**Birokrasi : Jurnal Ilmu Hukum dan Tata Negara**
**Volume. 3, Nomor. 1, Maret 2025**
e-ISSN : 2987-8632; dan p-ISSN : 2987-8624; Hal. 10-20
DOI: https://doi.org/10.55606/birokrasi.v3i1.1801
*Available online at:* https://journal-stiayappimakassar.ac.id/index.php/Birokrasi

# Analisis Kriminologi atas Kejahatan Dunia Maya *Phising* di Era Pandemi Covid-19

**Fitaria Bantara[1*], Margareta Theodora Simatupang[2], Mera Terangta[3], Nicholine[4], Reyane Dolimariz Putri Behuku[5]**
[1-5] Fakultas Hukum, Universitas Pelita Harapan, Indonesia
*01051220185@student.uph.edu* [1*], *01051220070@student.uph.edu* [2], *01051220159@student.uph.edu* [3], *01051220048@student.uph.edu* [4], *01051220017@student.uph.edu* [5]

Alamat: Jalan M.H. Thamrin Boulevard No.1100, Kelapa Dua, Tangerang Regency, Banten 15811
*Korespondensi penulis: 01051220185@student.uph.edu*

***Abstract:*** *The increase in phishing crimes during the COVID-19 pandemic has been influenced by various factors, including weak social control, lack of cybersecurity education, and technological disparities. This study aims to analyze the rise of phishing crimes from a criminological perspective, focusing on Social Control Theory and Differential Association Theory. Using a qualitative approach, this research examines how phishing offenders learn and operate within social groups. The findings indicate that phishing is not only motivated by financial gain but also intellectual satisfaction and organized criminal activities. Moreover, regulatory challenges persist, as existing laws such as the Electronic Information and Transactions Law (UU ITE) face enforcement limitations due to gaps in law enforcement capabilities. Strengthening cybersecurity awareness, enhancing digital literacy, and improving legal frameworks are crucial to mitigating phishing crimes. Future research should explore quantitative analyses of phishing trends and the effectiveness of policies in addressing cybercrime.*

***Keywords:*** *cybercrime, cybersecurity, law enforcement, phishing, social control theory*

***Abstrak:*** Peningkatan kejahatan *phising* selama pandemi COVID-19 dipengaruhi oleh berbagai faktor, termasuk lemahnya kontrol sosial, kurangnya edukasi keamanan siber, dan kesenjangan teknologi. Penelitian ini bertujuan untuk menganalisis peningkatan kejahatan phising dari perspektif kriminologi, dengan berfokus pada Teori Kontrol Sosial dan Teori Asosiasi Diferensial. Menggunakan pendekatan kualitatif, penelitian ini mengkaji bagaimana pelaku *phising* belajar dan beroperasi dalam kelompok sosial. Hasil penelitian menunjukkan bahwa phishing tidak hanya didorong oleh motif finansial, tetapi juga kepuasan intelektual dan aktivitas kriminal terorganisir. Selain itu, tantangan dalam regulasi masih menjadi hambatan, karena hukum yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), menghadapi keterbatasan dalam penerapannya akibat kurangnya kapasitas aparat penegak hukum. Peningkatan kesadaran keamanan siber, literasi digital, serta perbaikan kerangka hukum menjadi langkah krusial dalam menangani kejahatan phising. Penelitian lebih lanjut disarankan untuk mengeksplorasi analisis kuantitatif terkait tren phishing serta efektivitas kebijakan dalam menangani kejahatan siber.

**Kata kunci:** kejahatan dunia maya, keamanan dunia maya, penegakan hukum, phishing, teori kontrol sosial

## 1. LATAR BELAKANG

Serangan phishing kini semakin banyak ditemukan dan semakin rumit. Selain melalui *email*, phishing kini telah merambah ke SMS, pesan instan, situs media sosial, dan bahkan permainan daring multipemain. Dan Internet merupakan faktor utama penunjang komunikasi serta internet disebut sebagai jalur transportasi segala yang berbentuk file atau data pada komputer lain[1]. Para pelaku kejahatan pun beralih dari mengirim email massal

[1] Y. Maryono, B. Patmi Istiana,Teknologi Informasi & Komunikasi 3, (Jakarta:Quadra, 2008), hlm. 3

*Received: Februari 03, 2025; Revised: Februari 17, 2025; Accepted: Maret 01, 2025; Published: Marwt 03, 2025*

yang bertujuan menipu sembarang orang, menuju serangan *"spear-phishing"* yang lebih terarah, dengan memanfaatkan informasi kontekstual untuk menipu korban yang spesifik. Pandemi *COVID-19* telah mengubah lanskap kehidupan manusia secara global, termasuk dalam hal interaksi sosial dan ekonomi. Salah satu perubahan signifikan adalah peningkatan drastis dalam penggunaan teknologi digital untuk berbagai keperluan, seperti bekerja dari rumah, belajar daring, dan transaksi keuangan daring. Peningkatan ini, sayangnya, juga dimanfaatkan oleh pelaku kejahatan siber untuk melancarkan aksinya, terutama kejahatan *phishing*.

Menurut Yar dan Steinmetz pandemi menciptakan kondisi ideal bagi pelaku kejahatan siber karena masyarakat menjadi lebih rentan akibat ketidakpastian ekonomi dan tekanan psikologis.[2] Fenomena *phishing* selama pandemi tidak hanya menunjukkan peningkatan kuantitas, tetapi juga kompleksitas modus. Pelaku memanfaatkan ketakutan masyarakat terhadap virus dengan mengirimkan email atau pesan berisi informasi palsu tentang bantuan kesehatan, vaksin atau paket bantuan pemerintah yang sebenarnya dirancang untuk mencuri data korban yang sudah ditargetkan. Motivasi pelaku bervariasi baik dari keuntungan finansial secara langsung hingga eksploitasi data untuk kejahatan lain seperti pencucian uang. Konteks kriminologi menjadi relevan dalam menganalisis bagaimana faktor sosial, ekonomi, dan teknologi yang mendorong perilaku kriminal. Pada tahun 2021, data dari Badan Siber dan Sandi Negara (BSSN) mencatat setidaknya 262 kasus *phising*.[3] Pelaku biasanya menggunakan akun yang menyerupai akun resmi atau merekayasa akun agar memiliki reputasi sehingga dapat dipercaya untuk mengelabui korban.[4]

Di Indonesia, kejahatan *phising* diatur dalam beberapa regulasi terutama Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diubah dengan Undang-undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pada pasal 28 ayat (1) secara spesifik mengatur penyalahgunaan data pribadi melalui sistem elektronik,

[2] Majid Yar dan Kevin F. Steinmetz, *Cybercrime and Society*, edisi ketiga (London: SAGE Publications, 2019), 112.

[3] Prasetyo, A. D., Seta, H. B., & Pradnyana, I. W. (2023). Analisis Digital Forensik Spear phishing menggunakan metode National Institute of Justice (Studi Kasus: Instagram verified account). *Informatik : Jurnal Ilmu Komputer*, *19*(1), 58–67. https://doi.org/10.52958/iftk.v19i1.4675

[4] Wahyuni, N. K., Putu Putri Cahayani, I Gusti Ngurah Yogi Wicaksana, & Ida Ayu Kadek Bintang Wijayanti. (2023). Analisis Kerentanan Kejahatan online phising menggunakan tools ZPHISHER, Shellphish Dan Whphisher. *Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *3*(1), 23–31. https://doi.org/10.55606/teknik.v3i1.915

yang mencakup *phishing* yang dapat mengakibatkan kerugian material bagi korban, dengan sanksi yang lebih tegas untuk melindungi korban termuat dalam pasal 45A ayat (1) bahwa dapat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan dengan paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pelaku *phising* mempelajari keterampilan teknis melalui interaksi dengan kelompok kriminal, menunjukkan bahwa kejahatan ini bukan aksi individu spontan, melainkan hasil pembelajaran terorganisir. Faktor teknis seperti keterhubungan jaringan dan distribusi teknologi yang tidak merata mempermudah pelaku, sementara faktor ekonomi termasuk kesenjangan sosial akibat pandemi mendorong motivasi intelektual/kepuasan teknologi dan ekonomi/keuntungan materiil. Dampak bagi korban sangat luas cakupannya, mulai dari kerugian finansial akibat pencurian data perbankan, pencurian identitas, hingga tekanan psikologis seperti kecemasan dan ketakutan.[5] Upaya pencegahan *phishing* memerlukan penguatan kontrol sosial dan penegakan hukum yang lebih efektif.

Undang-undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga melindungi data pribadi tetapi kurangnya kesadaran hukum serta keterbatasan aparat dalam memahami teknologi siber yang cukup menghambat implementasi hukum kepada pelaku. Analisis kriminologi ini mengidentifikasi faktor utama seperti kurangnya edukasi internet yang bijak, kesenjangan sosial-ekonomi, dan kemajuan teknologi tanpa pengamanan memadai sebagai pemicu *phishing*. Dengan memperkuat *social attachment* melalui edukasi komunitas, komitmen melalui regulasi yang ketat serta *involvement* dalam kegiatan positif dapat menekan risiko kejahatan siber. Penulisan ini bertujuan mengeksplorasi modus operandi, motivasi pelaku dan dampak terhadap korban sembari mengusulkan strategi berbasis teori kontrol sosial serta hukum nasional untuk mengatasi ancaman *phishing* di era pandemi Covid-19, yang tidak hanya merugikan secara materiil tetapi juga mengancam stabilitas psikologis dan keamanan digital masyarakat.

## 2. KAJIAN TEORITIS

Teori Strain dan Teori Rutinitas Aktivitas bisa digunakan untuk menganalisis kejahatan *phising* di era COVID-19 karena faktor-faktor yang mendorong pelaku untuk melakukan kejahatan tersebut dijelaskan dalam dua teori ini. Teori Strain berfokus pada

[5] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, edisi kedua (Cambridge: Polity Press, 2021), 256.

tekanan sosial atau ekonomi yang dialami individu, yang dapat mempengaruhi perilaku mereka yang terlibat dalam kejahatan. Dalam pandemi COVID-19, banyak individu mengalami kesulitan ekonomi karena kehilangan pekerjaan atau pendapatan yang berkurang, yang dapat menimbulkan rasa frustasi dan ketidakpastian. Tekanan-tekanan ini menjadi pendorong bagi sebagian orang untuk melakukan tindakan kriminal, termasuk *phishing*. Selain tekanan ekonomi, faktor emosional seperti kecemasan atau depresi yang muncul akibat pandemi juga dapat memotivasi individu untuk terlibat dalam tindak kejahatan tersebut. Sehingga, menurut teori strain kejahatan *phising* meningkat sebagai respons terhadap ketidakstabilan sosial dan ekonomi yang dialami banyak orang selama pandemi. Teori Rutinitas Aktivitas menjelaskan bahwa *phishing* terjadi ketika terdapat pertemuan antara pelaku yang termotivasi, korban yang cocok, dan ketidakhadiran pengawasan[6]. Pandemi COVID-19 memaksa banyak orang beraktivitas secara online, menciptakan kesempatan bagi pelaku kejahatan untuk mengeksploitasi situasi ini.

Korban yang cocok dalam hal ini adalah individu yang tidak hanya lebih banyak beraktivitas di dunia maya, tetapi juga kurang waspada terhadap ancaman phishing. Selain itu, kurangnya pengawasan dan kesadaran masyarakat tentang bahaya phishing membuat pelaku memiliki kesempatan untuk melakukan aksinya. Motivasi pelaku *phising* umumnya berfokus pada keuntungan finansial, memanfaatkan ketidakpastian yang dirasakan oleh korban di tengah pandemi. Menurut Penelitian yang dilakukan oleh *cio africa.co*, serangan *phishing* meningkat 220% selama puncak pandemi global COVID-19[7]. Dibanding dengan rata-rata tahun sebelumnya, penelitian ini dilakukan karena melihat meningkatnya ketergantungan masyarakat terhadap teknologi digital. Oleh karena itu untuk mengurangi dampak negatif dari kejahatan *phising*, penting untuk meningkatkan kesadaran masyarakat mengenai potensi ancaman phishing dan pentingnya menjaga keamanan data pribadi secara digital[8]. Selain itu, langkah-langkah seperti penguatan sistem keamanan, misalnya dengan menerapkan otentikasi dua faktor, serta peningkatan pengawasan terhadap aktivitas mencurigakan di dunia maya, sangat penting untuk mengurangi angka kejahatan ini.

[6] Lawrence E. Cohen dan Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588-608.

[7] S. Writer, "Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies," *CIO Africa*, December 17, 2020,

[8] Jane Smith, "Phishing Attacks and Public Awareness," *Journal of Digital Security* 15, no. 3 (2024): 112-115, https://doi.org/10.1000/jds.2024.15.3.112.

## 3. METODE PENELITIAN

Penulisan ini menggunakan pendekatan Kualitatif Normatif yang dipadukan dengan analisis pada segi kriminologi untuk mengeksplorasikan kejahatan *phishing* pada era *COVID-19* yang berfokus pada modus operandi, motivasi pada pelaku serta dampak yang dirasakan oleh korban. Pendekatan normatif dalam bentuk Undang-undang no. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang memuat aturan serta sanksi terhadap tindakan phishing serta efektivitas nilai-nilai kriminologi. Menurut Soerjono Soekanto, pendekatan Normatif efektif dalam memahami *das sein* dan *das sollen* pada proses penegakan hukum yang dapat belum maksimal terhadap kejahatan siber, misalnya *phishing*.[9] Peraturan serta data yang ada yaitu Undang-undang no. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta laporan data dari Badan Siber dan Sandi Negara (BSSN) dipergunakan untuk membahas lebih lanjut terhadap efektivitas regulasi yang berlaku dalam menangani kejahatan teknologi dimana lebih spesifik pada salah satu tindakan *cybercrime* yaitu *phishing*.

## 4. HASIL DAN PEMBAHASAN

### Analisis Faktor Meningkatnya Kejahatan *Phising* Selama Pandemi *COVID-19* dalam Perspektif Kriminologi

Dalam konteks teori Kontrol Sosial, kejahatan siber berupa *Phising* dapat muncul akibat lemahnya kontrol sosial yang ada. Pelaku kejahatan siber sering kali tidak dapat dikenali secara fisik, sehingga sulit untuk mengawasi dan mengontrol perilaku mereka. Menurut Travis Hirschi, terdapat empat bentuk ikatan yaitu *social attachment, commitment, involvement,* dan *belief.*

a. *Social Attachment* merujuk pada kemampuan individu untuk terhubung dengan orang lain. Ketika ikatan ini kuat, individu lebih peka terhadap pikiran dan perasaan orang lain, yang mengurangi kemungkinan mereka melakukan penyimpangan. *Social Attachment* dibagi menjadi dua jenis:
    1) *Attachment Total:* Individu sepenuhnya mengesampingkan ego demi rasa kebersamaan, mendorong kepatuhan terhadap norma karena pelanggaran akan menyakiti orang lain.

[9] Soerjono Soekanto, *Pengantar Penelitian Hukum*, edisi ketiga (Jakarta: UI Press, 2007), 52.

2) *Attachment Partial:* Hubungan yang terbentuk tanpa menghilangkan ego, tetapi tetap ada pengawasan dari orang lain.

b. *Commitment* adalah keterikatan individu pada institusi sosial seperti sekolah atau pekerjaan. Keterikatan ini menciptakan investasi dalam bentuk reputasi dan masa depan, yang menjadi alasan bagi individu untuk mematuhi norma-norma sosial.
c. *Involvement* mengacu pada partisipasi aktif dalam kegiatan konvensional. Individu yang terlibat aktif dalam organisasi cenderung tidak memiliki waktu untuk melakukan tindakan menyimpang karena fokus pada aktivitas positif.
d. *Belief* mencakup kepercayaan individu terhadap nilai-nilai moral yang ada. Kepatuhan terhadap norma-norma ini berfungsi sebagai penghalang terhadap pelanggaran hukum.

Teori Kontrol Sosial berasumsi bahwa semakin kuat ikatan sosial, semakin kecil kemungkinan terjadinya delinkuensi. Sebaliknya, lemahnya ikatan sosial dapat menjadi faktor penyebab munculnya kejahatan, termasuk kejahatan siber. Dalam teori *differential association* yang dikemukakan oleh Sutherland, kejahatan dipelajari melalui interaksi dengan orang lain. Kejahatan siber membutuhkan keterampilan teknis tertentu, menunjukkan bahwa pelaku melalui proses pembelajaran dan latihan sebelum melakukan tindakan kriminal. [10]Kejahatan ini sering dilakukan oleh kelompok yang saling belajar dan bekerja sama, bukan hanya oleh individu saja. Dengan demikian, upaya untuk memperkuat kontrol sosial dan ikatan antar individu di masyarakat sangat penting dalam mencegah terjadinya kejahatan siber. Edukasi dan peningkatan kesadaran mengenai norma-norma keamanan siber juga diperlukan untuk mengurangi risiko kejahatan di dunia maya.

Beberapa faktor utama yang memicu munculnya kejahatan siber adalah sebagai berikut: (a) Kurangnya edukasi atau bimbingan, baik dari institusi pendidikan formal seperti sekolah maupun dari orang tua, mengenai penggunaan internet secara bijak, sehingga sering terjadi penyalahgunaan; (b) Ketika suatu negara mengalami kemajuan pesat tetapi tidak diiringi dengan peningkatan kesejahteraan masyarakat, hal ini dapat memperlebar kesenjangan sosial; (c) Popularitas media sosial, media elektronik, dan penyimpanan berbasis cloud yang semakin meningkat membuat masyarakat semakin bergantung pada akses internet dalam kehidupan sehari-hari; (d) Pola hidup masyarakat; (e) Kelalaian manusia itu sendiri dalam menjaga keamanan data atau informasi; (f)

[10] Maskun. (2013). *Kejahatan siber (cyber crime)*. Jakarta: Kencana.

Dorongan untuk mendapatkan pengakuan dari orang lain; (g) Kemajuan teknologi yang pesat serta kemudahan akses internet kapan saja dan di mana saja tanpa batasan waktu

Dalam perspektif yang lebih luas, penyebab terjadinya kejahatan siber *Phising* dapat dikelompokkan ke dalam dua faktor utama, yaitu:

a. Faktor Teknis: Keterhubungan antar jaringan mempermudah pelaku untuk melancarkan aksinya. Selain itu, distribusi teknologi yang tidak merata menciptakan kesenjangan kekuatan antara satu pihak dengan pihak lainnya.
b. Faktor Ekonomi: Kejahatan siber juga dapat dianggap sebagai bagian dari aktivitas ekonomi. Salah satu isu global yang berkaitan dengan kejahatan ini adalah keamanan jaringan. Keamanan jaringan menjadi perhatian dunia sejak berkembangnya internet dan kini dianggap sebagai komoditas ekonomi penting. Banyak negara membutuhkan teknologi keamanan jaringan untuk melindungi infrastruktur mereka. Dalam konteks ini, kejahatan siber sering kali menjadi bagian dari skenario besar dalam dinamika ekonomi global.

Motivasi pelaku kejahatan siber umumnya terbagi menjadi dua kategori, yaitu:

a. Motivasi intelektual, yaitu kejahatan yang dilakukan semata-mata untuk kepuasan pribadi dan menunjukkan kemampuan individu dalam menguasai serta memanipulasi teknologi informasi. Jenis kejahatan ini biasanya dilakukan oleh individu secara mandiri.
b. Motivasi ekonomi, politik, dan kriminal, yakni tindakan yang bertujuan untuk memperoleh keuntungan materiil atau mendukung kepentingan kelompok tertentu. Kejahatan dengan motivasi ini sering kali menyebabkan kerugian ekonomi atau politik bagi pihak lain. Karena dampaknya yang signifikan, jenis kejahatan ini umumnya dilakukan oleh kelompok atau organisasi besar.

Kurangnya kesadaran hukum di kalangan masyarakat juga turut menjadi masalah yang signifikan. Kesadaran hukum itu sendiri mencakup pemahaman tentang apa yang seharusnya dan tidak seharusnya dilakukan sesuai dengan aturan atau hukum yang berlaku. Saat ini, tingkat kesadaran hukum masyarakat masih dianggap rendah, terutama terkait dengan aktivitas kejahatan siber. Hal ini disebabkan oleh minimnya pemahaman mengenai *cybercrime*, baik dari segi tindakan maupun dampak yang ditimbulkan.[11]

[11] Golose, P. R. (2007). Penegakan hukum cyber crime dalam sistem hukum Indonesia. *Current date: Friday, February 28, 2025, 5:30 PM WIB.*

Tingkat kesadaran masyarakat terhadap teknologi dan aktivitas di dunia maya sangat berpengaruh pada situasi ini. Semakin rendah kesadaran terhadap teknologi, semakin besar kemungkinan pelaku kejahatan untuk memanfaatkan situasi tersebut.[12] Dengan pemahaman yang lebih baik mengenai cybercrime, masyarakat dapat berperan penting dalam upaya pencegahan kejahatan ini. Tanpa pengetahuan yang memadai, pelaku cybercrime dapat dengan mudah beraksi, menyebabkan kerugian seperti pencurian rekening dan penipuan lainnya. Keamanan yang ada di internet berbeda dengan keamanan dalam kejahatan konvensional. Pelaku *cybercrime* dapat mengakses internet dari mana saja, baik di tempat tertutup maupun terbuka. Namun, sistem keamanan internet masih belum sepenuhnya aman, sehingga memungkinkan siapapun untuk melakukan aktivitas di dunia maya tanpa menyadari batasan-batasan yang ada, yang pada gilirannya dapat meningkatkan risiko kejahatan siber. Di sisi lain, aparat penegak hukum juga mungkin memiliki keterbatasan dalam pengetahuan tentang teknologi yang digunakan oleh pelaku kejahatan siber.

Hal ini bisa membuat pelaku *cybercrime* lebih unggul dalam hal keterampilan dibandingkan aparat penegak hukum, sehingga intensitas kejahatan siber di Indonesia semakin meningkat. Selain itu, penerapan perundang-undangan juga menjadi masalah. Saat ini, Indonesia belum memiliki undang-undang khusus yang secara khusus mengatur tentang *cybercrime*.[13] Meskipun ada hukum umum seperti KUHP dan Undang-Undang ITE yang bisa diterapkan pada pelaku kejahatan siber, penerapan aturan tersebut masih kurang efektif karena aparat penegak hukum masih kurang dalam pengetahuan atau kemampuan dunia maya. Hukum pidana seharusnya berfungsi untuk mengatur dan menjaga ketertiban masyarakat. Oleh karena itu, peraturan terkait kejahatan siber perlu diperbarui dan dikembangkan agar sesuai dengan perkembangan zaman dan ditegakkan dengan lebih tegas.

**Analisis Dampak Kejahatan *Phising* bagi Korban**

Menurut *Internet World Stats*, sebuah situs web internasional yang menyediakan data pengguna internet global, Indonesia menempati peringkat ketiga sebagai negara dengan jumlah pengguna internet terbanyak di Asia. Pada Juni 2021, jumlah pengguna internet di Indonesia tercatat mencapai 212 juta orang, dari total populasi sekitar 276 juta jiwa. Data ini menunjukkan bahwa semakin lama, masyarakat semakin bergantung pada

[12] Suparni, N. (2009). *Cyberspace: Problematika & antisipasi pengaturannya*. Jakarta: Sinar Grafika.
[13] Yurizal. (2018). *Penegakan hukum tindak pidana cyber crime di Indonesia*. Malang: Media Nusa Creative.

internet dalam berbagai aspek kehidupan. Namun, ketergantungan ini juga membuka peluang lebih besar bagi munculnya ancaman kejahatan siber, termasuk phishing.Phishing merupakan salah satu bentuk upaya dari oknum yang tidak bertanggung jawab untuk mengakses dan mendapatkan berbagai informasi pribadi yang terdapat dalam perangkat milik korban. Informasi tersebut dapat berupa sistem keamanan seperti password, nomor-nomor penting, termasuk yang terdapat dalam kartu kredit, serta data sensitif lainnya. Modus yang digunakan oleh pelaku biasanya dengan menyamar sebagai pihak resmi dari suatu entitas terpercaya, sehingga korban tertipu dan tanpa sadar memberikan informasi pribadinya.[14] Kejahatan ini sering kali sulit dikenali karena modusnya yang semakin canggih dan menyerupai komunikasi resmi, sehingga banyak korban yang tertipu tanpa menyadarinya. Phishing tidak hanya berdampak pada kerugian finansial, tetapi juga dapat mengakibatkan penyalahgunaan data pribadi, pencurian identitas, hingga ancaman terhadap keamanan digital seseorang. Oleh karena itu, kesadaran dan kewaspadaan terhadap ancaman phishing sangat penting untuk mencegah meningkatnya jumlah korban kejahatan siber di era digital saat ini.

Kejahatan siber ***(cyber crime)*** yang dilakukan dengan teknik ***phishing*** merupakan salah satu bentuk kejahatan di internet yang mudah menarik perhatian korban kapan saja. Teknik ini memungkinkan pelaku menipu dan menjaring korban dalam jumlah besar dalam waktu singkat. Semakin banyak korban yang tertipu, semakin tinggi angka kejahatan *phising* yang terjadi. [15]Dampak dari kejahatan ini bagi korban sangat beragam, mulai dari kerugian finansial, di mana pelaku dapat mencuri data perbankan dan melakukan transaksi tanpa izin, hingga pencurian identitas, di mana informasi pribadi korban dapat disalahgunakan untuk kepentingan ilegal. Selain itu, korban juga berisiko mengalami penyalahgunaan data pribadi, seperti pemalsuan dokumen atau penipuan lainnya, yang dapat berdampak jangka panjang. Tidak hanya itu, serangan phishing juga dapat menimbulkan gangguan psikologis, seperti stres, kecemasan, dan ketakutan akibat kehilangan data atau uang yang dimana sangat dianggap penting. Di sisi lain, sistem keamanan digital korban menjadi lebih rentan terhadap serangan siber lainnya, meningkatkan risiko kebocoran informasi lebih lanjut. Oleh karena itu, penting bagi setiap individu untuk meningkatkan kesadaran dan kewaspadaan terhadap phishing, seperti tidak

[14] Sastya Hendri Wibowo et al.,Cyber Crime Di Era Digital, ed. Diana Purnama Sari, 1st ed. (Padang: PT Global Eksekutif Teknologi Anggota IKAPI, 2022).

[15] Malunsenge, L. M., Massie, C. Dj., & Rorie, R. E. (2022). Penegakan hukum terhadap pelaku dan korban tindak pidana cyber crime berbentuk phising di Indonesia. *Vol 1*(3).

mudah percaya pada email atau pesan mencurigakan serta selalu memverifikasi keaslian informasi sebelum memberikan data pribadi di internet.

## 5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa berbagai faktor, seperti kurangnya kontrol sosial, kurangnya instruksi keamanan siber, dan kesenjangan dalam distribusi teknologi, berkontribusi pada peningkatan kasus phishing selama pandemi COVID-19. Berdasarkan teori kriminologi, terutama teori Kontrol Sosial dan Asosiasi Diferensial, analisis menunjukkan bahwa proses pembelajaran dalam kelompok sosial adalah penyebab kejahatan siber. Pelaku memiliki berbagai alasan, mulai dari kepentingan intelektual hingga kepentingan finansial dan kriminal.

Meskipun undang-undang seperti UU ITE dapat digunakan untuk menangani kasus phishing, implementasinya masih sulit, terutama dalam hal penegakan hukum dan keterbatasan aparat dalam memahami teknologi yang terus berkembang. Oleh karena itu, perlu ada tindakan yang direncanakan untuk meningkatkan kesadaran masyarakat tentang hukum dan keamanan siber, yang mencakup pelatihan dan edukasi, serta penguatan regulasi yang lebih khusus dan responsif terhadap kemajuan teknologi.

Penelitian ini memiliki keterbatasan dalam cakupan analisis empiris terhadap pola kejahatan *phising* di Indonesia secara spesifik. Oleh karena itu, penelitian lebih lanjut dapat memperdalam aspek kuantitatif mengenai tren phishing serta efektivitas kebijakan yang telah diterapkan untuk menanggulangi kejahatan ini. Selain itu, eksplorasi lebih lanjut mengenai peran institusi dalam membangun ketahanan digital masyarakat juga menjadi rekomendasi penting bagi penelitian di masa depan.

## UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada Pak Pietro Grassio, SH, M.Krim, selaku dosen pengampu mata kuliah Kriminologi ini, atas segala bimbingan dan ilmu yang telah dibagikan selama proses penulisan jurnal ini. Bapak telah memberikan pemahaman yang sangat mendalam dan luas tentang ilmu kriminologi, serta memperkenalkan kami pada berbagai perspektif yang memperkaya wawasan kami. Kami merasa beruntung bisa belajar dari dosen yang tidak hanya menguasai materi dengan sangat baik, tetapi juga memiliki komitmen yang tinggi dalam membentuk mahasiswa yang kritis, kreatif, dan berdedikasi. Semoga ilmu yang Bapak ajarkan dapat terus kami aplikasikan dalam kehidupan sehari-hari dan menjadi modal berharga bagi kami untuk meraih kesuksesan di dunia akademik maupun

profesional. Terima kasih atas segala perhatian, kesabaran, dan dukungan yang Bapak berikan, yang sangat berarti bagi perjalanan akademik kami.

## DAFTAR REFERENSI

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Golose, P. R. (2007). *Penegakan hukum cyber crime dalam sistem hukum Indonesia*.

Jane Smith. (2024). Phishing attacks and public awareness. *Journal of Digital Security, 15*(3), 112-115. https://doi.org/10.1000/jds.2024.15.3.112

Malunsenge, L. M., Massie, C. Dj., & Rorie, R. E. (2022). Penegakan hukum terhadap pelaku dan korban tindak pidana cyber crime berbentuk phishing di Indonesia. *Jurnal Ilmu Hukum, 1*(3).

Maryono, Y., & Istiana, B. P. (2008). *Teknologi informasi & komunikasi 3*. Jakarta: Quadra.

Maskun. (2013). *Kejahatan siber (cyber crime).* Jakarta: Kencana.

Prasetyo, A. D., Seta, H. B., & Pradnyana, I. W. (2023). Analisis digital forensik spear phishing menggunakan metode National Institute of Justice (studi kasus: Instagram verified account). *Informatik: Jurnal Ilmu Komputer*, *19*(1), 58–67. https://doi.org/10.52958/iftk.v19i1.4675

Smith, J. (2024). Phishing attacks and public awareness. *Journal of Digital Security, 15*(3), 112-115. https://doi.org/10.1000/jds.2024.15.3.112

Soekanto, S. (2007). *Pengantar penelitian hukum* (3rd ed.). Jakarta: UI Press.

Suparni, N. (2009). *Cyberspace: Problematika & antisipasi pengaturannya*. Jakarta: Sinar Grafika.

Wahyuni, N. K., Putu Putri Cahayani, I. G. N. Wicaksana, & I. A. K. B. Wijayanti. (2023). Analisis kerentanan kejahatan online phishing.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). London: SAGE Publications.

Yurizal. (2018). *Penegakan hukum tindak pidana cyber crime di Indonesia.* Malang: Media Nusa Creative.