Inovasi : Jurnal Sosial Humaniora dan Pendidikan
Volume. 5 Nomor. 3 September 2026
e-ISSN : 2809-0268; p-ISSN : 2809-0403, Hal. 405-413
DOI: https://doi.org/10.55606/inovasi.v5i3.8129
Available online at: https://journalcenter.org/index.php/inovasi

Cybercrime Dalam Perspektif *Routine Activity* Analisis Kerentanan Korban dan Tantangan Pengawasan di Ruang Digital

[1]Alif Komaldi, *[2]Supardi Hamid

[1,2]sekolah Tinggi Ilmu Kepolisian
[1]alif.komaldi@gmail.com, *[2]supardiihamid@stik_ptik.ac.id

Abstrak. *Perkembangan teknologi digital telah mengubah pola aktivitas rutin masyarakat, mulai dari komunikasi, transaksi keuangan, perdagangan, pekerjaan, pendidikan, hingga penyimpanan data pribadi. Perubahan tersebut tidak hanya menghasilkan manfaat sosial dan ekonomi, tetapi juga menciptakan peluang baru bagi terjadinya cybercrime. Artikel ini bertujuan menganalisis cybercrime melalui Routine Activity Theory dengan menempatkan motivated offender, suitable target, dan absence of capable guardian sebagai tiga unsur utama yang menjelaskan terbentuknya peluang kejahatan di ruang digital. Penelitian menggunakan pendekatan kualitatif melalui studi kepustakaan dengan memanfaatkan jurnal ilmiah, buku, regulasi, serta data dan laporan resmi mengenai kejahatan digital di Indonesia. Hasil analisis menunjukkan bahwa ruang digital memperluas keterjangkauan pelaku terhadap target sekaligus meningkatkan visibilitas dan aksesibilitas target melalui aktivitas online. Kerentanan tidak semata-mata ditentukan oleh nilai ekonomi target, tetapi juga oleh keterbukaan data, pola penggunaan teknologi, dan rendahnya kesadaran terhadap risiko. Pada saat yang sama, guardianship dalam ruang digital bersifat multilapis dan melibatkan pengguna, keluarga, institusi, penyedia platform, lembaga keuangan, pemerintah, serta aparat penegak hukum. Oleh karena itu, pencegahan cybercrime tidak cukup berorientasi pada penindakan pelaku, tetapi perlu mengurangi peluang kejahatan melalui penguatan capable guardian, literasi digital, keamanan teknologi, mekanisme pelaporan cepat, dan kolaborasi antarlembaga. Routine Activity Theory dapat digunakan sebagai kerangka yang relevan untuk memahami dimensi kesempatan dan situasi dalam cybercrime, meskipun penerapannya perlu disesuaikan dengan karakteristik ruang digital yang tidak selalu mempertemukan pelaku dan korban dalam ruang fisik yang sama.*

Kata Kunci: *Cybercrime; Kriminologi; Routine Activity Theory; Kerentanan Korban; Kejahatan Siber*

1. PENDAHULUAN

Transformasi digital telah menjadikan internet sebagai bagian dari aktivitas rutin masyarakat. Komunikasi, perdagangan, perbankan, pembayaran, pendidikan, pekerjaan, hiburan, dan penyimpanan informasi pribadi semakin bergantung pada sistem elektronik. Perubahan tersebut membawa konsekuensi kriminologis karena aktivitas yang semula berlangsung dalam ruang fisik kini berlangsung dalam lingkungan digital yang memiliki karakteristik berbeda. Dalam perspektif kriminologi, perubahan pola aktivitas sehari-hari dapat mengubah struktur kesempatan terjadinya kejahatan. Cohen dan Felson (1979) menjelaskan melalui Routine Activity Theory bahwa suatu tindak kejahatan cenderung terjadi ketika motivated offender bertemu dengan suitable target dalam kondisi tidak terdapat capable guardian yang memadai. Dengan demikian, perubahan aktivitas rutin masyarakat dapat memengaruhi peluang kejahatan tanpa harus terlebih dahulu mengubah karakter dasar pelaku.

Cybercrime memperlihatkan dengan jelas bagaimana perubahan aktivitas rutin dapat menciptakan kesempatan kriminal baru. Pelaku tidak selalu membutuhkan pertemuan fisik dengan korban. Identitas, akun, data pribadi, rekening, perangkat, sistem elektronik, dan aktivitas transaksi dapat menjadi target dari jarak jauh. Leukfeldt dan Yar (2016)

Received: Juni 20, 2026; Revised: Juli 29, 2026; Accepted: Agustus 23, 2026;
Online Available: September 30, 2026; Published: September 15, 2026

menunjukkan bahwa sejumlah elemen Routine Activity Theory dapat diterapkan untuk menjelaskan cybercrime, terutama visibilitas dan aksesibilitas target. Penelitian tersebut juga memperlihatkan bahwa tidak semua komponen teori memiliki pengaruh yang sama terhadap seluruh jenis cybercrime. Temuan ini penting karena menunjukkan bahwa penerapan teori terhadap ruang digital harus mempertimbangkan karakteristik spesifik dari setiap bentuk kejahatan.

Fenomena tersebut relevan dalam konteks Indonesia. Data pemerintah menunjukkan bahwa penipuan digital telah menjadi persoalan serius. Kementerian Komunikasi dan Digital melaporkan bahwa ancaman spam dan scam telah menimbulkan kerugian besar bagi masyarakat, sementara pemerintah memperluas sistem anti-scam untuk mendeteksi dan menghambat komunikasi berisiko. Pada 2026, pemerintah melaporkan penguatan sistem anti-spam dan anti-scam sebagai salah satu instrumen pencegahan untuk mendeteksi komunikasi berisiko dan mempersempit ruang penyalahgunaan layanan digital. Data tersebut menunjukkan bahwa skala ancaman tidak lagi dapat dipandang sebagai persoalan individual, tetapi telah menjadi persoalan keamanan dan perlindungan masyarakat di ruang digital.

Ancaman tersebut semakin terlihat dalam data Indonesia Anti-Scam Centre (IASC). Otoritas Jasa Keuangan melaporkan bahwa sampai 17 Agustus 2025 terdapat 225.281 laporan scamming, 359.733 rekening terverifikasi, 72.145 rekening diblokir, dan kerugian dana yang dilaporkan mencapai Rp4,6 triliun. Pada perkembangan berikutnya, Kementerian Komunikasi dan Digital melaporkan bahwa sejak November 2024 hingga awal 2026, IASC mencatat kerugian masyarakat akibat penipuan mencapai Rp9,1 triliun dari lebih dari 432 ribu laporan. Perbedaan angka menurut periode dan sumber menunjukkan bahwa cybercrime merupakan fenomena dinamis dan pengukurannya sangat bergantung pada mekanisme pelaporan. Meskipun demikian, keseluruhan data memperlihatkan besarnya peluang dan dampak kejahatan digital terhadap masyarakat.

Kasus-kasus yang ditangani aparat penegak hukum juga memperlihatkan karakter transnasional dan berlapis dari cybercrime. Pada April 2026, Direktorat Tindak Pidana Siber Bareskrim Polri mengungkap jaringan internasional yang memperjualbelikan phishing tools melalui situs dan aplikasi pesan, dengan pelaku menggunakan cryptocurrency atau dompet digital untuk menampung hasil kejahatan. Pada Mei 2026, Bareskrim juga menuntaskan perkara SMS blast phishing yang menyamar sebagai situs resmi e-tilang. Kasus semacam ini menunjukkan bahwa cybercrime dapat melibatkan pelaku, infrastruktur digital, platform komunikasi, alat kejahatan, dan aliran dana yang berada pada yurisdiksi berbeda. Kondisi tersebut membuat pencegahan tidak cukup dilakukan melalui pendekatan penindakan setelah kejahatan terjadi.

Dari sudut pandang korban, masalahnya bukan semata-mata kurangnya kehati-hatian individu. Struktur ruang digital sendiri dapat meningkatkan visibilitas dan aksesibilitas target. Pengguna yang sering melakukan transaksi online, mempublikasikan informasi pribadi, menggunakan akun pada banyak platform, atau merespons komunikasi digital secara cepat dapat memiliki tingkat keterpaparan yang berbeda. Penelitian tentang cyber-victimization menunjukkan bahwa aktivitas online tertentu dapat meningkatkan peluang terpapar motivated offender, sedangkan kemampuan menggunakan pengaturan privasi dapat berfungsi sebagai bentuk guardianship personal. Oleh karena itu, korban perlu dipahami sebagai bagian dari situasi kriminal, bukan sebagai pihak yang secara otomatis bertanggung jawab atas terjadinya kejahatan.

Pada saat yang sama, konsep capable guardian di ruang digital tidak dapat dipahami hanya sebagai kehadiran polisi. Guardian dapat berupa individu yang menerapkan autentikasi dan pengaturan privasi, keluarga atau organisasi yang melakukan pengawasan, bank dan penyedia pembayaran yang mendeteksi transaksi mencurigakan, platform digital yang melakukan moderasi dan pemblokiran, operator telekomunikasi yang mendeteksi spam dan scam, lembaga negara yang menerima laporan dan melakukan pemutusan akses, serta aparat penegak hukum yang melakukan patroli dan penyidikan. Konsep guardianship yang

bersifat multilapis tersebut menjadi penting karena karakter cybercrime memungkinkan pelaku dan korban tidak pernah berada dalam ruang fisik yang sama.

Persoalan penelitian ini muncul dari adanya ketidakseimbangan antara meningkatnya intensitas aktivitas digital dengan kemampuan mekanisme perlindungan untuk mengurangi peluang kejahatan. Di satu sisi, masyarakat semakin bergantung pada ruang digital sehingga jumlah dan variasi suitable target bertambah. Di sisi lain, pelaku dapat memanfaatkan teknologi untuk memperluas jangkauan, menyamarkan identitas, dan mengotomatisasi serangan. Sementara itu, kemampuan guardian tidak selalu seragam pada tingkat individu, organisasi, platform, maupun negara. Kondisi tersebut menimbulkan kebutuhan untuk melihat cybercrime bukan hanya sebagai pelanggaran hukum yang harus ditindak, tetapi sebagai peristiwa kriminal yang dipengaruhi oleh struktur kesempatan.

Research gap artikel ini terletak pada kebutuhan untuk menghubungkan perkembangan cybercrime di Indonesia dengan kerangka Routine Activity Theory secara lebih integratif. Literatur sebelumnya telah menunjukkan bahwa teori ini dapat digunakan untuk menjelaskan sebagian bentuk cyber-victimization, tetapi juga menemukan bahwa pengaruh value, accessibility, visibility, dan guardianship dapat berbeda menurut jenis cybercrime. Penelitian yang lebih baru bahkan mengembangkan gagasan cyber capable guardian untuk menyesuaikan guardianship dengan lingkungan digital. Artikel ini memanfaatkan perkembangan tersebut dengan memfokuskan analisis pada konteks Indonesia, terutama hubungan antara peningkatan aktivitas digital, kerentanan target, dan kebutuhan penguatan guardianship sebagai strategi pencegahan.

Berdasarkan uraian tersebut, permasalahan dalam penelitian ini diarahkan pada tiga pertanyaan utama. Pertama, bagaimana perkembangan cybercrime di ruang digital menciptakan peluang baru bagi terjadinya kejahatan? Kedua, bagaimana Routine Activity Theory menjelaskan terjadinya cybercrime melalui unsur motivated offender, suitable target, dan absence of capable guardian? Ketiga, bagaimana penguatan capable guardian dapat menjadi strategi pencegahan cybercrime di ruang digital? Penelitian ini bertujuan menganalisis perkembangan cybercrime sebagai bentuk kejahatan yang memanfaatkan perubahan aktivitas rutin masyarakat, mengkaji terjadinya cybercrime berdasarkan tiga unsur utama Routine Activity Theory, serta merumuskan strategi pencegahan melalui penguatan capable guardian.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kepustakaan (library research). Pendekatan kualitatif dipilih karena penelitian tidak diarahkan untuk menguji hubungan statistik antarvariabel, melainkan untuk memahami cybercrime sebagai fenomena kriminologis dan menganalisisnya melalui kerangka Routine Activity Theory. Data penelitian diperoleh dari sumber akademik dan dokumen resmi yang relevan dengan cybercrime, victimization, guardianship, keamanan digital, serta kebijakan penanganan kejahatan siber di Indonesia.

Sumber data primer dalam konteks studi kepustakaan berupa karya teoritis utama mengenai Routine Activity Theory, terutama Cohen dan Felson (1979), serta penelitian empiris dan konseptual mengenai penerapan teori tersebut terhadap cybercrime. Sumber sekunder meliputi artikel jurnal ilmiah, buku kriminologi, laporan pemerintah, publikasi Otoritas Jasa Keuangan, Kementerian Komunikasi dan Digital, Kepolisian Negara Republik Indonesia, serta peraturan perundang-undangan yang berkaitan dengan informasi dan transaksi elektronik dan perlindungan data pribadi. Data aktual digunakan terutama untuk memberikan konteks empiris terhadap pembahasan, bukan untuk mengklaim adanya pengujian kausalitas.

Pengumpulan data dilakukan melalui penelusuran literatur berdasarkan kata kunci cybercrime, cyber-victimization, routine activity theory, suitable target, capable guardian, online fraud, phishing, digital crime, dan cyber security. Literatur kemudian diseleksi berdasarkan relevansi dengan fokus penelitian, kualitas sumber, kejelasan bibliografi, dan

keterbaruan informasi. Untuk data empiris Indonesia, penelitian memprioritaskan sumber resmi yang dapat diverifikasi dan membedakan secara jelas antara jumlah laporan, jumlah rekening yang terindikasi, nilai kerugian, serta potensi kerugian yang berhasil dicegah.

Analisis data dilakukan secara deskriptif-analitis. Tahap pertama adalah mengidentifikasi perkembangan dan karakteristik cybercrime. Tahap kedua adalah memetakan fenomena tersebut ke dalam tiga unsur Routine Activity Theory, yaitu motivated offender, suitable target, dan absence of capable guardian. Tahap ketiga adalah mengidentifikasi titik-titik intervensi yang dapat mengurangi peluang kejahatan, khususnya melalui penguatan guardianship. Dengan cara tersebut, penelitian tidak hanya mendeskripsikan cybercrime, tetapi berupaya menjelaskan mekanisme kesempatan kriminal dan implikasinya bagi strategi pencegahan.

3. HASIL DAN PEMBAHASAN

3.1 Cybercrime dan Perkembangan Kejahatan di Ruang Digital

Cybercrime merupakan istilah yang mencakup berbagai tindak pidana yang menggunakan, menyerang, atau bergantung pada teknologi informasi dan jaringan komunikasi. Karena sifatnya yang luas, cybercrime tidak dapat dipahami sebagai satu jenis kejahatan tunggal. Hacking, illegal access, malware, identity theft, online fraud, phishing, cyberstalking, cyberbullying, dan berbagai bentuk penipuan berbasis rekayasa sosial memiliki karakteristik yang berbeda. Leukfeldt dan Yar (2016) menekankan bahwa cybercrime mencakup spektrum pelanggaran yang berbeda sehingga kemampuan satu teori untuk menjelaskan seluruh bentuk cybercrime harus diuji secara hati-hati.

Dari perspektif kriminologi, karakter penting cybercrime adalah perubahan struktur kesempatan. Kejahatan dapat dilakukan tanpa kehadiran fisik pelaku di lokasi korban. Jaringan internet memungkinkan pelaku mengakses korban secara luas, mengirim pesan kepada banyak target secara bersamaan, menggunakan identitas palsu, dan memanfaatkan infrastruktur digital yang berada di negara berbeda. Dalam konteks ini, ruang digital tidak menghapus konsep waktu dan ruang dalam Routine Activity Theory, tetapi mengubah bentuknya. Konvergensi pelaku dan target dapat berlangsung melalui shared network, platform, aplikasi, atau sistem elektronik, bukan melalui ruang fisik yang sama.

Perubahan tersebut terlihat jelas pada penipuan digital. Modus phishing, impersonation, fake customer service, penipuan transaksi belanja, investasi palsu, love scam, dan penawaran kerja fiktif memanfaatkan aktivitas rutin yang sebenarnya legal. Korban menggunakan mesin pencari, media sosial, aplikasi pesan, marketplace, atau layanan perbankan untuk tujuan yang sah, tetapi aktivitas tersebut sekaligus menciptakan titik kontak dengan pelaku. Pratt, Holtfreter, dan Reisig (2010) menunjukkan bahwa perkembangan internet memperluas kesempatan bagi pelaku penipuan untuk menjangkau konsumen melalui rutinitas online.

Data Indonesia memperlihatkan bahwa penipuan digital memiliki skala yang signifikan. OJK melaporkan 225.281 laporan scamming sampai 17 Agustus 2025 dengan 359.733 rekening terverifikasi dan 72.145 rekening diblokir. Nilai kerugian dana yang dilaporkan mencapai Rp4,6 triliun. Data tersebut tidak hanya menunjukkan banyaknya korban, tetapi juga memperlihatkan bahwa rekening dan sistem pembayaran menjadi bagian penting dari ekosistem kejahatan. Pembentukan IASC menjadi contoh bahwa respons terhadap cybercrime mulai diarahkan pada mekanisme intervensi yang lebih cepat melalui koordinasi antara otoritas, lembaga keuangan, dan industri.

Di sisi lain, perkembangan sistem anti-scam pemerintah menunjukkan bahwa guardianship digital juga mulai berkembang. Pada Februari 2026, Komdigi melaporkan bahwa lebih dari dua miliar panggilan, pesan, dan tautan berisiko telah dideteksi dalam enam bulan dan potensi kerugian sekitar Rp8 triliun berhasil dicegah. Dalam perspektif Routine Activity Theory, mekanisme tersebut dapat dipahami sebagai upaya meningkatkan

kemampuan guardian untuk mengurangi keterpaparan target dan menghambat komunikasi pelaku dengan calon korban.

Perkembangan kasus yang ditangani Polri juga menunjukkan bahwa cybercrime semakin kompleks. Pengungkapan jaringan penjualan phishing tools lintas negara pada April 2026 menunjukkan adanya ekosistem yang tidak hanya terdiri atas pelaku yang menyerang korban, tetapi juga pihak yang menyediakan perangkat, infrastruktur, kanal komunikasi, dan mekanisme pembayaran. Bagi kriminologi, kondisi tersebut menunjukkan bahwa motivated offender tidak selalu berdiri sendiri. Kejahatan dapat berkembang menjadi ekosistem yang menyediakan pengetahuan, alat, dan layanan untuk mempermudah pelanggaran.

Karena itu, cybercrime sebaiknya dipahami sebagai kejahatan kesempatan yang berkembang mengikuti perubahan aktivitas rutin. Semakin banyak fungsi kehidupan dipindahkan ke ruang digital, semakin banyak pula objek, informasi, dan aktivitas yang dapat diekspos kepada pelaku. Namun, perubahan tersebut tidak berarti setiap pengguna internet otomatis menjadi korban. Yang menentukan adalah bagaimana karakter target, tingkat keterpaparan, aksesibilitas, motivasi pelaku, dan keberadaan guardian berinteraksi dalam situasi tertentu.

3.2 Analisis Cybercrime Berdasarkan Routine Activity Theory

Routine Activity Theory dikembangkan oleh Cohen dan Felson (1979) dengan perhatian pada situasi yang memungkinkan kejahatan terjadi. Teori ini menyatakan bahwa tindak kejahatan predatori membutuhkan konvergensi antara likely offender, suitable target, dan ketiadaan capable guardian pada waktu dan tempat yang sama. Fokus teori bukan terutama pada mengapa seseorang menjadi penjahat, tetapi pada bagaimana struktur aktivitas rutin menciptakan kesempatan bagi peristiwa kriminal.

Dalam konteks cybercrime, unsur pertama adalah motivated offender. Pelaku dapat berupa individu, kelompok, jaringan terorganisasi, atau aktor yang memiliki kemampuan teknis tertentu. Motivasi dapat berasal dari keuntungan finansial, pencurian data, pemerasan, keuntungan reputasional, ideologi, atau tujuan lain. Ruang digital memberikan keuntungan situasional berupa kemampuan melakukan kejahatan dari jarak jauh, mengotomatisasi kontak dengan banyak target, serta menyamarkan identitas. Akan tetapi, Routine Activity Theory tidak mengharuskan teori ini menjelaskan seluruh asal-usul motivasi pelaku. Motivasi dianggap sebagai salah satu kondisi yang sudah tersedia dalam lingkungan kriminal, sementara analisis diarahkan pada kapan dan bagaimana pelaku menemukan target yang sesuai dan menghadapi guardianship yang lemah.

Unsur kedua adalah suitable target. Cohen dan Felson menggunakan konsep VIVA—value, inertia, visibility, dan accessibility—untuk menjelaskan kesesuaian target. Dalam lingkungan digital, value tidak selalu berarti nilai uang langsung. Data identitas, kredensial akun, informasi bisnis, reputasi digital, akses ke sistem, dan hubungan sosial dapat memiliki nilai bagi pelaku. Inertia juga perlu ditafsirkan secara hati-hati karena objek digital tidak memiliki karakter fisik seperti benda dalam kejahatan konvensional. Karena itu, visibility dan accessibility menjadi sangat penting. Target yang mudah ditemukan, mudah dihubungi, dan memiliki informasi yang cukup terbuka dapat lebih mudah dijangkau oleh pelaku.

Visibility dalam cybercrime dapat muncul melalui unggahan media sosial, profil publik, informasi kontak, aktivitas marketplace, maupun jejak digital. Semakin banyak informasi tersedia, semakin besar peluang pelaku melakukan profiling terhadap calon korban. Penelitian Leukfeldt dan Yar (2016) menunjukkan bahwa visibility memiliki peran yang konsisten dalam beberapa jenis cybercrime yang mereka teliti. Temuan tersebut mendukung gagasan bahwa aktivitas online dapat meningkatkan kemungkinan seseorang terlihat oleh motivated offender.

Accessibility berkaitan dengan seberapa mudah target dijangkau atau dieksploitasi. Penggunaan akun tanpa autentikasi yang kuat, pengulangan kata sandi, perangkat yang tidak diperbarui, respons cepat terhadap pesan yang tampak resmi, atau penggunaan layanan digital tanpa verifikasi dapat meningkatkan aksesibilitas. Namun, aksesibilitas tidak semata-

mata merupakan kesalahan pengguna. Desain platform, keamanan sistem, prosedur autentikasi, dan mekanisme pemulihan akun juga memengaruhi seberapa mudah target dieksploitasi.

Unsur ketiga adalah absence of capable guardian. Dalam kejahatan konvensional, guardian dapat berupa orang yang berada di sekitar korban atau tempat kejadian. Dalam cybercrime, guardian bersifat lebih kompleks. Guardian dapat berupa pengguna yang mengaktifkan autentikasi multifaktor, administrator sistem, bank yang memantau transaksi, platform yang memblokir akun berbahaya, operator telekomunikasi yang mendeteksi spam, lembaga pemerintah yang melakukan pemutusan akses, serta kepolisian yang melakukan patroli dan penyidikan. Dengan demikian, guardianship dapat bersifat personal, teknis, institusional, dan publik.

Penelitian Leukfeldt dan Yar (2016) memberikan catatan penting bahwa tidak semua bentuk guardianship mempunyai pengaruh yang sama. Dalam penelitian mereka, visibility berperan pada berbagai jenis cybercrime, sementara accessibility dan personal guardianship menunjukkan hasil yang bervariasi, dan value serta technical guardianship memiliki pengaruh yang lebih terbatas pada model yang diuji. Temuan ini mengingatkan bahwa penguatan guardian tidak boleh dilakukan secara seragam. Intervensi harus disesuaikan dengan modus dan titik kerentanan setiap bentuk cybercrime.

Penelitian mengenai cyber-victimization generasi muda juga memperlihatkan relevansi unsur-unsur tersebut. Studi tahun 2023 mengenai hacking, penyebaran foto tanpa persetujuan, cyberbullying, dan cyberstalking menemukan bahwa pola aktivitas online tertentu dapat meningkatkan paparan terhadap motivated offender, sementara kemampuan menggunakan pengaturan privasi dapat berfungsi sebagai perlindungan terhadap victimization. Hal ini memperkuat argumentasi bahwa perilaku digital bukan sekadar latar belakang, tetapi bagian dari situasi yang memengaruhi peluang viktimisasi.

Dalam konteks Indonesia, pola tersebut dapat dilihat pada phishing dan impersonation. Pelaku dapat memperoleh akses ke calon korban melalui nomor telepon, media sosial, marketplace, atau pesan yang meniru institusi resmi. Korban menjadi suitable target karena memiliki akun, data, atau akses finansial yang bernilai. Ketika korban tidak dapat membedakan komunikasi resmi dan palsu, atau ketika platform tidak mampu mendeteksi dan menghentikan komunikasi berbahaya secara cepat, absence of capable guardian menjadi semakin nyata. Sebaliknya, verifikasi identitas, sistem anti-scam, pemblokiran rekening, dan respons cepat terhadap laporan dapat mengganggu konvergensi tersebut.

Routine Activity Theory dengan demikian membantu menjelaskan bahwa cybercrime tidak harus dipahami sebagai hasil dari kelemahan moral korban atau kecanggihan pelaku semata. Peristiwa kriminal muncul ketika kondisi situasional memungkinkan. Pelaku yang termotivasi dapat selalu tersedia, tetapi kejahatan menjadi lebih mungkin ketika target terlihat dan mudah diakses serta guardianship tidak memadai. Perspektif ini penting karena menggeser sebagian perhatian pencegahan dari sekadar mencari dan menghukum pelaku menuju pengurangan kesempatan kriminal.

Meski demikian, penerapan teori harus dilakukan secara kritis. Salah satu persoalan utama adalah bahwa konsep ruang dan waktu dalam Routine Activity Theory awalnya berkembang dari kejahatan yang melibatkan kedekatan fisik. Dalam cybercrime, pelaku dan korban dapat berada di negara berbeda dan tidak pernah bertemu. Yar dan penelitian setelahnya menunjukkan bahwa shared network dapat dipahami sebagai bentuk konvergensi yang menggantikan shared physical space. Dengan penyesuaian tersebut, teori tetap berguna untuk menganalisis situasi kriminal digital, tetapi tidak seharusnya digunakan secara mekanis.

Dengan demikian, model analitis artikel ini dapat diringkas sebagai berikut: digitalisasi meningkatkan intensitas aktivitas rutin online; aktivitas tersebut meningkatkan visibility dan accessibility berbagai target; motivated offender memanfaatkan kesempatan melalui platform dan jaringan digital; apabila capable guardian lemah atau terlambat

bertindak, konvergensi tersebut meningkatkan peluang cybercrime. Sebaliknya, setiap intervensi yang mengurangi visibility, membatasi accessibility, meningkatkan verifikasi, mempercepat deteksi, atau memperkuat guardianship dapat mengurangi peluang terjadinya kejahatan.

3.3 Strategi Pencegahan Cybercrime dan Penguatan Capable Guardian

Jika Routine Activity Theory digunakan sebagai dasar pencegahan, maka strategi utama bukan hanya meningkatkan kemungkinan pelaku ditangkap setelah kejahatan terjadi, tetapi juga mengubah kondisi yang memungkinkan konvergensi kriminal. Pencegahan diarahkan untuk membuat target lebih sulit dijangkau, meningkatkan risiko bagi pelaku, mempercepat deteksi, dan memperkuat kehadiran guardian. Dalam konteks cybercrime, pendekatan tersebut sejalan dengan prinsip situational crime prevention yang menekankan pengurangan kesempatan melakukan kejahatan.

Pertama, guardianship personal perlu diperkuat melalui literasi digital yang bersifat praktis. Edukasi tidak cukup berupa imbauan umum agar masyarakat berhati-hati, tetapi harus mengajarkan kemampuan memverifikasi alamat situs, mengenali impersonation, memeriksa nomor atau rekening, mengaktifkan autentikasi multifaktor, menggunakan kata sandi yang berbeda, membatasi informasi publik, serta segera melapor ketika terjadi indikasi penipuan. Tujuannya adalah meningkatkan kemampuan pengguna untuk mendeteksi ancaman sebelum terjadi kerugian.

Kedua, guardianship teknis harus dikembangkan secara berlapis. Platform dan penyedia layanan perlu meningkatkan deteksi pola komunikasi mencurigakan, phishing, spoofing, bot, akun palsu, dan aktivitas transaksi tidak wajar. Sistem anti-spam dan anti-scam yang telah diterapkan pemerintah menunjukkan arah tersebut. Teknologi kecerdasan buatan dan machine learning juga dapat digunakan sebagai alat bantu deteksi, meskipun penggunaannya harus disertai pengawasan manusia, mekanisme akuntabilitas, dan perlindungan terhadap privasi.

Ketiga, guardianship institusional perlu mempercepat respons terhadap laporan korban. Data IASC menunjukkan pentingnya mekanisme yang mampu menerima laporan, melakukan verifikasi, menghubungkan informasi dengan lembaga keuangan, dan memblokir rekening atau aliran dana dengan cepat. Dalam perspektif Routine Activity Theory, kecepatan intervensi penting karena dapat memutus proses konvergensi sebelum kerugian menjadi lebih besar. Korban juga perlu diberi informasi yang jelas mengenai prosedur pelaporan agar keterlambatan tidak memperbesar kerugian.

Keempat, perlindungan target perlu didukung dengan penguatan tata kelola data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum untuk melindungi data pribadi. Dalam perspektif suitable target, pengendalian data memiliki arti kriminologis karena mengurangi visibility dan accessibility informasi yang dapat digunakan pelaku. Semakin sedikit data sensitif yang tersedia secara terbuka atau tersebar tanpa kontrol, semakin kecil peluang pelaku melakukan profiling dan impersonation.

Kelima, penegakan hukum harus bergerak dari pendekatan reaktif menuju kombinasi pencegahan, deteksi, dan penindakan. Polri melalui Dittipidsiber memiliki peran dalam penyelidikan dan penyidikan cybercrime, tetapi penanganan cybercrime membutuhkan kerja sama dengan platform digital, operator telekomunikasi, bank, penyedia pembayaran, PPATK, Komdigi, OJK, dan mitra internasional. Kasus phishing tools lintas negara yang ditangani Bareskrim pada 2026 memperlihatkan bahwa kerja sama lintas institusi dan lintas yurisdiksi merupakan kebutuhan nyata.

Keenam, cyber patrol dapat dikembangkan sebagai bentuk guardianship proaktif. Patroli siber tidak hanya diarahkan untuk menemukan konten ilegal, tetapi juga memetakan pola kejahatan, akun atau infrastruktur yang digunakan berulang kali, modus baru, dan jaringan yang menyediakan tools kejahatan. Pendekatan ini dapat membantu aparat memahami bagaimana motivated offender menemukan dan mengeksploitasi target. Data

patroli juga dapat digunakan untuk mengembangkan indikator risiko dan memberikan peringatan dini kepada masyarakat maupun penyedia platform.

Ketujuh, pencegahan harus mempertimbangkan bahwa korban tidak selalu merupakan pengguna yang lalai. Kelompok tertentu dapat menjadi lebih rentan karena usia, pengalaman digital, keterbatasan literasi, kebutuhan ekonomi, atau ketergantungan pada layanan online. Karena itu, strategi pencegahan harus menghindari victim blaming. Prinsipnya adalah membuat sistem digital lebih aman bahkan ketika pengguna melakukan kesalahan yang wajar. Dalam kerangka Routine Activity Theory, penguatan guardian pada tingkat sistem dapat mengurangi ketergantungan terhadap kemampuan individu.

Konsep capable guardian juga perlu diperluas dari guardian manusia menjadi cyber capable guardian. Mabunda (2024) mengusulkan pentingnya mengembangkan guardianship yang mampu memanfaatkan artificial intelligence dan machine learning untuk mendeteksi serta mengintervensi ancaman yang tidak mungkin diawasi secara manual. Gagasan tersebut relevan bagi Indonesia karena jumlah komunikasi digital sangat besar. Namun, penggunaan teknologi sebagai guardian tidak boleh menghilangkan prinsip transparansi, akuntabilitas, perlindungan data, dan pengawasan terhadap potensi kesalahan sistem.

Pada akhirnya, pencegahan cybercrime harus dibangun sebagai ekosistem. Individu berperan menjaga akun dan data; keluarga dan institusi membangun budaya keamanan; platform meningkatkan desain keamanan dan moderasi; bank dan penyedia pembayaran memperkuat deteksi transaksi; operator telekomunikasi memblokir spam dan scam; pemerintah membangun regulasi dan koordinasi; sementara Polri menjalankan fungsi penegakan hukum dan patroli siber. Pendekatan ekosistem tersebut paling sesuai dengan karakter cybercrime yang tidak mengenal batas fisik dan dapat berlangsung melalui rangkaian infrastruktur yang berbeda.

4. KESIMPULAN

Cybercrime merupakan bentuk kejahatan yang berkembang seiring perubahan aktivitas rutin masyarakat ke ruang digital. Routine Activity Theory memberikan kerangka yang relevan untuk menjelaskan bahwa peluang cybercrime terbentuk ketika motivated offender dapat menjangkau suitable target dalam kondisi guardianship yang tidak memadai. Dalam lingkungan digital, suitability target terutama berkaitan dengan visibility dan accessibility, sementara guardianship berkembang dalam bentuk personal, teknis, institusional, dan publik. Data Indonesia mengenai penipuan digital, pemblokiran rekening, sistem anti-scam, serta pengungkapan kasus phishing menunjukkan bahwa persoalan cybercrime memiliki skala besar dan memerlukan respons yang lebih luas daripada penindakan terhadap pelaku setelah kejahatan terjadi. Analisis ini juga menunjukkan bahwa korban tidak dapat semata-mata dipandang sebagai pihak yang lalai karena kerentanan dipengaruhi oleh desain sistem, keterbukaan informasi, mekanisme keamanan, dan kualitas pengawasan. Oleh sebab itu, strategi pencegahan perlu diarahkan pada pengurangan kesempatan kriminal melalui penguatan capable guardian, peningkatan literasi digital, perlindungan data pribadi, deteksi teknis, respons cepat terhadap laporan, patroli siber, dan kolaborasi lintas sektor serta lintas negara. Penerapan Routine Activity Theory tetap perlu dilakukan secara kritis karena ruang digital mengubah makna kedekatan waktu dan tempat, tetapi teori tersebut tetap berguna untuk mengidentifikasi titik-titik intervensi yang dapat mengurangi peluang terjadinya cybercrime.

DAFTAR PUSTAKA

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief: Practical Theory for Crime Prevention. Home Office Research, Development and Statistics Directorate.

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. Crime Prevention and Community Safety, 15(1), 65–79. https://doi.org/10.1057/cpcs.2012.14.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409.

Mabunda, S. (2024). Applying the Routine Activities Theory to Cybercrime: A Cyber Capable Guardian. Journal of Anti-Corruption Law, 8, 60–84.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267–296. https://doi.org/10.1177/0022427810365903.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. Criminal Justice and Behavior, 38(11), 1149–1169.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407–427.

Yar, M. (2006). Cybercrime and Society. SAGE Publications.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Otoritas Jasa Keuangan. (2025). The Rise of Scams, OJK and the Government Launch National Campaign to Combat Scam and Illegal Financial Activities. Data IASC per 17 Agustus 2025.

Kementerian Komunikasi dan Digital Republik Indonesia. (2026). Angka Kerugian Scam di Indonesia Capai Rp7,5 Triliun, Wamen Nezar Dorong Pelindungan Konsumen Digital.

Kementerian Komunikasi dan Digital Republik Indonesia. (2026). Berita mengenai penguatan pengawasan registrasi biometrik dan data kerugian penipuan digital.

Kepolisian Negara Republik Indonesia. (2026). Bareskrim Polri Bongkar Sindikat Phishing Lintas Negara.

Kepolisian Negara Republik Indonesia. (2026). Dittipidsiber Bareskrim Polri Ungkap Penjualan Phishing Tools Lintas Negara.