



Eksplorasi Teknologi untuk Penipuan Digital

(Studi Kasus Penyebaran Undangan Pernikahan Palsu di WhatsApp dan Implikasi Hukumnya di Indonesia)

Ketut Ayu Asiti Sari^{1*}, Made Sugi Hartono², Ni Ketut Sari Adnyani³

¹⁻³ Program studi Ilmu Hukum, Universitas Pendidikan Ganesha, Indonesia

ayu.asiti@student.undiksha.ac.id¹, sugi.hartono@undiksha.ac.id², sari.adnyani@undiksha.ac.id³

*Penulis Korespondensi: ayu.asiti@student.undiksha.ac.id

Abstract. Digital fraud, particularly schemes involving the distribution of fake wedding invitations through instant messaging applications such as WhatsApp, has developed into a serious problem in Indonesia along with the increasing use of digital technology in everyday life. This fraudulent *modus operandi* exploits victims' curiosity, trust, and panic to prompt them to open malicious links or download harmful files containing malware. Such malware has the potential to damage device systems, steal personal data, and access sensitive information, including banking accounts and social media profiles. This form of fraud not only causes significant financial losses for victims but also results in psychological impacts, such as fear, trauma, and a loss of trust in digital communication. This article aims to comprehensively examine the *modus operandi* of digital fraud through fake wedding invitations, analyze the relevant legal framework, and assess the social and economic impacts on society. In addition, the article emphasizes the importance of improving digital literacy as an effective preventive measure to minimize the risk of digital fraud. To address this issue, the article proposes strengthening cooperation among law enforcement agencies, cybersecurity institutions, and technology service providers. Recommendations are also directed toward reinforcing regulations, enhancing the effectiveness of law enforcement, and intensifying public awareness campaigns to reduce the incidence of digital fraud in Indonesia.

Keywords: Cyber Literacy; Cybercrime; Digital Fraud; Information Technology Law; WhatsApp.

Abstrak. Penipuan digital, khususnya yang menggunakan modus penyebaran undangan pernikahan palsu melalui aplikasi pesan instan seperti WhatsApp, telah berkembang menjadi permasalahan serius di Indonesia seiring dengan meningkatnya penggunaan teknologi digital dalam kehidupan sehari-hari. Modus penipuan ini memanfaatkan rasa penasaran, kepercayaan, serta kepanikan korban untuk membuka tautan atau mengunduh file berbahaya yang mengandung malware. Malware tersebut berpotensi merusak sistem perangkat, mencuri data pribadi, serta mengakses informasi sensitif seperti akun perbankan dan media sosial. Praktik penipuan ini tidak hanya menimbulkan kerugian finansial yang signifikan bagi korban, tetapi juga berdampak pada kondisi psikologis, seperti rasa takut, trauma, dan hilangnya kepercayaan terhadap komunikasi digital. Artikel ini bertujuan untuk mengulas secara komprehensif modus operandi penipuan digital melalui undangan pernikahan palsu, menganalisis kerangka hukum yang relevan, serta mengkaji dampak sosial dan ekonomi yang ditimbulkan bagi masyarakat. Selain itu, artikel ini menekankan pentingnya peningkatan literasi digital sebagai upaya preventif yang efektif dalam meminimalisasi risiko penipuan digital. Untuk mengatasi permasalahan tersebut, artikel ini mengusulkan perlunya peningkatan kerja sama antara aparat penegak hukum, lembaga keamanan siber, dan penyedia layanan teknologi. Rekomendasi juga diarahkan pada penguatan regulasi, efektivitas penegakan hukum, serta intensifikasi sosialisasi kepada masyarakat guna menekan angka penipuan digital di Indonesia.

Kata Kunci: Hukum Teknologi Informasi; Kejahatan Siber; Literasi Siber; Penipuan Digital; WhatsApp.

1. LATAR BELAKANG

Penipuan digital telah menjadi ancaman yang semakin meresahkan di Indonesia, seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Modus kejahatan ini semakin beragam, salah satunya melalui penyebaran undangan pernikahan palsu melalui aplikasi pesan instan, seperti WhatsApp. Penipuan jenis ini memanfaatkan rasa penasaran dan kepanikan korban untuk membuka tautan atau file yang ternyata mengandung malware, yang dapat merusak perangkat dan mencuri data pribadi. Kasus ini menjadi contoh nyata bagaimana

pelaku penipuan digital menggunakan psikologi sosial dan teknologi untuk menjerat korban yang kurang waspada.

Menurut data yang dirilis oleh Kementerian Komunikasi dan Informatika (KOMINFO), penipuan digital di Indonesia telah menyebabkan kerugian yang sangat besar, dengan angka kejahatan siber mencapai lebih dari 1.700 kasus dan kerugian finansial mencapai 18 triliun rupiah dalam periode 2018 hingga 2023. Penipuan melalui undangan pernikahan palsu ini bukan hanya merugikan secara finansial, tetapi juga memberikan dampak psikologis bagi korban yang sering kali merasa kehilangan kendali atas data pribadi mereka. Fenomena ini menunjukkan betapa pentingnya untuk terus meningkatkan kesadaran dan kewaspadaan masyarakat terhadap ancaman siber yang semakin canggih.

Dalam konteks ini, penting untuk membahas aspek-aspek hukum yang terkait dengan penipuan digital, serta dampak sosial dan ekonomi yang timbul akibat kejahatan siber ini. Selain itu, literasi digital menjadi kunci dalam mencegah terjadinya penipuan serupa, karena hanya dengan pemahaman yang baik terhadap teknologi dan risiko yang ada, masyarakat dapat melindungi diri mereka dari potensi ancaman siber. Di sisi lain, aparat penegak hukum juga memegang peranan penting dalam menangani kasus penipuan digital, melalui pendekatan represif dan preventif yang efektif.

Artikel ini bertujuan untuk mengkaji modus operandi penipuan digital melalui undangan pernikahan palsu, menganalisis kerangka hukum yang relevan, serta mengeksplorasi dampak sosial dan ekonomi yang ditimbulkan. Selain itu, artikel ini juga akan membahas upaya yang telah dilakukan oleh aparat penegak hukum dalam menangani kasus penipuan digital dan mengusulkan langkah-langkah pencegahan yang dapat diambil untuk mengurangi angka kejahatan siber di Indonesia.

2. KAJIAN TEORITIS

Penipuan digital merupakan bagian dari kejahatan siber (*cybercrime*), yaitu perbuatan melawan hukum yang memanfaatkan sistem elektronik dan teknologi informasi sebagai sarana utama. Dalam konteks penyebaran undangan pernikahan palsu melalui WhatsApp, teknologi digunakan sebagai alat untuk menyebarkan malware dan mencuri data pribadi korban, sehingga menimbulkan kerugian ekonomi dan gangguan psikologis.

Modus penipuan tersebut dapat dijelaskan melalui teori rekayasa sosial (*social engineering*), yang menekankan pada manipulasi psikologis korban dengan memanfaatkan rasa percaya, norma sosial, dan dorongan emosional. Pelaku merancang pesan yang tampak meyakinkan agar korban terdorong membuka file atau tautan tanpa melakukan verifikasi.

Selain itu, teori perlindungan data pribadi menegaskan bahwa data pribadi merupakan bagian dari hak privasi yang wajib dilindungi oleh hukum. Penipuan digital dengan penyebaran malware secara langsung melanggar hak atas perlindungan data pribadi, sebagaimana diatur dalam UU ITE dan diperkuat dengan Undang-Undang Perlindungan Data Pribadi. Terakhir, teori literasi digital menekankan pentingnya kemampuan masyarakat dalam memahami dan mengenali risiko di ruang digital. Rendahnya literasi digital meningkatkan kerentanan terhadap penipuan siber, sehingga edukasi dan peningkatan kesadaran digital menjadi langkah preventif yang penting dalam menekan kejahatan penipuan digital.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan normatif dengan fokus pada analisis regulasi yang relevan, termasuk UU ITE dan KUHP. Selain itu, pendekatan konseptual digunakan untuk mengeksplorasi hubungan antara literasi digital dan kerentanan masyarakat terhadap penipuan digital. Penulis juga menganalisis beberapa kasus penipuan digital di Indonesia untuk memberikan gambaran empiris tentang dampak kejahatan ini. Data yang digunakan bersumber dari laporan resmi pemerintah, jurnal akademik, dan dokumentasi media.

4. HASIL DAN PEMBAHASAN

Modus Operandi Penipuan Digital Melalui Undangan Pernikahan Palsu Penipuan online sering terjadi di Indonesia melalui berbagai platform media sosial seperti WhatsApp, Facebook, Instagram, dan platform media sosial lainnya dengan menggunakan berbagai modus kejahatan. Dengan demikian, masyarakat khawatir tentang melakukan aktivitasnya di internet. Penipuan online telah tercatat kurang lebih 1.730 kasus dari 2018 hingga 2023, dengan korban mengalami kerugian sebesar 18 triliun, menurut KOMINFO. Ini jelas merugikan masyarakat, terutama bagi pengguna media sosial yang tidak tahu tentang hal itu (Mulyadi, 2024).

Penipuan online melalui media sosial memiliki berbagai modus kejahatan yang terjadi dalam masyarakat. Aplikasi WhatsApp adalah salah satu media sosial yang paling sering menjerat korban karena hampir semua orang menggunakannya. Survei yang dilakukan oleh Ding, platform top up seluler, menunjukkan bahwa orang Indonesia paling sering menggunakan WhatsApp sebagai layanan pesan instan untuk berinteraksi satu sama lain. Menurut survei, 89% orang Indonesia menggunakan WhatsApp sebagai alat komunikasi. Instagram memiliki persentase 41 persen dan Facebook 44 persen. Sniffing adalah modus yang paling umum digunakan untuk penipuan online melalui aplikasi WhatsApp, meminta pengguna

untuk mendownload file apk tertentu dari aplikasi WhatsApp yang dibuka, yang secara otomatis dapat mencuri data (Wahyuddin, 2024).

Penipuan digital melalui undangan pernikahan palsu merupakan salah satu bentuk kejahatan siber yang memanfaatkan perkembangan teknologi dan lemahnya kewaspadaan pengguna. Modus ini dimulai dengan penyebaran file atau tautan berbahaya yang diklaim sebagai undangan pernikahan melalui email atau aplikasi pesan instan seperti WhatsApp dan Telegram. File yang dikirim sering kali memiliki format pdf, docx, atau apk dan dirancang sedemikian rupa agar terlihat profesional serta meyakinkan, termasuk penggunaan nama pengirim yang tampaknya dikenal oleh korban. Rekayasa sosial ini berhasil karena korban terdorong oleh rasa penasaran dan kepanikan untuk segera membuka undangan tersebut (Pratama, 2021).

Ketika korban membuka file atau tautan tersebut, malware secara otomatis terunduh dan aktif di perangkat mereka. Malware ini memiliki berbagai jenis, mulai dari spyware yang mencuri data pribadi seperti informasi perbankan atau akun media sosial, hingga ransomware yang mengunci data korban dan meminta tebusan. Akibatnya, korban bisa mengalami kerugian finansial yang signifikan serta kebocoran data pribadi yang dapat disalahgunakan atau dijual di pasar gelap digital (*dark web*) (Setiawan, 2022). Selain itu, dampak psikologis juga dapat muncul, seperti trauma dan stres akibat kehilangan kendali terhadap akun atau data penting (Ardiansyah, 2023).

Menurut penelitian oleh Santoso (2022), modus penipuan digital dengan undangan pernikahan palsu telah menyumbang sekitar 12% dari laporan kejahatan siber di Indonesia. Hal ini menunjukkan bahwa modus tersebut cukup efektif dalam menjebak korban yang kurang berhati-hati. Oleh karena itu, upaya pencegahan harus ditingkatkan melalui berbagai langkah, seperti verifikasi sumber file atau tautan sebelum dibuka, menghindari mengklik file mencurigakan, serta menggunakan perangkat lunak keamanan seperti antivirus dan firewall (Santoso, 2022). Selain itu, edukasi literasi digital bagi masyarakat sangat penting agar pengguna lebih waspada terhadap ancaman siber yang terus berkembang (Nugraha et al., 2023).

Penipuan digital melalui undangan pernikahan palsu adalah salah satu bentuk kejahatan siber yang memanfaatkan psikologi sosial dan teknologi secara bersamaan. Modus operandi ini melibatkan penyebaran pesan yang tampak meyakinkan, sering kali didesain dengan elemen visual seperti nama, logo, atau gambar yang membuat pesan tampak sah. Pesan ini biasanya menyertakan tautan yang mengarahkan korban ke situs phishing atau lampiran berisi malware. Yang membuat modus ini sangat efektif adalah penggunaan teknik manipulasi

psikologis. Pelaku memanfaatkan rasa ingin tahu korban dan tekanan sosial, seperti perasaan tidak sopan jika tidak merespons undangan. Dalam beberapa kasus, pelaku juga menambahkan elemen urgensi waktu untuk mendorong korban bertindak tanpa berpikir panjang. Teknik ini membuat korban cenderung mengklik tautan atau membuka file tanpa memverifikasi keasliannya terlebih dahulu.

Analisis Hukum terhadap Penipuan Digital di Indonesia

Penipuan digital melalui undangan pernikahan palsu menjadi fenomena yang semakin memprihatinkan di era digital. Dalam perspektif hukum, tindakan ini masuk dalam kategori kejahatan siber sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016. Penipuan yang dilakukan melalui media elektronik, seperti penyebaran malware melalui file atau tautan undangan palsu, melanggar Pasal 28 Ayat (1) UU ITE yang menyatakan larangan penyebaran informasi bohong yang merugikan orang lain. Pelaku dapat dikenakan sanksi pidana berupa penjara maksimal 6 tahun atau denda hingga Rp1 miliar (Santoso, 2022).

Selain itu, penipuan digital dengan modus ini juga terkait erat dengan pencurian data pribadi, yang pada prinsipnya melanggar hak privasi seseorang. Kendati belum ada regulasi khusus mengenai perlindungan data pribadi pada saat itu, penyalahgunaan data pribadi tetap dapat dikenakan sanksi berdasarkan Pasal 32 UU ITE, yang melarang akses ilegal terhadap sistem elektronik dengan tujuan memperoleh informasi tertentu (Ardiansyah, 2023). Dengan adanya Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022, mekanisme perlindungan terhadap kebocoran data pribadi menjadi lebih kuat, meskipun implementasi di lapangan masih menghadapi berbagai tantangan, seperti rendahnya literasi hukum di kalangan masyarakat dan lemahnya penegakan hukum (Setiawan, 2022).

Kasus penipuan digital melalui undangan palsu sering kali sulit diungkap karena pelaku menggunakan identitas anonim dan jaringan siber yang sulit dilacak. Oleh karena itu, aparat penegak hukum perlu meningkatkan kerja sama dengan lembaga keamanan siber untuk menindak kasus semacam ini. Menurut penelitian Nugraha et al. (2023), kolaborasi antara aparat penegak hukum, pemerintah, dan penyedia layanan teknologi merupakan kunci utama dalam memberantas kejahatan siber, termasuk modus penipuan melalui undangan pernikahan palsu. Edukasi hukum bagi masyarakat juga perlu digalakkan agar korban memiliki pemahaman yang cukup untuk melaporkan kejahatan tersebut serta memahami mekanisme hukumnya.

Selain itu, Pasal 378 KUHP juga dapat diterapkan untuk menjerat pelaku penipuan yang menggunakan media elektronik. Pasal ini mengatur tentang tindak pidana penipuan secara umum, dengan ancaman hukuman penjara paling lama empat tahun. Namun, dalam konteks penipuan digital, penerapan KUHP sering kali terbatas oleh kurangnya bukti fisik dan sulitnya melacak pelaku.

Tantangan utama dalam penegakan hukum terhadap penipuan digital adalah sulitnya melacak identitas pelaku, terutama jika mereka menggunakan teknologi seperti Virtual Private Network (VPN) untuk menyembunyikan lokasi mereka. Selain itu, banyak pelaku yang beroperasi dari luar negeri, sehingga membutuhkan kerja sama internasional untuk menangani kasus ini. Indonesia perlu memperkuat partisipasinya dalam kerja sama internasional, seperti ASEAN Cybersecurity Cooperation, untuk mengatasi tantangan ini.

Dampak Sosial dan Ekonomi dari Penipuan Digital

Penipuan digital melalui undangan pernikahan palsu yang disebarakan lewat WhatsApp tidak hanya menimbulkan kerugian individu tetapi juga memberikan dampak yang luas secara sosial dan ekonomi. Secara ekonomi, korban sering mengalami kerugian finansial akibat malware yang mencuri data perbankan atau mengunci perangkat melalui ransomware. Berdasarkan penelitian Santoso (2022), kerugian akibat kejahatan siber di Indonesia mencapai angka 8,2 triliun rupiah pada tahun 2022, di mana modus undangan palsu berkontribusi signifikan terhadap total kerugian tersebut. Selain itu, korban harus mengeluarkan biaya tambahan untuk memperbaiki perangkat yang terinfeksi, mengganti akun yang dicuri, atau membayar tebusan agar data dapat dipulihkan.

Dampak sosial dari penipuan ini juga tidak kalah signifikan. Korban sering kali mengalami penurunan kepercayaan terhadap teknologi digital dan layanan komunikasi. Hal ini dapat menghambat adaptasi masyarakat terhadap digitalisasi yang semakin berkembang pesat. Menurut Ardiansyah (2023), pengalaman buruk akibat penipuan siber sering kali membuat individu cenderung menghindari transaksi atau komunikasi digital, yang pada akhirnya mempengaruhi produktivitas dan keterlibatan mereka dalam ekonomi digital. Selain itu, korban juga mengalami tekanan psikologis seperti kecemasan, stres, bahkan trauma akibat kehilangan data pribadi atau informasi penting (Setiawan, 2022).

Dampak tersebut tidak hanya dirasakan oleh individu tetapi juga oleh masyarakat secara luas. Penyebaran undangan palsu ini memicu kekhawatiran yang lebih besar terhadap keamanan siber di Indonesia, terutama dengan maraknya laporan kebocoran data. Penelitian Nugraha et al. (2023) menunjukkan bahwa rendahnya literasi digital dan lemahnya sistem keamanan siber memperburuk dampak kejahatan ini. Oleh karena itu, kolaborasi antara

pemerintah, penyedia teknologi, dan masyarakat menjadi sangat penting dalam upaya meminimalkan risiko penipuan digital, baik dari sisi kerugian ekonomi maupun dampak sosial yang diakibatkan.

Dari sisi ekonomi, penipuan digital dapat menghambat pertumbuhan ekonomi digital di Indonesia. Kepercayaan konsumen terhadap platform digital sangat penting untuk mendukung transaksi online, tetapi penipuan seperti ini merusak kepercayaan tersebut. Selain itu, perusahaan teknologi yang menjadi platform untuk modus penipuan ini juga menghadapi risiko kehilangan reputasi, yang dapat berdampak pada keberlanjutan bisnis mereka.

Pentingnya Literasi Digital dalam Mencegah Penipuan Digital

Literasi digital memiliki peran krusial dalam mencegah terjadinya penipuan digital, termasuk modus penipuan melalui penyebaran undangan pernikahan palsu. Literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga kemampuan menganalisis, mengevaluasi, dan mengenali potensi ancaman dalam dunia siber. Rendahnya literasi digital di kalangan masyarakat membuat individu lebih mudah terjebak dalam modus penipuan seperti undangan palsu yang disebarluaskan melalui WhatsApp. Menurut Pratama (2021), mayoritas korban penipuan digital berasal dari kelompok masyarakat yang tidak memahami cara memverifikasi sumber informasi atau file yang dikirimkan. Hal ini menyebabkan mereka lebih rentan membuka tautan atau file yang berisi malware tanpa menyadari konsekuensinya.

Peningkatan literasi digital diharapkan dapat memberikan kesadaran kepada masyarakat mengenai pentingnya verifikasi informasi dan pencegahan proaktif terhadap ancaman siber. Dengan pemahaman yang baik, individu dapat lebih berhati-hati saat menerima file atau tautan mencurigakan, seperti mengonfirmasi kebenaran undangan kepada pengirim yang bersangkutan atau menggunakan perangkat lunak keamanan untuk mendeteksi malware. Selain itu, literasi digital juga mencakup pemahaman tentang hukum yang berlaku, seperti Undang-Undang ITE dan Perlindungan Data Pribadi, sehingga masyarakat dapat memahami hak-hak mereka jika menjadi korban penipuan digital (Santoso, 2022).

Menurut penelitian Setiawan (2023), edukasi literasi digital yang terstruktur dan melibatkan semua lapisan masyarakat, baik melalui lembaga pendidikan, pemerintah, maupun media, dapat secara signifikan menekan angka kejahatan siber. Edukasi ini perlu difokuskan pada penguatan keterampilan dasar, seperti mengenali modus operandi penipuan, meningkatkan kewaspadaan saat menggunakan teknologi, serta menjaga data pribadi agar tidak mudah diakses pihak tak bertanggung jawab. Dengan demikian, literasi digital yang baik akan

menciptakan masyarakat yang lebih cerdas, waspada, dan mampu melindungi diri dari berbagai bentuk penipuan digital.

Upaya yang dilakukan aparat penegak hukum dalam menangani kasus tindak pidana penipuan dengan modus penyebaran undangan pernikahan digital melalui Whatsaap

Kasus penipuan digital dengan modus penyebaran undangan pernikahan palsu melalui WhatsApp telah menimbulkan keresahan di masyarakat. Penanganan kasus ini menuntut peran aktif aparat penegak hukum melalui dua pendekatan utama, yaitu upaya represif dan upaya preventif.

Upaya represif merupakan tindakan tegas terhadap pelaku setelah tindak pidana terjadi. Aparat kepolisian bekerja sama dengan unit siber menggunakan teknologi forensik digital untuk melacak keberadaan pelaku, menganalisis perangkat elektronik, serta mengidentifikasi bukti elektronik seperti alamat IP, metadata file, dan jejak komunikasi pelaku. Hal ini sesuai dengan Pasal 30 dan Pasal 32 UU ITE, yang melarang akses ilegal dan manipulasi data elektronik. Dalam konteks ini, penyidik siber sering kali bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) dan Kominfo untuk mengidentifikasi sumber malware yang tersebar melalui file undangan palsu. Menurut penelitian Nugraha et al. (2023), kerja sama lintas lembaga sangat penting untuk menangani kompleksitas tindak pidana siber, karena modus penipuan sering melibatkan teknologi yang sulit dilacak secara konvensional. Selain itu, pelaku yang terbukti bersalah dapat dikenakan sanksi pidana sesuai Pasal 28 Ayat (1) UU ITE, yang melarang penyebaran informasi bohong atau menyesatkan yang merugikan masyarakat, dengan ancaman hukuman 6 tahun penjara dan denda maksimal Rp1 miliar (Santoso, 2022).

Di sisi lain, upaya preventif bertujuan untuk mencegah terjadinya tindak pidana penipuan digital melalui peningkatan literasi digital dan kesadaran hukum di kalangan masyarakat. Aparat penegak hukum bekerja sama dengan lembaga pendidikan, pemerintah daerah, dan media untuk mengedukasi masyarakat terkait modus penipuan digital serta langkah pencegahannya. Edukasi ini mencakup cara memverifikasi tautan atau file mencurigakan, mengenali tanda-tanda serangan malware, dan melaporkan kasus penipuan melalui jalur hukum yang tersedia. Menurut Setiawan (2023), sosialisasi hukum dan literasi digital terbukti efektif dalam menekan angka kejahatan siber karena meningkatkan kewaspadaan dan pemahaman masyarakat tentang cara melindungi data pribadi. Selain itu, pemerintah melalui Kominfo terus melakukan upaya pencegahan dengan memblokir tautan atau situs berbahaya yang berpotensi menyebarkan malware.

Kombinasi upaya represif dan preventif sangat diperlukan untuk menangani kasus penipuan digital secara menyeluruh. Upaya represif memberikan efek jera kepada pelaku melalui penegakan hukum yang tegas, sementara upaya preventif berfokus pada edukasi dan perlindungan dini kepada masyarakat. Namun, tantangan yang dihadapi aparat penegak hukum masih cukup signifikan, seperti keterbatasan sumber daya manusia yang kompeten di bidang forensik digital serta pesatnya perkembangan teknologi yang dimanfaatkan oleh pelaku kejahatan siber (Ardiansyah, 2023). Oleh karena itu, penguatan kapasitas aparat, regulasi hukum yang adaptif, serta sinergi antar-lembaga menjadi kunci dalam memberantas kasus penipuan digital, termasuk modus penyebaran undangan pernikahan palsu melalui WhatsApp.

5. KESIMPULAN DAN SARAN

Penipuan digital melalui penyebaran undangan pernikahan palsu lewat aplikasi WhatsApp menjadi salah satu bentuk kejahatan siber yang merugikan masyarakat baik secara ekonomi maupun sosial. Modus ini memanfaatkan teknik manipulasi psikologis dan kecanggihan teknologi untuk menjerat korban. Malware yang tersembunyi dalam file undangan dapat menyebabkan kerugian finansial yang signifikan, serta kebocoran data pribadi yang berpotensi disalahgunakan. Penipuan ini juga menimbulkan dampak psikologis yang mendalam bagi korban, yang dapat menurunkan kepercayaan masyarakat terhadap teknologi dan merugikan pertumbuhan ekonomi digital di Indonesia.

Untuk menangani kasus ini, aparat penegak hukum mengandalkan dua pendekatan, yaitu upaya represif dan preventif. Upaya represif berfokus pada penegakan hukum yang tegas terhadap pelaku melalui pemanfaatan teknologi forensik digital dan kerja sama dengan lembaga terkait, seperti BSSN dan Kominfo. Sementara itu, upaya preventif mengutamakan pendidikan literasi digital yang bertujuan untuk meningkatkan kewaspadaan masyarakat terhadap ancaman siber dan memperkenalkan cara-cara melindungi diri dari penipuan digital. Keterbatasan sumber daya dalam penegakan hukum serta pesatnya perkembangan teknologi menjadi tantangan utama dalam menangani kejahatan ini. Oleh karena itu, penguatan kapasitas aparat penegak hukum, sinergi antar-lembaga, serta edukasi yang lebih masif mengenai literasi digital sangat penting untuk mengurangi jumlah korban dan meminimalisir dampak sosial serta ekonomi dari penipuan digital.

DAFTAR REFERENSI

- Adolf, H. (2015). *Hukum siber di Indonesia*. Rajawali Pers.
- Ardiansyah, T. (2023). Analisis dampak kejahatan siber terhadap masyarakat digital di Indonesia. *Jurnal Teknologi Informasi*, 11(2), 65–78.
- Ardiansyah, T. (2023). Analisis serangan malware dalam kejahatan siber di Indonesia. *Jurnal Teknologi Informasi*, 11(2), 45–55.
- Ardiansyah, T. (2023). Pendekatan preventif dan represif dalam menangani kejahatan siber. *Jurnal Hukum dan Teknologi*, 12(1), 45–58.
- Brown, I. (2020). *Cybersecurity: Protecting personal data in the digital age*. Wiley.
- Cyber Crime Research Center. (2022). *Modus penipuan digital terbaru*. <https://ccrc.or.id>
- Hartono, B. (2022). *Kejahatan siber: Tinjauan hukum dan teknologi*. Kencana Media.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Laporan tahunan kejahatan siber*. <https://kominfo.go.id>
- Nugraha, R., Sudirman, A., & Dewi, S. (2023). Forensik digital sebagai solusi penanganan kejahatan siber. *Jurnal Keamanan Digital*, 7(1), 50–62.
- Nugraha, R., Sudirman, A., & Dewi, S. (2023). Tren penipuan digital dan upaya penanganannya. *Jurnal Keamanan Siber Indonesia*, 5(1), 21–35.
- Pramudya, T. (2018). *Keamanan data digital*. Andi Offset.
- Pratama, H. (2021). Pentingnya literasi digital dalam menghadapi kejahatan siber. *Jurnal Teknologi Masyarakat*, 9(3), 35–48.
- Pratama, H. (2021). Rekayasa sosial sebagai metode dalam kejahatan siber. *Jurnal Komputer dan Masyarakat*, 9(3), 30–42.
- Raharjo, S. (2019). *Teknologi informasi dan hukum*. Alfabeta.
- Santoso, M. (2022). Kajian hukum dan literasi digital dalam pencegahan kejahatan siber. *Jurnal Hukum Teknologi*, 8(2), 42–55.
- Santoso, M. (2022). Kajian hukum terhadap penipuan digital berbasis UU ITE di Indonesia. *Jurnal Hukum dan Teknologi*, 8(3), 60–72.
- Santoso, M. (2022). Strategi penegakan hukum terhadap kasus penipuan digital di Indonesia. *Jurnal Hukum Siber*, 8(3), 33–47.
- Santoso, M. (2022). Studi kasus kerugian finansial akibat kejahatan siber di Indonesia. *Jurnal Ekonomi Digital*, 7(2), 50–60.
- Setiawan, F. (2022). Dampak psikologis dari kejahatan siber berbasis malware. *Jurnal Kriminalitas Digital*, 6(4), 32–45.

- Setiawan, F. (2022). Dark web dan perdagangan data pribadi. *Jurnal Kriminalitas Digital*, 6(4), 12–25.
- Setiawan, F. (2022). Perlindungan data pribadi dan tantangannya di era digital. *Jurnal Kriminalitas Digital*, 6(4), 15–27.
- Setiawan, F. (2023). Peran literasi digital dalam mencegah penipuan siber di masyarakat. *Jurnal Literasi Siber*, 6(2), 15–28.
- Setiawan, F. (2023). Strategi edukasi literasi digital untuk mencegah penipuan siber. *Jurnal Literasi Digital Indonesia*, 6(1), 25–38.