**Tindak Pidana Kejahatan Phising Dalam Dunia Cybercrime Ditinjau Menurut Aspek Yuridis Indonesia**

# Yazid Haikal Lokapala, Fuad Januar Nurfauzi, Yeni Widowaty

Program Studi Hukum, Fakultas Hukum, Universitas Muhammadiyah Yogyakarta

Email : yazid.haikal.law21@mail.umy.ac.id

|  |  |
| --- | --- |
| **Info Artikel****Riwayat:**Diajukan : …Ditelaah : …Direvisi : …Diterima : …**Kata Kunci :** *Efektivitas, UU ITE, cybercrime, Tantangan, Hambatan.**(Keywords : effectiveness, ite law, cybercrime, challenges, obstacles)***DOI:***10.18196/ijclc……..* | **Abstrak***Phising adalah salah satu bentuk kejahatan cybercrime yang dilakukan dengan cara menipu korban untuk memberikan informasi pribadi atau rahasia melalui email, situs web, atau media sosial yang palsu. Kejahatan phising dapat menimbulkan kerugian materiil maupun immateriil bagi korban, seperti pencurian identitas, penyalahgunaan kartu kredit, atau pencemaran nama baik. Oleh karena itu, perlu adanya upaya hukum untuk memberantas kejahatan phising dan melindungi hak-hak korban.**Tulisan ini bertujuan untuk mengkaji tindak pidana kejahatan phising dalam dunia cybercrime ditinjau menurut aspek yuridis Indonesia. Metode penelitian yang digunakan adalah metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Data yang digunakan adalah data sekunder berupa bahan hukum primer, sekunder, dan tersier. Teknik analisis data yang digunakan adalah teknik analisis kualitatif. Hasil penelitian menunjukkan bahwa tindak pidana kejaahatan phising dalam dunia cybercrime dapat dikategorikan sebagai tindak pidana kejahatan penipuann sebagaimana diatur dalam Pasal 378 KUHP atau tindak pidana kejahatan penggelapann sebagaimana diatur dalam Pasal 372 KUHP. Selain itu, tindak pidana kejahatan phising juga dapat dikenakan sanksi berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 28 ayat (1) dan Pasal 45 ayat (1) UU ITE. Namun, dalam praktiknya,* *Masih terdapat ketidakjelasan dalam penerapan hukum terhadap kasus phishing , seperti kesulitan dalam mengidentifikasi pelaku, kurangnya koordinasi antara penegak hukum, dan rendahnya kesadaran masyarakat untuk melaporkan kasus phising. Oleh karena itu, diperlukan upaya-upaya preventif dan represif untuk mengatasi masalah tersebut, seperti meningkatkan literasi digital masyarakat, melakukan sosialisasi dan edukasi tentang bahaya phising, serta memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum.****Abstract****Phishing is a form of cybercrime that is committed by tricking victims into providing personal or confidential information via email, websites or fake social media. Phishing crimes can cause material and immaterial losses for victims, such as identity theft, misuse of credit cards, or defamation. Therefore, it is necessary to have legal efforts to eradicate phishing crimes and protect the rights of victims. This paper aims to examine the criminal acts of phishing crimes in the world of cybercrime in terms of Indonesian juridical aspects. The research method used is a normative legal research method with a statutory approach and a case approach. The data used is secondary data in the form of primary, secondary and tertiary legal materials. The data analysis technique used is a qualitative analysis technique.**The results of the research show that the crime of phishing in the world of cybercrime can be categorized as a crime of fraud as regulated in Article 378 of the Criminal Code or an act of embezzlement as regulated in Article 372 of the Criminal Code. In addition, phishing crimes can also be subject to sanctions based on Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), specifically Article 28 paragraph (1) and Article 45 paragraph (1) of the ITE Law. However, in practice, there are still obstacles in law enforcement against phishing crimes, such as difficulties in identifying perpetrators, lack of coordination between law enforcement, and low public awareness to report phishing cases. Therefore, preventive and repressive efforts are needed to overcome this problem, such as increasing people's digital literacy, conducting socialization and education about the dangers of phishing, and strengthening cooperation between related parties in law enforcement.* |

1. **Pendahuluan**

Penggunaan teknologi informasi dan komunikasi di era globalisasi telah mengubah cara hidup orang dan menciptakan tatanan kehidupan baru, yang mendorong perubahan sosial, ekonomi, budaya, dan pertahana keamanan. Oleh karena itu, peran teknologi informasi dan komunikasi telah menjadi sangat strategis karena memungkinkan dunia tanpa batas, jarak, ruang, dan waktu.[[1]](#footnote-1)

Dalam era digital yang semakin berkembang pesat, teknologi informasi dan komunikasi telah membawa dampak yang signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam hal aktivitas ekonomi dan komunikasi. Namun, perkembangan teknologi ini juga memberikan peluang bagi tindakan kejahatan yang semakin canggih dan kompleks. Salah satu bentuk kejahatan yang muncul di dunia maya adalah tindak pidana kejahatan phishing, yang dalam bahasa Indonesia sering disebut sebagai "phising."

Phishing merupakan tindakan penipuan yang dilakukan secara daring dengan tujuan memperoleh informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dari korban. Pelaku phishing umumnya menyamar sebagai entitas yang sah, seperti perusahaan atau lembaga keuangan terkemuka, untuk memancing korban agar memberikan informasi pribadi mereka dengan dalih palsu. Dengan memanfaatkan teknik sosial, manipulasi, dan teknologi, para pelaku phising dapat merugikan individu dan organisasi dengan mencuri identitas, merampas dana, atau merusak reputasi.

Phising mewakili salah satu jenis layanan kesehatan elektronik dalam konteks keamanan kompute.Jenis penipuan ini bertujuan untuk meniru sebuah organisasi yang dapat dipercaya dan dapat diandalkan untuk mendapatkan informasi sensitif seperti username, password, dan detail kartu kredit.[[2]](#footnote-2)

Dalam konteks Indonesia, tindak pidana kejahatan phising menjadi perhatian serius karena mengancam keamanan data pribadi, kenyamanan bertransaksi daring, serta integritas ekonomi negara. Keberadaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah memberikan dasar hukum untuk mengatasi tindak pidana dalam dunia cybercrime, termasuk phising. Namun, perkembangan teknologi dan modus operandi pelaku kejahatan terus berubah, sehingga diperlukan pemahaman yang mendalam mengenai aspek yuridis yang terkait dengan penanganan tindak pidana kejahatan phising.

Dalam hal ini, penelitian yang mengkaji aspek yuridis tindak pidana kejahatan phising dalam konteks Indonesia menjadi sangat relevan. Melalui analisis aspek yuridis, termasuk ketentuan hukum yang ada, mekanisme penanganan kasus, serta kendala-kendala yang dihadapi oleh aparat penegak hukum, akan memungkinkan identifikasi celah hukum dan saran-saran perbaikan dalam penanganan tindak pidana kejahatan phising. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi bagi upaya penguatan sistem hukum dan penegakan hukum dalam menghadapi tantangan dunia cybercrime, khususnya tindak pidana kejahatan phising di Indonesia.

Peretasan dapat dilakukan dengan berbagai cara untuk mendapatkan data pribadi. Salah satunya adalah menyamar sebagai orang atau organisasi yang berwenang melalui email, juga disebut email phising. serupa dilaporkan oleh Badan Siber dan Sandi Negara (BSSN), total 164.131 kasus email phising yang terjadi di Indonesia pada tahun 2022. Kasus email phising yang paling banyak berasal dari email pribadi (59.210 kasus), dengan 52.744 kasus berasal dari email grup, dan 52.177 kasus berasal dari email lainnya. Adapun, 93.897 kasus email phising terjadi selama jam kerja, yaitu dari pukul 09.00 hingga 17.00; 70.234 kasus lainnya terjadi di luar jam kerja, yaitu dari pukul 17.00 hingga 09.00. Email phising yang terjadi pada tahun 2022 juga sering memasukkan file. Format file yang paling umum adalah dengan lebih dari 100.000 kasus.

Contoh kasus phising di dunia cybercrime, seperti kasus penipuan WhatsAapp yang kembali muncul. Ini adalah undangan palsu yang menghilangkan lebih dari satu miliar rupiah. Pengusaha aksesori kendaraan Silvia YAP adalah korbannya. Dia berasal dari Malang, Jawa Timur. Dia menerima undangan pernikahan palsu melalui aplikasi pesan yang dia gunakan. Ada enam aplikasi mobile banking di ponselnya, tetapi hanya beberapa yang kebobolan dengan total Rp 1,4 miliar. Selain itu, enam aplikasi perbankan mobile tersedia di handphonenya. Tapi hanya bank (BUMN) itu yang kebobol. Pada 25 Mei 2023, Silvia diberitahu bahwa ada perangkat lain yang mencoba mengakses emailnya. Untuk menghindari hal yang tidak diinginkan, dia langsung mengganti dan membeli HP baru. Dana ditransfer dari rekening kliennya pada hari yang sama, yang Silvia ketahui melalui emailnya. Aksi tersebut berlangsung selama tiga jam, dari pukul 21:00 hingga pukul 23:59 WIB. Dana ditransfer ke dua rekening klien kami. Oleh karena itu, dana tersebut ditransfer melalui aplikasi perbankan mobile. Meskipun klien kami tidak menggunakan aplikasi itu, dana mereka disimpan sebagai tabungan.

Berdasarkan informasi di atas, artikel ini membahas bagaimana hukum Indonesia efektif dalam kasus phishing di dunia kejahatan siber. dan juga apa saja hambatan dan tantangan apa saja dalam menangani tindak pidana phising dalam dunia cybercrime.

1. **Metode Penelitian**

Penelitian hukum normative juga dikenal sebagai penelitian hukum kepustakaan—dilakukan dengan melihat bahan pustaka atau data sekunder. Metode penelitian hukum normative digunakan dalam penelitian ini. Ini adalah jenis penelitian yang melihat bagaimana asas hukum, norma hukum, pendapat sarjana (teori), dan aturan lainnya yang berkaitan dengan masalah yang dibahas.

Penelitian ini menggunakan dua jenis penalaran deduktif: metode penalaran deduktif (pendekatan undang-undang) dan pendekatan penalaran konseptual (conseptual approach). Kajian hukum normatif disebut juga kajian dokumen atau kajian kepustakaan, karena kajiannya hanya terbatas pada undang-undang tertulis atau bahan hukum pelengkap lainnya.[[3]](#footnote-3) Tiga kategori bahan hukum yang digunakan dalam penelitian ini: primer, kedua, dan tersier. Hukum primer adalah jenis hukum yang mempunyai sifat otoritatif sehingga mempunyai pengamat. Bahan hukum terdiri dari catatan resmi dan undangan resmi.[[4]](#footnote-4)

Metode pemecahan masalah yang digunakan bersifat konseptual dan berbasis aturan. Peraturan yang berkaitan dengan kekayaan suatu bangsa serta ditambahkan oleh pejabat yang berwenang dengan menggunakan ketentuan-ketentuan yaitu termuat suatu norma yang mengikat setiap orang secara umum. Sebaliknya, kerangka konseptual diterima secara luas di masyarakat.

1. **Hasil dan Pembahasan**

**3.1 Efektivitas Sistem Hukum Indonesia Dalam Menangani Tindak Pidana Kejahatan Phishing Dalam Konteks Dunia Cybercrime**

Salah satu jenis penipuan elektronik yang dikenal sebagai phishing adalah meniru sebuah organisasi yang dapat dipercaya dan berkomunikasi secara elektronik untuk mendapatkan informasi pribadi. seperti nama pengguna, kata sandi, dan detail kartu kredit [[5]](#footnote-5) Regulasi Hukum dan Implementasi di Indonesia: Di Indonesia, tindak pidana kejahatan phishing diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal-pasal yang berkaitan dengan penipuan elektronik, pemalsuan identitas, dan pencurian data pribadi dapat diterapkan untuk kasus phishing. Selain itu, regulasi ini juga menegaskan sanksi hukum bagi pelaku tindak pidana ini.

Seiring dengan peningkatan penggunaan internet, kejahatan dunia maya meningkat. Banyak jenisnya. Teknologi informasi dan komunikasi tidak hanya memiliki banyak manfaat, tetapi mereka juga dapat digunakan untuk melakukan tindak kejahatan baru yang dikenal sebagai cybercrime, yang membutuhkan perlindungan. Ada kemungkinan bahwa teknologi informasi dan komunikasi berfungsi sebagai pedang bermata dua: selain membantu meningkatkan kesejahteraan, kemajuan, dan peradaban manusia, mereka juga dapat menjadi alat untuk melakukan kejahatan.[[6]](#footnote-6)

Penegakan hukum terhadap pelaku phishing di Indonesia melibatkan aparat kepolisian, Ditjen Pajak, dan lembaga terkait lainnya. Namun, tantangan dalam mengidentifikasi dan melacak pelaku di dunia maya seringkali menjadi kendala. Upaya peningkatan kemampuan aparat dalam teknologi digital dan forensik cyber sangat penting. Efektivitas Hukuman dan Sanksi: Efektivitas hukuman dan sanksi terhadap pelaku tindak pidana phishing masih menjadi perdebatan. Beberapa berpendapat bahwa hukuman yang lebih tegas diperlukan untuk memberikan efek jera, sementara yang lain menganggap bahwa pendekatan edukatif dan rehabilitatif juga penting agar pelaku dapat mengubah perilaku.

Efektivitas perjanjian ITE dipengaruhi oleh subteks dan struktur sistem hukum yang mencakup pelanggaran hukum, jumlah hari pelanggaran, dan keterlibatan masyarakat dalam pelanggaran hukum. Untuk menangkal pelanggaran hukum, sarana dan prasarana juga harus dijadikan tameng. Di zaman globalisasi saat ini, kita dapat dengan jujur ​​mengatakan bahwa kita bersyukur atas kemudahan dan manfaat yang diperoleh dari komputer, informasi, dan telekomunikasi—yang secara kolektif dikenal sebagai "revolusi informasi". Salah satu hasil utama dari konvergensi ini adalah aktivitas di dunia Siberia yang berdampak pada seluruh aspek kehidupan manusia.. Meskipun terdapat berbagai kegiatan yang ditujukan pada berbagai subjek, namun hal tersebut tidak efektif dalam menyelesaikan permasalahan hukum siber.

Awalnya UU ITE diundangkan menjadi UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kemudian diubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Revisi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang masih berlaku hingga saat ini. Yang dimaksud dengan “Lex Specialis Derogat Legi Generali” adalah peraturan perundang-undangan khusus yang berlaku meskipun bertentangan dengan peraturan perundang-undangan yang umum. Oleh karena itu, Undang-Undang Pencegahan Kejahatan Dunia Maya No. 19 Tahun 2016 Tentang Perubahan Atas Kejahatan Dunia Maya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan undang-undang khusus yang menyasar kejahatan dunia maya dalam bentuk spear phishing.

Tindak pidana kejahatan phishing dalam dunia cybercrime merupakan salah satu permasalahan hukum yang cukup kompleks dan multidimensi. Phishing adalah suatu bentuk penipuan yang dilakukan dengan cara mengirimkan email, situs web, atau media sosial yang palsu yang mengatasnamakan lembaga resmi atau terpercaya, dengan tujuan untuk memperoleh informasi pribadi atau rahasia dari korban, seperti nomor rekening, password, PIN, atau kode verifikasi. Kejahatan phishing dapat menimbulkan kerugian materiil maupun immateriil bagi korban, seperti pencurian identitas, penyalahgunaan kartu kredit, atau pencemaran nama baik.

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 28 ayat (1) dan Pasal 45 ayat (1), tindak pidana kejahatan phishing juga dapat dikenakan sanksi berdasarkan Undang-Undang tersebut. Dalam konteks Indonesia, tindak pidana phishing dapat dikategorikan sebagai tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP atau tindak pidana penggelapan sebagaimana diatur dalam Pasal 372 KUHP.

Indonesia telah memiliki beberapa peraturan perundang-undangan nasional yang mengatur masalah cybercrime secara umum maupun khusus. Peraturan perundang-undangan tersebut antara lain:

* Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan payung hukum utama dalam bidang cyberlaw di Indonesia. UU ITE mengatur berbagai aspek hukum terkait dengan informasi dan transaksi elektronik, termasuk tindak pidana siber. Beberapa pasal yang berkaitan dengan phishing adalah:
	+ Pasal 28 ayat (1) berkaitan dengan penyebaran informasi dan dokumen elektronik yang mengandung informasi palsu yang dapat merugikan pelanggan saat melakukan transaksi elektronik.[[7]](#footnote-7)
	+ Pasal 30 ayat (1) tentang akses ilegal terhadap sistem elektronik milik orang lain atau masyarakat umum tanpa izin atau hak.
	+ Pasal 31 ayat (1) Untuk mengubah, menambah, mengurangi, mengirim, merusak, menghilangkan, memindahkan, atau menyembunyikan dokumen elektronik dan informasi elektronik milik orang lain atau masyarakat umum tanpa hak.
	+ Pasal 32 ayat (1) tentang pemalsuan dokumen dan/atau informasi elektronik dengan kehati-hatian yang memadai agar dapat dianggap sebagai dokumen dan/atau informasi elektronik asli.
	+ Pasal 35 ayat (1) tentang penggunaan informasi elektronik dan/atau dokumen elektronik palsu sebagai alat bukti dalam transaksi elektronik.
	+ Pasal 36 ayat (1) tentang manipulasi terhadap sistem elektronik milik orang lain atau masyarakat umum dengan maksud untuk mendapatkan keuntungan bagi diri sendiri atau orang lain secara tidak sah.[[8]](#footnote-8)
* Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan), yang merupakan revisi dari UU ITE sebelumnya. UU ITE Perubahan menambahkan beberapa pasal baru yang berkaitan dengan phishing, yaitu:
	+ Pasal 28A tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung ancaman kekerasan atau menakut-nakuti yang dapat menimbulkan rasa takut atau keresahan pada masyarakat umum.[[9]](#footnote-9)
	+ Pasal 28B tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung penghinaan dan/atau pencemaran nama baik.
	+ Pasal 28C tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung fitnah atau pemerasan.
	+ Pasal 28D tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung hasutan untuk melakukan tindak pidana.
	+ Pasal 28E tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung kebencian atau permusuhan terhadap suku, agama, ras, dan antargolongan (SARA).
	+ Pasal 28F tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung pornografi atau perbuatan asusila.
	+ Pasal 28G tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung perjudian.[[10]](#footnote-10)

Namun, masih terdapat beberapa tantangan atau hambatan dalam aspek struktural ini, seperti: - Belum adanya koordinasi atau sinergi yang optimal antara lembaga-lembaga penegak hukum tersebut dalam menangani tindak pidana phishing. Hal ini dapat menyebabkan tumpang tindih atau konflik kewenangan antara lembaga-lembaga tersebut. - Belum adanya standar atau pedoman operasional yang seragam dan terintegrasi dalam menangani tindak pidana phishing. Hal ini dapat menyebabkan inkonsistensi atau ketidakefisienan dalam proses penegakan hukumnya. - Belum adanya sumber daya manusia (SDM) yang memadai dan kompeten dalam bidang cybercrime, khususnya phishing. Hal ini dapat menyebabkan kesulitan atau keterbatasan dalam melakukan penyelidikan, penyidikan, penuntutan, atau pemeriksaan terhadap tindak pidana phishing. - Belum adanya fasilitas atau peralatan yang memadai dan canggih dalam bidang cybercrime, khususnya phishing. Hal ini dapat menyebabkan kesulitan atau keterbatasan dalam melakukan pengumpulan, pengolahan, penyimpanan, atau penganalisisan bukti-bukti elektronik terkait dengan tindak pidana phishing.

* Aspek kultural, yaitu sejauh mana kesadaran dan partisipasi masyarakat dalam mencegah dan menangani tindak pidana phishing. Dari paparan di atas, dapat diketahui bahwa Indonesia telah memiliki beberapa inisiatif atau program yang bertujuan untuk meningkatkan literasi dan edukasi siber bagi masyarakat, seperti:
	+ Gerakan Nasional Siber Bersih (Gernas Cinta Siber), yang merupakan gerakan bersama antara pemerintah, swasta, akademisi, dan masyarakat sipil untuk menciptakan lingkungan siber yang bersih, sehat, dan aman di Indonesia.
	+ Indonesia Cyber Security Forum (ICSF), yang merupakan forum yang menghimpun berbagai pemangku kepentingan di bidang keamanan siber untuk berbagi informasi, pengetahuan, dan pengalaman dalam menghadapi tantangan siber di Indonesia.
	+ Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), yang merupakan tim tanggap insiden keamanan siber yang berfokus pada infrastruktur internet di Indonesia, termasuk memberikan layanan pemberitahuan, peringatan, dan rekomendasi terkait dengan ancaman siber.
	+ Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), yang merupakan asosiasi yang mewadahi para penyelenggara jasa internet di Indonesia, termasuk memberikan edukasi dan sosialisasi mengenai etika dan tata cara berinternet yang baik dan benar.

Namun, dalam praktiknya, masih terdapat kendala-kendala dalam penegakan hukum terhadap kejahatan phishing di Indonesia, seperti kesulitan dalam mengidentifikasi pelaku, kurangnya koordinasi antara penegak hukum, dan rendahnya kesadaran masyarakat untuk melaporkan kasus phishing. Oleh karena itu, diperlukan upaya-upaya preventif dan represif untuk mengatasi masalah tersebut, seperti meningkatkan literasi digital masyarakat, melakukan sosialisasi dan edukasi tentang bahaya phishing, serta memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum. Selain itu, juga diperlukan perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan phishing, agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.

Tindak pidana kejahatan phishing dalam dunia cybercrime merupakan salah satu permasalahan hukum yang cukup kompleks dan multidimensi. Phishing adalah suatu bentuk penipuan yang dilakukan dengan cara mengirimkan email, situs web, atau media sosial yang palsu yang mengatasnamakan lembaga resmi atau terpercaya, dengan tujuan untuk memperoleh informasi pribadi atau rahasia dari korban, seperti nomor rekening, password, PIN, atau kode verifikasi. Kejahatan phishing dapat menimbulkan kerugian materiil maupun immateriil bagi korban, seperti pencurian identitas, penyalahgunaan kartu kredit, atau pencemaran nama baik.

Dari analisis di atas, dapat disimpulkan bahwa sistem hukum Indonesia dalam menangani tindak pidana kejahatan phishing dalam konteks dunia cybercrime masih memiliki beberapa kelemahan, kekurangan, tantangan, dan hambatan yang perlu diperbaiki dan ditingkatkan. Oleh karena itu, diperlukan upaya-upaya konkret dari berbagai pihak untuk meningkatkan efektivitas sistem hukum tersebut, seperti:

* Melakukan revisi atau penyempurnaan terhadap peraturan perundang-undangan yang ada agar dapat mengatur secara lebih jelas dan tegas mengenai definisi, unsur-unsur, dan sanksi pidana terkait dengan phishing.
* Meningkatkan koordinasi atau sinergi antara lembaga-lembaga penegak hukum yang berwenang dalam menangani tindak pidana phishing agar dapat bekerja secara lebih optimal dan terintegrasi.
* Meningkatkan kapasitas dan kompetensi SDM serta fasilitas dan peralatan penegak hukum dalam bidang cybercrime, khususnya phishing agar dapat melakukan penegakan hukum secara lebih profesional dan cermat.
* Meningkatkan literasi dan edukasi siber bagi masyarakat.

**3.2 Tantangan dan Hambatan yang dihadapi oleh sistem hukum Indonesia dalam menangani tindak pidana kejahatan phishing dalam dunia cybercrime**

Sistem hukum Indonesia, seperti banyak negara lainnya, menghadapi berbagai tantangan dan hambatan dalam memberantas kejahatan phishing di dunia kejahatan siber. Phishing adalah praktik penipuan di mana penyerang mencoba mendapatkan informasi pribadi, seperti kata sandi dan informasi keuangan, dengan menyamar sebagai individu tepercaya melalui pesan elektronik atau situs web palsu. Berikut adalah beberapa tantangan utama yang dihadapi sistem hukum Indonesia dalam hal ini:[[11]](#footnote-11)

1.Kurangnya kesadaran masyarakat:

Banyak individu dan organisasi mungkin tidak memiliki pengetahuan yang memadai tentang ancaman phishing dan cara melindungi diri dari serangan tersebut. Kurangnya kesadaran ini dapat membuat orang lebih rentan terhadap serangan phishing.

2. Batasan Sumber Daya:

Berurusan dengan kejahatan dunia maya seperti phishing memerlukan sumber daya yang memadai, termasuk profesional keamanan siber yang terlatih dan peralatan teknis yang canggih. Sumber daya yang terbatas ini dapat menjadi hambatan dalam mengidentifikasi dan menuntut penjahat phishing.

 3.Batasan Yurisdiksi:

Dalam kasus phishing, serangan seringkali dilancarkan dari luar Indonesia. Hal ini dapat mempersulit upaya penegakan hukum karena keterbatasan yurisdiksi yang berlaku. Investigasi dan penuntutan penjahat di luar negeri bisa jadi rumit dan memakan waktu.

4. Kompleksitas Teknis:

Kejahatan phishing seringkali menggunakan teknik kamuflase yang canggih, seperti membuat website palsu yang sulit dibedakan dengan website asli. Hal ini memerlukan pemahaman mendalam tentang teknologi dan keamanan siber untuk mendeteksi dan mempertahankan diri dari serangan semacam itu.

5. Ketidakpastian hukum:

Dalam beberapa kasus, mungkin terdapat ketidakpastian hukum mengenai penerapan undang-undang yang ada terhadap aktivitas tertentu di dunia maya. Hal ini dapat memperlambat hukum dan mempersulit upaya pencegahan dan penegakan hukum.

6. Kerjasama internasional:

Karena sifat kejahatan dunia maya yang bersifat lintas batas, kerja sama internasional menjadi penting. Namun, bekerja sama dengan negara lain untuk menyelidiki dan menuntut kasus phishing bisa jadi rumit karena perbedaan sistem hukum, bahasa, dan proses hukum. Kurangnya undang-undang khusus: Meskipun Indonesia memiliki Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang mencakup beberapa aspek kejahatan dunia maya, undang-undang ini mungkin tidak lengkap atau cukup spesifik untuk menangani kasus phishing.

 7.Pengumpulan Bukti Digital:

Dalam investigasi phishing, penting untuk mengumpulkan bukti digital yang kuat untuk membantu penegakan hukum. Namun, teknologi yang digunakan untuk mengumpulkan dan menyimpan bukti digital dapat menjadi tantangan tersendiri.

 Untuk menghadapi tantangan-tantangan ini, Indonesia harus melanjutkan upaya untuk meningkatkan kesadaran masyarakat mengenai keamanan siber, membekali lembaga penegak hukum dengan keterampilan dan alat yang diperlukan, memperkuat kerja sama internasional dalam memerangi kejahatan siber lintas batas negara, dan mempertimbangkan untuk memperbaiki undang-undang yang ada agar dapat memberantasnya secara lebih efektif. . dengan kejahatan phishing dan kejahatan dunia maya pada umumnya.[[12]](#footnote-12)

Beberapa akibat hukum yang disebutkan dalam tindak pidana penipuan penggunaan tanda tangan elektronik dalam hal ini adalah berkaitan dengan beberapa faktor yang ada pada aparat penegak hukum itu sendiri serta kesadaran masyarakat terhadap penerapan tanda tangan elektronik tertentu agar dapat lebih memahaminya. permasalahan seputar penggunaannya. Kurangnya pemahaman masyarakat terhadap sistem hukum terhadap gugatan-gugatan kecil yang mereka yakini belum sepenuhnya mewakili keadaan, sehingga masyarakat menilai hal tersebut merupakan langkah yang tidak perlu dilakukan jika kerugian masyarakat tidak terlalu besar. Selain itu, kendala lainnya adalah belum meratanya sarana dan prasarana yang dimiliki aparat penegak hukum dalam menangani perkara yang melibatkan sarana elektronik. Sebab, modus operasional aparat penegak hukum saat menggunakan sarana elektronik semakin tidak menentu dan menyatu dengan modus operasional baru. Hal ini menjadi kendala bagi aparat penegak hukum untuk terus melakukan pengumpulan sarana dan prasarana dalam rangka memberikan penegakan hukum yang terjadi di tengah masyarakat.[[13]](#footnote-13)

Dalam memerangi kejahatan phishing, beberapa negara seperti Indonesia biasanya menghadapi beberapa kendala:

1.Teknis yang rumit:

Kejahatan phishing sering kali melibatkan teknik kamuflase yang rumit dan manipulasi teknis. Penipu menggunakan berbagai cara untuk menyamarkan berita atau situs palsu, sehingga menyulitkan korban atau bahkan peneliti untuk mengetahui bahwa mereka sedang ditipu. Hal ini dapat mempersulit upaya deteksi dan pencegahan.

2. Keterbatasan Bukti Digital:

Untuk mengadili penjahat phishing, penyidik ​​memerlukan bukti digital yang kuat. Namun, bukti-bukti ini seringkali tidak stabil dan dapat dihapus atau dimodifikasi oleh penulisnya. Mengumpulkan dan melestarikan bukti digital dengan baik merupakan sebuah tantangan tersendiri.

3. Kurangnya pelaporan:

Banyak korban phishing yang merasa malu atau tidak tahu ke mana harus melaporkan penipuan tersebut. Akibatnya, banyak insiden phishing yang tidak dilaporkan ke penegak hukum. Kurangnya pelaporan dapat membuat kasus menjadi sulit.

4.Yurisdiksi lintas batas:

Pelaku serangan phishing seringkali beroperasi dari negara lain sehingga menimbulkan masalah hukum. Para peneliti mungkin mengalami kesulitan dalam menjangkau pemangku kepentingan di luar yurisdiksi negara mereka dan mungkin diperlukan kerja sama internasional.

5.Tingkat Keberhasilan Rendah:

Kasus phishing sulit dimenangkan di pengadilan karena bukti elektronik dan digital cenderung rumit dan pelaku dapat menggunakan teknik yang sulit dijelaskan kepada juri yang mungkin tidak memiliki pemahaman teknis yang kuat.

6. Ketidakcocokan hukum:

Beberapa undang-undang yang ada mungkin tidak sepenuhnya memadai untuk menangani kejahatan di dunia digital. Undang-undang yang ada sebelum teknologi Internet ada mungkin tidak efektif melawan phishing.

7.Kebijakan pribadi:

Dalam beberapa kasus, penyelidik harus mengumpulkan informasi tentang pelaku yang mungkin merupakan pelanggaran privasi. Hal ini dapat menimbulkan masalah etika dan hukum, terutama jika informasi tersebut dikumpulkan tanpa izin yang semestinya.

8. Kesadaran dan pendidikan yang rendah:

Pengguna atau lembaga penegak hukum mungkin tidak memiliki pengetahuan yang memadai tentang teknik dan taktik yang digunakan dalam serangan phishing. Hal ini dapat melemahkan upaya pencegahan dan pengobatan.

9. Perubahan Taktik Serangan Cepat:

Pelaku serangan phishing terus-menerus mengubah taktik mereka seiring kemajuan teknologi dan orang-orang menggunakan internet. Oleh karena itu, sulit bagi lembaga penegak hukum untuk selangkah lebih maju. Batasan Sumber Daya: Penanganan kasus phishing memerlukan sumber daya yang memadai, termasuk peralatan teknis dan personel terlatih. Keterbatasan sumber daya dapat menghambat penyelidikan dan penuntutan. Untuk mengatasi hambatan-hambatan ini, penting bagi negara-negara untuk terus membangun kapasitas penegakan hukum, meningkatkan kesadaran masyarakat dan mungkin merumuskan undang-undang atau kebijakan yang lebih spesifik untuk memerangi kejahatan phishing dan ancaman dunia maya lainnya.[[14]](#footnote-14)

Hambatan dalam Pemberantasan Kejahatan Dunia Maya Kadang-kadang, ada beberapa bagian yang dapat menghambat orang yang melakukan pembelaan terhadap kejahatan dunia maya. Namun demikian, masih terdapat beberapa permasalahan dalam cara penanganannya di lapangan, beberapa di antaranya adalah sebagai berikut:

1. Belum terpenuhinya ketentuan hukum mengenai tata cara yang ada dalam KUHP, maka penyidik ​​(khususnya Polri) melakukan dialog dan kolaborasi, serta memberikan bukti bahwa kudu dibuat oleh undang-undang khusus yang dimaksudkan untuk memberantas kejahatan dunia maya.

Kemampuan penyidikSecara umum, pengetahuan dan pemahaman tentang prosedur operasi komputer yang digunakan oleh Penyidik ​​Polri mengenai peretas komputer, serta kemampuannya dalam menyelidiki kasus-kasus tersebut, cukup rendah.

Beberapa faktor (penentu) yang sangat berpengaruh adalah sebagai berikut:

1. Pemahaman umum tentang komputerPengetahuan teknologi dan pengalaman penyidik ​​dalam menangani berbagai kasus kejahatan dunia maya masih terbatas.

2. Aspek sistem pembuktian yang mengurungkan niat penyidik, antara lain:

Alat buktiàPermasalahan yang timbul dalam proses penegakan hukum terhadap kejahatan dunia maya antara lain, namun tidak terbatas pada, hal-hal berikut: sasaran atau media kejahatan dunia maya adalah informasi atau sistem komputer (internet) yang dapat dengan mudah diidentifikasi, dilacak, atau ditahan oleh mereka yang melakukan kejahatan dunia maya. Kejahatan dunia maya umumnya ditangani dengan sedikit skeptisisme. Sebaliknya, tindak pidana sering terjadi di luar batas negara sehingga perlu dilakukan penyidik ​​untuk melakukan penyidikan dan pendataan.

B. Fasilitas forensik komputerUntuk mengidentifikasi taktik hacker dan cracker ketika melakukan serangan, penting untuk dicatat bahwa program komputer dan informasi yang dimiliki polisi agak ketinggalan jaman karena kurangnya komputer forensik. Pemindai ini diperlukan untuk menangkap informasi dan gambar digital, serta mengekstrak data dalam bentuk soft copy (program, grafik, dan materi lainnya). Dalam kasus ini, Polri masih belum memiliki strategi komputasi forensik yang meyakinkan. Alat bukti forensik yang tidak dibangun dengan baik oleh kepolisian diharapkan mampu memberikan tiga layanan krusial, antara lain: pengumpulan bukti melalui barangay (pengumpulan bukti), analisis forensik, dan saksi ahli. [[15]](#footnote-15)

Dalam rencana pelayanan kesehatan ini Perlunya analisis bias tertuang dalam Ayat 184 Ayat (1) KUHAP yang menjelaskan instrumen biologi baru dan progresif yang peka terhadap perubahan dunia. Namun bila diterapkan sebagai instrumen biologi, data elektronik atau instrumen biologi mempunyai permasalahan tertentu, seperti:

 1. Pertanyaan mengenai lokasi TKP Penyelidik mungkin kesulitan mengidentifikasi lokasi pasti kejahatan atau lokalisasi maya dunia. Oleh karena itu, penyerang memiliki kemampuan untuk melemahkan atau bahkan menghancurkan perangkat "sidik jari digital" yang mereka perlukan untuk menjalankan tugas sehari-hari atau membandingkan satu lokasi dengan lokasi lainnya.

2. Deliciti tempus (waktu timbulnya masalah kesehatan), penyidik, dan perkara Tidak mungkin dapat menentukan waktu pasti timbulnya penyakit karena dunia Maya secara teratur mempunyai kemampuan untuk mengukur berlalunya waktu dan lamanya tindakan.

 3. Masalah pembuktian juga khusus berkaitan dengan Petugas Hukum. Berikut ini bukti relevan untuk setiap aspek dan digunakan untuk persiapan, pelaksanaan, dan hasil kesehatan. Alasannya adalah jaringan sulit dilacak merupakan sumber kecanggihan sistem internet, dan juga memiliki manfaat bagi mereka yaitu memberikan mereka kemampuan untuk mengubah atau mengubah identitas mereka di dunia. Sebaliknya, dalam teknologi informasi adalah teknologi yang belum berkembang yang tidak dapat digunakan secara langsung atau diungkapkan dengan cara yang tidak sah. Namun, individu yang kompeten di bidangnya dapat mengelola data, memodifikasi data, dan khususnya mengubah data mentah menjadi data numerik . [[16]](#footnote-16)

1. **Simpulan**

Kejahatan tindak pidana phising di era globalisasi sekarang ini sudah tidak asing lagi dikalangan masyarakat. Tindak pidana kejahatan ini sebenarnya sudah di atur ketentuan hukum yang mencakup kejahatan phising tersebut. Tetapi dalam pelaksanaanya masih terdapat kendala dan kendala hukum dalam penanganan kejahatan tersebut. Masih banyak permasalahan/peraturan terkait perbuatan yang belumKarena adanya ketidakpastian mengenai syarat-syarat perjanjian, maka ITE sudah diratifikasi sehingga tidak ada pihak yang dapat menggugat isi perjanjian tersebut, sehingga menimbulkan perselisihan hukum. Undang-undang informasi elektronik tidak efektif dalam melindungi kepentingan masyarakat seluruh warga negara Indonesia. Tidak hanya demi kepastian hukum tetapi juga keadilan dan kemanfaatan hukum. Selain itu, tanpa adanya kerja sama antara aparat penegak hukum dan masyarakat setempat, ITE tidak akan dapat diterapkan dan ditegakkan secara efektif. Oleh karena itu, salah satu faktor yang dapat mempengaruhi efektifitas suatu undang-undang adalah struktur, falsafah, dan fungsinya yang mendasarinya sebagai lembaga penegak hukum yang profesional dan ideal, baik dalam rangka melaksanakan tugas yang diberikan maupun dalam rangka penegakan undang-undang itu sendiri..

Tindak pidana phishing pada dasarnya sama dengan penipuan konvesional . Hanya itu Perbedaannya terletak pada buktinya atau sarana tindakan menggunakan sistem elektronik (komputer, Internet, peralatantelekomunikasi). Oleh karena itu aplikasinya Hukum terkait penipuan masih tunduk pada KUHP berdasarkan pasal 378, dan perkuat landasannyaperaturan perundang-undangan, hal ini juga dapat diperhitungkan melalui ketentuan Tindak pidana phising merupakan kejahatan penipuan. Pengaturan mengenai tindak pidana cybercrime phising diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Itu adalah undang-undang khusus (Lex Spesialis Derogat Lex Generale. Dalam pembahasan perkembangan hukum pidana ke depan, maka pencegahan dan pemberantasan kejahatan.

Reformasi dan sistem pengembangan pidana pidana secara menyeluruh mencakup pengembangan struktur, budaya, dan ancaman hukum pidana. sama siber diimbangi. Situasi seperti ini memerlukan sistem peradilan pidana untuk mengenali lokasi penting dalam evolusi hukum pidana kontemporer. Mengingat perlunya pertimbangan lebih lanjut terhadap sistem keadilan restoratif, hal ini berpotensi menjadi solusi yang berguna untuk menghubungkan korban, pelaku, kelompoknya, dan pihak-pihak terkait lainnya yang terlibat dalam proses kerja sama untuk mengatasi masalah kesehatan tersebut. masalah

**Daftar Pustaka.**

**Undang-Undang:**

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan).

**Buku:**

Abdul Wahid & Mohammad Labib. 2010 Kejahatan Mayantara (Cyber Crime).Bandung: PTRefika Aditama, hlm. 134-135.

Arifah, “Kasus Cybercrime di Indonesia,” 193

Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung

Fiorida Mathilda, 2012 “Cyber Crime dalam Sistem Hukum Indonesia,” Sigma-Mu4.

Maskun, 2013, Kejahatan Siber(Cyber Crime), kencana, Jakarta

Siswanto Sunarso, 2009, Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta

Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung

Thantawi, “Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia,”38.

**Jurnal:**

Dian Rachmawati, ”Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,” Jurnal Saintkom, Vol. 13, No. 3, 2014.

Tampubolon, M. H. P., Pawennei, M., & Zainuddin, Z. 2021. Hambatan Penyidikan Tindak Pidana cyber crime . Journal ofLex Generalis (JLG), 2(4), 1585-1600.

1. Siswanto Sunarso, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, PT. Rineka Cipta, Jakarta, 2009, hlm. 39. [↑](#footnote-ref-1)
2. Dian Rachmawati, ”Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,” Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211. [↑](#footnote-ref-2)
3. Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung, hlm 84 [↑](#footnote-ref-3)
4. Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung hlm 65 [↑](#footnote-ref-4)
5. Dian Rachmawati, ”Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber,” Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211. [↑](#footnote-ref-5)
6. Siswanto Sunarso, 2009, Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta, hlm. 39 [↑](#footnote-ref-6)
7. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). [↑](#footnote-ref-7)
8. Ibid [↑](#footnote-ref-8)
9. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan). [↑](#footnote-ref-9)
10. Ibid [↑](#footnote-ref-10)
11. Fiorida Mathilda, “Cyber Crime dalam Sistem Hukum Indonesia,” Sigma-Mu4, no. 2 (September 2012): 36 [↑](#footnote-ref-11)
12. Maskun, 2013, Kejahatan Siber(Cyber Crime), Jakarta: Kencana [↑](#footnote-ref-12)
13. Tampubolon, M. H. P., Pawennei, M., & Zainuddin, Z. (2021). Hambatan Penyidikan Tindak Pidana cyber crime . Journal ofLex Generalis (JLG), 2(4), 1585-1600 [↑](#footnote-ref-13)
14. Thantawi, “Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia,” 38. [↑](#footnote-ref-14)
15. Arifah, “Kasus Cybercrime di Indonesia,” 193 [↑](#footnote-ref-15)
16. Abdul Wahid & Mohammad Labib. 2010 Kejahatan Mayantara (Cyber Crime).Bandung: PTRefika Aditama, hlm. 134-135 [↑](#footnote-ref-16)