IMPLEMENTASI PENEGAKAN HUKUM DALAM MENANGANI KASUS PHISHING DI KOTA SAMARINDA

Alif Naufal Istiqlal[1], Ivan Zairani Lisi[2], Yennita Astarina[3]
alifnaufal057@gmail.com[1]
Universitas Mulawarman

ABSTRAK

Perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan berbagai kemudahan dalam aktivitas masyarakat, terutama dalam bidang ekonomi dan transaksi digital. Namun demikian, kemajuan teknologi tersebut juga menimbulkan berbagai bentuk kejahatan baru yang memanfaatkan teknologi sebagai sarana, salah satunya adalah penipuan online melalui metode phishing. Phishing merupakan suatu bentuk kejahatan siber yang dilakukan dengan cara memperoleh informasi pribadi korban, seperti data perbankan atau akun digital, melalui penyamaran sebagai pihak yang terpercaya. Fenomena ini juga terjadi di Kota Samarinda dan menimbulkan kerugian bagi masyarakat, sehingga diperlukan penegakan hukum yang efektif dalam menangani kasus tersebut. Pendekatan penelitian ini dilakukan dengan pendekatan sosio legal research dengan tambahan buku dan jurnal yang bertujuan guna menganalisis dua pokok pembahasan: pertama, menganalisis bagaimana kendala yang dihadapi penegak hukum pada penanganan kasus penipuan online phishing di Kota Samarinda. Kedua, menganalisis bagaimana Upaya yang dihadapi penegak hukum pada penanganan kasus penipuan online phishing di Kota Samarinda. Berdasarkan hasil penelitian ini ditemukan bahwa aparat penegak hukum menghadapi berbagai kendala dalam permasalahan penipuan online phishing di Kota Samarinda dan para aparat penegak hukum juga melakukan Upaya terhadap permasalahan penipuan online Phishing di kota Samarinda.
Kata Kunci: Penegakan Hukum, Kejahatan Siber, Phishing.

ABSTRACT

The rapid development of information and communication technology has provided various conveniences in community activities, especially in the economic and digital transaction fields. However, this technological advancement has also given rise to various new forms of crime that utilize technology as a means, one of which is online fraud through phishing methods. Phishing is a form of cybercrime carried out by obtaining victims' personal information, such as banking data or digital accounts, by posing as a trusted party. This phenomenon also occurs in the city of Samarinda and causes losses to the community, so effective law enforcement is needed to handle such cases.
This research approach was conducted using a socio-legal research approach with additional books and journals aimed at analyzing two main topics: first, analyzing the obstacles faced by law enforcement officials in handling online phishing fraud cases in Samarinda City. Second, analyzing the efforts made by law enforcement officials in handling online phishing fraud cases in Samarinda City. Based on the results of this study, it was found that law enforcement officials face various obstacles in dealing with online phishing fraud in Samarinda City, and law enforcement officials are also making efforts to address the problem of online phishing fraud in Samarinda City.
Keywords: *Law Enforcement, Cybercrime, Phishing.*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa dampak positif dalam berbagai bidang kehidupan manusia, seperti pendidikan, ekonomi, pemerintahan, hingga layanan kesehatan. Namun, seiring dengan manfaatnya, teknologi juga memunculkan tantangan baru dalam bentuk kejahatan siber yang semakin kompleks. Salah satu bentuk

kejahatan yang cukup meresahkan masyarakat digital adalah phishing, yakni penipuan berbasis elektronik yang bertujuan mendapatkan data pribadi korban.

Phishingmerupakan tindakan penipuan yang dilakukan secara daring dengan tujuan memperoleh informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dari korbandengan mencuri identitas, merampas dana, atau merusak reputasi.Phishingmenjadi kejahatan yang perlu mendapatkan perhatian serius karena mengancam keamanan data pribadi, kenyamanan bertransaksi daring, serta integritas ekonomi negara.

Samarinda memiliki posisi strategis sebagai pusat pemerintahan, ekonomi, dan teknologi di wilayah Kalimantan Timur. Samarinda mengalami pertumbuhan pesat dalam adopsi teknologi digital dan layanan berbasis internet. . Perubahan perilaku masyarakat manusia secara global dipengaruhi oleh kemajuan teknologi informasi dan komunikasi yang berkembang secara pesat. Pada masa Era digital membawa kemudahan dalam akses informasi, pelayanan publik, dan komunikasi, namun juga menimbulkan kerentanan baru di bidang keamanan digital. Meningkatnya pelanggaran terhadap hak privasi dan penyalahgunaan data pribadi yang disebabkan oleh salah satu bentuk kejahatan siber atau Phishing yang merupakan salah satu bentuk kejahatan siber (cybercrime) yang dilakukan dengan cara memanipulasi psikologis korban untuk memperoleh data pribadi secara melawan hukum. Phishing umumnya dilakukan dengan cara menyamar sebagai pihak yang sah atau terpercaya seperti lembaga perbankan, instansi pemerintah, perusahaan teknologi, atau platform perdagangan elektronik—melalui media elektronik seperti email, pesan singkat, media sosial, maupun situs web palsu. Tujuan utama dari tindakan phishing adalah mengelabui korban agar secara sukarela memberikan informasi sensitif, seperti identitas pribadi, data perbankan, kata sandi, kode OTP, dan informasi autentikasi lainnya.

Beberapa data jumlah kasus phishing yang terjadi dan merugi masyarakat indonesia dari tahun 2021-2023:

No.	Tahun	Jumlah Kasus
1.	2021	28.000 Kasus
2.	2022	61.000 Kasus
3.	2023	69.117 Kasus
	Total	158.117 Kasus

Sumber : Indonesia Anti-Phishing Data Exchange (IDADX)

Berdasarkan data diatas jumlah kasus phishing pada domain .id mengalami peningkatan signifikan dari tahun ke tahun. Pada tahun 2021 tercatat sebanyak 28.000 kasus, meningkat menjadi 61.000 kasus pada tahun 2022, dan mencapai 69.117 kasus pada tahun 2023. Secara keseluruhan, jumlah kasus phishing dalam kurun waktu tersebut mencapai 158.117 kasus. Meskipun data kasus phishing domain .id dari tahun 2021 hingga 2023 menunjukan angka yang jelas dan terverifikasi, perkembangan pada tahun 2024 hingga 2026 tidak dapat disajikan dalam bentuk angka tahunan yang pasti. Hal ini disebabkan karena data yang tersedia pada periode tersebut masih bersifat dinamis dan diperbarui secara real time melalui dashboard Indonesia Anti-Phishing Data Exchange (IDADX).

Di Kota Samarinda, berdasarkan data dari Polresta Samarinda pada tahun 2021 sampai dengan tahun 2025 terdapat 204 laporan kasus phishing.

No	Tahun	Jumlah Kasus
1.	2021	36
2.	2022	52
3.	2023	25
4.	2024	34

5.	2025	57
	Total	204 Kasus

Sumber : Kepolisian Resor Kota Samarinda

Terjadinya transformasi menuju masyarakat digital tidak hanya menghadirkan kemudahan dalam berkomunikasi, bekerja, belajar, maupun bertransaksi, tetapi juga membentuk suatu ekosistem sosial yang terhubung tanpa batas ruang dan waktu. Transformasi dunia digital yang terus berkembang telah menimbulkan cela untuk pelaku agar dapat melakukan berbagai bentuk kejahatan siber. Pelaku memanfaatkan informasi dan data digital agar dapat melawan hukum. Khususnya informasi pribadi, sebagai sasaran empuk untuk memperoleh keuntungan dan menimbulkan kerugian bagi korbannya. Teknologi itu sendiri dipahami sebagai penerapan ilmu pengetahuan untuk menghasilkan alat, sistem, atau metode yang di gunakan memudahkan aktivitas manusia. Perkembangan era digital tidak hanya memberikan dampak positif terhadap kegiatan masyarakat, tetapi juga memiliki dampak negatif dengan munculnya berbagai bentuk tindak pidana yang dapat merugikan masyarakat.

Maraknya kejahatan siber di era digital menuntut penguatan dan kepastian hukum bagi masyarakat. Indonesia telah memiliki dasar hukum untuk menjerat pelaku Phishing, seperti UU No.1 Tahun 2024 Tentang Perubahan Kedua Atas UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, KUHP Pasal 492, dan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Meskipun telah tersedia berbagai peraturan perundang-undangan yang mengatur dan menjerat tindak pidana Phsihing, dalam praktiknya penegakan hukum terhadap kejahatan tersebut di Kota Samarinda masih menghadapi berbagai kendala. Peningkatan jumlah kasus Phishing menunjukan adanya persoalan dalam implementasi penegakan hukum, baik dari subtansi hukum, aparat penegak hukum, maupun kesadaran hukum masyarakat. Oleh karena itu, timbul isu hukum mengenai bagaimana implementasi penegakan hukum dalam penanganan kejahatan Phishing di Kota Samarinda serta upaya yang dilakukan untuk mengatasi hambatan dalam penegakanya.

METODE PENELITIAN

Metode penelitian hukum merupakan serangkaian langkah yang dilakukan secara sistematis untuk memperoleh jawaban atas suatu permasalahan hukum melalui pendekatan ilmiah. Peter Mahmud menjelaskan bahwa penelitian hukum memiliki tujuan untuk menemukan suatu kebenaran berdasarkan konsep koherensi, yaitu dengan menguji kesesuaian antara aturan hukum, noorma hukum, dan prinsip hukum yang berlaku. Dengan demikian penelitian hukum tidak hanya menitikberatkan pada apakah suatu tindakan telah sesuai dengan ketentuan peraturan perundang-undangan, tetapi juga untuk menilai kesesuaiannya dengan norma dan prinsip hukum yang menjadi dasar aturan tersebut.

HASIL DAN PEMBAHASAN

UPAYA PENEGAK HUKUM DALAM PENANGANAN KASUS PENIPUAN ONLINE PHISHING DI KOTA SAMARINDA

A. Penegakan Hukum Terhadap Kejahatan Phishing di Kota Samarinda

Penegakan hukum adalah proses yang dilakukannya sebagai upaya untuk mewujudkan tegaknya norma-norma hukum secara nyata. Penegakkan ini ditunjukan sebagai pedoman perilaku dalam hubungan-hubungan hukum pada kehidupan bermasyarakat dan bernegara.

Penegakan hukum ini juga merupakan suatu bentuk upaya dalam pelaksanaan hukum secara nyata dengan melalui usaha usaha yang bertujuan untuk mewujudkan ide keadilan, kepastian hukum, kemanfaatan sosial dan keadilan menjadi nyata.

Kemajuan teknologi digital yang berjalan beriringan dengan tingginya angka pengguna internet turut memicu lonjakan kasus kejahatan siber salah satunya yaitu kejahatan phishing. Praktik phishing sendiri dapat dipahami sebagai tindak penipuan yang mengincar data pribadi korban secara ilegal melalui sarana elektronik, dengan maksud memperoleh keuntungan yang yang ada pada korban dengan cara melanggar hukum. Di Indonesia, penindakan atas kejahatan phishing mengacu pada sejumlah landasan hukum yang berlaku, termasuk pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) terkait penipuan, serta regulasi yang mengatur informasi dan transaksi elektronik. Pasal 492 KUHP mengatur mengenai tindak pidana penipuan yang dilakukan baik untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum dengan menggunakan nama palsu, tipu muslihat, atau rangkaian kebohongan.

Penegakan hukum pada kejahatan phishing di Kota Samarinda menghadapi berbagai kendala, terutama dalam upaya mengidentifikasi dan melakukan penangkapan terhadap pelaku. karaktestik kejahatan phishing yang menyebar melalui media digital menyebabkan pelaku dapat beroperasi tanpa bertemu secara langsung dengan korban. Pelaku umumnya memanfaatkan identitas palsu, nomor telepon yang telah diregistrasi menggunakan data orang lain, akun media sosial fiktif, rekening penampung hasil kejahatan, serta perangkat elektronik yang sulit dilacak keberadaannya. Kondisi ini menyebabkan penegak hukum mengalami kesulitan dalam memastikan identitas pelaku sebelum dilakukanya tindakan penangkapan.

Aparat penegak hukum harus melakukan penyelidikan dan penyidikan dengan alat bukti yang cukup sesuai dalam ketentuan hukum acara pidana. Namun, dalam perkara phishing, sebagian besar alat bukti berbentuk digital sehingga memerlukan proses analisis forensik digital yang membutuhkan waktu, keahlian, dan dukungan teknologi. Aparat tidak dapat melakukan penangkapan hanya berdasarkan laporan korban atau dugaan semata, melainkan harus memastikan adanya keterkaitan antara identitas pelaku dengan akun, perangkat elektronik, alamat IP, rekening bank, maupun jejak transaksi digital yang digunakan dalam melakukan tindak pidana tersebut. Proses pembuktian ini sering kali menjadi hambatan karena pelaku berupaya menghilangkan atau menyamarkan jejak digital yang ditinggalkan.

Pelaku phishing umumnya bekerja secara terorganisasi dan tidak jarang berada di luar wilayah hukum Kota Samarinda, bahkan terdapat kemungkinan jaringan pelaku beroperasi lintas provinsi maupun lintas negara. Akibatnya, proses penangkapan tidak dapat dilakukan secara cepat karena memerlukan koordinasi dengan kepolisian di daerah lain, penyedia layanan telekomunikasi, pihak perbankan, serta instansi terkait lainnya guna melakukan pelacakan terhadap keberadaan pelaku . Koordinasi tersebut membutuhkan waktu karena setiap instansi memiliki prosedur dan mekanisme tersendiri dalam memberikan data yang diperlukan untuk kepentingan penyidikan.

Menambahkan bahwa perkembangan teknologi informasi yang sangat cepat turut dimanfaatkan oleh pelaku untuk menghindari proses penegakan hukum. Pelaku sering menggunakan aplikasi komunikasi terenkripsi, jaringan virtual (VPN), server luar negeri, hingga rekening yang dipinjam dari pihak lain sebagai sarana untuk menyembunyikan identitasnya. Modus operandi tersebut semakin menyulitkan aparat dalam menentukan

lokasi keberadaan pelaku dan mengumpulkan alat bukti yang dapat menghubungkan pelaku dengan tindak pidana.

Menurut Bapak Bripka Budi Susanto, S.I.Kom Kendala utama yang dihadapi dalam penanganan perkara phishing bukan sekadar pada tahap penyelidikan, melainkan juga pada usaha menangkap pelaku kejahatan tersebut. Penangkapan hanya dapat terlaksana apabila pihak berwajib sudah mengantongi bukti yang cukup kuat serta mampu mengidentifikasi keberadaan pelaku dengan pasti. Alhasil, penanganan tindak pidana phishing membutuhkan tahapan yang lebih rumit dibandingkan kejahatan konvensional, sebab melibatkan pembuktian secara digital, pelacakan yang menembus batas wilayah, serta koordinasi lintas pihak yang berhubungan dengan penggunaan teknologi informasi.

Proses penegakan hukum terhadap kejahatan siber tidak hanya bergantung pada kemampuan aparat penegak hukum, tetapi juga dipengaruhi oleh karakteristik tindak pidana yang memanfaatkan perkembangan teknologi informasi. Berbeda dengan tindak pidana konvensional yang umumnya meninggalkan barang bukti fisik dan memungkinkan pelaku segera diketahui identitasnya, tindak pidana phishing lebih banyak meninggalkan jejak digital yang perlu dianalisis secara mendalam melalui proses digital forensik. Oleh karena itu, proses pengungkapan pelaku memerlukan waktu yang lebih lama karena penyidik harus melakukan penelusuran terhadap berbagai data elektronik, seperti riwayat komunikasi, transaksi keuangan, alamat Internet Protocol (IP), lokasi akses perangkat, hingga aktivitas rekening yang digunakan sebagai sarana menerima hasil kejahatan.

Seluruh proses tersebut harus dilakukan secara cermat agar alat bukti yang diperoleh memiliki kekuatan yang sah untuk membuktikan kejahatan dalam proses peradilan. Praktiknya tidak semua laporan masyarakat dapat langsung ditindaklanjuti hingga tahap penangkapan pelaku. Hal ini disebabkan oleh adanya keterbatasan informasi yang dimiliki korban. Banyak korban hanya mengetahui nomor telepon, tautan (link), akun media sosial, atau nomor rekening yang digunakan oleh pelaku, sedangkan identitas asli pelaku tidak diketahui . Bahkan dalam beberapa kasus, rekening yang digunakan merupakan rekening milik orang lain yang diperoleh melalui praktik jual beli rekening atau dipinjam dengan berbagai modus. Kondisi tersebut menyebabkan proses identifikasi menjadi semakin kompleks karena penyidik harus memastikan keterkaitan antara pemilik rekening, pengguna rekening, serta pihak yang memperoleh keuntungan dari hasil tindak pidana tersebut.

Temuan hasil wawancara tersebut sejalan dengan kondisi penanganan perkara phishing yang menunjukkan bahwa tidak seluruh laporan yang diterima dapat diselesaikan melalui penangkapan pelaku. Rumitnya proses pembuktian digital, maraknya pemakaian identitas palsu, serta luasnya jaringan yang dimiliki pelaku menjadi faktor-faktor utama yang berpengaruh terhadap efektivitas penegakan hukum. Oleh karena itu, keberhasilan pengungkapan suatu perkara phishing sangat bergantung pada kelengkapan alat bukti digital, kerja sama antarinstansi, serta kemampuan aparat dalam melakukan analisis terhadap bukti elektronik.

Berdasarkan data yang diperoleh dari Polresta Samarinda, jumlah laporan tindak pidana phishing dalam beberapa tahun terakhir menunjukkan bahwa kejahatan ini masih menjadi ancaman bagi masyarakat. Meskipun laporan yang masuk mengalami peningkatan, tidak seluruh perkara dapat diselesaikan melalui proses penangkapan pelaku. Hal tersebut disebabkan oleh berbagai kendala yang telah dijelaskan sebelumnya, seperti sulitnya melacak identitas pelaku, penggunaan teknologi untuk menyamarkan jejak digital, serta adanya jaringan pelaku yang beroperasi di luar wilayah hukum Kota Samarinda.

Berdasarkan data dari penegak hukum Polresta Samarinda dari tahun 2021 sampai dengan tahun 2025 terdapat 204 laporan kusus phishing di Kota Samarinda.

No	Tahun	Jumlah Kasus
1.	2021	36
2.	2022	52
3.	2023	25
4.	2024	34
5.	2025	57
	Total	204 Kasus

Data tersebut mengindikasikan bahwa masih ada kesenjangan antara banyaknya laporan yang masuk dengan jumlah perkara yang berhasil diselesaikan. Hal ini bukan berarti kinerja aparat penegak hukum lemah, melainkan menunjukkan bahwa tindak pidana phishing memang memiliki tingkat kerumitan yang lebih tinggi ketimbang kejahatan konvensional. Oleh karena itu, penguatan kapasitas sumber daya manusia di bidang teknologi informasi, peningkatan fasilitas digital forensik, serta optimalisasi kerja sama dengan berbagai instansi terkait menjadi hal krusial guna meningkatkan efektivitas penegakan hukum atas tindak pidana phishing di Kota Samarinda.

Selain itu, ketentuan mengenai kejahatan yang berkaitan dengan penggunaan teknologi informasi juga diatur dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Undang-undang tersebut memberikan dasar hukum bagi aparat penegak hukum untuk menindak pelaku kejahatan siber termasuk phishing.

Secara praktik, upaya penegakan hukum atas kejahatan phishing di Kota Samarinda dijalankan oleh aparat melalui sejumlah tahapan, mulai dari penerimaan laporan dari masyarakat hingga proses penuntutan di meja pengadilan. Proses tersebut turut melibatkan berbagai lembaga penegak hukum, seperti kepolisian, kejaksaan, dan lembaga peradilan. Tahap pertama dalam proses penegakan hukum adalah penerimaan laporan dari masyarakat. Dalam banyak kasus phishing, proses penanganan perkara biasanya dimulai dari adanya laporan korban yang merasa dirugikan akibat tindakan penipuan online. Laporan tersebut kemudian ditindaklanjuti oleh aparat kepolisian dengan melakukan pemeriksaan awal terhadap korban serta mengumpulkan informasi awal mengenai kronologi kejadian dan bukti-bukti yang dimiliki oleh korban. Tahapan berikutnya adalah proses penyelidikan dan penyidikan yang dijalankan oleh pihak kepolisian. Pada tahap ini, aparat penegak hukum melakukan berbagai tindakan untuk mengumpulkan bukti serta mengidentifikasi pelaku kejahatan. Dalam kasus phishing, proses penyidikan seringkali melibatkan analisis terhadap bukti elektronik seperti riwayat transaksi perbankan, percakapan digital, alamat IP, maupun data akun yang digunakan oleh pelaku. Pengumpulan bukti digital ini sangat penting untuk memastikan keterlibatan pelaku dalam tindak pidana yang dilakukan.

Setelah proses penyidikan dinyatakan lengkap, perkara tersebut kemudian dilimpahkan kepada pihak kejaksaan untuk dilakukan proses penuntutan di pengadilan. Jaksa penuntut umum memegang peran krusial dalam membuktikan kesalahan terdakwa selama persidangan berlangsung, dengan memanfaatkan alat bukti yang telah dihimpun sepanjang tahap penyidikan. Dalam perkara kejahatan siber seperti phishing, alat bukti elektronik dapat digunakan sebagai alat bukti yang sah sepanjang memenuhi ketentuan yang diatur dalam peraturan perundang-undangan.

Penegakan hukum terhadap kejahatan phishing di Kota Samarinda juga tidak terlepas dari kerja sama antara berbagai pihak, seperti lembaga perbankan, penyedia layanan internet, serta lembaga pemerintah yang bergerak di bidang keamanan siber. Kerja sama

tersebut sangat diperlukan terutama dalam proses pelacakan aliran dana hasil kejahatan serta identifikasi akun atau perangkat yang digunakan oleh pelaku. Dengan adanya kerja sama tersebut diharapkan proses penanganan kasus phishing dapat berjalan lebih efektif dan memberikan efek jera kepada pelaku kejahatan.

Dengan demikian, penegakan hukum terhadap kejahatan phishing di Kota Samarinda merupakan bagian penting dari upaya negara dalam menjaga keamanan masyarakat di era digital. Melalui penegakan hukum yang efektif serta dukungan dari berbagai pihak, diharapkan tindak pidana phishing dapat diminimalisir sehingga masyarakat dapat menggunakan teknologi informasi dengan lebih aman dan nyaman. Berdasarkan hasil wawancara dan data yang diperoleh, dapat disimpulkan bahwa penegakan hukum terhadap tindak pidana phishing di Kota Samarinda masih menghadapi berbagai tantangan, khususnya dalam proses mengidentifikasi dan menangkap pelaku. Kompleksitas kejahatan yang memanfaatkan teknologi informasi, penggunaan identitas palsu, serta sulitnya memperoleh alat bukti digital yang memadai menjadi faktor utama yang memengaruhi efektivitas penegakan hukum. Oleh karena itu, diperlukan peningkatan kemampuan aparat penegak hukum di bidang teknologi informasi dan forensik digital, didukung dengan penguatan koordinasi antarinstansi, agar proses penyelidikan, penyidikan, hingga penangkapan pelaku dapat dilaksanakan secara lebih efektif dan memberikan kepastian hukum bagi masyarakat sebagai korban tindak pidana phishing.

B. Proses Penanganan Kasus Phishing oleh Aparat Penegak Hukum

Penanganan terhadap tindak pidana phishing pada dasarnya merupakan bagian dari upaya penegakan hukum terhadap kejahatan siber (cyber crime) yang dilakukan melalui media elektronik. Dalam sistem peradilan pidana di Indonesia, proses penanganan perkara pidana dilakukan melalui beberapa tahapan yang dimulai dari penerimaan laporan hingga penetapan tersangka oleh aparat penegak hukum. Tahapan tersebut dilakukan untuk memastikan bahwa proses penegakan hukum berjalan sesuai dengan prosedur yang diatur dalam peraturan perundang-undangan yang berlaku.

Menurut Maskun, penanganan tindak pidana yang berkaitan dengan teknologi informasi memerlukan metode penyelidikan dan penyidikan yang berbeda dengan kejahatan konvensional karena melibatkan sistem elektronik serta bukti digital sebagai alat bukti utama. Oleh karena itu, aparat penegak hukum dituntut memiliki kemampuan teknis serta dukungan teknologi digital forensik untuk dapat mengungkap pelaku kejahatan tersebut secara efektif.

Keterangan bahwa penanganan tindak pidana yang berkaitan dengan teknologi informasi memiliki karakteristik yang berbeda dibandingkan dengan tindak pidana konvensional. Perkembangan teknologi digital menuntut aparat penegak hukum untuk menerapkan metode penyelidikan dan penyidikan yang lebih kompleks, terutama dalam proses pengumpulan alat bukti elektronik, pelacakan identitas pelaku, serta koordinasi dengan berbagai pihak terkait. Dalam penanganan tindak pidana phishing, proses penegakan hukum diawali dengan adanya laporan dari korban atau masyarakat kepada kepolisian. Tahap pelaporan merupakan langkah awal yang sangat penting karena menjadi dasar bagi aparat penegak hukum untuk melakukan penyelidikan dan menentukan ada atau tidaknya dugaan tindak pidana. Pada tahap ini, korban diminta untuk menjelaskan kronologi kejadian secara lengkap serta menyerahkan bukti-bukti yang dimiliki, seperti tangkapan layar (screenshot) percakapan, tautan (link) phishing, bukti transfer, mutasi rekening, nomor telepon pelaku, alamat surat elektronik (e-mail), maupun bukti elektronik lainnya yang berkaitan dengan peristiwa tersebut. Selanjutnya, laporan yang telah diterima akan

dilakukan verifikasi dan pencatatan sebagai dasar bagi penyidik untuk menindaklanjuti proses penanganan perkara sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Adapun tahapan dalam penanganan kasus phishing di Polresta Kota Samarinda adalah sebagai berikut:

1. **Penerimaan Laporan**

   Hasil wawancara saya dengan Bapak Bripka Budi Susanto, S.I.Kom., selaku Banit Eksus Polresta Samarinda, diperoleh keterangan bahwa tahapan pertama dalam penanganan tindak pidana phishing diawali dengan penerimaan laporan dari korban atau masyarakat yang mengalami tindak pidana tersebut. Laporan yang disampaikan oleh korban menjadi dasar bagi kepolisian untuk melakukan tindakan awal dalam rangka mengetahui ada atau tidaknya dugaan tindak pidana. Pada tahap ini, korban diminta menjelaskan kronologi kejadian secara lengkap serta menyerahkan bukti-bukti awal yang dimiliki, seperti tangkapan layar (screenshot) percakapan atau pesan penipuan, tautan (link) situs phishing, bukti transfer, mutasi rekening, riwayat transaksi, nomor telepon, alamat surat elektronik (e-mail), maupun bukti elektronik lainnya yang berkaitan dengan peristiwa yang dilaporkan. Kelengkapan bukti tersebut akan memudahkan penyidik dalam melakukan penelusuran terhadap jejak digital pelaku dan menentukan langkah penanganan selanjutnya. Keterangan tersebut sejalan dengan pendapat para ahli yang menyatakan bahwa penerimaan laporan merupakan tahapan awal dalam proses penanganan suatu tindak pidana. Laporan yang diterima oleh aparat penegak hukum akan dicatat dan diverifikasi sebagai dasar untuk dilakukan penyelidikan guna menilai apakah peristiwa yang dilaporkan memenuhi unsur-unsur tindak pidana sebagaimana diatur dalam ketentuan peraturan perundang-undangan. Oleh karena itu, dalam penanganan tindak pidana phishing, penerimaan laporan tidak hanya berfungsi sebagai administrasi awal, tetapi juga menjadi dasar hukum bagi aparat kepolisian untuk melakukan serangkaian tindakan penyelidikan dan penyidikan terhadap dugaan tindak pidana yang terjadi.

2. **Penyelidikan**

   Berdasarkan hasil wawancara dengan Bapak Bripka Budi Susanto, S.I.Kom., selaku Banit Eksus Polresta Samarinda, diperoleh keterangan bahwa setelah laporan dari korban diterima dan dilakukan pemeriksaan awal terhadap bukti-bukti yang disampaikan, penyidik akan melaksanakan tahap penyelidikan. Menurut beliau, pada tahap ini petugas berfokus untuk memastikan terlebih dahulu apakah peristiwa yang dilaporkan mengandung unsur tindak pidana serta memiliki keterkaitan dengan kejahatan siber, khususnya phishing.

   Beliau menjelaskan bahwa penyelidikan dilakukan dengan mengumpulkan dan menelaah informasi awal yang berkaitan dengan laporan korban. Aparat kepolisian akan memeriksa bukti elektronik yang diserahkan, seperti tangkapan layar percakapan, alamat situs atau tautan yang digunakan pelaku, nomor telepon, akun media sosial, alamat surat elektronik (e-mail), hingga data transaksi keuangan yang berkaitan dengan dugaan tindak pidana. Dari hasil penelusuran tersebut, penyelidik berupaya mengidentifikasi pola atau modus yang digunakan pelaku serta menelusuri jejak digital yang dapat dijadikan dasar untuk menentukan langkah penanganan berikutnya. Apabila dari hasil penyelidikan ditemukan adanya indikasi yang cukup bahwa telah terjadi tindak pidana, maka perkara akan ditingkatkan ke tahap penyidikan sesuai dengan ketentuan hukum yang berlaku.

3. Pengumpulan Alat Bukti Digital

Keterangan yang diberikan oleh Bapak Bripka Budi Susanto, S.I.Kom., selaku Banit Eksus Polresta Samarinda. bahwa dalam penanganan tindak pidana phishing, pengumpulan alat bukti digital merupakan salah satu tahapan yang sangat menentukan berhasil atau tidaknya proses pengungkapan suatu perkara. Menurut beliau, berbeda dengan tindak pidana konvensional yang umumnya meninggalkan barang bukti fisik, pada kasus phishing sebagian besar alat bukti berupa data elektronik sehingga penyidik harus lebih teliti dalam melakukan penelusuran dan pengamanannya. Apabila bukti digital tidak segera diamankan, terdapat kemungkinan bukti tersebut dihapus, diubah, atau dipindahkan oleh pelaku sehingga dapat menyulitkan proses penyidikan.

Bahwa penyidik terlebih dahulu mengidentifikasi seluruh bukti elektronik yang berkaitan dengan laporan korban. Bukti tersebut dapat berupa tangkapan layar percakapan dengan pelaku, bukti transfer dana, mutasi rekening, tautan atau alamat situs phishing, nomor telepon yang digunakan pelaku, alamat surat elektronik (e-mail), hingga data yang tersimpan pada telepon seluler maupun perangkat komputer milik korban. Selain itu, apabila memungkinkan, penyidik juga melakukan penelusuran terhadap jejak digital lainnya, seperti alamat IP atau informasi elektronik lain yang dapat membantu mengidentifikasi pelaku maupun mengetahui bagaimana tindak pidana tersebut dilakukan. Seluruh bukti elektronik yang berhasil dikumpulkan tidak dapat langsung digunakan begitu saja, melainkan harus terlebih dahulu diperiksa, dianalisis, dan didokumentasikan sesuai dengan prosedur yang berlaku. Hal tersebut dilakukan agar keaslian, keutuhan, dan nilai pembuktian dari bukti digital tetap terjaga sehingga dapat dipertanggungjawabkan dalam proses hukum. Menurut beliau, kelengkapan alat bukti digital sangat berpengaruh terhadap keberhasilan penyidik dalam mengungkap identitas pelaku, membuktikan adanya tindak pidana phishing, serta memperkuat proses pembuktian pada tahap penyidikan hingga persidangan.

4. Penyidikan

Apabila dalam tahap penyelidikan ditemukan adanya unsur tindak pidana, maka proses penanganan perkara akan dilanjutkan ke tahap penyidikan. Penyidikan merupakan serangkaian tindakan yang dilakukan oleh penyidik untuk mencari serta mengumpulkan alat bukti yang dengan bukti tersebut membuat terang suatu tindak pidana serta menemukan tersangkanya. Dalam kasus phishing, penyidik biasanya melakukan pemeriksaan terhadap korban, saksi, serta pihak-pihak lain yang terkait dengan kejadian tersebut.

5. Penetapan Tersangka

Tahap selanjutnya dalam proses penanganan kasus phishing adalah penetapan tersangka. Penetapan tersangka dilakukan apabila penyidik telah memperoleh minimal dua alat bukti yang sah sebagaimana diatur dalam hukum acara pidana. Dalam kasus phishing, tersangka dapat ditetapkan setelah aparat penegak hukum berhasil mengidentifikasi pelaku melalui analisis bukti digital, pelacakan alamat IP, maupun hasil pemeriksaan terhadap saksi dan korban. Setelah penetapan tersangka dilakukan, proses hukum selanjutnya dapat dilanjutkan ke tahap penuntutan di pengadilan.

Berdasarkan uraian tersebut dapat dipahami bahwa penanganan kasus phishing oleh aparat penegak hukum dilakukan melalui serangkaian tahapan yang sistematis, mulai dari penerimaan laporan hingga penetapan tersangka. Setiap tahapan memiliki peran yang penting dalam memastikan bahwa proses penegakan hukum terhadap kejahatan phishing dapat berjalan secara efektif serta mampu memberikan kepastian hukum bagi korban maupun masyarakat secara luas. Oleh karena itu, dapat dianalisis bahwa keberhasilan penanganan kasus phishing sangat bergantung pada keterpaduan dan konsistensi dalam setiap tahapan proses penegakan hukum. Setiap tahap tersebut memiliki keterkaitan yang tidak dapat dipisahkan, sehingga kelemahan pada salah satu tahap dapat mempengaruhi keseluruhan proses penegakan hukum.

Salah satu kendala utama dalam melakukan penangkapan pelaku phishing adalah keterbatasan alat bukti pada tahap penyelidikan dan penyidikan. Praktik di lapangan, tindak pidana phishing umumnya melibatkan transaksi keuangan melalui rekening bank sebagai media penampungan hasil kejahatan . Namun demikian, penyidik tidak dapat secara langsung memperoleh data rekening koran maupun informasi mengenai identitas dan mutasi rekening yang digunakan oleh pelaku, karena bank terikat oleh ketentuan mengenai rahasia bank.

Walaupun penyidik telah mengetahui nomor rekening tujuan transfer yang digunakan oleh pelaku, bank tidak dapat serta-merta memberikan informasi mengenai pemilik rekening maupun riwayat transaksi kepada penyidik tanpa melalui prosedur yang telah ditentukan dalam peraturan perundang-undangan. Kondisi tersebut menyebabkan proses pelacakan aliran dana hasil kejahatan menjadi lebih lama, sehingga berdampak pada keterlambatan dalam mengidentifikasi keberadaan pelaku. Dalam beberapa kasus, selama proses permintaan data kepada pihak perbankan berlangsung, pelaku telah lebih dahulu memindahkan dana ke rekening lain atau menarik seluruh hasil kejahatan sehingga semakin menyulitkan proses penangkapan.

Kondisi tersebut sejalan dengan ketentuan Pasal 40 Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, yang mewajibkan bank untuk menjaga kerahasiaan informasi mengenai nasabah penyimpan dan simpanannya. Meskipun undang-undang memberikan pengecualian bagi kepentingan peradilan pidana melalui mekanisme pembukaan rahasia bank, penyidik tetap harus mengikuti prosedur yang telah ditentukan sehingga informasi rekening tidak dapat diperoleh secara langsung. Oleh karena itu, proses memperoleh alat bukti dari sektor perbankan memerlukan waktu dan koordinasi dengan berbagai pihak, yang pada akhirnya menjadi salah satu faktor penghambat dalam mengungkap dan menangkap pelaku tindak pidana phishing di Kota Samarinda.

C. Upaya Penegak Hukum Terhadap Penipuan Online Phishing Di Kota Samarinda

Tindak kejahatan penipuan online Phishing yang sangat besar dalam wilayah Kota Samarinda berdasarkan data yang di dapatkan dari pihak Kepolisian Kota Samarinda pada tahun 2021 sampai dengan tahun 2025 terdapat sebanyak 204 kasus penipuan online Phishing yang di laporkan.

Menanggulangi upaya Penegak Hukum Dalam Penanganan Kasus Penipuan Online Phishing dalam pencegahan adalah dengan memberikan upaya berupa upaya preventif, upaya represif,upaya kerja sama antara lembaga, dan upaya perlindungan dan pemulihan yang dapat diuraikan dibawah:

1. Melakukan Upaya Preventif

Upaya preventif merupakan langkah yang dilakukan sebelum terjadinya tindak pidana dengan tujuan meminimalisir peluang terjadinya kejahatan. Dalam konteks penipuan online melalui metode phishing di Kota Samarinda, aparat penegak hukum, khususnya Kepolisian Resor Kota (Polresta) Samarinda, melakukan berbagai langkah preventif seperti sosialisasi kepada masyarakat, penyuluhan hukum di sekolah dan perguruan tinggi, serta edukasi melalui media sosial resmi kepolisian. Pendekatan preventif ini merupakan bagian dari kebijakan penanggulangan kejahatan yang tidak hanya berorientasi pada penindakan, tetapi juga pada pencegahan melalui peningkatan kesadaran hukum masyarakat. Upaya ini sejalan dengan fungsi preventif kepolisian sebagaimana diatur dalam Pasal 13 Undang-Undang Nomor 2 Tahun 2002, yang menegaskan bahwa kepolisian bertugas memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan dan pelayanan kepada masyarakat. Lebih lanjut, Pasal 14 ayat (1) huruf a dan c undang-undang tersebut memberikan kewenangan kepada kepolisian untuk melaksanakan pembinaan masyarakat guna meningkatkan partisipasi dan kesadaran hukum. Selain itu, pendekatan preventif juga dilakukan melalui kerja sama dengan perbankan dan penyedia layanan digital guna meningkatkan sistem keamanan transaksi elektronik. Landasan hukum mengenai perlindungan dalam transaksi elektronik diatur dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang memberikan dasar hukum bagi upaya pencegahan penyalahgunaan teknologi informasi. Di samping itu, aspek perlindungan data pribadi yang kerap menjadi objek dalam modus phishing diperkuat melalui Undang-Undang Nomor 27 Tahun 2022.

Dalam praktiknya, edukasi kepada masyarakat menjadi faktor penting mengingat banyak korban phishing berasal dari kurangnya pemahaman terhadap modus operandi pelaku. Hal ini sejalan dengan pendapat Soerjono Soekanto yang menyatakan bahwa efektivitas penegakan hukum dipengaruhi oleh faktor masyarakat dan budaya hukum, sehingga pembinaan dan penyuluhan hukum merupakan instrumen penting dalam membangun kesadaran hukum masyarakat. Dengan demikian, pendekatan preventif tidak hanya berorientasi pada aparat penegak hukum, tetapi juga menuntut partisipasi aktif masyarakat sebagai pengguna teknologi informasi. Upaya ini mencerminkan implementasi kebijakan non-penal dalam penanggulangan kejahatan sebagaimana dikemukakan oleh Barda Nawawi Arief, bahwa pencegahan kejahatan melalui sarana di luar hukum pidana merupakan bagian integral dari kebijakan kriminal modern.

Selain itu ada Upaya yang di lakukan dari instansi lain seperti Menkominfo, dengan menghimbau dan memberikan Upaya penanggulangan dengan cara yaitu:

a. Masyarakat dapat menggunakan layanan yang dapat digunakan untuk mengecek status atau tingkat kepercayaan dari nomor rekening atau nomor telepon seperti layanan CekRekening.id atau aplikasi GetContact;
b. Waspada jika ada yang meminta kode OTP melalui email, aplikasi chat, telepon maupun SMS dari mereka yang mengaku sebagai suatu institusi resmi;
c. Waspada terhadap situs palsu atau phshing dan penipuan dengan menggunakan fitur penerusan panggilan (call forwarding);
d. Jangan mudah tergiur oleh harga murah dari suatu produk;
e. Membaca ulasan dan testimoni dan pembeli lainya dari suatu platform penjualan;

f. Selalu menyimpan bukti transaksi pembayaran dan bukti percakapan;
g. Melakukan pengecekan terhadap identitas penjual, dengan cara:
    1) Memerikasa followers akun yang bersangkutan, apakah masuk akal antara jumlah followers dengan like dan comment di setiap postingan,
    2) Memeriksa apakah kolom komentar akun tersebut dimatikan atau tidak. Apabila dimatikan maka masyrakat patut untuk curiga,
    3) Mengecek jumlah barang yang terjual. Apabila barang yang dijual terdeteksi hanya sedikit, maka patut menjadi pertimbangan untuk melakukan transaksi;
    4) Perhatikan metode pembayaran, disarankan untuk menghindari pembayaran langsung ke rekening bank penjual dengan alasan apapun. Agar lebih aman, bisa bertransaksi langsung melalui metode pembayaran tersedia di e-commerce.

2. Melakukan Upaya Represif

Sebagai petugas polisi, tindakan terakhir yang bisa dilakukan adalah represif. Langkah represif merupakan langkah terakhir setelah kejahatan seperti penipuan online Phishing terjadi. Bagi pelaku sendiri, berarti tindakan tersebut adalah sebuah tindakan yang dilakukan oleh aparat penegak hukum setelah kejahatan terjadi, dan perilaku ini dihukum dalam bentuk penegakan hukum ketika kejahatan terjadi. Upaya represif dilakukan setelah terjadinya tindak pidana, yaitu melalui proses penyidikan, penyidikan lanjutan, penuntutan pidana, sidang pengadilan, eksekusi, bahkan pembinaan pelaku tindak pidana. Upaya penertiban yang kami lakukan sendiri turut mengoptimalkan kekuatan kerjasama antara Kepolisian dengan beberapa instansi tekait seperti Bank, Kementerian Komunikasi dan Informatika, Pakar kriminal dan Bahasa, serta himbauan kepada masyarakat tentang penipuan cyber dan kejahatan lainnya.

Dalam kasus phishing aparat penegak hukum kota Samarinda mendasarkan penindakan pada beberapa ketentuan hukum, antara lain:

a. Pasal 492 Kitab Undang-Undang Hukum Pidana (KUHP) Tentang Pebuatan Curang
b. Pasal 28 ayat (1) jo. Pasal 45A ayat (1) Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang mengatur penyebaran berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik;

Ketentuan lain dalam UU ITE yang berkaitan dengan akses ilegal dan manipulasi data elektronik.

Namun, dalam praktiknya, penegakan hukum terhadap tindak pidana phishing menghadapi sejumlah kendala, seperti penggunaan identitas palsu, rekening penampung (rekening nominee), serta jaringan pelaku lintas daerah bahkan lintas negara. Modus operandi yang semakin kompleks ini sering kali melibatkan pemanfaatan teknologi spoofing, social engineering, dan penggunaan server atau akun anonim yang sulit dilacak secara konvensional. Akibatnya, proses penyelidikan dan penyidikan membutuhkan waktu yang lebih panjang serta ketelitian dalam pengumpulan dan analisis alat bukti elektronik.

3. Upaya Kerja Sama Antara Lembaga

Penanganan tindak pidana penipuan online melalui metode phishing tidak dapat dilakukan secara efektif apabila hanya mengandalkan satu institusi penegak hukum saja. Karakteristik kejahatan siber yang memanfaatkan teknologi informasi serta

jaringan internet menyebabkan pelaku dapat melakukan aksinya dari berbagai lokasi yang berbeda, bahkan melintasi batas wilayah hukum. Oleh karena itu, diperlukan kerja sama yang terkoordinasi antara berbagai lembaga terkait guna mendukung proses penegakan hukum serta meminimalisir terjadinya kejahatan serupa di masyarakat. Kerja sama antar lembaga ini menjadi salah satu faktor penting dalam meningkatkan efektivitas penegakan hukum, karena keberhasilan penegakan hukum tidak hanya ditentukan oleh aturan hukum semata, tetapi juga oleh koordinasi antara aparat penegak hukum dan lembaga terkait yang memiliki kewenangan dalam proses penanganan perkara. Salah satu bentuk kerja sama yang dilakukan adalah koordinasi antara aparat penegak hukum dengan lembaga perbankan. Dalam banyak kasus penipuan online phishing, pelaku menggunakan rekening bank sebagai sarana untuk menampung dana hasil kejahatan yang diperoleh dari korban. kerja sama antara aparat penegak hukum dengan lembaga keuangan sangat diperlukan dalam menelusuri aliran dana hasil kejahatan, termasuk melakukan pemblokiran terhadap rekening yang digunakan sebagai sarana tindak pidana. Selain itu, kerja sama juga diperlukan dengan penyedia layanan telekomunikasi dan penyedia platform digital. Pelaku penipuan online phishing sering kali menggunakan berbagai sarana komunikasi digital seperti pesan singkat, media sosial, maupun tautan yang mengarah pada situs palsu guna memperoleh data pribadi korban. Dalam penanganan kejahatan siber, peran penyedia layanan teknologi informasi sangat penting, terutama dalam memberikan data digital yang dapat digunakan sebagai alat bukti elektronik dalam proses penyidikan . Di samping itu, instansi pemerintah yang memiliki kewenangan di bidang teknologi informasi juga memiliki peran penting dalam upaya pencegahan dan penanganan kejahatan siber. Di samping itu, instansi pemerintah yang memiliki kewenangan di bidang teknologi informasi juga memiliki peran penting dalam upaya pencegahan dan penanganan kejahatan siber.

4. Upaya Perlindungan Dan Pemulihan

Dalam penanganan tindak pidana penipuan online melalui metode phishing, perhatian tidak hanya difokuskan pada penindakan terhadap pelaku, tetapi juga pada upaya perlindungan serta pemulihan terhadap korban yang mengalami kerugian. Korban penipuan online sering kali mengalami kerugian finansial, kerugian psikologis, serta kehilangan rasa aman dalam menggunakan teknologi digital. Oleh karena itu, perlindungan terhadap korban menjadi salah satu aspek penting dalam sistem penegakan hukum agar hak-hak korban tetap dapat terpenuhi. Perlindungan terhadap korban merupakan bagian dari kebijakan hukum pidana yang bertujuan untuk memberikan jaminan rasa aman serta pemulihan terhadap kerugian yang dialami oleh korban akibat suatu tindak pidana . Dalam konteks penipuan online phishing, perlindungan tersebut dapat dilakukan melalui berbagai langkah, seperti memberikan akses kepada korban untuk melaporkan tindak pidana yang dialaminya kepada aparat penegak hukum serta memperoleh pendampingan selama proses penanganan perkara berlangsung. Selain itu, upaya pemulihan kerugian korban juga dapat dilakukan melalui kerja sama dengan lembaga perbankan atau lembaga keuangan yang berkaitan dengan transaksi yang digunakan oleh pelaku. Dalam banyak kasus penipuan online phishing, pelaku menggunakan rekening tertentu sebagai sarana untuk menampung dana hasil kejahatan. Oleh karena itu, apabila korban segera melaporkan kejadian tersebut, pihak bank dapat melakukan tindakan pemblokiran terhadap rekening yang digunakan oleh pelaku sehingga dana yang

masih berada dalam rekening tersebut dapat diamankan. Dalam sistem hukum pidana modern, pemulihan kerugian korban merupakan salah satu tujuan penting yang harus diperhatikan dalam proses penegakan hukum, karena keadilan tidak hanya ditujukan kepada pelaku tetapi juga kepada korban yang mengalami kerugian akibat tindak pidana. Oleh karena itu, aparat penegak hukum perlu melakukan penelusuran terhadap aliran dana hasil kejahatan untuk mengetahui kemungkinan pengembalian dana kepada korban.

Di samping itu, korban juga perlu memperoleh perlindungan dalam bentuk pendampingan hukum serta informasi mengenai proses hukum yang sedang berlangsung. Hal ini penting agar korban memahami hak-haknya serta dapat berpartisipasi dalam proses penegakan hukum. Pendampingan tersebut dapat dilakukan oleh aparat penegak hukum maupun lembaga yang bergerak di bidang perlindungan korban kejahatan. Perlindungan terhadap korban kejahatan pada dasarnya merupakan tanggung jawab negara yang harus diwujudkan melalui berbagai kebijakan dan mekanisme hukum guna menjamin terpenuhinya hak-hak korban. Dengan adanya perlindungan tersebut, korban tidak hanya memperoleh keadilan secara hukum tetapi juga memperoleh dukungan dalam proses pemulihan dari kerugian yang dialaminya. Selain upaya pemulihan kerugian finansial, perlindungan terhadap korban penipuan online phishing juga dapat dilakukan melalui peningkatan edukasi mengenai keamanan digital. Masyarakat perlu diberikan pemahaman mengenai cara mengenali berbagai modus penipuan online serta langkah-langkah yang harus dilakukan apabila mengalami tindak pidana tersebut. Dengan meningkatnya kesadaran masyarakat terhadap keamanan digital, diharapkan jumlah korban penipuan online phishing dapat diminimalisir. Upaya perlindungan terhadap korban tidak hanya dilakukan setelah terjadinya tindak pidana, tetapi juga melalui langkah-langkah preventif yang bertujuan untuk mencegah masyarakat agar tidak menjadi korban kejahatan . Oleh karena itu, perlindungan terhadap korban harus dilakukan secara komprehensif melalui penegakan hukum, pemulihan kerugian, serta peningkatan kesadaran masyarakat mengenai bahaya kejahatan siber.

D. Konsep Ideal Dalam Penegakan Hukum Terhadap Kejahatan Phishing Di Kota Samarinda

Kejahatan phishing merupakan salah satu bentuk kejahatan siber yang memanfaatkan perkembangan teknologi informasi untuk memperoleh data atau informasi milik korban melalui berbagai bentuk penipuan dan manipulasi. Oleh karena itu, penegakan hukum terhadap kejahatan phishing tidak hanya dapat dilakukan melalui tindakan represif setelah tindak pidana terjadi, tetapi juga perlu disertai dengan upaya pencegahan yang dilakukan secara sistematis. Berdasarkan hasil penelitian mengenai kendala dan upaya penegakan hukum terhadap kejahatan phishing di Kota Samarinda, konsep ideal dalam menghadapi kejahatan phishing dapat dilakukan melalui edukasi dan peningkatan kesadaran masyarakat, penggunaan teknologi keamanan, pemantauan dan respons cepat, serta kepatuhan terhadap regulasi.

Penulis memakai konsep yang dipakai oleh penelitian sebelumnya, yaitu Gina Sonia Kafiar, yang melakukan penelitian dengan judul Phishing dan Upaya Perlindungan Hukum di Indonesia Sebagai Ancaman Kejahatan Siber (2026), yang dimana menyimpulkan beberapa konsep, yaitu akan saya uraikan dan saya gunakan sebagai landasan konsep ideal agar terciptanya Penegakan Hukum Terhadap Kejahatan Phishing Di Kota Samarinda, yaitu sebagai berikut:

1. **Edukasi dan Kesadaran Masyarakat**

Edukasi dan kesadaran masyarakat merupakan salah satu bagian penting dalam upaya mencegah terjadinya kejahatan phishing. Upaya tersebut dapat dilakukan melalui sosialisasi dan pelatihan kepada masyarakat mengenai karakteristik dan modus phishing serta cara mengenali bentuk-bentuk komunikasi atau tautan yang mencurigakan. Peningkatan literasi digital diperlukan agar masyarakat memiliki kemampuan untuk menggunakan teknologi informasi secara lebih aman dan bertanggung jawab.

Masyarakat sebagai pengguna teknologi informasi perlu diberikan pemahaman mengenai pentingnya menjaga data pribadi, tidak mudah memberikan informasi kepada pihak yang tidak dikenal, serta melakukan pemeriksaan terhadap sumber komunikasi sebelum melakukan suatu tindakan. Hal tersebut menjadi penting karena phishing pada dasarnya memanfaatkan kelengahan dan kepercayaan korban melalui penyamaran sebagai pihak yang sah atau terpercaya. Dengan meningkatnya pengetahuan dan kesadaran masyarakat, risiko masyarakat menjadi korban phishing dapat diminimalkan.

Konsep edukasi tersebut juga berkaitan dengan kondisi yang ditemukan dalam penelitian, bahwa penanganan kejahatan phishing tidak hanya bergantung pada kemampuan aparat penegak hukum, tetapi juga pada kesadaran masyarakat dalam menggunakan teknologi informasi. Oleh karena itu, sosialisasi dan pelatihan mengenai keamanan digital perlu dilakukan secara berkelanjutan dan tidak hanya diberikan setelah terjadinya tindak pidana.

2. **Penggunaan Teknologi Keamanan**

Konsep ideal selanjutnya adalah meningkatkan penggunaan teknologi keamanan sebagai bentuk perlindungan terhadap data dan akun pengguna. Penggunaan teknologi keamanan dapat dilakukan melalui penerapan antivirus, filter spam, serta autentikasi dua faktor atau two-factor authentication (2FA). Penerapan teknologi tersebut dapat menjadi lapisan perlindungan tambahan untuk mengurangi kemungkinan akses yang tidak sah terhadap akun maupun data pengguna.

Penggunaan teknologi keamanan menjadi penting karena kejahatan phishing berkembang seiring dengan perkembangan teknologi informasi. Pelaku dapat menggunakan berbagai sarana digital untuk mengirimkan pesan, tautan, atau bentuk komunikasi lain yang dirancang menyerupai layanan resmi. Oleh karena itu, perlindungan terhadap pengguna tidak cukup hanya mengandalkan kewaspadaan individu, tetapi juga perlu didukung oleh sistem keamanan teknologi yang mampu mendeteksi dan membatasi aktivitas yang mencurigakan.

Dalam konteks penanganan phishing di Kota Samarinda, penggunaan teknologi keamanan juga dapat mendukung upaya pencegahan sebelum suatu serangan menimbulkan kerugian. Dengan demikian, teknologi tidak hanya digunakan sebagai sarana yang dapat dimanfaatkan oleh pelaku kejahatan, tetapi juga dapat dimanfaatkan sebagai instrumen perlindungan bagi masyarakat.

3. **Pemantauan dan Respons Cepat**

Konsep ideal berikutnya adalah adanya pemantauan terhadap aktivitas sistem serta respons yang cepat ketika ditemukan adanya indikasi serangan phishing. Pemantauan diperlukan untuk mengetahui adanya aktivitas yang mencurigakan sehingga tindakan dapat dilakukan sebelum serangan berkembang dan menimbulkan

kerugian yang lebih besar. Selain itu, diperlukan pembentukan tim respons insiden yang memiliki kemampuan untuk menangani serangan secara cepat dan terkoordinasi.

Respons yang cepat memiliki arti penting dalam penanganan kejahatan phishing karena bukti dan jejak digital dapat mengalami perubahan, dihapus, atau menjadi sulit untuk ditelusuri. Kondisi tersebut juga ditemukan dalam penelitian, di mana aparat penegak hukum menghadapi kesulitan dalam memperoleh dan mempertahankan bukti elektronik karena akun, nomor telepon, maupun tautan yang digunakan pelaku dapat dinonaktifkan atau dihapus. Oleh sebab itu, pemantauan dan respons cepat tidak hanya diperlukan untuk mencegah kerugian, tetapi juga dapat membantu mengamankan informasi dan bukti digital yang diperlukan dalam proses penegakan hukum.

4. **Kepatuhan terhadap Regulasi**

Konsep ideal yang terakhir adalah peningkatan kepatuhan terhadap regulasi, khususnya dalam hal perlindungan data pribadi. Setiap institusi yang mengelola data masyarakat perlu memastikan bahwa pengelolaan dan perlindungan data dilakukan sesuai dengan ketentuan hukum yang berlaku. Dalam konteks penelitian ini, kepatuhan tersebut berkaitan dengan penerapan standar perlindungan data sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi.

Kepatuhan terhadap regulasi menjadi penting karena phishing tidak hanya berkaitan dengan kerugian finansial, tetapi juga dengan penguasaan dan penyalahgunaan data pribadi korban. Perlindungan data yang baik dapat mengurangi risiko data digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan penipuan. Oleh karena itu, institusi yang mengelola data masyarakat perlu menerapkan langkah-langkah perlindungan data secara konsisten serta memastikan adanya mekanisme keamanan yang memadai.

Berdasarkan keempat konsep tersebut, dapat dipahami bahwa konsep ideal dalam penanganan kejahatan phishing di Kota Samarinda harus dilakukan secara terpadu melalui pendekatan preventif dan perlindungan terhadap pengguna teknologi. Edukasi dan peningkatan kesadaran masyarakat diperlukan untuk mengurangi kerentanan korban, penggunaan teknologi keamanan diperlukan untuk memperkuat perlindungan data dan akun, pemantauan serta respons cepat diperlukan untuk mengantisipasi dan menangani serangan, sedangkan kepatuhan terhadap regulasi diperlukan untuk memastikan bahwa perlindungan data dilakukan sesuai dengan ketentuan hukum yang berlaku. Keempat aspek tersebut dapat menjadi dasar dalam meningkatkan efektivitas penanganan kejahatan phishing di Kota Samarinda.

KESIMPULAN

Pada bab akhir ini, penulis akan memaparkan kesimpulan dari hasil pembahasan dan memberikan beberapa pihak yang terlibat antara lain :

1. Kendala yang dihadapi penegak hukum dalam penanganan kasus penipuan online phishing di Kota Samarinda berasal dari kompleksitas karakteristik kejahatan siber yang terus berkembang. Pelaku phishing memanfaatkan teknologi informasi dengan menggunakan identitas palsu, alamat IP yang disamarkan, rekening nominee, serta berbagai modus operandi yang terus berubah sehingga menyulitkan aparat penegak hukum dalam mengidentifikasi, melacak, dan menangkap pelaku. Selain itu, proses pengumpulan alat bukti elektronik juga menghadapi berbagai hambatan karena bukti digital mudah dihapus atau diubah serta memerlukan keahlian khusus di bidang teknologi informasi dan digital forensik. Penanganan perkara juga dipengaruhi oleh

keterbatasan sumber daya manusia, sarana dan prasarana pendukung, serta perlunya koordinasi dengan lembaga lain seperti perbankan dan penyedia layanan telekomunikasi. Berbagai kendala tersebut menyebabkan proses penegakan hukum terhadap tindak pidana phishing di Kota Samarinda belum dapat berjalan secara optimal.

2. Upaya penegak hukum dalam penanganan kasus penipuan online phishing di Kota Samarinda dilakukan melalui beberapa tahapan penegakan hukum, yaitu penerimaan laporan dari korban, proses penyelidikan dan penyidikan, serta pengumpulan alat bukti termasuk bukti digital yang berkaitan dengan tindak pidana tersebut. Dalam prosesnya, aparat penegak hukum juga melakukan koordinasi dan kerja sama dengan lembaga lain seperti perbankan, penyedia layanan telekomunikasi, serta pihak terkait lainnya guna melacak aliran dana dan identitas pelaku. Selain itu, upaya preventif juga dilakukan melalui peningkatan sosialisasi dan edukasi kepada masyarakat agar lebih waspada terhadap berbagai modus penipuan online, khususnya phishing yang semakin berkembang seiring dengan kemajuan teknologi informasi.

Saran

1. Aparat penegak hukum harus meningkatkan sinergi dan koordinasi dengan masyarakat serta penyedia layanan internet dalam upaya pencegahan dan penanggulangan tindak pidana phishing, khususnya dalam pemantauan, pelacakan, dan penanganan aktivitas digital yang mencurigakan. Selanjutnya, aparat penegak hukum diharapkan dapat menerapkan sanksi yang proporsional terhadap pelaku phishing sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, baik berupa denda maupun pidana penjara yang sebanding dengan tingkat kesalahan dan dampak yang ditimbulkan, sehingga dapat memberikan efek jera sekaligus mendukung terciptanya penegakan hukum yang efektif.
2. Aparat penegak hukum diharapkan dapat meningkatkan kemampuan dan keahlian di bidang teknologi informasi serta forensik digital guna mendukung proses penyelidikan dan penyidikan tindak pidana siber. Selain itu, perlu dilakukan peningkatan sarana dan prasarana pendukung dalam penanganan kejahatan siber agar proses pelacakan pelaku dan pengumpulan alat bukti digital dapat dilakukan secara lebih efektif. Pengaturan hukum mengenai tindak pidana phishing juga perlu diperkuat melalui pembaruan dan penyesuaian regulasi yang secara khusus mengatur mengenai bentuk, modus operandi, serta sanksi terhadap pelaku kejahatan phishing agar dapat memberikan kepastian hukum dan efek jera. Kerja sama antara aparat penegak hukum dengan lembaga perbankan, penyedia layanan telekomunikasi, dan penyedia layanan digital perlu diperkuat untuk mempercepat proses penelusuran pelaku, pemblokiran sarana yang digunakan dalam melakukan kejahatan phishing, serta perlindungan terhadap masyarakat sebagai pengguna layanan digital.
3. Diperlukan peningkatan efektivitas penanganan kasus penipuan online phishing melalui penguatan koordinasi dan kerja sama antara aparat penegak hukum dengan lembaga perbankan, penyedia layanan telekomunikasi, serta instansi terkait. Selain itu, perlu dilakukan sosialisasi dan edukasi kepada masyarakat agar lebih waspada terhadap berbagai modus penipuan online dan tidak mudah memberikan data pribadi.

DAFTAR PUSTAKA

BUKU

Arief, N, B., 2016, Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia, Jakarta, RajaGrafindo Persada.

Asshiddiqie, J., 2006, Penegakan Hukum, Jakarta, Konstitusi Press.

Atmasasmita. R, 2014, Sistem Peradilan Pidana Kontemporer, Jakarta, Kencana.

Friedman. M. L, 1975 Sistem Hukum: Perspektif Ilmu Sosial, New York, Russel Sage Foundation.

Hamzah, A., 2016, Hukum Acara Pidana Indonesia, Jakarta, Sinar Grafika.

Harahap, Y,M., 2012, Pembahasan Permasalahan dan Penerapan KUHAP, Jakarta, Sinar Grafika.

Husen. M. H, 1990, Kejahatan dan Penegakan Hukum di Indonesia, Jakarta, Rineka Cipta.

Kanter. E,Y., Sianturi. S,R., 2002, Asas-Asas Hukum Pidana di Indonesia dan Penerapanya, Jakarta, Storia Grafik.

Mahmud. P,M., 2016, Penelitian Hukum, Jakarta, Kencana Prenda Media Group, Edisi Revisi.

Makarim, E., 2013, Kejahatan Siber (Cyber Crime), Jakarta, RajaGrafindo Persada.

Mansur, A, M., Gultom, E. 2009, Cyber Law: Aspek Hukum Teknologi Informasi, Bandung, Refika Aditama.

Maskun, 2013, Kejahatan Siber Cyber Crime suatu Pengantar, Jakarta: Kencana hlm.

Muladi,2002, Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana, Semarang.

Nazir. M., 2003, Metode Penelitian, Jakarta, Pt. Ghalia Indonesia. Hlm 19.

Rahardjo. S., 2006, Ilmu Hukum, Bandung, Citra Aditya Bakti/

Rahardjo. S., 2009, Penegakan Hukum Suatu Tinjauan Sosiologis, Yogyakarta: Genta publishing.

Rahardjo. S.,1983, Masalah Penegakan Hukum, Bandung, Sinar Baru.

Remy. S,S. 2009, Kejahatan & Tindak Pidana Komputer, Jakarta, Pustaka Utama Grafiti.

Rena Yulia, Viktimologi,2010, Perlindungan Hukum terhadap Korban Kejahatan, Yogyakarta: Graha ilmu.

Rosadi. S. D., 2022, Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, PT Refika Aditama, Bandung.

Sadi Is. M., 2021, Aspek Hukum Informasi di Indonesia, Kencana, Jakarta,.

Soekanto. S., 2007, Faktor-faktor yang Mempengaruhi Penegakan Hukum,

Soekanto. S., 2007, Pengantar Penelitian Hukum, Jakarta, UI Press.

Usman. S., 2009, Dasar-Dasar Sosiologi,Yogyakarta, Pustaka Belajar.

Wahid, A., Labib, M., 2005, Kejahatan Mayantara (Cyber Crime), Bandung, Refika Aditama.

Widodo., 2011, Aspek Hukum Kejahatan Mayantara, Yogyakarta, Aswindo.

UNDANG-UNDANG

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE).

Undang-Undang Republik Indonesia Nomor 2 Tahun 2022 Tentang Kepolisian Negara Republik Indonesia.

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

JURNAL

Benuf, K., Azhar,m, 2020. Metedologi Penelitian Hukum Sebagai Instrumen, Gema Keadilan. 7(1).

Cahyaningsih. R. D., Faufan .A., Hasbi. S., Winanti. A., (2025), Kebijakan Hukum Pidana Phishing Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia Malaysia. Vol 1, No.4.

Dwiananda. A. R., Suryanto. H. V. B., Penegakan Hukum Pidana Terhadap Penyebaran Berita Bohong Di Sosial Media, Jurnal Panaroma Hukum Vol. 4, No. 2 (2 Desember 2019).

Gina Sonia Kafiar, Phishing dan Upaya Perlindungan Hukum di Indonesia Sebagai Ancaman Kejahatan Siber, Jembatan Hukum : Kajian ilmu Hukum, Sosial dan Administrasi Negara, Vol 3, No. 1, (2026)

Lokapala. Y. H., Nurfauzi. F. J., Widowaty. Y., (2024), Aspek Yuridis Kejahatan Phishing dalam

Ketentuan Hukum di Indonesia, Universitas Muhammadiyah, Yogyakarta, Indonesia.
M Lalu. Ahadi. A., Efektivitas Hukum Dalam Perspektif Filsafat Hukum: Relasi Urgensi Sosialisasi Terhadap Eksistensi Produk Hukum, Jurnal USM Law Review, Vol 5 No 1.
Vadil. N., Pratama. A. R., Analisis Kesadaran Keamanan Terhadap Ancaman Phishing, Universitas Islam Indonesia, Yogyakarta, Indonesia.
Vikran Fasyadhiyaksa Putra, Modus Operandi Tindak Pidana Phising Menurut UU ITE, Jurist-Diction, Vol 4, No. 6, (2021) hlm, 2532-2533.
Yudho,Winarno, Heri Tjandrasari, Efektivatis Hukum Dalam Masyarakat, Jurnal Hukum & Pembangunan, Vol. 17, No. 1, (April 2017).
Yusuf. M., Analisis terhadap Modus-Modus Dalam Hukum Cybercrime, Jurnal Hukum, Politik dan Ilmu Sosial, Vol.2, No2, (2022).

Skripsi

Akram. 2025, Penegakan Hukum Terhadap Tindak Pidana Pencurian Data Pribadi Dengan Cara Phishing di Media Elektronik.
Ashar Subakti. 2024, Perlindungan Hukum Terhadap Korban Kejahatan Phishing di Kota Samarinda.

Internet

Efektivitas, 2016. Pada Kamus Besar Bahasa Indonesia Daring. Pada 23 September 2025, dari https://kbbi.kemdikbud.go.id/entri/perlindungan.
Indonesia Anti-Phishing Data Exchange, Report All Data Phishing Domain .id, diakses melalui https://idadx.id/report-all

WAWANCARA

Hasil wawancara dengan Bapak Bripka Budi Susanto, S.I,Kom, Banit Eksus Polresta Samarinda, Oleh Alif Naufal Istiqlal, Di Kota Samarinda, 29 SePTEMBER 2025.