Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

ANALYSIS OF LOVE SCAM: CASE STUDY OF SEXTORTION INVOLVING A MEMBER OF THE MEDAN DPRD

Handy Senonugroho[1)] *,
[1]Sekolah Tinggi Ilmu Kepolisian-Indonesia
Corresponding Author: handysenonugroho.68@gmail.com

ABSTRACT

The rapid advancement of communication technology has brought about significant changes in societal interactions, but it has also amplified the threat of cybercrimes, including love scams and sextortion. This article explores cases of sextortion involving a convict and a member of a regional legislative council, while delineating the cyberculture and space transition factors that facilitate these crimes. Furthermore, the article adopts a qualitative approach with case study method and literature study to comprehend the phenomena of love scams, sextortion, and related cases. Policing strategies for tackling sextortion are presented, with an emphasis on e-policing. Conclusions and recommendations for effectively combating sextortion are also discussed, including the importance of prevention, the utilization of technology, and a focus on victim recovery. The article proposes a collaborative effort to address this issue comprehensively.

Keywords: Sextortion, Cybercrime, E-Policing, Love scams, Cyberculture.

ABSTRAK

Perkembangan pesat teknologi komunikasi telah membawa perubahan besar dalam interaksi masyarakat, tetapi juga meningkatkan ancaman kejahatan cyber, termasuk love scams dan sextortion. Artikel ini membahas kasus-kasus sextortion yang melibatkan seorang narapidana dan seorang anggota DPRD, serta menguraikan faktor-faktor dalam cyberculture dan space transition yang memungkinkan terjadinya kejahatan ini. Selain itu, artikel ini mengadopsi pendekatan kualitatif dengan metode studi kasus dan studi literatur untuk memahami fenomena love scam, sextortion, dan kasus serupa. Strategi pemolisian untuk mengatasi sextortion juga disajikan, dengan fokus pada pendekatan e-policing. Kesimpulan dan saran untuk penanggulangan efektif kejahatan sextortion juga dibahas, termasuk pentingnya pencegahan, penggunaan teknologi, dan perhatian terhadap pemulihan korban. Artikel ini mengusulkan upaya kolaboratif untuk mengatasi masalah ini secara holistik.

Kata Kunci: Pemerasan seksual, Kejahatan dunia maya, E-Policing, Penipuan cinta, Budaya dunia maya

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Pendahuluan

Pesatnya perkembangan teknologi komunikasi telah membawa perubahan besar dalam cara hidup dan interaksi masyarakat. Namun, dampak negatifnya juga muncul dalam bentuk *cybercrime* yang menjadi kekhawatiran serius. Kejahatan *cyber* terhadap individu dapat diklasifikasikan menjadi empat bagian (Marie-Helen, 2014), yaitu pencurian identitas, predasi seksual, penipuan, dan predasi keuangan. Hal ini menimbulkan kerugian materiil dan non-materiil, serta mempengaruhi citra dan transaksi bisnis *online* di Indonesia. Menurut perusahaan keamanan *Symantec* dalam *Internet Security Threat Report* volume 17, Indonesia masuk dalam peringkat sepuluh negara dengan aktivitas kejahatan *cyber* terbanyak di dunia dan menyumbang sebesar 2,4% kejahatan *cyber* di dunia (Juditha, 2015). Faktor ini dipengaruhi oleh peningkatan pengguna internet dan jejaring sosial di Indonesia. Pengguna sering kali mudah percaya terhadap *link* atau konten yang diterima dari teman-teman mereka di jejaring sosial, membuka celah bagi penjahat *cyber*.

Salah satu modus kejahatan *cyber* yang merugikan adalah *love scams*, di mana para pelaku penipuan berhasil memanipulasi korban melalui hubungan yang dibangun secara *online* sebelum meminta uang. Pola komunikasi dalam dunia maya cenderung lebih dipercaya oleh korban, yang berdampak pada penurunan interaksi fisik dan tingkat keakraban antar individu (Madonna et al., 2022; Pratama, 2017). Kasus-kasus *sextortion* juga menjadi perhatian, di mana pelaku merekam foto dan video korban selama *Video Call Sex* (VCS) dan memeras mereka dengan ancaman penyebaran. Kejahatan *sextortion* ini menyebabkan *multi-victim* bagi korbannya yang menimbulkan kerugian selain materi juga harga diri dan nama baik (Silver, 2004).

Kasus *sextortion* yang terbaru menjadi perhatian publik dan menimbulkan keresahan adalah kasus pemerasan dengan modus VCS di Kalimantan Tengah dengan korban mencapai 12 orang yang memiliki latar belakang profesi bermacam-macam ada yang PNS dan profesi lainnya. Pihak kepolisian saat ini masih melacak pelaku *scammers* tersebut. Terdapat penelitian terdahulu yang telah melakukan analisis terkait dengan *love scam*, yaitu penelitian berjudul "Pola Komunikasi Dalam *Cybercrime* (Kasus *Love Scams*)" yang diteliti oleh Christiany Juditha (2015). Penelitian tersebut membahas tentang salah satu jenis *cybercrime* yang sering dialami oleh perempuan Indonesia adalah *love scams*, yaitu penipuan dalam hubungan cinta melalui internet. Pola komunikasi yang dilakukan oleh pelaku *cybercrime (scammers)* yang belum dikenal oleh korban cenderung lebih dipercaya daripada komunikasi

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

langsung dari orang yang sudah dikenal dekat. Penelitian tersebut bertujuan untuk menggambarkan pola komunikasi dalam kasus *cybercrime* (Juditha, 2015).

Pada sekitar Juli 2020 terjadi juga kasus yang cukup menjadi perhatian publik, yaitu *sextortian* dengan pelakunya adalah seorang narapidana yang sedang menjalani hukuman pidananya di lapas dan korbannya adalah seorang perempuan yang merupakan anggota DPRD Medan (Fasya et al., 2023). Hal yang menarik untuk membahas kasus tersebut dalam penulisan ini dilihat dari perspektif *Computer Mediated Communication*, *Cyber Culture* dan *Space Transition Theory* (Walther, 1996), mengapa orang yang sudah menjadi narapidana dapat melakukan aksi kejahatan kembali dari dalam Lapas, dan seorang anggota DPRD yang memiliki latar belakang pendidikan kesarjanaan serta tingkatan sosial yang tinggi sebagai wakil rakyat yang terhormat dapat menjadi korban *sextortian*. Serta bagaimana upaya pemolisian dalam melakukan pencegahan *sextortian* yang semakin marak.

Metode Penelitian

Penelitian ini mengadopsi pendekatan kualitatif yang bertujuan untuk memahami fenomena yang dialami oleh subjek penelitian, sesuai dengan pandangan Lexy J. Moleong (2019). Metode penelitian yang digunakan melibatkan studi kasus, di mana beberapa kasus konkret terkait dengan love scam, sextortion, dan peristiwa serupa diselidiki secara mendalam. Selain itu, penelitian ini juga mengandalkan studi literatur, yang melibatkan peninjauan sumber-sumber yang telah terpublikasi sebelumnya tentang topik tersebut (Sugiono, 2014). Dengan berfokus pada sumber-sumber terpercaya, penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif tentang fenomena love scam, sextortion, dan kasus sejenis yang telah terjadi.

Metode penelitian yang digunakan adalah analisis isi kualitatif dengan menggunakan model *Computer Mediated Communication* (CMC) yang terdiri dari *impersonal, interpersonal, dan hyperpersonal* (Sumanti, 2023). Penelitian tersebut menyimpulkan bahwa ketiga pola komunikasi ini terjadi dalam kasus *love scam*. Faktor sumber pesan (*scammers*) memiliki kendali yang besar terhadap identitas mereka sendiri dan mengatur komunikasi dengan korban tanpa diketahui oleh korban mengenai siapa sebenarnya mereka. Oleh karena itu, para *scammers* umumnya berusaha untuk menyampaikan unsur-unsur diri yang terbaik, termasuk kepribadian, prestasi, dan bahkan penampilan (foto) melalui saluran komunikasi internet. Penerima pesan (korban) yang sedang merasa kesepian dan mencari jodoh sering kali langsung terpancing oleh pesan cinta dan tanpa berpikir panjang memberikan umpan balik.

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Komunikasi intensif pun terjalin, dan akibatnya korban terjebak dan mengalami kerugian finansial yang mencapai ratusan juta rupiah.

Hasil dan Pembahasan

Kasus *Sextortian* Pelaku Narapidana dan Korban Oknum Anggota Dewan

Dikutip dari https://cirebon.tribunnews.com/, pemberitaan tanggal 18 Januari 2022 dengan judul "Video Panas Anggota DPRD VCS dengan Napi yang Ngaku Polisi Tersebar hingga Diperas, Ini Sosoknya". Anggota DPRD Medan berinisial SS menjadi korban tipu daya oleh narapidana bernama Porsea Paulus Bartolomeus Hutapea alias Muhammad Rajaf. Pelaku menggunakan akun Facebook dengan nama Eligius Fernatubun dan berhasil merayu SS melalui messenger. Mereka menjalin hubungan yang semakin intim dan melakukan *video call sex*. Tanpa sepengetahuan SS, pelaku merekam adegan tersebut dan memotongnya menjadi 5 bagian.

Setelah itu, pelaku mulai memeras SS dengan mengancam akan menyebarkan video tersebut jika tidak memenuhi permintaannya. Pelaku bahkan mengajak korban untuk terlibat dalam bisnis batubara di Manokwari, Papua Barat, dan berhasil memperoleh sejumlah uang dari korban. Namun, SS mulai curiga dan memutuskan komunikasi dengan pelaku. Pelaku kemudian mengancam akan menyebar video porno tersebut di media sosial dan memeras SS untuk mendapatkan uang. SS melaporkan kasus ini ke polisi, namun pelaku tetap mengunggah video bugil SS di Facebook menggunakan akun palsu milik korban. Video tersebut menjadi viral di media sosial.

Pada Maret 2021, pelaku divonis hukuman penjara selama 4 tahun atas pembuatan dan penyebaran video asusila SS. Kasus ini menyoroti pentingnya literasi digital serta kesadaran dan kewaspadaan dalam interaksi *online* serta perlindungan terhadap privasi dan keamanan pribadi.

Computer Mediated Communication (CMC) Sebagai Interaksi Impersonal, Interpersonal dan Hyperpersonal dalam Sextortian.

Analisis artikel tersebut berdasarkan teori *Computer Mediated Communication* (CMC) menunjukkan adanya interaksi impersonal, interpersonal, dan hyperpersonal dalam kasus *sextortion* yang melibatkan korban SS. Dalam konteks ini, CMC mengacu pada komunikasi yang terjadi melalui media komputer, seperti pesan teks, *video call*, dan jejaring sosial (Georgakopoulou, 2011; Kiesler et al., 1984).

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Interaksi impersonal terjadi saat pelaku menggunakan akun palsu dan identitas palsu (Eligius Fernatubun) untuk merayu dan membangun hubungan dengan korban SS. Pelaku berusaha menciptakan keterhubungan dengan korban dengan mengaku sebagai anggota polisi yang tugas di Papua. Melalui CMC, pelaku dapat memanipulasi informasi dan identitas dirinya untuk mengelabui korban. Selanjutnya, interaksi interpersonal terjadi saat korban SS dan pelaku saling berkenalan dan saling berinteraksi melalui pesan teks dan *video call*. Mereka mulai menjalin hubungan yang semakin intim dan pribadi (Hadiono, 2018). Pelaku berhasil memanfaatkan kerentanan emosional korban dengan menggunakan romantisisme dan cinta palsu sebagai strategi untuk memperoleh kepercayaan SS. Dalam konteks hyperpersonal, CMC memberikan kesempatan bagi pelaku untuk memperkuat dan mempercepat pembangunan hubungan dengan korban. Pelaku dapat memilih dan menyaring informasi yang ingin disampaikan kepada korban, memanfaatkan waktu dalam membangun kedekatan, dan memanipulasi gambaran dirinya agar terlihat lebih meyakinkan dan menarik bagi korban. Hal ini memungkinkan intensitas hubungan dan perasaan yang tumbuh antara korban dan pelaku menjadi lebih kuat daripada interaksi yang terjadi secara fisik. Pada interaksi *hyperpersonal* muncul rasa ketergantungan terhadap komunikasi CMC dibandingkan dengan interaksi tatap muka. Hal ini dipengaruhi oleh beberapa aspek diantaranya:

a. Sumber Pesan: Pelaku yang berperan aktif sebagai pengirim pesan memberikan komunikasi intens romantisme dan cinta palsu kepada korbannya dengan penggunaan bahasa, gaya bahasa dan tehnik manipulasi. Dengan mengaku sebagai anggota polisi, pelaku terus memanfaatkan kerentanan korban yang sudah terpedaya yang pada akhirnya melakukan kominikasi VCS.
b. Penerima Pesan: korban yang menjadi penerima pesan merespons pesan yang diterimanya, dengan anggapan dan imajinasinya yang dibentuk oleh pelaku. Korban akan menganggap benar identitas pelaku yang dibangun dengan menebar cinta dan kata-kata indah. Korban yang seorang wanita berumur tentunya jarang mendapatkan hal semacam itu baik didunia nyatanya maupun dengan orang lain di dunia digital, sehingga korban lebih mudah terpedaya.
c. Saluran Komunikasi: Komunikasi dilakukan melalui saluran CMC berupa handphone melalui platform media sosial, meliputi pesan teks, panggilan telepon, atau *video call*. Dimana hal tersebut dimanfaatkan pelaku untuk membangun dan menunjukan identitas diri seolah-olah sebagai seorang anggota polisi dengan karakter yang baik dan romantis.

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

d. Umpan Balik Berkelanjutan: Interaksi *hyperpersonal* melibatkan umpan balik yang berkelanjutan antara pelaku dan korban. Interaksi ini terjadi secara terus menerus dan berkelanjutan hingga terbentuk hubungan ketergantungan untuk terus menjalin komunikasi. Disaat inilah pelaku meminta VCS dengan korban. Korban yang sudah terpedaya dengan karakter yang dibangun oleh pelaku, tanpa disadari dengan akal sehat menuruti permintaan pelaku. Dan pelaku memanfaatkan kesempatan tersebut dengan merekam VCS tanpa disadari korban.

Dalam kasus *sextortion* ini, pemanfaatan kerentanan gender korban SS menjadi faktor yang dimanfaatkan oleh pelaku (HANAVIA, 2022). Pelaku memanfaatkan keinginan SS untuk menjalin hubungan dan memanipulasi perasaannya melalui romantisme dan cinta palsu. Melalui CMC, pelaku dapat memanipulasi informasi, identitas, dan komunikasi untuk mencapai tujuan kejahatannya. Analisis ini menunjukkan betapa pentingnya kesadaran dan kewaspadaan dalam berinteraksi melalui media komputer . Pengguna CMC harus mewaspadai potensi penipuan, memeriksa keaslian identitas orang yang mereka temui online, dan melindungi privasi dan keamanan pribadi mereka. Selain itu, perlindungan terhadap kerentanan gender dalam konteks online juga perlu diperhatikan untuk mencegah kasus-kasus seperti *sextortion*.

Pelaku dan Korban Sextortian Dalam Perspektif *Cyber Culture*

Dalam perspektif *Cyber Culture*, kasus tersebut menunjukkan bagaimana pelaku dan korban *sextortion* terlibat dalam praktik yang melanggar norma dan nilai-nilai yang seharusnya ada dalam interaksi *online*. Pelaku *sextortion* mengabaikan norma dan nilai-nilai etika yang seharusnya diterapkan dalam *Cyber Culture*. Mereka memanfaatkan anonimitas dan *pseudonymity* untuk menyamarkan identitas asli mereka, yang memungkinkan mereka untuk beroperasi dengan kebebasan dan keberanian yang lebih besar. Mereka juga mungkin memiliki banyak akun yang berbeda untuk menjaring korban lebih banyak lagi. Pelaku menggunakan modus operandi yang dimulai dengan interaksi teks dan kemudian berkembang menjadi keintiman hingga melakukan *video call seksual*. Beberapa pelaku bahkan mungkin sudah sering melakukan praktik *sextortion* secara *online* dengan berbagai korban, yang membuat mereka merasa mudah mendapatkan keuntungan finansial dari tindakan mereka. Hal ini dapat mempengaruhi gaya hidup dan perilaku mereka di dunia nyata, seperti terlihat dalam artikel dengan pelaku mengkonsumsi narkotika di dalam penjara.

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Di sisi korban, mereka juga terlibat dalam tindakan yang melanggar norma dan nilai-nilai *Cyber Culture*. Sebagai seorang anggota DPRD, korban menggunakan identitas asli mereka dan berinteraksi dalam kapasitas mereka sebagai pejabat publik. Hal ini membuat mereka menjadi target potensial bagi pelaku, yang melihat mereka sebagai korban yang berpeluang memberikan keuntungan finansial. Korban terlibat dalam interaksi teks dan akhirnya terperdaya dalam hubungan yang mengandung romantisme dan cinta palsu, yang membuat mereka terlibat dalam *video call seksual*. Akibatnya, video asusila korban tersebar, yang berdampak pada kehidupan nyata mereka secara psikologis dan juga pada harga diri mereka sebagai anggota DPRD. Kurangnya literasi digital korban terkait dengan bahaya dan ancaman di dunia digital juga menjadi faktor yang mempengaruhi mereka menjadi korban *sextortion*.

Kesimpulannya, baik pelaku maupun korban *sextortion* dalam artikel tersebut terlibat dalam tindakan yang melanggar norma dan nilai-nilai *Cyber Culture*. Mereka mengabaikan etika yang seharusnya diterapkan dalam interaksi *online* dan terjebak dalam praktik yang berbahaya dan merugikan. Penting untuk meningkatkan kesadaran dan literasi digital bagi semua pengguna internet untuk menghindari menjadi korban atau terlibat dalam praktik yang melanggar hukum di dunia *online.*

Pelaku dan Korban Sextortian Dalam Perspektif *Space Transition Theory*

Dalam perspektif *Space Transition Theory*, kasus tersebut dapat dianalisis dalam konteks bagaimana pelaku dan korban *sextortion* berpindah dari ruang fisik ke ruang digital dan bagaimana hal tersebut mempengaruhi tindakan dan interaksi mereka. Pelaku *sextortion* dalam artikel tersebut menggunakan ruang digital (CMC) sebagai sarana untuk melancarkan kejahatan mereka (Rizki & Yulida, 2020). Mereka memanfaatkan kebebasan dan fleksibilitas yang ada dalam dunia siber, di mana norma dan nilai cenderung lebih samar dan tidak terlihat seperti dalam dunia fisik. Pelaku dapat menyembunyikan identitas mereka dengan menggunakan *pseudonymity*, memperdaya korban dengan modus romantis palsu, dan memanfaatkan kelemahan teknologi dan penegakan hukum di lapas untuk bersembunyi dari identifikasi dan pengejaran polisi. Selain itu, pelaku juga dapat menciptakan ikatan dengan sesama narapidana atau individu di dalam lingkungan sosial tertutup lapas, yang mendorong mereka untuk bekerjasama dalam melakukan kejahatan siber. Interaksi sosial yang terjadi di dalam lapas dapat menjadi ruang di mana pelaku mendapatkan dukungan dan dorongan untuk melanjutkan kegiatan kriminal mereka.

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Di sisi korban, transisi ke ruang digital juga terjadi. Sebagai seorang anggota DPRD, korban di dunia fisik harus menjaga wibawa dan menjalankan tugasnya dengan etika. Namun, ketika berinteraksi dalam ruang digital, korban dapat lebih terbuka dan rentan terhadap hubungan interpersonal dan hiperpersonal yang dapat terjalin. Kurangnya literasi digital dan pemahaman tentang risiko kejahatan siber membuat korban mudah terperdaya oleh pelaku *sextortion*. Selain itu, norma dan nilai dalam ruang digital seringkali lebih fleksibel dan kurang terlihat dibandingkan dengan dunia fisik. Korban dapat merasa lebih nyaman dalam berinteraksi secara *online* dan mungkin melanggar batasan etika yang berlaku dalam perannya sebagai anggota dewan. Interaksi di ruang digital memberikan rasa anonimitas yang membuat korban merasa lebih bebas untuk melakukan *video call seksual*, walaupun pada akhirnya korban sadar bahwa tindakan tersebut tidak sesuai dengan norma dan nilai yang seharusnya mereka pegang (Syauket et al., 2022).

Dalam Teori *Space Transition* terdapat beberapa variabel atau faktor yang dapat mempengaruhi terjadinya kejahatan siber termasuk sextortion, diantaranya:

a. *Valued Status and Position*

   Korban yang memiliki status dan posisi yang dihargai dalam masyarakat, seperti anggota DPRD, dapat menjadi target pelaku *sextortion*. Faktor ini meningkatkan risiko korban terlibat dalam interaksi berisiko di dunia digital karena mereka mungkin rentan terhadap manipulasi yang mengancam reputasi dan wibawa mereka. Sedangkan pada pelaku mencoba memanipulasi status atau posisi tertentu yang mereka miliki dalam masyarakat atau lingkungan sosial tertentu untuk menarik perhatian dan memperdaya korban. Pelaku yang memiliki pengetahuan tentang status dan posisi berharga korban dapat menggunakan informasi ini untuk meningkatkan peluang keberhasilan kejahatan mereka.

b. *Identity Anonymity with No Deterrence Factor*

   Korban yang tidak mempertimbangkan faktor anonimitas identitas di ruang digital dapat terjebak dalam interaksi dengan orang asing yang berpura-pura menjadi teman atau mitra romantis. Ketika korban tidak memiliki mekanisme pencegahan yang efektif atau pemahaman tentang risiko yang terkait, mereka dapat terperdaya untuk melakukan tindakan yang melibatkan keintiman, seperti *video call seks* (VCS), yang dapat dimanfaatkan oleh pelaku *sextortion*. Sedangkan pada pelaku sextortion sering menggunakan identitas palsu atau anonimitas tersebut untuk menyamarkan diri mereka dan menghindari pertanggungjawaban. Kemampuan untuk bersembunyi di

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

balik identitas palsu ini memungkinkan pelaku untuk melakukan kejahatan dengan lebih leluasa tanpa adanya faktor penghalang yang signifikan.

c. *Closed Society*

Korban yang terlibat dalam lingkungan sosial tertutup di dunia fisik, seperti lingkungan politik atau organisasi yang terbatas, mungkin terkadang merasa terlalu penat. Namun, ketika berinteraksi di ruang digital, norma dan nilai terkait dengan kehidupan sosial tertutup ini mungkin tidak berlaku dengan tegas, sehingga korban dapat terbawa oleh kenyamanan dan kebebasan dalam interaksi CMC. Sedangkan pada pelaku yang terlibat dalam lingkungan sosial tertutup, seperti di dalam lapas, dapat merasa lebih aman dan terlindungi dalam melancarkan kejahatan mereka. Lingkungan yang tertutup ini dapat memberikan dukungan, dorongan, atau kolaborasi dengan sesama pelaku yang memiliki minat dan tujuan yang sama.

d. *Cyber World Strangers*

Korban yang berinteraksi dengan orang asing di dunia siber yang belum dikenalnya sebelumnya, rentan terhadap manipulasi dan penipuan, termasuk *sextortion*. Keterbatasan informasi terhadap orang asing di ruang digital dapat membuat korban mudah jatuh ke dalam perangkap pelaku yang memanfaatkan kebutuhan emosional atau kerentanan korban. Sedangkan pada pelaku Pelaku *sextortion* sering kali mengincar korban yang memang tidak mereka kenal sebelumnya. Mereka menggunakan ketidaktahuan korban tentang identitas dan niat mereka untuk memanipulasi dan memperoleh keuntungan. Interaksi dengan orang asing di dunia siber memberikan peluang bagi pelaku untuk menciptakan hubungan palsu dan memperoleh kepercayaan korban.

e. *Open Society*

Meskipun korban mungkin memiliki norma dan nilai terkait kehidupan sosial yang terbuka di dunia fisik, interaksi dalam ruang digital dapat mengaburkan batasan-batasan ini. Hal ini dapat membuat korban merasa lebih nyaman dan cenderung untuk terlibat dalam interaksi yang mungkin tidak sejalan dengan norma dan nilai yang berlaku dalam kehidupan nyata. Begitu juga dengan pelaku dapat memanfaatkan kebebasan dan fleksibilitas yang diberikan oleh norma dan nilai yang lebih longgar di dunia digital. Mereka dapat mengabaikan batasan-batasan sosial dan hukum yang berlaku dalam kehidupan nyata, sehingga merasa lebih bebas untuk melancarkan kejahatan dan memanipulasi korban.

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Strategi Pemolisian Sebagai Upaya Pencegahan *Sextortian*

Strategi pemolisian dalam menangani dan mencegah kejahatan *sextortion* dengan mengedepankan paradigma *prevention* dan *proactive* berbasis *community* melalui konsep *e-policing* dapat melibatkan langkah-langkah seperti berikut:

a. Bekerjasama dengan stakeholder bidang teknologi dan informasi.

   Pemolisian dapat bekerja sama dengan berbagai stakeholder di bidang komunikasi dan informasi, baik dari pemerintah maupun swasta seperti Kementerian Teknologi dan Informatika, BIN, serta Telkom dan provider internet. Kolaborasi ini dapat memetakan dan memonitor IP Address yang mencurigakan, termasuk yang beroperasi di Lapas. Dapat dibuatkan aplikasi menggunakan kecerdasan buatan (*Artificial Intelligence*) yang dapat menganalisis dan mempelajari pola interaksi di media sosial terhadap akun-akun yang mencurigakan, misalnya profil dengan foto yang umum digunakan di internet.

b. Penguatan *comment center*

   Pemolisian dapat memperbanyak akses CCTV di setiap sudut kota dan tempat publik dengan bekerja sama dengan perkantoran dan pertokoan untuk akses CCTV yang mengarah ke jalan. CCTV juga dapat dilengkapi dengan teknologi pengenalan wajah (*face recognition*) untuk membantu mengidentifikasi pelaku yang terlibat dalam kejahatan *sextortion*.

c. Kerjasama dengan stakeholder terkait edukasi literatur digital.

   Pemolisian dapat menjalin kerjasama dengan pemerintah, kementerian perlindungan perempuan, LSM, ormas, dan komunitas digital dalam memberikan edukasi dan sosialisasi tentang literasi digital. Kerjasama ini dapat dilakukan melalui seminar, lokakarya, dan perbanyak literasi media sosial di lingkungan pendidikan dan perkantoran. Media juga dapat berperan dalam memberikan edukasi yang massif kepada masyarakat luas. Stakeholder juga dapat membantu melakukan patroli *cyber* untuk meminimalisir ruang gerak pelaku dan melaporkan kepada polisi jika ada kegiatan mencurigakan.

d. Penggunaan big data.

   Polisi dapat menggunakan big data yang berisi daftar pelaku kriminal dengan riwayat kejahatan yang pernah dilakukan beserta modus operandinya. Hal ini akan

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

memudahkan dalam mendeteksi kemungkinan pelaku residivist dan membantu kolaborasi antar kepolisian di seluruh Indonesia.

e. Patroli *cyber* dan monitoring *online*.

Polisi dapat melakukan patroli *cyber* dan monitoring *online* pada *platform*, forum, atau grup media sosial untuk memantau aktivitas yang mencurigakan. Selain itu, polisi juga perlu melakukan patroli konvensional di lokasi-lokasi yang rawan dijadikan tempat aktivitas *online* para pelaku, seperti area dengan wifi gratis di tempat umum.

f. Percepatan penanganan hukum

Polisi perlu mempercepat penanganan kasus *cybercrime* khususnya *sextortion* dengan menyamakan persepsi atau merumuskan kebijakan yang dapat mempercepat penanganan kasus. Aplikasi terintegrasi antar lembaga penegak hukum dapat digunakan untuk mempercepat penanganan administrasi.

g. Optimalisasi *victim service*.

Polisi perlu bekerja sama dengan pemerintah dan stakeholder terkait untuk memberikan pelayanan baik kesehatan maupun psikologis kepada korban. Kerjasama dengan stakeholder yang bergerak dalam sensor internet juga diperlukan untuk membantu penelusuran dan *takedown* terhadap video asusila korban yang beredar di internet.

h. Penguatan keamanan *cyber*

Polisi perlu memperkuat keamanan *cyber*, khususnya pada big data atau penyimpanan data lain yang bersifat rahasia. Ini akan membantu mencegah akses tidak sah dan penggunaan data sensitif oleh pihak yang tidak berwenang.

i. Kerjasama lintas negara.

Melakukan kerjasama lintas negara, baik antar pemerintah maupun *police to police*, dalam pencegahan dan penanganan *cybercrime* dan *sextortion*. Kerjasama ini mencakup pertukaran data informasi, dukungan sarana fasilitas, pelatihan dan *couching clinic*, serta penyelenggaraan *joint investigation*.

j. Perekrutan *state hacker*.

Jika memungkinkan, polisi dapat melakukan perekrutan *state hacker* dengan seleksi dan pengawasan ketat. *State hacker* dapat membantu tugas kepolisian dan negara, misalnya dalam penelusuran video korban yang sudah beredar di media sosial dan internet. Hecker dapat menerobos masuk ke delam web atau platform secara diam-

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

diam dan menghapus video korban. Hacker juga dapat membantu memperkuat keamanan sistem dengan menguji kelemahan keamanan (*web security*).

k. Perkuat regulasi

Pemerintah perlu memperkuat regulasi sebagai landasan bertindak dalam pelaksanaan tugas. Regulasi yang diperkuat akan memberikan landasan hukum yang jelas dan mendukung tindakan dalam pencegahan dan penanganan kejahatan *sextortion*.

Kesimpulan

Dari uraian pembahasan di atas dapat diambil beberapa kesimpulan, Pelaku yang merupakan narapidana dan korban yang merupakan oknum anggota DPRD awalnya berkenalan di media sosial kemudian mulai menjalin hubungan kedekatan dan korban terpedaya melakukan video call sex yang direkam oleh pelaku tanpa disadari korban. Rekaman tersebut digunakan oleh pelaku untuk memeras korban, dan bahkan walaupun korban telah memberikan uang kepada pelaku, rekaman video tersebut tetap disebarkan di internet. Pelaku yang merupakan narapidana dan korban yang merupakan anggota DPRD dapat terlibat dalam *sextortian* melalui media *online* dikarenakan faktor-faktor dalam *cyberculture* dan *space transition*, diantarnya: *Valued Status and Position, Identity Anonymity with No Deterrence Factor, Closed Society, Cyber World Strangers* dan *Open Society*.

Strategi pemolisian yang digunakan untuk menanggulangi dan mencegah sextortion adalah dengan e-policing dengan mengedepankan prevention, proactive dan community, diantaranya: Bekerjasama dengan stakeholder bidang teknologi dan informasi, Penguatan *comment centre*, Kerjasama dengan stakeholder terkait edukasi literatur digital, Penggunaan *big data* dan *Artificial Intelligent*, Patroli *cyber* dan monitoring *online*, Percepatan penanganan hukum, Optimalisasi *victim service*, Penguatan keamanan *cyber*, Kerjasama lintas negara, Perekrutan *state hacker* dan Perkuat regulasi.

Pada kesempatan ini penulis menyarankan beberapa hal untuk peningkatan efektifitas penanggulangan kejahatan sextortion, diantaranya: 1). Perkuat paradigma prevention, proactive dan collaborative policing sebagai pencegahan, karena penanggulangan kejahatan jangan hanya berfokus pada hilirnya saja (saat terjadai kejahatan), tetapi yang juga tidak kalah penting adalah secara proaktif penanganan pada hulu atau penyebabnya lebih mendalam dari berbagai perspektif agar dapat melakukan upaya pencegahan berulangnya kejahatan serupa

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

atau perkembangan kejahatan, dengan menjalin kolaborasi bersama stakeholder terkait. 2). Manfaatkan seoptimal mungkin teknologi yang ada untuk mendukung pelaksanaan tugas baik pengungkapan maupun pencegahannya, seperti optimalisasi *e-policing*/ *internet policing.* 3). Pemulihan kondisi korban juga harus diperhatikan dengan mengedepankan *victim service,* karena korban biasanya mengalami multi-victim dengan banyak kerugian, sehingga jangan sampai menjadi *re-victim* karena perlakuan tindakan kepolisian yang kurang memperhatikan kondisi dan perasaan korban.

Daftar Pustaka

Fasya, T. K., Yunanda, R., & Fariadi, D. (2023). Depoliticization of the Uleebalangs Descendants Due to a History of Past Violent Conflicts. *Jurnal Ilmu Sosial Dan Ilmu Politik Malikussaleh (JSPM)*, *4*(1), 102–111.

Georgakopoulou, A. (2011). Computer-mediated communication. *Pragmatics in Practice*, *9*, 93.

Hadiono, A. F. (2018). Pernikahan dini dalam perspektif psikologi komunikasi. *Jurnal Darussalam: Jurnal Pendidikan, Komunikasi Dan Pemikiran Hukum Islam*, *9*(2), 385–397.

HANAVIA, N. V. (2022). *THE INTERPRETATION OF SEXTORTION IN INDONESIAN CRIMINAL LAW AND ITS PREVENTION*. Universitas Gadjah Mada.

Juditha, C. (2015). Pola Komunikasi Dalam Cybercrime (Kasus Love Scams). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *6*(2), 29–40.

Kiesler, S., Siegel, J., & McGuire, T. W. (1984). Social psychological aspects of computer-mediated communication. *American Psychologist*, *39*(10), 1123.

Lexy J. Moleong, D. M. A. (2019). Metodologi Penelitian Kualitatif (Edisi Revisi). *PT. Remaja Rosda Karya*. https://doi.org/10.1016/j.carbpol.2013.02.055

Madonna, M., Sumardjo, S., Amanah, S., & Anwas, E. O. M. (2022). Mobilization of Cyber Extension Participants to Build Household Food Security. *Jurnal Penelitian Pendidikan IPA*, *8*(SpecialIssue), 67–75.

Marie-Helen, M. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. *Burlington, Jones & Bartlett Learning*, *29*, 19.

Pratama, C. S. P. (2017). *Cyberpolitics Remotivi Pada Kampanye Pemilihan Presiden Tahun 2014 (Kampanye Dan Strategi Remotivi Melawan Media Televisi)*. Universitas Jenderal Soedirman.

Rizki, J. D., & Yulida, D. (2020). Penerapan Hukum Menggunakan Metode Ekstensif Konstruktif Hukum Kepada Pelaku Kejahatan Sextortion. *Al-Hakam Islamic Law & Contemporary Issues*, *1*(1), 7–10.

Silver, D. (2004). Internet/cyberculture/digital culture/new media/fill-in-the-blank studies. *New Media & Society*, *6*(1), 55–64.

Sugiono, P. D. (2014). Metode penelitian pendidikan pendekatan kuantitatif.pdf. In *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D*.

Sumanti, S. T. (2023). Analysis of Interpersonal Communication Patterns of Love Scams Mode on Social Media in Female Students in Medan City. *Jurnal Lensa Mutiara Komunikasi*, *7*(1), 74–85.

Syauket, A., Saimima, I. D. S., Simarmata, R. P., Aidy, W. R., Zainab, N., Prayitno, R. B., & Cabui, C. E. (2022). Sextortion Fenomena Pemerasan Seksual di Lingkungan Pendidikan. *Jurnal Kajian Ilmiah*, *22*(3), 219–230.

Jurnal Sosiologi Dialektika Sosial
Volume 10 No. 2. September 2024
E-ISSN: 2828-4224
DOI: 10.29103/jsds.v%vi%i.17588

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, *23*(1), 3–43.

‖ Submitted: 2024-07-19 ‖ Accepted: 2024-08-30 ‖ Published: 2024-09-30