

**ANALISIS KRIMINAL KEJAHATAN *CYBER EXTORTION* BERKEDOK
LOVE SCAMMING DI LINGKUNGAN LEMBAGA PEMASYARAKATAN
*CRIMINAL ANALYSIS OF CYBER EXTORTION CRIMES UNDER THE
GUESS OF LOVE SCAMMING IN CORRECTIONAL INSTITUTIONS***

Rizky Pratama dan Ery Setyanegara

Universitas Muhammadiyah Kotabumi

Korespondensi Penulis : erysetyanegara71@gmail.com

Citation Structure Recommendation :

Pratama, Rizky dan Ery Setianegara. *Analisis Kriminal Kejahatan Cyber Extortion Berkedok Love Scamming di Lingkungan Lembaga Pemasyarakatan*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.7 (2026).

ABSTRAK

Cyber extortion berkedok *love scamming* merupakan kejahatan siber yang memanfaatkan hubungan emosional palsu untuk melakukan pemerasan melalui media elektronik. Penelitian ini bertujuan menganalisis cara kerja dan struktur pengoperasian sindikat *cyber extortion* berkedok *love scamming* serta faktor yang menyebabkan peredaran alat komunikasi ilegal di lembaga pemasyarakatan. Penelitian menggunakan metode hukum empiris dengan pendekatan kriminologis dan perundang-undangan. Data diperoleh melalui wawancara dan studi kepustakaan, kemudian dianalisis secara kualitatif. Hasil penelitian menunjukkan kejahatan dilakukan melalui pencarian korban, pembentukan hubungan emosional, pemanfaatan data pribadi, pemerasan dan menyembunyikan hasil kejahatan. Faktor penyebabnya meliputi overkapasitas, keterbatasan petugas, keterlibatan oknum, lemahnya teknologi pengamanan dan dukungan jaringan eksternal.

Kata Kunci: *Cyber Extortion, Kriminologi, Lembaga Pemasyarakatan*

ABSTRACT

Cyber extortion under the guise of love scamming is a cybercrime that exploits false emotional connections to commit blackmail through electronic media. This study aims to analyze the workings and operational structure of cyber extortion syndicates under the guise of love scamming and the factors that contribute to the circulation of illegal communication devices in correctional institutions. The study used empirical legal methods with a criminological and legislative approach. Data were obtained through interviews and literature review, then analyzed qualitatively. The results indicate that the crime is committed through victimization, establishing emotional relationships, exploiting personal data, extortion, and concealing the proceeds of crime. Contributing factors include overcapacity, limited officers, the involvement of individuals, weak security technology, and external network support.

Keywords: *Cyber Extortion, Criminology, Correctional Institution*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat. Pemanfaatan internet, media sosial, dan aplikasi komunikasi digital tidak hanya memberikan manfaat dalam bidang ekonomi, pendidikan dan sosial, tetapi juga melahirkan berbagai bentuk kejahatan baru yang dikenal sebagai kejahatan siber (*cybercrime*).¹ Salah satu bentuk kejahatan siber yang mengalami perkembangan pesat adalah *cyber extortion* atau pemerasan siber, yaitu tindakan memperoleh keuntungan dengan cara mengancam korban melalui media elektronik. Dalam praktiknya, *cyber extortion* sering dikombinasikan dengan modus *love scamming*, yaitu penipuan yang memanfaatkan hubungan asmara palsu untuk memperoleh kepercayaan korban sebelum melakukan pemerasan atau pengambilan keuntungan secara melawan hukum.²

Fenomena *love scamming* menunjukkan adanya perubahan pola kejahatan konvensional menjadi kejahatan berbasis teknologi yang lebih sulit dideteksi. Pelaku biasanya menggunakan identitas palsu, foto hasil pencurian digital, serta narasi kehidupan yang direkayasa untuk membangun hubungan emosional dengan korban. Setelah memperoleh kepercayaan, pelaku meminta data pribadi, foto, video, atau sejumlah uang kepada korban. Dalam beberapa kasus, korban kemudian diancam akan disebarkan informasi atau konten pribadinya apabila tidak memenuhi permintaan pelaku. Pola tersebut menunjukkan bahwa *cyber extortion* berkedok *love scamming* tidak hanya menimbulkan kerugian materiil, tetapi juga kerugian psikologis, sosial dan reputasional bagi korban.

Secara yuridis, perbuatan tersebut bertentangan dengan berbagai ketentuan hukum pidana di Indonesia. Ketentuan mengenai pemerasan dan ancaman diatur dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP), sedangkan penggunaan sarana elektronik untuk melakukan ancaman, penyebaran informasi elektronik yang melanggar hukum,

¹ Mohamad Revaldy Fairuzzen, dkk., *Perkembangan Hukum dan Kejahatan Siber 'Cybercrime' di Indonesia*, Indonesian Journal of Islamic Jurisprudence Economic and Legal Theory, Vol.2, No.1 (Januari 2024), p.139–53.

² Normatriya Sofiana, dkk., *Analisis Yuridis Tindak Pidana Love Scamming Sebagai Kejahatan Siber 123*, Semarang Law Review, Vol.6, No.2 (Oktober 2024), p.282–98.

dan manipulasi data elektronik diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).³ Selain itu, apabila kejahatan tersebut melibatkan penyalahgunaan data pribadi korban, maka pelaku juga dapat dikenakan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.⁴ Dengan demikian, *cyber extortion* berkedok *love scamming* merupakan kejahatan yang memiliki dimensi hukum pidana, hukum siber dan perlindungan data pribadi secara sekaligus.⁵

Permasalahan hukum yang menarik untuk dikaji muncul ketika berbagai kasus *cyber extortion* berkedok *love scamming* justru dikendalikan dari dalam lembaga pemasyarakatan. Secara normatif, Pasal 3 Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan menegaskan bahwa sistem pemasyarakatan bertujuan membentuk warga binaan agar menyadari kesalahan, memperbaiki diri dan tidak mengulangi tindak pidana sehingga dapat kembali berperan sebagai anggota masyarakat yang bertanggung jawab.⁶ Namun dalam kenyataannya, sejumlah lembaga pemasyarakatan justru ditemukan menjadi pusat pengendalian berbagai tindak pidana siber, termasuk penipuan daring, perjudian online, pemerasan elektronik, hingga *love scamming*.

Kondisi tersebut menunjukkan adanya kesenjangan antara *das sollen* dan *das sein*. Kesenjangan yang dimaksud bukan karena tidak adanya aturan hukum mengenai keamanan dan penggunaan alat komunikasi di lembaga pemasyarakatan, melainkan terletak pada pelaksanaan dan efektivitas pengawasan terhadap ketentuan tersebut. Secara normatif, warga binaan dilarang memiliki, membawa, atau menggunakan alat komunikasi ilegal di dalam lembaga pemasyarakatan.

³ Indonesia, *Undang-Undang tentang Informasi dan Transaksi Elektronik*, UU No.11 Tahun 2008, LN Tahun 2008 No.58, TLN No.4843.

⁴ Indonesia, *Undang-Undang tentang Pelindungan Data Pribadi*, UU No.27 Tahun 2022, LN Tahun 2022 No.196, TLN No.6820.

⁵ Hendri Gunawan, Deny Guntara dan Muhamad Abas, *Tinjauan Yuridis Penegakan Hukum terhadap Pelaku Tindak Pidana Pemerasan dengan Ancaman Kekerasan di Hubungkan Asas Kepastian Hukum (Studi Putusan Nomor 187/Pid.B/2021/Pn.Kwg)*, Unes Law Review, Vol.6, No.1 (September 2023), p.1168–76.

⁶ Indonesia, *Undang-Undang tentang Pemasyarakatan*, UU No.22 Tahun 2022, LN Tahun 2022 No.165, TLN No.6811.

Namun, dalam praktiknya masih ditemukan penggunaan alat komunikasi oleh warga binaan untuk menjalankan tindak pidana dari dalam lembaga pemasyarakatan. Salah satu contoh konkret terjadi di Rumah Tahanan Negara Kelas IIB Kotabumi, Lampung Utara, yang pada Mei 2026 terungkap menjadi tempat pengendalian praktik *love scamming*. Berdasarkan hasil investigasi bersama Kementerian Imigrasi dan Pemasyarakatan dengan Polda Lampung, sebanyak 137 dari 145 warga binaan yang diperiksa diduga terlibat dalam praktik tersebut, dengan korban yang teridentifikasi mencapai lebih dari 1.200 orang. Praktik tersebut dilakukan melalui media sosial dan *video call* dengan memanfaatkan alat komunikasi yang seharusnya dilarang berada di dalam rutan. Kondisi tersebut memperlihatkan bahwa ketentuan hukum yang secara normatif telah mengatur keamanan dan melarang penggunaan alat komunikasi ilegal belum sepenuhnya terlaksana secara efektif dalam praktik. Dengan demikian, *das sollen* dalam penelitian ini menggambarkan kondisi ketika aturan keamanan dan pengawasan berjalan sebagaimana mestinya, sedangkan *das sein* menunjukkan kenyataan bahwa alat komunikasi ilegal masih dapat beredar dan dimanfaatkan untuk mengendalikan kejahatan dari dalam rutan.

Isu hukum yang muncul tidak hanya berkaitan dengan pertanggungjawaban pidana pelaku, tetapi juga menyangkut efektivitas sistem pengawasan dan keamanan di lembaga pemasyarakatan. Berdasarkan ketentuan peraturan perundang-undangan, narapidana dilarang memiliki atau menggunakan alat komunikasi secara ilegal di dalam lembaga pemasyarakatan. Akan tetapi, fakta menunjukkan bahwa telepon genggam, kartu SIM, akses internet, hingga rekening penampung dana masih dapat beredar dan digunakan oleh narapidana untuk menjalankan kejahatan secara terorganisir.⁷ Keadaan tersebut menimbulkan pertanyaan mengenai efektivitas pengawasan petugas pemasyarakatan, kecukupan sarana pengamanan teknologi, serta kemungkinan adanya faktor internal dan eksternal yang mendukung berlangsungnya aktivitas kejahatan dari dalam lembaga pemasyarakatan.

⁷ Mohammad Dyo Agung Purnomo, Nadir, Nur Hidayat, *Penegakan Hukum terhadap Narapidana yang Memiliki Alat Komunikasi di Dalam Lapas*, Jurnal Hukum dan Administrasi Publik, Vol.1, No. 1 (Februari 2023), p.1–10.

Dalam perspektif kriminologi, kejahatan *cyber extortion* berkedok *love scamming* di lingkungan lembaga pemasyarakatan dapat dianalisis melalui beberapa teori. *Teori Differential Association* yang dikemukakan Edwin H. Sutherland menjelaskan bahwa perilaku kriminal dipelajari melalui interaksi dengan kelompok yang memiliki orientasi menyimpang.⁸ Lingkungan lembaga pemasyarakatan yang mempertemukan berbagai pelaku kejahatan dapat menjadi tempat transfer pengetahuan dan teknik kejahatan baru. Selain itu, *Teori Opportunity dan Routine Activity Theory* menjelaskan bahwa kejahatan terjadi karena adanya pelaku yang termotivasi, target yang sesuai, serta lemahnya pengawasan. Keberadaan alat komunikasi ilegal di dalam lembaga pemasyarakatan menciptakan peluang yang memungkinkan narapidana tetap melakukan tindak pidana meskipun sedang menjalani masa pidana.⁹

Penelitian mengenai kejahatan siber dan lembaga pemasyarakatan sebenarnya telah dilakukan oleh beberapa peneliti sebelumnya. Pertama, penelitian yang dilakukan oleh Rahmawati (2022) berjudul *Penanggulangan Tindak Pidana Penipuan Online yang Dikendalikan dari Dalam Lembaga Pemasyarakatan*. Hasil penelitian menunjukkan bahwa lemahnya pengawasan dan overkapasitas lapas menjadi faktor utama terjadinya penipuan online oleh narapidana. Namun penelitian tersebut lebih berfokus pada aspek penanggulangan hukum dan belum mengkaji secara khusus modus *love scamming* maupun struktur organisasi pelaku.

Kedua, penelitian Pratama dan Nugroho (2023) berjudul *Analisis Kriminologis Kejahatan Siber di Lingkungan Pemasyarakatan*. Penelitian tersebut membahas faktor-faktor kriminogen yang menyebabkan narapidana tetap melakukan kejahatan siber selama menjalani pidana. Akan tetapi penelitian tersebut belum secara spesifik membahas *cyber extortion* berbasis hubungan romantis palsu serta mekanisme kerja sindikat yang terorganisir.

⁸ Khoirunnisa, *Peran Subdit V Cyber Crime Ditreskrimsus dalam Upaya Penanggulangan Tindak Pidana Penipuan Online dengan Bermotuskan Cinta (Romance Scam/Love Scam) (Studi Kasus Pada Kepolisian Daerah Lampung)*, Skripsi, Universitas Lampung, 2025.

⁹ M. Dhadhat Wicaksana dan Syahril Yuska, *Implementasi Manajemen Security Sebagai Upaya Pencegahan Penyelundupan Alat Komunikasi Ilegal*, *Innovative: Journal Of Social Science Research*, Vol.5, No.3 (Mei 2025), p.3156–66.

Ketiga, penelitian Sari (2024) berjudul *Pertanggungjawaban Pidana Pelaku Love Scamming melalui Media Sosial*. Penelitian ini menitikberatkan pada aspek pertanggungjawaban pidana pelaku *love scamming* berdasarkan UU ITE dan KUHP. Meskipun demikian, penelitian tersebut tidak mengkaji fenomena *love scamming* yang dikendalikan dari dalam lembaga pemasyarakatan serta tidak menganalisis faktor kelemahan sistem keamanan lapas yang memungkinkan kejahatan tersebut terjadi.

Berdasarkan ketiga penelitian terdahulu tersebut, terdapat perbedaan dan kebaruan dalam penelitian ini. Penelitian terdahulu umumnya hanya membahas kejahatan siber di lembaga pemasyarakatan, penipuan online, atau *love scamming* secara terpisah. Sementara itu, penelitian ini secara khusus mengkaji *cyber extortion* berkedok *love scamming* yang dilakukan secara terorganisir dari dalam lembaga pemasyarakatan dengan pendekatan kriminologis, termasuk analisis mengenai cara kerja, struktur pengoperasian sindikat, serta faktor-faktor yang menyebabkan sistem pengawasan dan keamanan lembaga pemasyarakatan masih dapat ditembus oleh peredaran alat komunikasi ilegal. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi teoritis dalam pengembangan kajian kriminologi siber serta kontribusi praktis bagi pembenahan sistem pemasyarakatan dan kebijakan penanggulangan kejahatan siber di Indonesia. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara kerja para pelaku serta pembagian tugas dalam menjalankan sindikat *cyber extortion* secara massal dari dalam sel tahanan?
2. Mengapa sistem pengawasan dan keamanan di lembaga pemasyarakatan masih belum mampu mencegah masuk dan beredarnya alat komunikasi yang digunakan sebagai sarana utama dalam melakukan kejahatan *cyber extortion*?

B. PEMBAHASAN

1. Cara kerja dan Struktur Pengoperasian Sindikat *Cyber Extortion* Berkedok *Love Scamming* di Dalam Sel Tahanan

Cyber extortion berkedok *love scamming* merupakan salah satu bentuk kejahatan siber yang memadukan unsur penipuan, manipulasi psikologis dan

pemerasan melalui media elektronik. Perkembangan teknologi informasi dan semakin luasnya penggunaan media sosial telah membuka peluang bagi pelaku untuk menjangkau korban tanpa dibatasi oleh ruang dan waktu. Dalam praktiknya, kejahatan ini tidak hanya dilakukan oleh individu yang berada di luar lembaga pemasyarakatan, tetapi juga ditemukan dijalankan oleh narapidana dari dalam lapas dengan memanfaatkan telepon genggam dan akses internet yang diperoleh secara ilegal. Kondisi tersebut menunjukkan bahwa perkembangan teknologi turut mengubah pola kejahatan dari bentuk konvensional menjadi kejahatan siber yang lebih terorganisir dan kompleks.¹⁰

Ditinjau dari aspek hukum, tindakan para pelaku dapat dikategorikan sebagai tindak pidana yang memenuhi unsur penipuan, pemerasan, pengancaman, serta penyalahgunaan sistem elektronik sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.^{11,12} Selain itu, apabila pelaku menggunakan atau menyebarluaskan data pribadi korban tanpa persetujuan yang sah, maka perbuatannya juga dapat dijerat dengan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

a. Cara kerja *Cyber Extortion Berkedok Love Scamming*

Pelaksanaan kejahatan ini umumnya dilakukan melalui beberapa tahapan yang saling berkaitan dan dirancang secara sistematis untuk memperoleh keuntungan dari korban.

1) Identifikasi dan Pemilihan Korban

Tahap pertama diawali dengan pencarian calon korban melalui berbagai platform digital, seperti media sosial Facebook, Instagram, WhatsApp, Telegram, TikTok, maupun aplikasi pencarian pasangan.

¹⁰ Dika Anggara Putra, Dian Rosita, *Mitigasi Love Scamming: Penegakan dan Perlindungan Hukum Tindak Pidana Pemerasan Bermodus Cinta Dika*, Bacarita Law Journal, Vol.5, No.2 (April 2025), p.315–22.

¹¹ Indonesia, *Undang-Undang tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, UU No.1 Tahun 2024, LN Tahun 2024 Nomor 1, TLN No.6905.

¹² Indonesia, *Undang-Undang tentang Kitab Undang-Undang Hukum Pidana*, UU No.1 Tahun 2023, LN Tahun 2023 No.1, TLN No. 6842.

Pelaku biasanya memilih individu yang aktif di media sosial dan secara terbuka menampilkan informasi mengenai kehidupan pribadinya. Informasi tersebut kemudian digunakan untuk mempelajari karakter, kondisi ekonomi, maupun keadaan psikologis korban sehingga memudahkan pelaku menentukan pendekatan yang akan digunakan.

Dalam perspektif kriminologi, tindakan tersebut mencerminkan proses pemilihan target (*target selection*), yaitu upaya pelaku mencari individu yang dianggap rentan dan memiliki kemungkinan besar untuk dieksploitasi.¹³

2) Pembentukan Hubungan Emosional

Setelah menentukan target, pelaku mulai membangun komunikasi dengan menggunakan identitas palsu yang sengaja dirancang agar tampak meyakinkan. Tidak jarang pelaku mengaku sebagai anggota militer, dokter, pengusaha sukses, atau warga negara asing yang memiliki kehidupan mapan. Melalui komunikasi yang dilakukan secara intensif, pelaku berusaha memperoleh kepercayaan korban dan menciptakan hubungan emosional yang kuat.

Pada tahap ini, korban diyakinkan bahwa hubungan yang terjalin merupakan hubungan yang serius dan memiliki masa depan. Berbagai janji mengenai pernikahan, investasi bersama, maupun kehidupan yang lebih baik sering digunakan sebagai sarana untuk memperkuat ketergantungan emosional korban terhadap pelaku.

3) Pemanfaatan Kepercayaan Korban

Ketika korban telah memiliki kedekatan emosional, pelaku mulai meminta informasi pribadi, foto, video, atau data lain yang bersifat sensitif. Dalam beberapa kasus, pelaku bahkan mengarahkan korban untuk melakukan komunikasi yang bersifat intim melalui panggilan video yang kemudian direkam secara diam-diam.

¹³ Fitriani, *Penegakan Hukum terhadap Kejahatan Videopenegakan Hukum terhadap Kejahatan Video Call Sex di Kota Palangka Rayangkaraya*, Skripsi, UIN Palangkaraya, 2025.

Data dan informasi yang berhasil diperoleh tersebut selanjutnya dijadikan sarana untuk mengendalikan korban. Pada tahap ini korban umumnya belum menyadari bahwa dirinya sedang menjadi sasaran kejahatan yang terencana.

Dari sudut pandang hukum, tindakan memperoleh dan menggunakan data pribadi tanpa persetujuan yang sah bertentangan dengan prinsip perlindungan data pribadi yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.¹⁴

4) Pelaksanaan *Cyber Extortion*

Setelah memperoleh materi yang dapat digunakan sebagai alat tekanan, pelaku mulai melakukan pemerasan. Korban diancam bahwa foto, video, atau informasi pribadinya akan disebarluaskan kepada keluarga, rekan kerja, maupun masyarakat luas apabila tidak memberikan sejumlah uang sesuai dengan permintaan pelaku.

Ancaman tersebut biasanya dilakukan melalui pesan elektronik, media sosial, maupun panggilan telepon. Tidak sedikit korban yang mengalami tekanan mental, rasa malu dan ketakutan sehingga memilih memenuhi tuntutan pelaku untuk menghindari penyebaran informasi pribadi yang dapat merusak reputasi mereka.

Perbuatan tersebut pada hakikatnya merupakan bentuk pemerasan yang dilakukan melalui sarana elektronik dengan tujuan memperoleh keuntungan ekonomi secara melawan hukum.¹⁵

5) Penyembunyian Hasil Kejahatan

Untuk menghindari pelacakan oleh aparat penegak hukum, dana hasil pemerasan umumnya tidak langsung diterima oleh pelaku utama. Dana tersebut dialihkan melalui rekening pihak ketiga, rekening pinjaman, dompet digital, atau individu tertentu yang berperan sebagai penampung hasil kejahatan.

¹⁴ Mohammad Teja Sali Susiana, A. Muchaddam Fahham, Lukman Nul Hakim, Fieka Nurul Arifa, *Kekerasan Seksual terhadap Perempuan di Era Digital*, Pusat Penelitian Badan Keahlian DPR RI bekerja sama dengan Intelegensia Intrans Publishing, Jakarta, 2019.

¹⁵ M. Arva Zada Subarkah, *Analisis Perlindungan Hukum terhadap Korban Transmisi Informasi Elektronik yang Melanggar Kesusilaan dan Mengandung Pemerasan*, Jurnal Publikasi Ilmu Hukum, Vol.3, No.2 (Juni 2025).

Pola tersebut menunjukkan bahwa *cyber extortion* berkedok *love scamming* sering kali dilakukan secara terorganisir dengan melibatkan jaringan yang memiliki peran masing-masing dalam mengelola hasil tindak pidana.

2. Struktur Pengoperasian Sindikat di dalam Lembaga Pemasyarakatan

Berdasarkan kajian kriminologis, tindak pidana *cyber extortion* yang dijalankan dari dalam lembaga pemasyarakatan umumnya dilakukan secara terstruktur dan melibatkan beberapa individu dengan fungsi yang berbeda-beda. Kejahatan ini tidak lagi bersifat individual, melainkan telah berkembang menjadi suatu bentuk kejahatan terorganisir.

a. Koordinator atau Pengendali

Koordinator berperan sebagai pihak yang mengatur seluruh aktivitas kelompok. Tugasnya meliputi penentuan target, penyusunan strategi operasional, pembagian peran kepada anggota, serta pengelolaan hasil kejahatan yang diperoleh.

b. Operator Akun

Operator bertanggung jawab membuat dan mengelola akun media sosial palsu yang digunakan untuk berinteraksi dengan korban. Selain itu, mereka juga mengoperasikan perangkat komunikasi dan menjaga keberlangsungan aktivitas digital kelompok.

c. Komunikator atau Scammer

Komunikator merupakan pihak yang berinteraksi langsung dengan korban. Tugas utamanya adalah membangun kedekatan emosional, memperoleh kepercayaan korban, serta menggali informasi yang dapat dimanfaatkan untuk kepentingan kelompok.

d. Eksekutor Pemerasan

Setelah materi yang dapat digunakan sebagai alat ancaman berhasil diperoleh, eksekutor mengambil peran untuk melakukan tekanan dan pemerasan terhadap korban. Mereka menentukan nominal uang yang diminta serta mengatur pola ancaman yang digunakan.

e. Penampung Dana

Bagian ini bertugas menerima, menyimpan, dan mendistribusikan hasil kejahatan. Dalam banyak kasus, penampung dana berada di luar lembaga pemasyarakatan sehingga dapat membantu menyamarkan aliran dana dan mempersulit proses pelacakan oleh aparat penegak hukum.

3. Analisis Kriminologis terhadap *Cyber Extortion* di dalam Lembaga Pemasyarakatan

Keberadaan sindikat *cyber extortion* di dalam lembaga pemasyarakatan menunjukkan bahwa tujuan pembinaan narapidana sebagaimana diamanatkan dalam Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan belum sepenuhnya tercapai.¹⁶ Lembaga pemasyarakatan yang seharusnya menjadi sarana rehabilitasi dan reintegrasi sosial justru dalam beberapa kasus dimanfaatkan sebagai tempat untuk merencanakan dan mengendalikan tindak pidana baru.

Menurut *Teori Differential Association* yang dikemukakan oleh Edwin H. Sutherland, perilaku kriminal dipelajari melalui interaksi dengan individu atau kelompok yang memiliki nilai dan pola perilaku menyimpang. Dalam konteks lembaga pemasyarakatan, interaksi antar narapidana dapat menjadi sarana pertukaran pengetahuan mengenai teknik penipuan, pemerasan, serta pemanfaatan teknologi digital untuk melakukan kejahatan.

Selain itu, *Teori Opportunity* menjelaskan kejahatan cenderung terjadi ketika terdapat kesempatan yang memungkinkan pelaku menjalankan aksinya. Keberadaan telepon genggam, kartu SIM, serta akses internet ilegal di dalam lembaga pemasyarakatan menjadi faktor yang membuka peluang bagi narapidana untuk tetap melakukan tindak pidana meskipun sedang menjalani hukuman.

Fenomena ini juga dapat dipahami melalui *Routine Activity Theory* yang menyatakan bahwa kejahatan muncul karena adanya pelaku yang termotivasi, target yang mudah dijangkau, dan lemahnya pengawasan. Dalam kasus *cyber extortion* berkedok *love scamming*, ketiga unsur tersebut hadir secara bersamaan. Pelaku memiliki motif ekonomi, korban dapat ditemukan dengan mudah melalui media sosial, sedangkan pengawasan terhadap penggunaan alat komunikasi di dalam lembaga pemasyarakatan masih belum berjalan secara optimal.

¹⁶ Afdhal Mahatta Agus Budianto, *Pembaharuan Hukum terhadap Kebijakan Pengelolaan Lembaga Pemasyarakatan*, Law Review, Vol.21, No. 3 (Maret 2022), p.389–407.

Dengan demikian, keberlangsungan *cyber extortion* yang dikendalikan dari dalam lembaga pemasyarakatan tidak hanya disebabkan oleh faktor individu pelaku, tetapi juga dipengaruhi oleh lemahnya kontrol institusional, pengawasan keamanan dan efektivitas sistem pembinaan narapidana. Oleh karena itu, selain penegakan hukum terhadap pelaku, diperlukan penguatan sistem keamanan, peningkatan integritas petugas, serta optimalisasi pengawasan terhadap peredaran alat komunikasi agar lembaga pemasyarakatan tidak lagi menjadi pusat pengendalian kejahatan siber.

4. Faktor Penyebab Sistem Pengawasan dan Keamanan Lembaga Pemasyarakatan Masih Dapat Ditembus oleh Peredaran Alat Komunikasi

Masih terjadinya praktik *cyber extortion* berkedok *love scamming* yang dikendalikan dari dalam lembaga pemasyarakatan menunjukkan bahwa sistem pengawasan dan pengamanan yang diterapkan belum sepenuhnya efektif. Padahal, lembaga pemasyarakatan pada hakikatnya merupakan institusi yang bertujuan membina dan mengembalikan narapidana menjadi anggota masyarakat yang taat hukum sebagaimana diamanatkan dalam Pasal 3 Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan. Namun, kenyataan bahwa narapidana masih dapat mengakses telepon genggam dan jaringan internet secara ilegal memperlihatkan adanya berbagai kelemahan dalam sistem pengawasan yang membuka peluang terjadinya kejahatan siber dari balik tembok penjara.

Dalam perspektif kriminologi, kejahatan tidak hanya dipengaruhi oleh niat pelaku, tetapi juga oleh adanya kesempatan dan lemahnya mekanisme pengendalian sosial. Oleh karena itu, keberadaan alat komunikasi ilegal di dalam lapas dapat dipahami sebagai akibat dari berbagai faktor yang saling berkaitan, baik yang berasal dari aspek kelembagaan, sumber daya manusia, maupun faktor eksternal.

a. Kondisi Overkapasitas Lembaga Pemasyarakatan

Salah satu permasalahan mendasar yang dihadapi sistem pemasyarakatan di Indonesia adalah tingginya tingkat hunian yang melebihi kapasitas. Jumlah warga binaan yang jauh lebih besar dibandingkan daya tampung lapas menyebabkan fungsi pengawasan menjadi tidak optimal.

Dalam kondisi seperti ini, petugas mengalami kesulitan untuk memantau aktivitas setiap narapidana secara menyeluruh.¹⁷

Kepadatan penghuni juga berdampak pada efektivitas pelaksanaan pengeledahan kamar, pemeriksaan barang bawaan, serta pengawasan terhadap pergerakan narapidana. Situasi tersebut memberikan ruang bagi warga binaan untuk menyembunyikan barang-barang terlarang, termasuk telepon genggam, kartu SIM, modem internet, maupun perangkat elektronik lainnya yang dapat digunakan sebagai sarana melakukan tindak pidana.

Apabila dikaitkan dengan tujuan pemasyarakatan, kondisi overkapasitas jelas menghambat proses pembinaan dan pengawasan sebagaimana yang dikehendaki oleh Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan. Dari sudut pandang kriminologi, keadaan ini menciptakan peluang (*opportunity*) yang memungkinkan terjadinya penyimpangan karena kemampuan pengawasan petugas menjadi terbatas.

b. Keterbatasan Kuantitas dan Kapasitas Petugas Pemasyarakatan

Efektivitas pengamanan suatu lembaga pemasyarakatan sangat dipengaruhi oleh jumlah dan kualitas petugas yang tersedia. Pada kenyataannya, jumlah petugas di banyak lapas masih belum sebanding dengan jumlah warga binaan yang harus diawasi. Ketimpangan tersebut menyebabkan pengawasan tidak dapat dilakukan secara maksimal sehingga berbagai pelanggaran tata tertib lebih mudah terjadi.

Selain persoalan jumlah personel, perkembangan teknologi yang begitu pesat juga menghadirkan tantangan baru. Modus kejahatan siber saat ini semakin kompleks karena memanfaatkan berbagai aplikasi digital, akun anonim, dompet elektronik, hingga teknologi komunikasi yang sulit dilacak. Kondisi tersebut menuntut petugas pemasyarakatan untuk memiliki kemampuan dan pemahaman yang memadai mengenai perkembangan kejahatan siber.

¹⁷ Yustiana, Muhammad Yunus, Sarmila Sanjaya, *Implikasi Hukum atas Pelaksanaan Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan terhadap Pemenuhan Hak Warga Binaan Khususnya Pembinaan dan Asimilasi pada Narapidana dengan Kasus Narkotika dan Over Capacity di Rumah Tahanan Negara Kelas II B Sen*, Legal Journal of Law, Vol.2, No.1 (Mei 2023), p.91–105.

Apabila kompetensi petugas tidak berkembang seiring dengan perkembangan teknologi, maka upaya deteksi dan pencegahan terhadap aktivitas ilegal yang dilakukan narapidana akan menjadi kurang efektif. Akibatnya, keberadaan perangkat komunikasi dan aktivitas siber ilegal di dalam lapas sering kali baru diketahui setelah menimbulkan kerugian bagi masyarakat.

c. Keterlibatan Oknum Petugas dalam Peredaran Barang Terlarang

Masuknya telepon genggam dan perangkat komunikasi lainnya ke dalam lembaga pemasyarakatan tidak selalu terjadi karena kelalaian sistem semata. Dalam sejumlah kasus yang pernah terungkap, ditemukan adanya keterlibatan oknum petugas yang secara sengaja membantu memasukkan atau memfasilitasi penggunaan alat komunikasi oleh narapidana.¹⁸

Tindakan tersebut biasanya dilatarbelakangi oleh faktor ekonomi, rendahnya integritas, penyalahgunaan jabatan, maupun lemahnya pengawasan internal. Keadaan ini menjadi persoalan serius karena petugas pemasyarakatan merupakan pihak yang seharusnya bertanggung jawab menjaga keamanan dan ketertiban di dalam lapas.

Dari perspektif hukum, keterlibatan oknum petugas dalam memfasilitasi tindak pidana tidak hanya merupakan pelanggaran disiplin, tetapi juga dapat menimbulkan pertanggungjawaban pidana apabila terbukti turut serta atau membantu terlaksananya suatu kejahatan. Fenomena ini menunjukkan bahwa keberhasilan pelaku menjalankan *cyber extortion* tidak terlepas dari adanya kelemahan pada sistem pengawasan internal lembaga pemasyarakatan.

d. Belum Optimalnya Penggunaan Teknologi Pengamanan

Di era digital, pengamanan lembaga pemasyarakatan tidak lagi cukup dilakukan melalui pengawasan fisik semata. Diperlukan dukungan teknologi yang mampu mendeteksi dan mencegah penggunaan alat komunikasi secara ilegal. Namun, tidak semua lapas memiliki sarana dan prasarana keamanan yang memadai.

¹⁸ M. Risky, *Penerapan Sanksi Terhadap Narapidana Yang Membawa Alat Elektronik Di Lembaga Pemasyarakatan Kelas Ii A Pekanbaru*, Skripsi, Universitas Lancang Kuning Pekanbaru, 2024.

Beberapa lembaga pemasyarakatan masih menghadapi keterbatasan dalam penggunaan alat pemutus sinyal (*signal jammer*), kamera pengawas (*CCTV*), sistem pemantauan digital, alat pendeteksi telepon genggam, maupun perangkat keamanan elektronik lainnya. Akibatnya, aktivitas komunikasi ilegal yang dilakukan narapidana sering kali luput dari pengawasan.

Keterbatasan teknologi tersebut memberikan kesempatan bagi pelaku untuk mengakses internet dan menjalankan berbagai aktivitas kejahatan siber dari dalam lapas. Bahkan dalam beberapa kasus, narapidana mampu mengoperasikan sejumlah akun media sosial dan aplikasi komunikasi tanpa terdeteksi dalam waktu yang cukup lama.

e. Adanya Dukungan Jaringan Kejahatan dari Luar Lembaga Pemasyarakatan

Kejahatan *cyber extortion* berkedok *love scamming* pada umumnya tidak dilakukan secara individual, melainkan melibatkan jaringan yang terorganisir. Walaupun pelaku utama berada di dalam lapas, operasional kejahatan sering kali didukung oleh pihak-pihak yang berada di luar lembaga pemasyarakatan.

Jaringan eksternal tersebut berperan menyediakan perangkat komunikasi, kartu SIM, rekening penampung, identitas palsu, hingga membantu proses pencairan dan distribusi dana hasil kejahatan. Dukungan tersebut memungkinkan aktivitas sindikat tetap berjalan meskipun pengendali utama sedang menjalani pidana.

Keberadaan jaringan luar menunjukkan bahwa *cyber extortion* yang dikendalikan dari dalam lapas telah berkembang menjadi bentuk kejahatan siber terorganisir (*organized cybercrime*). Oleh karena itu, penanggulangannya tidak dapat hanya difokuskan pada pelaku yang berada di dalam lembaga pemasyarakatan, tetapi juga harus menasar jaringan pendukung yang beroperasi di luar lapas.¹⁹

¹⁹ Dicky Putra Arumawan, *Upaya Kepolisian dalam Rangka Menjaga Keamanan Sistem M-Banking terhadap Ancaman Serangan Siber Melalui Teknik Scamming*, Tesis, Universitas Lampung, 2023.

f. Analisis Berdasarkan Teori Kontrol Sosial

Menurut Travis Hirschi dalam Teori Kontrol Sosial (*Social Control Theory*), seseorang cenderung menaati norma dan hukum apabila terdapat kontrol sosial yang kuat dalam lingkungannya. Sebaliknya, apabila kontrol tersebut melemah, peluang terjadinya perilaku menyimpang akan semakin besar.

Dalam konteks lembaga pemasyarakatan, kontrol sosial diwujudkan melalui pengawasan petugas, penegakan tata tertib, pembinaan kepribadian, serta pengendalian terhadap seluruh aktivitas warga binaan. Ketika fungsi-fungsi tersebut tidak berjalan secara efektif, maka peluang bagi narapidana untuk melakukan pelanggaran, termasuk kejahatan siber, menjadi semakin terbuka.

Dengan demikian, keberhasilan pelaku menjalankan *cyber extortion* dari dalam lapas bukan hanya disebabkan oleh faktor individu, tetapi juga menunjukkan adanya kelemahan dalam sistem kontrol institusional yang seharusnya mampu mencegah terjadinya penyimpangan.

g. Analisis Berdasarkan Teori Aktivitas Rutin

Teori Aktivitas Rutin (*Routine Activity Theory*) yang dikemukakan oleh Lawrence Cohen dan Marcus Felson menjelaskan bahwa suatu kejahatan terjadi karena bertemunya tiga unsur, yaitu pelaku yang memiliki motivasi, target yang mudah dijangkau dan tidak adanya pengawasan yang efektif.

Ketiga unsur tersebut dapat ditemukan dalam kasus *cyber extortion* berkedok *love scamming* yang dijalankan dari dalam lembaga pemasyarakatan. Narapidana memiliki motivasi ekonomi untuk memperoleh keuntungan, korban dapat ditemukan dengan mudah melalui media sosial, sedangkan pengawasan terhadap penggunaan alat komunikasi masih memiliki berbagai kelemahan.²⁰

Keberadaan telepon genggam dan akses internet ilegal menjadi sarana memertemukan ketiga unsur itu sehingga kejahatan dapat terus berlangsung.

²⁰ Rianti Zahrotul Aini dan Nadia Utami Larasati, *Analisis Teori Aktivitas Rutin terhadap Korban Eksibisionisme*, *Anomie: Jurnal Kriminologi*, Vol.3, No.3 (Desember 2021), p.138–50.

Oleh sebab itu, selama peredaran alat komunikasi ilegal belum dapat diberantas secara menyeluruh, potensi terjadinya kejahatan siber yang dikendalikan dari dalam lembaga pemasyarakatan akan tetap ada.

Berdasarkan uraian di atas, dapat disimpulkan bahwa masih mudahnya peredaran alat komunikasi di dalam lembaga pemasyarakatan merupakan akibat dari berbagai faktor yang saling berkaitan, yaitu overkapasitas penghuni, keterbatasan jumlah dan kompetensi petugas, keterlibatan oknum petugas, belum optimalnya pemanfaatan teknologi pengamanan, serta kuatnya jaringan kejahatan yang beroperasi di luar lapas. Faktor-faktor tersebut menunjukkan bahwa upaya pencegahan kejahatan siber di lingkungan pemasyarakatan memerlukan pembenahan yang menyeluruh, baik melalui peningkatan kualitas sumber daya manusia, penguatan sistem pengawasan, pemanfaatan teknologi keamanan yang lebih modern, maupun penegakan hukum yang tegas terhadap setiap pihak yang terlibat dalam peredaran alat komunikasi ilegal.

C. PENUTUP

Berdasarkan hasil penelitian, dapat disimpulkan bahwa *cyber extortion* berkedok *love scamming* yang dikendalikan dari dalam lembaga pemasyarakatan merupakan kejahatan siber terorganisir yang dilakukan melalui pemanfaatan teknologi informasi, manipulasi emosional korban dan penggunaan alat komunikasi ilegal. Kejahatan ini dapat terus berlangsung karena dipengaruhi oleh berbagai faktor, antara lain overkapasitas lapas, keterbatasan jumlah dan kompetensi petugas, keterlibatan oknum petugas, lemahnya pemanfaatan teknologi pengamanan, serta adanya dukungan jaringan kejahatan di luar lembaga pemasyarakatan. Oleh karena itu, diperlukan penguatan sistem pengawasan dan keamanan lapas melalui peningkatan integritas dan kapasitas petugas, optimalisasi penggunaan teknologi pengamanan, serta kerja sama yang lebih efektif antara lembaga pemasyarakatan dan aparat penegak hukum guna mencegah serta memberantas kejahatan siber yang dikendalikan dari dalam lapas.

DAFTAR PUSTAKA

Buku

Susiana, Mohammad Teja Sali, A. Muchaddam Fahham, Lukman Nul Hakim, Fieka Nurul Arifa. 2019. *Kekerasan Seksual terhadap Perempuan di Era Digital*. (Jakarta: Pusat Penelitian Badan Keahlian DPR RI bekerja sama dengan Intelegensia Intrans Publishing).

Publikasi

Afdhal Mahatta Agus Budianto. Pembaharuan Hukum terhadap Kebijakan Pengelolaan Lembaga Pemasyarakatan. *Law Review*. Vol.21. No.3 (Maret 2022).

Aini, Rianti Zahrotul dan Nadia Utami Larasati. *Analisis Teori Aktivitas Rutin terhadap Korban Eksibisionisme*. *Anomie: Jurnal Kriminologi*. Vol.3. No.3 (Desember 2021).

Fairuzzen, Mohamad Revaldy, dkk.. *Perkembangan Hukum dan Kejahatan Siber 'Cybercrime' di Indonesia*. *Indonesian Journal of Islamic Jurisprudence Economic and Legal Theory*. Vol.2. No.1 (Januari 2024).

Gunawan, Hendri, Deny Guntara dan Muhamad Abas. *Tinjauan Yuridis Penegakan Hukum terhadap Pelaku Tindak Pidana Pemerasan dengan Ancaman Kekerasan dihubungkan Asas Kepastian Hukum (Studi Putusan Nomor 187/Pid.B/2021/PN Kwg)*. *Unes Law Review*. Vol.6. No.1 (September 2023).

Purnomo, Mohammad Dyo Agung, Nadir dan Nur Hidayat. Penegakan Hukum terhadap Narapidana yang Memiliki Alat Komunikasi di Dalam Lapas. *Jurnal Hukum dan Administrasi Publik*. Vol.1. No.1 (Februari 2023).

Putra, Dika Anggara dan Dian Rosita. *Mitigasi Love Scamming: Penegakan dan Perlindungan Hukum Tindak Pidana Pemerasan Bermodus Cinta*. *Bacarita Law Journal*. Vol.5. No.2 (April 2025).

Sofiana, Normatriya, dkk.. *Analisis Yuridis Tindak Pidana Love Scamming sebagai Kejahatan Siber*. *Semarang Law Review*. Vol.6. No.2 (Oktober 2024).

Subarkah, M. Arva Zada. *Analisis Perlindungan Hukum terhadap Korban Transmisi Informasi Elektronik yang Melanggar Kesusilaan dan Mengandung Pemerasan*. *Jurnal Publikasi Ilmu Hukum*. Vol.3. No.2 (Juni 2025).

Wicaksana, M. Dhadhat dan Syahril Yuska. *Implementasi Manajemen Security sebagai Upaya Pencegahan Penyelundupan Alat Komunikasi Ilegal*. *Innovative: Journal of Social Science Research*. Vol.5. No.3 (Mei 2025).

Yunus, Yustiana, Muhammad dan Sarmila Sanjaya. *Implikasi Hukum atas Pelaksanaan Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan terhadap Pemenuhan Hak Warga Binaan Khususnya Pembinaan dan Asimilasi pada Narapidana dengan Kasus Narkotika dan Over Capacity di Rumah Tahanan Negara Kelas II B Sen*. *Legal Journal of Law*. Vol.2. No.1 (Mei 2023).

Karya Ilmiah

- Arumawan, Dicky Putra. 2023. *Upaya Kepolisian dalam Rangka Menjaga Keamanan Sistem M-Banking terhadap Ancaman Serangan Siber Melalui Teknik Scamming*. Tesis. Lampung: Universitas Lampung.
- Fitriani. 2025. *Penegakan Hukum terhadap Kejahatan Videopenegakan Hukum terhadap Kejahatan Video Call Sex di Kota Palangkaraya Rayangkaraya*. Skripsi. Palangkaraya: UIN Palangkaraya.
- Khoirunnisa. 2025. *Peran Subdit V Cyber Crime Ditreskrimsus dalam Upaya Penanggulangan Tindak Pidana Penipuan Online dengan Bermoduskan Cinta (Romance Scam/Love Scam) (Studi Kasus Pada Kepolisian Daerah Lampung)*. Skripsi. Lampung: Universitas Lampung.
- Risky, M.. 2024. *Penerapan Sanksi Terhadap Narapidana Yang Membawa Alat Elektronik Di Lembaga Pemasyarakatan Kelas II A Pekanbaru*. Skripsi. Pekanbaru: Universitas Lancang Kuning Pekanbaru.

Sumber Hukum

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.
- Undang-Undang Nomor 22 Tahun 2022 tentang Pemasyarakatan. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 165. Tambahan Lembaran Negara Republik Indonesia Nomor 6811.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.
- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6905.