



Efektivitas Penyidikan Tindak Pidana Dalam Undang-Undang Tentang Informasi Dan Transaksi Elektronik Terkait Phishing Di Wilayah Hukum Kepolisian Daerah Riau

Ihsan Riznawara¹, Syaifullah Yophi Ardianto², Riyanda Elsera Yozani³

^{1,2,3}Universitas Riau

Abstract

Received: 18 April 2026

Revised: 29 April 2026

Accepted: 11 Mei 2026

The rapid advancement of technology has become an inseparable part of human life. On one hand, this progress brings numerous benefits to daily activities; on the other hand, it also opens opportunities for criminal acts. One prevalent crime is phishing, which aims to obtain victims' electronic information, particularly related to financial data. This information is then used to unlawfully access and take the victim's funds without their consent.

This research is a sociological study based on social realities to uncover the facts on the ground and answer the research problems. The study was conducted in the jurisdiction of the Riau Regional Police. The population and sample include parties who are directly related to the issues being investigated. The sources of data used in this research consist of primary, secondary, and tertiary data. Data collection techniques include interviews, questionnaires, and literature review.

The results of the study indicate that the investigation of criminal acts under the Law on Electronic Information and Transactions (ITE Law) related to phishing within the jurisdiction of the Riau Regional Police has not been running optimally. This is evident from the relatively low number of resolved cases. The investigation process begins with examining the victim, collecting evidence that can identify the perpetrator, and establishing cooperation with stakeholders. Once all procedures are properly carried out, the suspect is named and the case is submitted to the Prosecutor's Office. The obstacles faced during the investigation include limited human resources and supporting technology within the police force, difficulties in identifying perpetrators operating in an organized manner, challenges in tracking the bank accounts used by the perpetrators, and low public awareness levels. To overcome these obstacles, the Riau Regional Police have made efforts to enhance human resources and technological infrastructure, collaborate with stakeholders such as banks, other regional police departments, the National Police Headquarters, and social media platforms, as well as conduct public education and outreach programs. Repressive measures involve investigation and prosecution. The main challenges in law enforcement are limited human resources and facilities, difficulties in identifying and tracking perpetrators who operate in an organized manner, and low public awareness. To overcome these obstacles, the Riau Regional Police have taken steps such as improving personnel capacity and resources, cooperating with stakeholders including banks, other regional police departments, the National Police Headquarters, and social media platforms, as well as providing continuous public education and outreach.

Keywords: Cyber Crime, Effectiveness, Investigation, Phishing

(*) Corresponding Author: ihsanriznawaraa@gmail.com, syaifullahyophi23@gmail.com, riyandayozani@lecturer.unri.ac.id

How to Cite: Riznawara, I., Ardianto, S., & Yozani, R. (2026). Efektivitas Penyidikan Tindak

Pidana Dalam Undang-Undang Tentang Informasi Dan Transaksi Elektronik Terkait Phishing Di Wilayah Hukum Kepolisian Daerah Riau. *Jurnal Ilmiah Wahana Pendidikan*, 12(5.C), 285-299. Retrieved from <https://jurnal.peneliti.net/index.php/JIWP/article/view/14206>.

INTRODUCTION

Latar Belakang Masalah

Hadirnya internet membawa kemudahan dan kemanfaatan dalam kehidupan modern sekarang ini. . Namun selain membawa kemanfaatan, internet dapat juga dimanfaatkan untuk melakukan kejahatan. Kejahatan yang muncul telah beralih dari bentuk konvensional menjadi inkonvensional (kejahatan canggih) dengan modus operandi yang semakin canggih dan kompleks.¹ Perkembangan internet telah menciptakan berbagai jenis kejahatan yang terjadi di dunia maya, yang kemudian melahirkan istilah baru yang dikenal dengan *cyber crime*.²

Salah satu klasifikasi *cyber crime* yakni adanya tindakan pencurian informasi elektronik dan/atau dokumen elektronik dengan metode penipuan yang menunjukkan manipulasi sebuah data seolah data tersebut merupakan data otentik yang disebut dengan *phishing* (*password harvesting fishing*).³ *Phishing* bertujuan untuk memancing korban agar memberikan informasi elektronik dan informasi sensitif yang seharusnya tidak dibagikan kepada siapa pun.⁴ *Phishing* saat ini semakin marak, terutama di kalangan pengguna internet, khususnya di *Social Networking Services* atau sosial media seperti Facebook, X, dan Instagram, *Electronic Communication Channels* seperti *Electronic Mail* (Email), *Hypertext Transfer Protocol Secure* (HTTPS), dan *Short Message Service* (SMS) serta di *Electronic Commerce* seperti Shopee, Lazada, dan TikTok Shop.⁵

Dalam penanganan tindak pidana *phishing* secara umum, terdapat beberapa tantangan utama. Pertama, belum terdapat regulasi yang secara spesifik mengatur mengenai *phishing*, sehingga penegakan hukum masih mengacu pada Pasal 32 ayat (1) jo Pasal 48 ayat (1) atau Pasal 35 jo Pasal 51 ayat (1) UU ITE, yang menimbulkan ketidakpastian hukum. Kedua, keterbatasan sumber daya manusia dan teknologi di kalangan aparat penegak hukum menghambat efektivitas penanganan kasus, terutama karena modus *phishing* terus berkembang seiring kemajuan teknologi. Ketiga, perbedaan lokasi antara pelaku dan korban menyulitkan proses penyelidikan dan penindakan hukum. Keempat, rendahnya literasi digital masyarakat menyebabkan tingginya kerentanan terhadap serangan *phishing*.⁶

¹ Erdianto Effendi, Mukhlis Ridwan, dan Davit Ramadhan, "Legal Protection for Teenagers in the Use of Social Media at SMKN 1 Bangkinang Kampar", Artikel pada Jurnal Pengabdian Hukum Indonesia, Vol. 6, No. 1, 2023, hlm. 122.

² Sahat Maruli T. Situmeang, *Cyber Law*, Cakra, Bandung, 2020, hlm. 22

³ Henny Saida Flora, et. al, *Hukum Pidana di Era Digital*, Rey Media Grafika, Batam, 2022, hlm. 24.

⁴ Nurul Fadila dan Tamaulina Br. Sembiring, " Analisis Yuridis Putusan Hakim dalam Perkara Tindakan Pidana Phishing yang dilakukan melalui Media Sosial (Studi Putusan Nomor: 155/Pid.Sus/2018/PN Cbn), Artikel pada *Jurnal of International Multidisciplinary Research*, Vol. 2, No. 1 Januari 2024, hlm. 315

⁵ *Ibid*

⁶ Yazid Haikal Lokapala, Fuad Januar Nurfauzi, dan Yeni Widowaty, " Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia", Artikel pada Indonesian Journal of Criminal Law and Criminology, Vol. 05, No. 01, 2024, hlm. 23.

Penulis memperoleh angka laporan tindak pidana terkait phishing dari Kepolisian Daerah Riau yang terjadi dalam kurun waktu 4 (empat) tahun terakhir, sebagai berikut:

No	Tahun	Jumlah Angka Laporan Tindak Pidana terkait <i>Phishing</i>
1.	2021-2022	13
2.	2023	19
3.	2024	24

Beberapa kasus *phishing* yang ditangani oleh Kepolisian Daerah Riau menunjukkan semakin kompleksnya modus kejahatan siber di Indonesia. Pada tahun 2022, pelaku berinisial AS ditangkap karena membobol sejumlah akun Coinbase milik warga negara asing melalui metode *phishing*. Diketahui bahwa pelaku mempelajari teknik tersebut secara otodidak melalui video *tutorial* di YouTube.⁷ Selanjutnya, pada tahun 2024, pelaku berinisial VK didakwa melanggar Pasal 32 ayat (2) jo Pasal 48 ayat (2) UU ITE setelah melakukan *phishing* melalui pengiriman tautan palsu kepada calon korban. VK memperoleh data akun email korban, yang kemudian digunakan untuk mengakses rekening bank dan e-wallet terhubung. VK bekerja sama dengan rekan luar negeri untuk menarik dana dari akun korban dan memperoleh keuntungan sebesar Rp 181 juta.

Berdasarkan latar belakang yang telah dipaparkan, maka penulis tertarik untuk mengangkat masalah ini dalam bentuk skripsi dengan judul **“Efektivitas Penyidikan Tindak Pidana dalam Undang-Undang tentang Informasi Dan Transaksi Elektronik terkait *Phishing* di Wilayah Hukum Kepolisian Daerah Riau”**

Rumusan Masalah

Berdasarkan latar belakang tersebut di atas, adapun rumusan masalahnya adalah sebagai berikut:

1. Bagaimanakah pelaksanaan penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau?
2. Apakah kendala dalam penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau?
3. Bagaimanakah upaya yang dilakukan oleh Kepolisian Daerah Riau untuk mengatasi penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau?

Tujuan dan Kegunaan Penelitian

1) Tujuan Penelitian

Berdasarkan dari perumusan masalah yang telah diuraikan di atas maka tujuan dilakukan penelitian ini adalah sebagai berikut :

- a. Untuk mengetahui pelaksanaan penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau;

⁷ <https://pekanbaruini.com/belajar-dari-youtube-warga-pekanbaru-bobol-akun-coinbase-milik-wna-senilai-belasan-miliar>, diakses, tanggal, 22 Oktober 2024.

- b. Untuk mengetahui kendala dalam penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau.
- c. Untuk mengetahui upaya yang dilakukan oleh Kepolisian Daerah Riau untuk mengatasi penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau.

2) Kegunaan Penelitian

Sedangkan kegunaan yang penulis harapkan dari penelitian ini adalah sebagai berikut :

- a. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi ilmu pengetahuan, yang terkhusus di ilmu Hukum Pidana terutama yang berkaitan dengan penyidikan tindak pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik terkait *phishing* di wilayah hukum Kepolisian Daerah Riau.
- b. Hasil penelitian ini dapat diharapkan dapat menjadi referensi bagi penelitian-penelitian sejenis.

Kerangka Teori

1. Teori Penegakan Hukum

Inti dan makna penegakan hukum secara konseptual terletak pada upaya untuk menyelaraskan hubungan antara nilai-nilai yang tercemrin dalam kaidah-kaidah yang kokoh yang sebagaimana dikemukakan oleh Soerjono Soekanto.⁸

Penegakan hukum dapat terlaksana secara efektif apabila pelaksanaannya didukung oleh berbagai faktor pendukung. Pertama, aparatur penegak hukum yang berkualitas, yaitu mereka yang profesional dan bertindak sesuai dengan ketentuan peraturan perundang-undangan. Kedua, ketersediaan sarana dan prasarana hukum yang memadai guna menunjang proses penegakan hukum. Ketiga, tingkat kesadaran hukum masyarakat yang tinggi, sehingga masyarakat patuh terhadap hukum yang berlaku. Keempat, dukungan dari birokrasi pemerintah yang konsisten dalam menjalankan kebijakan dan regulasi, sehingga menciptakan sistem penegakan hukum yang efektif dan berkeadilan.⁹

Pelaksanaan hukum pada dasarnya dapat berjalan dengan baik dan menciptakan ketertiban, namun dalam praktiknya tidak menutup kemungkinan terjadi pelanggaran hukum. Dalam kondisi demikian, penegakan hukum menjadi hal yang esensial, karena melalui proses inilah hukum memperoleh kekuatan nyata dan dapat berfungsi sebagaimana mestinya. Dalam pelaksanaannya, penegakan hukum harus memperhatikan tiga unsur utama, yaitu kepastian hukum, kemanfaatan, dan keadilan.¹⁰

2. Teori Efektivitas Hukum

Menurut Soerjono Soekanto, teori efektivitas hukum mengacu pada sejauh mana suatu sistem hukum mampu mencapai tujuan yang telah ditetapkan. Suatu

⁸ Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum*, PT Raja Grafindo Persada, Jakarta, 1980 hlm. 203

⁹ Soerjono Soekanto. *Faktor-Faktor yang Mempengaruhi Penegakkan Hukum*. Raja Grafindo. Jakarta. 1983. hlm. 7.

¹⁰ Soerjono Soekanto. *Faktor-Faktor yang Mempengaruhi Penegakkan Hukum*. Raja Grafindo. Jakarta. 1983. hlm. 7.

hukum dikatakan efektif apabila mampu menimbulkan akibat hukum yang positif, yaitu ketika hukum tersebut berhasil mengarahkan, mengendalikan, atau mengubah perilaku manusia agar sesuai dengan norma hukum yang berlaku. Dengan demikian, efektivitas hukum berkaitan erat dengan kemampuan hukum dalam mengatur masyarakat serta menegakkan kepatuhan terhadap peraturan hukum yang berlaku.¹¹

Teori efektivitas hukum yang dikemukakan oleh Soerjono Soekanto mengukur efektivitas penegakan hukum berdasarkan lima aspek, yaitu faktor hukum, faktor penegakan hukum, faktor sarana atau fasilitas pendukung, faktor masyarakat, dan faktor kebudayaan. Pada unsur pertama, efektivitas tergantung pada kualitas aturan hukum itu sendiri, yang menentukan apakah hukum tersebut berfungsi dengan baik atau tidak.¹²

Kerangka Konseptual

1. Efektivitas dimaknai dengan pemanfaatan sumber daya, sarana dan prasarana dalam jumlah tertentu yang secara sadar ditetapkan sebelumnya untuk menghasilkan sejumlah barang atas jasa kegiatan yang dijalankannya.¹³
2. Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.¹⁴
3. Tindak Pidana merupakan setiap perbuatan yang diancam dengan hukuman dalam perundang-undangan sebagai pelanggaran atau kejahatan.¹⁵
4. *Phishing* merupakan ancaman keamanan siber yang signifikan, di mana penyerang menggunakan teknik rekayasa sosial untuk menipu individu agar mengungkapkan informasi pribadi atau kredensial sensitif.¹⁶
5. Kepolisian Daerah adalah pelaksana tugas dan wewenang Polri di wilayah provinsi yang berada di bawah Kapolri.¹⁷

Metode Penelitian

1. Jenis Penelitian.

Penelitian hukum adalah penelitian yang menekankan pada aspek praktis untuk menemukan hukum yang dapat dipergunakan untuk menyelesaikan suatu peristiwa konkrit. Penelitian ini termasuk dalam kategori penelitian hukum empiris atau sosiologis yang berfokus pada realitas hukum, khususnya dalam

¹¹ Soerjono Soekanto, *Efektivitas Hukum dan Penerapan Sanksi*, CV Ramadja Karya, Bandung, 1988, hlm. 80

¹² Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, PT Raja Grafindo, Jakarta, 2007, hlm. 5

¹³ Sondang P. Siagian, *Kiat Meningkatkan Produktivitas kerja*, PT Rineka Cipta, Jakarta, 2002, hlm.8.

¹⁴ Pasal 1 angka 2 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

¹⁵ Imron Rosyadi, *Hukum Pidana*, Revka Prima Media, Surabaya, 2022, hlm. 53.

¹⁶ Lutfi Azis Febrika Ardy, et, al, "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial", Artikel pada *Journal of Internet and Software Engineering*, Vol. 1, No. 4, 2024, hlm. 9.

¹⁷ Pasal 1 angka 3 Peraturan Kepolisian Negara Republik Indonesia Nomor 3 Tahun 2024 Tentang Perubahan Atas Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2018 Tentang Susunan Organisasi Dan Tata Kerja Kepolisian Daerah.

aspek dan sein dari hukum.¹⁸

Penelitian hukum empiris atau sosiologis adalah penelitian yang melihat hubungan antara hukum dan masyarakat, sehingga penelitian tersebut mempunyai kemampuan untuk mengkaji suatu hukum yang berlaku di dalam masyarakat itu sudah efektif. Oleh karena itu, penelitian ini dilakukan untuk mengkaji efektivitas penyidikan tindak pidana dalam Undang-Undang Informasi dan Transaksi Elektronik terkait phishing di wilayah hukum Kepolisian Daerah Riau.

2. Lokasi Penelitian

Lokasi penelitian yang dilakukan oleh penulis adalah Kepolisian Daerah Riau. Penulis mengambil lokasi ini karena instansi ini berkaitan langsung dengan penegakan hukum tindak pidana pencurian informasi elektronik dengan metode phishing.

3. Populasi dan Sampel

1) Populasi

Adapun yang menjadi populasi dalam penelitian ini adalah: Panit Subdirektorat V Direktorat Reserse Kriminal Khusus Kepolisian Daerah Riau, Personel Bagian Pengawasan Penyidikan Reserse Kriminal Khusus Kepolisian Daerah Riau, Personel Subdirektorat V Reserse Kriminal Khusus Kepolisian Daerah Riau, Masyarakat di Kecamatan Binawidya, Kecamatan Marpoyan Damai, Kecamatan Limapuluh, dan Kecamatan Sukajadi.

2) Sampel

Metode ini menetapkan sejumlah sampel yang mewakili jumlah populasi yang ada, yang kategori sampelnya itu ditetapkan sendiri oleh peneliti. Komposisi populasi dan sampel dapat dilihat dari tabel berikut:

No.	Jenis Populasi	Jumlah Populasi	Jumlah Sampel	Persentase (%)
1.	Panit Subdirektorat V Direktorat Reserse Kriminal Khusus Kepolisian Daerah Riau	7	1	14,29%
2.	Anggota Subdirektorat V Reserse Kriminal Khusus Kepolisian Daerah Riau	20	2	10%
4.	Personel Bagian Pengawasan Penyidikan Reserse Kriminal Khusus Kepolisian Daerah Riau	9	1	11,11%
5.	Masyarakat Kecamatan Binawidya	80.132	74	0,0898%
6.	Masyarakat Kecamatan Marpoyan Damai	150.131	135	0,0899%
7.	Masyarakat Kecamatan Limapuluh	45.021	41	0,0911%
8.	Masyarakat Kecamatan Sukajadi	48.026	43	0,0895%
Jumlah		323.346	295	0,09%

¹⁸ Niko Ngani, *Metode Penelitian dan Penulisan Hukum*, Pustaka Yustisia, Yogyakarta, 2012, hlm. 82.

4. Sumber Data

Data pertama dinamakan data primer yang diperoleh langsung dari lapangan berdasarkan populasi dan sampel dengan tujuan untuk mencari solusi dari rumusan permasalahan melalui wawancara di lapangan mengenai hal-hal yang berkaitan dengan rumusan permasalahan.

Data kedua dinamakan data sekunder yang diperoleh melalui studi kepustakaan yang berkaitan dengan rumusan permasalahan serta mendukung data primer. Data sekunder didukung dengan tiga bahan hukum, yang dijelaskan sebagai berikut.

a. Bahan hukum primer :

1. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana;
3. Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

b. Bahan hukum sekunder :

Yaitu bahan-bahan yang berkaitan dengan bahan hukum primer dan memberikan penjelasan terhadap bahan hukum primer, seperti dokumen, arsip, artikel, makalah, literatur, dan data dari internet yang berhubungan dengan penelitian yang penulis teliti.

c. Bahan Hukum Tersier

Yaitu bahan yang memberikan petunjuk atau penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, seperti kamus dan ens

5. Teknik Pengumpulan Data

1) Kuesioner

Kuesioner adalah salah satu metode data elektronik dengan mempersiapkan pertanyaan-pertanyaan yang memiliki hubungan dengan permasalahan yang diteliti dan jawaban-jawaban dari pertanyaan tersebut telah disediakan untuk responden yang menjawab pertanyaan-pertanyaan tersebut.

2) Wawancara

Wawancara adalah salah satu metode pengumpulan data dengan bentuk tanya jawab antara penulis dengan narasumber sebagai informan. Metode wawancara yang digunakan adalah wawancara terstruktur. Wawancara terstruktur dipilih sebagai metode dikarenakan pertanyaan yang disampaikan lebih diperolehnya data yang dibutuhkan

3) Kajian Kepustakaan

Kajian pustaka adalah salah satu metode pengumpulan data melalui membaca literatur-literatur kepustakaan yang memiliki korelasi dengan permasalahan yang diteliti. Data-data yang dikumpulkan, merupakan data sekunder yang bertujuan untuk mendukung data primer.

6. Analisis Data

Analisis data dalam penelitian ini menggunakan data primer dan data sekunder yang diolah dan dianalisis dengan metode kualitatif, yaitu metode yang menguraikan data dalam bentuk kalimat yang logis, sistematis, dan teratur. Untuk menarik kesimpulan, penelitian ini menggunakan metode berpikir deduktif, yaitu cara berpikir yang berangkat dari pernyataan umum menuju pada kesimpulan yang bersifat khusus.

TINJAUAN UMUM

Tinjauan Umum tentang Penyidikan

M. Yahya Harahap mengemukakan bahwa penyidikan merupakan tahap lanjutan dari proses penyelidikan yang dilakukan dengan adanya persyaratan dan pembatasan ketat dalam penggunaan upaya paksa, setelah terkumpulnya bukti awal yang cukup yang menunjukkan bahwa suatu peristiwa patut diduga sebagai tindak pidana dan dalam tindakan pidana tersebut ada yang layak diduga.¹⁹ Noor Rohmat berpendapat bahwa tujuan penyidikan merupakan suatu proses yang mengumpulkan bukti-bukti tindak pidana yang diperlukan untuk mengidentifikasi pelaku tindak pidana dan membuktikan tindak pidana pelaku di pengadilan.²⁰ Tujuan dari proses penyidikan ialah menemukan pihak yang bertanggung jawab atas terjadinya tindak pidana serta mengumpulkan bukti-bukti yang berhubungan dengan tindak pidana dengan tujuan untuk membuktikan kesalahan dari pihak yang bertanggung jawab. Untuk mencapai tujuan tersebut, penyidik melakukan pengumpulan informasi yang berkaitan dengan berbagai aspek peristiwa pidana yaitu, informasi peristiwa tindak pidana, para pihak tindak pidana, lokasi tindak pidana, waktu tindak pidana, tujuan pelaku tindak pidana, dan identitas pelaku tindak pidana.²¹

Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 8 Tahun 1981 sebagaimana dijelaskan bahwa penyidik merupakan pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.²² Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana menetapkan bahwa tanggung jawab pelaksanaan fungsi penyidikan berada pada instansi kepolisian, yang dijalankan oleh penyidik dan penyidik pembantu. Sementara itu, penyidik pegawai negeri sipil juga diberikan kewenangan untuk melakukan penyidikan, namun terbatas pada tindak pidana yang diatur dalam undang-undang pidana khusus. Selain itu, pelaksanaan tugas penyidik pegawai negeri sipil tetap berada di bawah koordinasi dan pengawasan penyidik Kepolisian Negara Republik Indonesia.

Tinjauan Umum tentang *Cyber Crime*

Debatri Halder dan K. Jaishankar mendefinisikan *cyber crime* sebagai pelanggaran yang dilakukan terhadap individu atau kelompok dengan motif kriminal, yang bertujuan untuk sengaja merusak reputasi korban atau menyebabkan kerugian fisik, mental, atau kerugian lainnya, baik secara langsung maupun tidak langsung, dengan memanfaatkan jaringan telekomunikasi modern.²³ Sementara itu, Wisnubroto memberikan pengertian lain, yakni *cyber crime* sebagai tindakan ilegal yang dilakukan dengan memanfaatkan komputer sebagai

¹⁹ Tinuk Dwi Cahyani, *Hukum Acara Pidana Indonesia (Dalam Teori dan Praktek)*, Universitas Muhammadiyah Malang, Malang, 2023, hlm. 22.

²⁰ Noor Rohmat, *Sistem Peradilan Pidana*, K-Media, 2024, hlm. 73.

²¹ Lusla Sulastri, *Buku Ajar Hukum Acara Pidana*, Jejak Pustaka, Yogyakarta, 2024, hlm 72.

²² Pasal 1 angka 1 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

²³ Hanafi, *Dasar Cyber Security dan Forensic*, Deepublish, Yogyakarta, 2022, hlm. 14.

sarana atau objek, baik untuk memperoleh keuntungan pribadi maupun tidak, yang pada akhirnya merugikan pihak lain.²⁴

Dalam perkembangan teknologi, *cyber crime* mengalami perkembangan juga dalam jenis-jenis ataupun modusnya. Jenis-jenis *cyber crime* yang terjadi diantara lain adalah *Unauthorized Access to Computer System and Service*, *Offense Against Intellectual Property*, *Illegal Contents*, *Cyberstalking*, *Hacking* dan *Cracking*, *Cybersquatting* dan *Typosquatting*, *Cybersquatting*, *Arp Spoofing*, *Carding*, *Defacing*, dan *Phising*.²⁵ Di Indonesia, pengaturan mengenai cyber crime tercantum dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Tinjauan Umum tentang Phishing

Collins menyatakan bahwa definisi dari phishing adalah kegiatan yang menggunakan email palsu atau situs web palsu yang sama dengan salinan dari situs web asli dengan tujuan untuk mengekstraks informasi elektronik yang bersifat finansial dari sistem komputer korban ke sistem komputer pelaku. Merriam-Webster juga menyatakan bahwa phishing adalah penipuan yang di mana pengguna email ditipu untuk mengungkapkan informasi yang bersifat pribadi atau rahasia yang informasi tersebut dapat digunakan oleh pelaku secara tidak sah. Dan dari Lastdrager sendiri, phishing merupakan praktik penipuan yang dapat diskalakan di mana pelaku meniru identitas yang bertujuan mendapatkan informasi dari korban.²⁶

HASIL PENELITIAN DAN PEMBAHASAN

Pelaksanaan Penyidikan Tindak Pidana dalam Undang-Undang Informasi dan Transaksi Elektronik terkait Phishing di Wilayah Hukum Kepolisian Daerah Riau

Berdasarkan hasil penelitian wawancara dan kuesioner, dapat disimpulkan bahwa terdapat beberapa faktor yang menyebabkan terjadinya tindak pidana dalam Undang-Undang Informasi dan Transaksi Elektronik terkait phishing. Dengan adanya perkembangan teknologi yang mempermudah akses dan pembelajaran *phishing* melalui platform seperti YouTube dan forum online dengan biaya yang rendah. Perihal ini menyebabkan pelaku *phishing* (*phisher*) mudah mengidentifikasi target melalui data pribadi yang tersebar di dunia maya atau hasil kebocoran data dari pengendali data pribadi. Sementara itu, kurangnya pemahaman masyarakat tentang sistem dan kejahatan siber meningkatkan kerentanan terhadap informasi yang menyesatkan di ruang digital.

Berdasarkan hasil wawancara, dapat dipahami bahwa ada beberapa upaya untuk mendukung pelaksanaan penyidikan yang sebagai berikut.

1) Upaya Preventif

²⁴ Miftakhur Rokhman Habibi dan Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia", Artikel pada *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, Vol. 23, No. 2, Desember 2023, hlm. 424.

²⁵ Utin Indah Permata Sari, "Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime yang Dilakukan oleh Virtual Police di Indonesia", Artikel pada *Mimbar Jurnal Hukum*, Vol. 02, No. 01, 2021, hlm. 10.

²⁶ Elmer Lastdrager, *From Fishing to Phishing, TRESPASS*, Enschede, 2018, hlm. 14.

- a) Menyampaikan informasi dan penyuluhan melalui media sosial terkait tindak pidana elektronik termasuk pencurian informasi elektronik;
- b) Melaksanakan sosialisasi di lingkungan masyarakat, sekolah, dan instansi sebagai upaya peningkatan kesadaran akan bahaya pencurian informasi elektronik yang banyak terjadi;
- c) Jika adanya laporan dugaan dan/atau dari korban tindak pidana terkait phishing, biasanya akan diedukasi terkait tindak pidana tersebut. Bertujuan untuk memberikan pemahaman dan dapat mencegah di kemudian harinya;
- d) Dilakukan kerja sama dalam bentuk kegiatan penyuluhan antara Subdit V Direktorat Reserse Kriminal Khusus Polda Riau dengan Unit Pembinaan Masyarakat (Binmas), yang memiliki tugas untuk membina serta mengembangkan peran aktif masyarakat melalui pendekatan Perpolisian Masyarakat (Polmas).

2) Upaya Represif

a) Penyelidikan

Biasanya penyelidikan tindak pidana tersebut, diawali dengan adanya laporan dari korban. Berdasarkan wawancara dengan Ipda Hendri Joni, S.H. selaku Panit III Subdit V dari barang-barang bukti yang dikumpulkan melalui laporan, akan diidentifikasi melalui Bidang Laboratorium Forensik Digital. Identifikasi di Bidang Laboratorium Forensik Digital bertujuan mengidentifikasi barang bukti untuk membantu dalam penyelidikan. Jika hasil identifikasi Bidang Laboratorium Forensik Digital di Polda Riau kurang maksimal, maka barang bukti akan dikirimkan ke Pusat Laboratorium Forensik Digital di Markas Besar Kepolisian Republik Indonesia (Mabes Polri) untuk diperiksa. Jika ditemukan adanya indikasi kuat tindak pidana phishing, perkara dapat ditingkatkan ke penyidikan.

b) Penyidikan

Dalam tahapan penyidikan, penyidik pada Subdit V Ditreskrimsus Polda Riau melakukan serangkaian langkah awal penyidikan yakni memeriksa korban guna menelusuri dan memahami modus operandi pelaku phishing (*phisher*) dan mengumpulkan alat bukti dari perangkat korban dan/atau sumber digital lainnya untuk mengidentifikasi pelaku serta membuktikan tindak pidana yang memiliki keterkaitan dengan *phisher*. Setelah bukti dianalisis, penyidik memeriksa saksi, korban, dan ahli IT untuk memperkuat konstruksi pidana. Berdasarkan hasil tersebut, penyidik menetapkan tersangka, melakukan penangkapan, dan menyita barang bukti elektronik seperti komputer, ponsel, hard disk, atau perangkat jaringan yang digunakan dalam phishing.

Dalam proses penyidikan, penyidik dibantu perangkat seperti system pelacakan digital (*digital footprint tracing*), NetworkMiner untuk menganalisis lalu lintas jaringan, IP Tracker, dan Traceroute Analyzer untuk melacak lokasi pelaku. Jika diperlukan pemeriksaan yang mendalam, maka Polda Riau juga bekerja sama dengan Pusat Laboratorium Forensik Digital (Puslabfor) di Direktorat Tindak Pidana Siber Markas Besar Kepolisian Republik Indonesia ((Dittipidsiber Mabes Polri). Selain itu, Polda Riau juga meminta bantuan kepada pihak eksternal jika *phisher* dan/atau korban berada di luar yurisdiksinya, seperti Kepolisian Daerah lainnya dan Dittipidsiber Mabes Polri.

Polda Riau telah menangani sejumlah kasus tindak pidana terkait phishing dari tahun ke tahun, dengan rincian sebagai berikut.

No	Tahun	Jumlah Kasus	Jumlah Kasus yang P21
1	2021-2022	4	1
2	2023	7	3
3	2024	12	4
Total		23	8

Berdasarkan tabel di atas, terlihat bahwa total kasus tindak pidana terkait *phishing* mencapai 23 (dua puluh tiga) kasus. Dari jumlah tersebut, kasus yang berhasil mencapai tahap P21 berjumlah 8 (delapan) kasus. Menurut informasi yang diperoleh penulis, beberapa kasus tidak sampai ke tahap P21 dikarenakan barang bukti tidak lengkap ataupun pelaku tidak berhasil dilacak.

Berdasarkan hasil wawancara, modus *phishing* yang sering terjadi meliputi pembuatan *fake website*, pengiriman tautan melalui email, Facebook, WhatsApp, Instagram, serta penyebaran file APK yang disamarkan sebagai undangan pernikahan atau tawaran kerja. *Phisher* menggunakan rekayasa sosial untuk mendorong korban membuka tautan atau mengunduh APK, sehingga informasi sensitif, terutama terkait finansial, berhasil dicuri.

Kendala dalam Penyidikan Tindak Pidana dalam Undang-Undang Informasi dan Transaksi Elektronik terkait *Phishing* di Wilayah Hukum Kepolisian Daerah Riau

Berdasarkan hasil wawancara, didapatkan berbagai macam kendala pada penyidikan tindak pidana dalam Undang-Undang Informasi dan Transaksi Elektronik terkait *phishing* yang sebagai berikut.

1) Keterbatasan Sumber Daya Manusia

Polda Riau, khususnya Subdit V Ditreskrimsus, masih menghadapi kendala internal dalam penanganan kasus *phishing* terkait pemahaman teknologi dan modus *phishing* yang semakin berkembang. Saat ini, mereka masih bergantung pada bantuan Pusat Laboratorium Forensik Digital untuk analisis forensik digital yang mendalam, serta Dittipidsiber Mabes Polri untuk penanganan kasus tertentu. Ketergantungan ini menyebabkan proses penanganan menjadi lebih lama karena harus melalui tahapan tambahan dan koordinasi lintas wilayah.

2) Kurangnya Sarana Teknologi Pendukung

Penanganan tindak pidana phishing memerlukan pemahaman hukum, kemampuan investigasi, dan perangkat canggih untuk mendeteksi jejak digital, menganalisis data elektronik, serta mengamankan barang bukti forensik. Di Laboratorium Forensik Digital Polda Riau, perangkat seperti pelacak *Internet Protocol* (IP), analisis *metadata*, dan *log* jaringan masih kurang tersedia atau terpelihara. Kekurangan teknologi ini memengaruhi kualitas SDM, di mana penyidik Subdit V belum mampu mengikuti perkembangan teknik phishing seperti *spear phishing*, *spoofing*, dan *deepfake*. Akibatnya, pelacakan pelaku menjadi lambat dan risiko kehilangan barang bukti digital meningkat.

3) Kesulitan Menelusuri dan Mengidentifikasi *Phisher*

Kesulitan menelusuri dan mengidentifikasi pelaku *phishing* (*phisher*) menjadi tantangan utama dalam penyidikan UU ITE. *Phisher* menggunakan teknik seperti IP palsu, VPN, dan proxy untuk menyembunyikan jejak dan lokasi asli. Mereka juga memanfaatkan akun media sosial, email palsu, dan nomor rekening yang tidak terkait langsung dengan identitas asli, sehingga menyulitkan pengungkapan pelaku. Selain itu, *phisher* sering menggunakan layanan digital di luar yurisdiksi Indonesia, seperti *hosting* dan aplikasi pesan instan, sehingga aparat hukum harus melalui prosedur *Mutual Legal Assistance* (MLA), sehingga penyidikan memakan waktu yang lama.

Phisher biasanya bekerja dalam kelompok dengan pembagian tugas yang jelas, mulai dari perancang skema di satu daerah, pengelola *server* di tempat lain, hingga pencair dana di lokasi berbeda. Misalnya, perancang di Surabaya, nomor rekening di Padang, pencari korban di Pekanbaru, dan pencair dana di Pontianak. Struktur terorganisir ini membuat aparat sulit mengidentifikasi dan menangkap seluruh anggota sindikat sekaligus.

4) Kurangnya Pemahaman Masyarakat

Kurangnya pemahaman masyarakat tentang teknologi, *cyber space*, dan *cyber crime* menjadi kendala besar dalam penyidikan tindak pidana terkait *phishing*. Rendahnya literasi digital membuat masyarakat sulit mengenali *phishing* seperti tautan palsu, situs tiruan, atau permintaan informasi pribadi yang tidak sah. Akibatnya, banyak yang mudah memberikan informasi sensitif seperti kode OTP, kata sandi, dan data perbankan tanpa verifikasi. Banyak laporan masyarakat yang hampir atau menjadi korban *phishing* disebabkan oleh kurangnya pengetahuan dan kewaspadaan. Ketidaktahuan ini juga menghambat penyidikan karena pelaporan terlambat dan kronologi yang tidak tepat sering menyebabkan hilangnya jejak digital penting sebagai bukti.

Upaya yang Dilakukan oleh Kepolisian Daerah Riau untuk Mengatasi Kendala Penegakan Hukum Tindak Pidana Pencurian Informasi elektronik dengan Metode Phishing

Untuk mengatasi kendala-kendala tersebut, terdapat beberapa upaya yang dapat dilakukan oleh Polda Riau, antara lain sebagai berikut:

1) Meningkatkan Sumber Daya Manusia

Untuk meningkatkan kualitas SDM penyidik, Polda Riau mengikutsertakan mereka dalam pelatihan terkait *cyber crime*, terutama *phishing*. Pelatihan ini biasanya diselenggarakan oleh Biro SDM Polda Riau, kepolisian daerah lain, Mabes Polri, serta pihak lainnya seperti BSSN dan Kementerian Kominfo. Selain itu, peningkatan SDM juga dilakukan melalui evaluasi gelar perkara kasus terhadap kasus yang ditangani untuk mengidentifikasi kendala penyelidikan dan penyidikan.

2) Meningkatkan Sarana Teknologi Pendukung

Polda Riau telah meningkatkan sarana teknologi untuk mendukung penyidikan tindak pidana terkait *phishing*. Teknologi yang telah ditingkatkan seperti sistem pelacakan digital (*digital footprint tracing*) dan penambahan server penyimpanan data telah. Selain itu, Polda Riau juga memiliki Bidang Laboratorium Forensik Digital sendiri untuk membantu proses penyidikan *cyber crime*.

3) Kerja Sama dengan Instansi yang Berwenang (*Stakeholder*)

Polda Riau menghadapi berbagai kendala dalam menangani tindak pidana terkait *phishing*, sehingga diperlukan kerja sama dengan *stakeholder*, seperti pihak perbankan, kepolisian daerah lain, dan Mabes Polri.

Karena adanya ketentuan kerahasiaan data nasabah bank, kerja sama dilakukan melalui nota kesepakatan yang mengatur pengecualian dalam UU Perbankan berdasarkan Peraturan OJK Nomor 44 Tahun 2024, agar kepolisian dapat melakukan penyidikan dan menemukan *phisher*. Polda Riau juga bekerja sama dengan kepolisian daerah lain untuk melacak pelaku dan korban di luar wilayah hukumnya, serta mencegah penghilangan jejak. Selain itu, kerja sama dengan Pusat Laboratorium Forensik Digital dan Dittipidsiber Mabes Polri memungkinkan Polda Riau mendapatkan bantuan teknologi canggih dan operasi gabungan, terutama bila pelaku ataupun korban berada di luar wilayah hukum Indonesia. Melalui kolaborasi ini, diharapkan efektivitas penyidikan Polda Riau dapat meningkat.

4) Melaksanakan Edukasi kepada Masyarakat

Polda Riau rutin memberikan edukasi kepada masyarakat, terutama korban dari *phishing*. Selain itu, mereka aktif menggelar sosialisasi lewat seminar dan diskusi publik yang melibatkan pelajar, mahasiswa, dan pelaku usaha. Materi yang disampaikan biasanya bertemakan *cyber crime* yang di mana saat pembahasan juga akan membahas pengenalan modus *phishing* dan pentingnya literasi digital dalam menghadapi informasi di internet dan media sosial. Upaya ini bertujuan meningkatkan kesadaran masyarakat agar dapat mengenali dan menghindari tindak pidana terkait *phishing*, sehingga jumlah korban berkurang.

5) Kerja Sama dengan Platform Media Sosial

Polda Riau juga menjalin kerja sama dengan platform media sosial seperti WhatsApp, Facebook, dan Instagram. Kerja sama ini bertujuan agar pihak media sosial memberikan data dan identitas pengguna yang diduga terlibat dalam tindak pidana tersebut, sehingga proses identifikasi *phisher* bisa dipercepat. Dengan demikian, kerja sama ini memperlancar penyidikan tindak pidana terkait *phishing*.

PENUTUP

Kesimpulan

Berdasarkan hasil penelitian dan uraian pembahasan yang penulis sampaikan diatas, maka terdapat beberapa kesimpulan yang dapat diambil yaitu :

1. Penyidikan tindak pidana terkait *phishing* di wilayah hukum Polda Riau, khususnya Subdit V Ditreskrimsus dinyatakan belum optimal. Perihal ini dibuktikan dengan jumlah kasus yang diselesaikan masih rendah. Proses penyidikan meliputi pemeriksaan korban, pengumpulan alat bukti, dan kerja sama dengan Polda lain, perbankan, serta Dittipidsiber Mabes Polri, sebelum menetapkan tersangka dan melimpahkan kasus ke Kejaksaan.
2. Kendala penyidikan terbagi menjadi dua, yaitu kendala internal berupa keterbatasan SDM dan teknologi di kepolisian, serta kendala eksternal seperti sulitnya mengidentifikasi *phisher* dan rendahnya kewaspadaan masyarakat.
3. Untuk mengatasi kendala tersebut, Polda Riau meningkatkan kualitas SDM lewat diklat, memperbaiki sarana teknologi, menjalin kerja sama dengan perbankan, kepolisian lain, Mabes Polri, dan platform media sosial. Selain itu, upaya preventif dilakukan melalui edukasi dan sosialisasi kepada masyarakat.

Saran

Berdasarkan hasil penelitian dan uraian pembahasan yang penulis sampaikan diatas, maka terdapat beberapa saran yang dapat diperoleh yaitu :

1. Polda Riau, khususnya Subdit V Ditreskrimsus, perlu meningkatkan kompetensi penyidik agar mampu menghadapi perkembangan teknologi dan modus *phishing* yang semakin kompleks, sehingga penyidikan menjadi lebih efektif.
2. Peningkatan sarana teknologi secara berkala sangat penting untuk mendukung proses penyidikan dan mengurangi ketergantungan pada bantuan Pusat Laboratorium Forensik Digital Mabes Polri, agar penyelesaian kasus dapat lebih efektif.
3. Peningkatan literasi digital masyarakat juga harus diperhatikan dengan rutin mengadakan sosialisasi dan edukasi agar masyarakat lebih paham modus *phishing* dan cara pencegahannya, sehingga jumlah korban berkurang dan partisipasi masyarakat dalam penyidikan meningkat.

BIBLIOGRAPHY

- Cahyani, Tinuk Dwi, Hukum Acara Pidana Indonesia (Dalam Teori dan Praktek), Universitas Muhammadiyah Malang, Malang, 2023.
- Erdianto Effendi, Mukhlis Ridwan, dan Davit Ramadhan. "Legal Protection for Teenagers in the Use of Social Media at SMKN 1 Bangkinang Kampar". *Jurnal Pengabdian Hukum Indonesia*, Vol. 6, No. 1 (2023)
- Flora, Henny Saida, et. al, Hukum Pidana di Era Digital, Rey Media Grafika, Batam, 2022.
- Hanafi, Dasar Cyber Security dan Forensik, Deepublish, Yogyakarta, 2022.
- <https://pekanbaru.kini.com/belajar-dari-youtube-warga-pekanbaru-bobol-akun-coinbase-milik-wna-senilai-belasan-miliar>, diakses, tanggal, 22 Oktober 2024.
- Lastdrager, Elmer, From Fishing to Phishing, TRESPASS, Enschede, 2018.
- Lutfi Azis Febrika Ardy, et, al. "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial", Artikel pada *Journal of Internet and Software Engineering*, Vol. 1, No. 4, (2024)
- Miftakhur Rokhman Habibi dan Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia". *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, Vol. 23, No. 2 (Desember 2023)
- Ngani, Niko, Metode Penelitian dan Penulisan Hukum, Pustaka Yustisia, Yogyakarta, 2012.
- Nurul Fadila dan Tamaulina Br. Sembiring. "Analisis Yuridis Putusan Hakim dalam Perkara Tindakan Pidana Phishing yang dilakukan melalui Media Sosial (Studi Putusan Nomor: 155/Pid.Sus/2018/PNCbn). *Jurnal of International Multidisciplinary Research*, Vol. 2, No. 1 (Januari 2024)
- Peraturan Kepolisian Negara Republik Indonesia Nomor 3 Tahun 2024 Tentang Perubahan Atas Peraturan Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2018 Tentang Susunan Organisasi Dan Tata Kerja Kepolisian Daerah Berita Negara No. 182, 2024.
- Rohmat, Noor, Sistem Peradilan Pidana, K-Media, 2024.

- Rosyadi, Imron, Hukum Pidana, Revka Prima Media, Surabaya, 2022.
- Siagian, Sondang P, Kiat Meningkatkan Produktivitas Kerja, PT Rineka Cipta, Jakarta, 2002.
- Situmeang, Sahat Maruli T, Cyber Law, Cakra, Bandung, 2020.
- Soekanto, Soerjono, Efektivitas Hukum dan Penerapan Sanksi, CV Ramadja Karya, Bandung, 1988.
- Soekanto, Soerjono, Faktor-Faktor yang Mempengaruhi Penegakan Hukum, PT Raja Grafindo, Jakarta, 2007.
- Soekanto, Soerjono, Faktor-Faktor yang Mempengaruhi Penegakkan Hukum, Raja Grafindo, Jakarta, 1983.
- Soekanto, Soerjono, Pokok-Pokok Sosiologi Hukum, PT Raja Grafindo Persada, Jakarta, 1980.
- Sulastri, Lusia, Buku Ajar Hukum Acara Pidana, Jejak Pustaka, Yogyakarta, 2024.
- Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana Lembaran Negara Republik Indonesia No. 76, 1981 Penjelasan dalam Tambahan Lembaran Negara Republik Indonesia No. 3209.
- Utin Indah Permata Sari. “Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime yang Dilakukan oleh Virtual Police di Indonesia”, *Mimbar Jurnal Hukum*, Vol. 02, No. 01 (2021)
- Yazid Haikal Lokapala, Fuad Januar Nurfauzi, dan Yeni Widowaty. “Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia”. Artikel pada *Indonesian Journal of Criminal Law and Criminology*, Vol. 05, No. 01 (2024)