Rating Skala Likert

Description	Likert Scale
Sangat Setuju	5
Setuju	4
Ragu-ragu	3
Tidak setuju	2
Sangat Tidak Setuju	1

Hasil dari perhitungan komponen sistem akan dikategorikan berdasarkan kriteria tertentu. Untuk menghasilkan nilai akhir setiap komponen digunakan rumus sebagai berikut:

$$Index\ formula\% = \frac{Skor\ Total}{Y} \times 100 \dots\dots\dots Persamaan\ 1$$

Y = Skor Likert Tertinggi x Jumlah Responden (Nomor 5 teratas) "Catat Nilai Bobot"

X = Skor Likert terendah x Jumlah Responden (Nomor 1 terendah) "Catat Nilai Bobot"

Persentase nilai dimulai dari 0% - 19,99% karena sangat tidak setuju, kemudian 20% - 39,99% karena sangat setuju. Persentase nilai dijelaskan pada Tabel 2:

Table 2. Persentase Nilai [10]

Respon	Penjelasan
0% - 19.99%	Sangat Tidak Setuju
20% - 39.99%	Tidak Setuju
40% - 59.99%	Ragu-ragu
60% - 79.99%	Setuju
80% - 100%	Sangat Setuju

**III. HASIL DAN PEMBAHASAN**

Dalam penelitian ini, kami membagikan kuisisioner yang berisi 15 pertanyaan kepada mahasiswa dan masyarakat umum yang disebarkan menggunakan media Google Forms. Pengguna mengisi kuisisioner yang telah dibagikan berdasarkan pengalamannya saat menggunakan aplikasi *e-commerce*. Setiap pertanyaan dalam kuisisioner bertujuan untuk melihat apakah pengguna *e-commerce* mengetahui dampak *cybercrime* pada aplikasi *e-commerce*, kemudian dievaluasi dengan menggunakan skala likert.

Total skor tertinggi untuk item sangat setuju adalah 5 x 55 = 275, sedangkan item sangat tidak setuju adalah 1 x 55 = 55. Oleh karena itu, jika total skor responden adalah 275, maka penjelasan responden atas pertanyaan kuisisioner adalah hasil dari nilai yang dihasilkan dengan rumus Indeks (%). Setelah menyebarkan kuisisioner kepada 55 responden, hasil kuisisioner tersebut direview. Hasil kuisisioner dijelaskan pada Tabel 3.



Tabel 3. Rekap Nilai

No.	Pertanyaan	Nilai
1	Penggunaan <i>E-commerce</i> membuat komunikasi antara produsen dan konsumen menjadi lebih mudah	88.3%
2	Menggunakan <i>E-commerce</i> memudahkan dalam menjual atau membeli barang	87.2%
3	Menggunakan <i>E-commerce</i> memudahkan untuk mempromosikan barang dan jasa.	86.5%
No.	Pertanyaan	Nilai
4	Penggunaan <i>E-commerce</i> memudahkan dalam melakukan transaksi pembayaran	85.8%
5	Transaksi melalui <i>E-commerce</i> Aman Untuk melakukan pembayaran	75.6%
6	Banyaknya Kejahatan Cyber menimpa <i>E-commerce</i>	73.8%
7	Terjadinya kejahatan seperti melakukan transaksi tidak melalui aplikasi <i>E-commerce</i>	76%
8	Terjadinya kejahatan seperti carding atau seseorang menggunakan kartu kredit orang lain untuk melakukan transaksi online	75.4%
9	<i>Cybercrime</i> yang terjadi ibarat bocornya data pengguna <i>e-commerce</i>	80.7%
10	Kejahatan seperti menyebarkan virus ke Aplikasi <i>E-commerce</i> atau sistem	71.3%
11	<i>Cybercrime</i> berdampak pada saat membeli dan mentransfer uang, namun barang tidak sesuai / barang tidak sampai	74.5%
12	<i>Cybercrime</i> berdampak pada saat membeli dan mentransfer uang, namun barang tidak sesuai / barang tidak sampai	86.2%
13	<i>Cybercrime</i> berdampak pada saat membeli dan mentransfer uang, namun barang tidak sesuai / barang tidak sampai	73.8%
14	Pihak <i>E-commerce</i> menambahkan sistem keamanan untuk melakukan transaksi pembayaran	89.8%
15	Menambahkan perlindungan bagi pengguna <i>E-commerce</i> secara legal	90.9%

Penelitian ini menunjukkan bahwa penggunaan *e-commerce* memberikan kemudahan dalam komunikasi antara produsen dan konsumen. Responden memberikan tanggapan bahwa waktu yang dibutuhkan lebih efisien dengan *e-commerce* (skor 88,3%). Penggunaan *e-commerce* juga memudahkan untuk membeli dan menjual barang. Tanggapan responden sebesar 87,2% menunjukkan bahwa keefektifan transaksi lebih efektif dengan penggunaan *e-commerce*. Penggunaan *e-commerce* dalam hal promosi termasuk dalam kategori mempermudah kegiatan. Skor tanggapan responden sebesar 86,5% artinya promosi melalui *e-commerce* sangat menguntungkan. Calon pembeli dapat dengan mudah melihat dan mengetahui spesifikasi barang dengan cepat dan membandingkannya dengan produk lain dengan cepat. *E-commerce* merupakan aktivitas bisnis yang memberikan akses kepada semua pengguna untuk memudahkan aktivitas jual beli [1].

*E-commerce* memberikan kemudahan dalam transaksi pembayaran. Responden memberikan respon sebesar 85,8% yang menunjukkan bahwa penggunaan *e-commerce* memudahkan transaksi pembayaran. Ini karena *e-commerce* terhubung dengan berbagai platform pembayaran untuk memberikan kemudahan dalam setiap detail transaksi pembayaran. Efektivitas dan efisiensi penggunaan *e-commerce* belum menunjukkan keamanan konsumen dalam melakukan transaksi pembayaran. Hasil tanggapan responden menunjukkan skor 75,6%. Artinya masih ada sebagian konsumen yang merasa tidak aman dalam melakukan transaksi pembayaran dengan menggunakan *e-commerce*. Rasa tidak aman ini muncul karena masih adanya tindakan *Cybercrime* yang dapat terjadi pada aplikasi *e-commerce*. Berdasarkan hasil penelitian ditemukan bahwa 73,8% responden sudah mengetahui bahwa *Cybercrime* terjadi di *e-commerce*. Sebagian besar responden menyadari ketidakamanan dalam menggunakan transaksi pembayaran *e-commerce* karena mengetahui bahwa peristiwa *Cybercrime* sering terjadi di *e-commerce*. Hal tersebut didukung oleh tanggapan responden selanjutnya bahwa *Cybercrime* terjadi tidak hanya melalui aplikasi *e-commerce*. 76% responden memberikan tanggapan bahwa *Cybercrime* juga bisa terjadi tidak melalui *e-commerce*. Sisanya menjawab bahwa *Cybercrime* terjadi melalui penggunaan aplikasi *ecommerce*. Penerapan teknologi ini tidak diimbangi dengan tingkat keamanan yang tinggi. Teknologi ini masih sangat rentan terhadap aktivitas kriminal seperti skimming, hacking, dan malware. Oleh karena itu, diperlukan adanya inovasi pada tingkat keamanan sistem perbankan untuk melindungi dan mencegah terjadinya tindak pidana dalam transaksi elektronik [2].



Kejahatan Cyber atas penggunaan kartu kredit orang lain untuk transaksi online sering terjadi dalam penggunaan *e-commerce*. Skor 75,4%, dalam hal ini, menunjukkan tanggapan responden. Kejahatan ini tentunya dapat menimbulkan kerugian materi yang cukup besar karena selain nilai rupiah yang material, kerugian juga bisa timbul. Bagaimanapun, kerahasiaan data pribadi diungkapkan. Penyalahgunaan informasi pribadi oleh seseorang yang tidak bertanggung jawab. Responden memberikan tanggapan dengan skor 80,7% atas kebocoran data pengguna *e-commerce* sebagai bagian dari tindakan *Cybercrime*. Hal ini menunjukkan bahwa sebagian besar responden pengguna *e-commerce* mengetahui kebocoran data dalam *Cybercrime* melalui *e-commerce*. Perilaku *Cybercrime* dapat merugikan dan sangat memengaruhi ketidakamanan pengguna. Kejahatan terkait ketidakamanan penggunaan *e-commerce* juga dapat terjadi dengan menyebarkan virus ke aplikasi *e-commerce*. Skor tanggapan responden menunjukkan nilai 71,3%. Responden yang dapat muncul di aplikasi *e-commerce* dan mengetahui penyebaran virus ini tentunya memberikan rasa tidak aman bagi pengguna *e-commerce*. Perilaku *cybercrime* dapat merusak sistem *e-commerce*. Kejahatan dalam *e-commerce* juga terjadi pada ketidaksesuaian antara barang dan harga, baik kualitas maupun ketepatan waktu pembayaran versus penerimaan barang. Responden memberikan tanggapan dengan total skor 74,5%. Besarnya skor ini berarti pengguna *ecommerce* mengalami waktu yang cukup dan kehilangan barang selama penggunaan *e-commerce* dalam transaksi pembelian. Pengguna *e-commerce* atau konsumen merasakan kerugian, seperti waktu yang terpakai selama proses pembelian online dan ternyata produk atau layanan tersebut tidak sesuai ekspektasi. Semua pengguna mengetahui perilaku kejahatan dunia maya ini, yang dapat merugikan dan sangat memengaruhi ketidaknyamanan pengguna. Terdapat kendala dalam penerapan *e-commerce* yaitu kurangnya sumber daya manusia dan rendahnya kepercayaan pada tingkat keamanan *e-commerce* [3].

Penggunaan aplikasi *e-commerce* dipengaruhi oleh tindakan *Cybercrime*. Munculnya kerugian bagi pengguna, mengurangi kepercayaan pengguna pada *e-commerce*, memberikan tambahan kunci keamanan yang merepotkan, membutuhkan perlindungan hukum yang tinggi bagi pengguna merupakan indikator dalam *ecommerce* karena adanya tindak *Cybercrime*. Banyaknya kerugian yang menimpa pengguna *e-commerce* akibat adanya *Cybercrime* berdasarkan hasil penelitian sangat mempengaruhi penggunaan *e-commerce* oleh pengguna di kemudian hari. *Cybercrime* sangat merugikan pengguna seperti kehilangan banyak waktu, kehilangan finansial, atau kehilangan data. Hal ini ditanggapi oleh responden dengan skor 86,2%. Kepercayaan pengguna pada *e-commerce* akibat kejahatan ini menurun. Tanggapan responden dengan skor 73,8% menunjukkan bahwa pengguna *e-commerce* tidak memberikan kepercayaan pada *e-commerce*. Sebagai solusi dalam aksi *Cybercrime* ini, *e-commerce* memberikan solusi dengan menambahkan tingkat keamanan dalam bertransaksi pembayaran. Memiliki banyak platform pembayaran juga memungkinkan kejahatan dunia maya terus berlanjut. Hal ini ditanggapi oleh responden dengan skor 89,8%. Banyaknya lapisan keamanan dalam pembayaran tentunya berdampak pada proses pembayaran yang semakin rumit. Solusi lain yang dilakukan *e-commerce* adalah meningkatkan perlindungan hukum bagi pengguna *e-commerce*. Pengguna membutuhkan perlindungan ini; skor 90,9% menunjukkan respon bahwa pengguna membutuhkan perlindungan hukum yang lebih jelas dan tegas untuk menindaklanjuti tindak pidana dalam bertransaksi di aplikasi *e-commerce* agar merasa aman dalam proses transaksi.

#### IV. KESIMPULAN

Kejahatan dunia maya telah menimbulkan ketakutan di benak banyak orang yang telah aktif menggunakan *e-commerce*. *Cybercrime* berdampak tidak langsung pada dunia bisnis global. Salah satu penyebab kerentanan *cybercrime* adalah perkembangan teknologi internet yang sangat pesat, sehingga memudahkan penyebaran data informasi secara tidak langsung. Daftar kejahatan dunia maya yang semakin meningkat mencakup kejahatan komputer, misalnya, penyebaran intrusi jaringan dan virus komputer. Selain itu, varian kejahatan yang tak terbantahkan berbasis komputer dapat berupa pencurian, penguntitan, intimidasi, dan pemaksaan. Perilaku *cybercrime* masih sangat sulit diantisipasi. Mengetahui dampak dari pengguna *e-commerce* sekarang lebih waspada terhadap kejahatan ini.

#### REFERENSI

- [1] Acharya, S. 2018. Implication of International Law in Electronic Commerce and Cyber Crime: An Experience of Nepal. Available at SSRN 3273915.



- 
- [2] Faridi, M. K. 2019. Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security dan Forensik Digital*, 1(2), pp. 57-61.
- [3] Batmetan, JR. 2018. *The Effect of Cyber Crime Behavior on E-Commerce Application Users*. 1-5.
- [4] Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. 2020. Cyber Security Challenges and its Emerging Trends on Latest Technologies. In *IOP Conference Series: Materials Science and Engineering 981*(2), p. 022062. IOP Publishing.



- [5] Trautman, L. J. 2015. E-Commerce, cyber, and electronic payment system risks: lessons from PayPal. *UC Davis Bus. LJ*, 16, pp. 261.
- [6] Leena, N. 2011. Cyber crime effecting e-commerce technology. *Oriental Journal of Computer Science & Technology*, 4(1), pp. 209-212.
- [7] Munjal, S. 2016. Cyber Crimes–Threat for the e-commerce. *Journal of Maharaja Agrasen College of Higher Education*, 3(1).
- [8] Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Hallatu, T. G. R. 2019. Cybercrime Case as Impact Development of Communication Technology That Troubling Society. *International Journal of Scientific & Technology Research*. 8(9), pp. 1224-1228.
- [9] Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. 2019. Cybercrime Business Digital in Indonesia. In *E3S Web of Conferences 125*, p. 21001. EDP Sciences.
- [10] Salena, I. Y., Safriani, M., & Amin, M. A. R. 2020. Identification of fire protection system availability in faculty of engineering, University of Teuku Umar. In *IOP Conference Series: Materials Science and Engineering 933*(1), p. 012001. IOP Publishing.

Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/). DOI: <https://doi.org/10.52362/jisamar.v5i3.478>