PENERAPAN SANKSI ATAS KASUS TINDAK PIDANA *PHISING* ATAU *SCAM* DALAM *CYBERSPACE* (STUDI KASUS PUTUSAN PN MEDAN NOMOR 3006/PID.SUS/2017/PN MDN)[1]

Oleh :
Nathaniel Gabriel Djohan [2]
Imelda Gracia Onibala [3]
Vonny Anneke Wongkar [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui apa peraturan yang diterapkan oleh pemerintah dalam menekan kasus *Phising* atau *scam* di Indonesia dan untuk mengetahui apakah jerat hukum yang diterapkan kepada pelaku *Phising* atau *scam* dalam *cyberspace* telah efektif. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Pasal 35 UU ITE menjadi pasal yang paling relevan dalam kasus *phising*. Undang-undang khusus lainnya yang memiliki alasan relevansi dan kontribusi yang berbeda-beda dalam kasus tindak pidana *phising*, yaitu UU Perlindungan Data Pribadi yang berperan melindungi data dan korban, UU Tindak Pidana Pencucian Uang yang berperan mengatur kejahatan lanjutan, dan UU Perbankan yang berperan dalam konteks finansial. 2. Tindak kejahatan *phising* dalam kasus tersebut terbukti digunakan sebagai sarana untuk memperoleh akses akun media sosial orang lain secara tidak sah. Meskipun unsur *phising* terbukti secara faktual, tindakannya tidak dikategorikan sebagai delik khusus yang berdiri sendiri. Jaksa penuntut umum dan majelis hakim menempatkan *phising* sebagai modus operandi atau alat untuk melaksanakan tindak pidana utama, yaitu penyebaran informasi elektronik yang mengandung penghinaan dan/atau pencemaran nama baik.

Kata Kunci : *phising, scam, ciberspace*

PENDAHULUAN

A. Latar Belakang Masalah

Internet merupakan suatu hal yang selalu di akses oleh orang-orang dan sering digunakan dalam kehidupan sehari-hari, salah satunya adalah penggunaan Informasi dan Transaksi Elektronik. Informasi dan Transaksi Elektronik mencakupi hal-hal berupa media sosial, internet banking, dompet digital, dan lain-lain yang mengandung informasi pribadi tentang pengguna dan kegiatan transaksi melalui internet. Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu, yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan, keamanan, dan penegakan hukum.[5]

Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan tindak kejahatan-kejahatan baru (*cyber crime*) sehingga diperlukan upaya proteksi. Dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.[6]

Penggunaan internet yang hampir tak terkendali mengakibatkan berbagai tindak kejahatan baru seperti: *Phising, hacking, skimming*, peretasan situs atau surat elektronik (*e-mail*), *carding*, dan serangan *ransomware* yang dimana kejahatan tersebut hanya bisa terjadi di dunia maya. Pada awalnya kejahatan dunia maya atau *cybercrime* diartikan sebagai *computer crime* atau kejahatan komputer. *The british Law Commission* dalam memaknakan suatu kata majemuk dari "*computer crime*" sebagai tipu daya dalam komputer yang menggunakan berbagai cara apa pun untuk diniatkan dalam memperoleh kekayaan atau keuntungan lainnya atau dimaknai dalam memunculkan kemalangan terhadap orang lain.

Salah satu yang sering terjadi antara lain adalah *Cyber Crime Phising*, masyarakat sering tidak menyadari kejahatan *Cyber Crime Phising* sangat merugikan bagi korban yang pernah mengalami kejahatan ini. *Phising* adalah praktik penipuan online di mana penyerang menciptakan situs web palsu yang meniru situs web asli dengan tujuan untuk mencuri informasi sensitif seperti

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010392
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari*, PT. Rineka Cipta, Jakarta, 2009.
[6] Swangga Prabhaswara, *Jurnal Bevinding* Vol 01 No 03 Tahun 2023.

kata sandi, informasi keuangan, atau, data pribadi pengguna. Teknik ini seringkali digunakan dalam upaya untuk merampas identitas, mengakses akun online, atau melakukan penipuan finansial. Media sosial rentan terhadap teknik *Phising*.

Pembuatan Undang-Undang tentang Informasi dan Transaksi Elektronik diharapkan agar terwujud keadilan, ketertiban umum, dan kepastian hukum. Dengan demikian diharapkan undang-undang dan pasal-pasal di dalamnya dapat mengatur dan mengantisipasi sistem hukum dalam dunia maya untuk mencegah kejahatan yang biasa disebut *Cyber Crime*. UU ITE tidak mengatur secara khusus mengenai kejahatan *Phising*, namun secara tersirat terdapat beberapa pasal yang berhubungan dengan tindakan *Phising* yang merupakan perbuatan menggunakan *e-mail* imitasi atau *website* imitasi yang berniat untuk memperdayai korban yang memberikan keuntungan kepada pelaku untuk memperoleh informasi pribadi yang bersifat sensitif.[7]

Perkara atau kasus yang pernah terjadi dalam *Cyber Crime Phising*, yaitu pencurian akun facebook seseorang dengan berkedok penipuan link yang berisikan kuis berhadiah untuk melakukan kejahatan yang berupa penipuan dan penyebaran berita palsu atau hoax. Pada tanggal 02 Juli 2017 pelaku bernama Muhammad Balatif alias MB melakukan hal tersebut dengan cara menyebarkan postingan yang mengundang korban untuk berpartisipasi dalam kuis dengan iming-iming hadiah, untuk berpartisipasi korban diarahkan untuk mengakses link yang tertera di dalam postingan tersebut yang mengarah ke suatu *website*, MB membuat *website* yang mengimitasi *website* resmi facebook dan korban diminta untuk *login* menggunakan akun facebook serta mengisi informasi data diri dan informasi keuangannya, saat korban login dalam *website* tersebut *email* dan *password* nya terkirim kepada MB dan MB dapat mengambil ahli akun facebook korban, MB berpura-pura menjadi korban dan memposting penipuan yang sama dengan mengaku bahwa telah memenangi kuis dan menerima hadiah berharap ada korban lainnya lagi yang akan terpancing dalam strategi si MB.

Berdasarkan dari contoh kasus atau perkara diatas, putusan Majelis Hakim Pengadilan Negeri Medan dengan Putusan No: 3006/Pid.Sus/2017/PN.Mdn, memutuskan untuk menjatuhi hukuman terhadap pelaku dengan tindak pidana *Cyber*, yang berawal dari *Phising* dengan tujuan untuk melakukan penipuan dan penyebaran berita palsu atau *hoax*.

[7] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, Andi, Yogyakarta, 2013.

B. Rumusan Masalah

1. Bagaimana pengaturan hukum yang diterapkan terhadap tindak pidana *Phising*?
2. Bagaimana penerapan sanksi hukum terhadap pelaku *Phising* pada Putusan Nomor 3006/Pid.Sus/2017/PN MDN?

C. Metode Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah metode penelitian Yuridis Normatif.

PEMBAHASAN

A. Pengaturan hukum yang diterapkan terhadap tindak pidana *Phising*

Kasus kejahatan *phising* sendiri merupakan salah satu kejahatan yang paling sering terjadi di dalam dunia maya, terlepas sudah adanya peraturan yang secara tersirat mengatur mengenai kejahatan *phising* akan tetapi tidak dapat mengurangi kejahatan itu sendiri secara signifikan karena kurang spesifiknya aturan yang mengatur kejahatan *phising*.

Laporan kasus *phising* menurut lembaga *Indonesia Anti-Phising Data Exchange* (IDADX) yang tercatat pada tahun 2023. Pada quartal 1 tahun 2023 jumlah laporan *phising* yang diterima oleh IDADX menunjukkan kenaikan yang signifikan dimana pada quartal 1 tahun 2023 terdapat sebanyak 26.675 laporan *phising* sedangkan pada quartal 4 2022 terdapat 6.106 laporan *phising*. Jumlah laporan dalam quartal kedua 2023 sebanyak 20.330, dimana mengalami penurunan sebanyak 6.345 laporan *phising* dari kuartal pertama 2023.[8] Jumlah laporan *phising* yang diterima oleh IDADX dalam quartal ketiga 2023 sebanyak 9.823, dimana mengalami penurunan sebanyak 10.507 laporan dari kuartal kedua 2023.[9] Jumlah laporan *phising* yang diterima oleh IDADX dalam quartal 4 2023 sebanyak 8.161, dimana mengalami penurunan sebanyak 1.662 laporan *phising* dari kuartal ketiga 2023.[10]

Kasus *phising* yang tercatat di dalam laporan diatas mencakup juga sasaran atau target dari *phising*, mulai dari industrial hingga brand-brand

[8] *Laporan Aktivitas Phising Domain ~.ID*, https://api.idadx.id/documents/uploads/170504 8370_Laporan%20Q2%202023.pdf.pdf, (Diakses pada tanggal 19 Juni 2025)

[9] *Laporan Aktivitas Phising Domain ~.ID*, https://api.idadx.id/documents/uploads/170504 7952_Laporan%20Q3%202023.pdf.pdf, (Diakses pada tanggal 19 Juni 2025)

[10] *Laporan Aktivitas Phising Domain ~.ID*, https://api.idadx.id/documents/uploads/170589 2888_Laporan%20Q4%202023.pdf.pdf, (Diakses pada tanggal 19 Juni 2025)

dari industri yang menjadi sasaran *phising* seperti sosial media, *eCommerce*, institusi finansial atau jasa keuangan, bahkan sampai ranah industri video game online.

Industri sosial media merupakan industri yang paling sering menjadi target serangan *phising* dengan persentasi hingga 64,34%, yang diikuti oleh industri finansial pada urutan kedua dengan persentase hingga 20,58%. Ini merupakan data yang terlapor pada laporan quartal 4 tahun 2023.[11]

Facebook menjadi platform andalan para pelaku *phising* sebab mudahnya untuk menjangkau para pemirsa. Bebasnya jaringan Facebook membuat pelaku dengan mudah dapat melakukan aksinya, berawal dari pembuatan akun yang mudah tanpa perlu identitas asli, postingan yang mudah untuk di upload karena minimnya persyaratan yang perlu dipatuhi serta minimnya peraturan yang melarang mengenai isi postingan yang akan diupload menjadikan platform Facebook ranah dengan kasus *phising* terbanyak.

Penyebab lain mengapa Facebook sering terdapat kasus *phising* adalah faktor banyaknya orang tua yang menggunakan aplikasi Facebook, di bandingkan dengan aplikasi platform sosial media lainnya. Ini karena Facebook lebih dulu hadir dan sudah lebih dulu dikenal di kalangan masyarakat Indonesia, tepatnya Facebook hadir pada bulan September 2008. Dikutip blog Nick Burcher, dalam dua tahun terakhir (2008-2010), pengguna Facebook di Indonesia tumbuh delapan ribu persen (8223,2%). Bila pada bulan September 2008 jumlahnya hanya 322 ribu pengguna, pada September 2010, angka tersebut naik menjadi 26,8 juta pengguna.[12] Dengan ini tidak terlepasnya kemungkinan orang tua juga menggunakan Facebook.

Begitu banyaknya orang-orang tua yang menggunakan Facebook membuat persentase keberhasilan para pelaku *phising* menaik, ini dikarenakan sifat polosnya para orang tua dan ketidak telitinya terhadap isi konten postingan yang ada di dalam aplikasi Facebook menjadikan mereka para orang tua target *phising* yang empuk. Sebab itulah kasus *phising* di aplikasi Facebook tak pernah berakhir dan terus terjadi.

Penanganan kasus *phising* sendiri memiliki proses dan ranah yang khusus, dibutuhkan yang namanya ilmu forensik digital atau forensik komputer untuk memproses kasus *phising*. Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital. Investigasi forensik digital memiliki penerapan yang sangat beragam. Bidang ilmu forensik atau forensik adalah istilah yang diberikan untuk penyelidikan kejahatan menggunakan sarana ilmiah atau digunakan untuk menggambarkan deteksi kejahatan secara umum. Ini adalah aplikasi dari spektrum ilmu yang luas untuk menjawab pertanyaan yang menarik bagi sistem hukum. Munculnya forensik berasal dari timbulnya perilaku kriminal, ilegal dan tidak pantas.[13]

Perkembangan teknologi informasi memiliki dampak terhadap meningkatnya tindak kejahatan terutama pada Computer-related Crime maka ilmu forensik digital pun mengalami perkembangan yang terbagi dalam beberapa subbidang forensik digital. Adapun subbidang forensik digital dalam pengungkapan *cybercrime* di antaranya:

a. Forensik Komputer
b. Forensik Media Penyimpanan
c. Forensik Perangkat Bergerak
d. Forensik Audio
e. Forensik Video
f. Forensik Citra
g. Forensik Jaringan
h. Forensik Komputasi Awan
i. Forensik Internet of Things[14]

Forensik jaringan merupakan bagian dari forensik digital yang terfokus pada pemantauan dan analisis aliran data di dalam jaringan komputer. Tujuannya adalah untuk mengumpulkan informasi, bukti hukum, dan mendeteksi akses ilegal pada jaringan tersebut.

Peraturan-peraturan dalam merumuskan delik pidana terkait dengan tindakan *phising*, beberapa pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang dapat menjadi acuan untuk menegakkan hukum terkait dengan *phising* adalah Pasal 378 KUHP yang berkaitan dengan penipuan, Pasal 263 KUHP yang terkait dengan pemalsuan surat, dan Pasal 362 KUHP yang berkaitan dengan penggelapan data elektronik atau informasi. Sebelumnya, pengaturan hukum terhadap kejahatan siber dalam bentuk *phising* diatur dalam Pasal 378 KUHP tentang penipuan, karena *phising* pada dasarnya merupakan tindakan

[11] *Ibid., 6*

[12] Julian Sukmana Putra, *Why Facebook is So Popular in Indonesia*, https://www.techinasia.com/why-facebook-is-so-popular-in-indonesia?, (Diakses pada tanggal 14 Juli 2025)

[13] Aris Susanto, *Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)*, https://www.academia.edu/86326782/Analisa_Perkembangan_Digital_Forensik_dalam_Penyelidikan_Cybercrime_di_Indonesia_Systematic_Review_, (Diakses pada tanggal 14 Oktober 2025)

[14] Dedy Hariyadi, *Buku Panduan Dasar Forensik Digital*, Baskara Media, Yogyakarta, 2022

penipuan.[15] Berikut bunyi dari pasal KUHP tersebut :

Pasal 378 KUHP : Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun.

Pasal 263 KUHP :

1. Barang siapa membuat surat palsu atau memalsukan surat yang dapat menimbulkan sesuatu hak, perikatan atau pembebasan hutang, atau yang diperuntukkan sebagai bukti daripada sesuatu hal dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak dipalsu, diancam jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, dengan pidana penjara paling lama enam tahun.
2. Diancam dengan pidana yang sama, barang siapa dengan sengaja memakai surat palsu atau yang dipalsukan seolah-olah sejati, jika pemakaian surat itu dapat menimbulkan kerugian.

Pasal 362 KUHP : Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama 5 tahun atau pidana denda paling banyak Rp900 ribu.

Pasal 378 merupakan delik yang relevan karena melibatkan unsur hak. Namun pasal 378 tidak menguraikan mengenai unsur ITE sehingga kurang cocok dalam menangani *cybercrime*. Pasal 263 memiliki relevansi unsur-unsur yang sesuai dengan *phising*, unsur-unsur yang dimaksud adalah pembuatan atau pemalsuan surat elektronik dan bujukan atau imingan kepada korban yang mengakibatkan kerugian, pelaku dapat dijerat dengan pasal 263 jika terbukti merugikan korban dengan pemalsuan surat elektronik. Pasal 362 berhubungan dengan serangkaian tindakan mencuri data pribadi milik korban untuk dimanfaatkan demi keuntungan seorang individu.

Kitab Undang-Undang Hukum Pidana baru yang ditetapkan pada tanggal 02 Januari 2023 akan mulai berlaku pada Tahun 2026 mendatang, KUHP baru ini juga memiliki relevansi terhadap *Phising* yang dapat menjadi antisipasi hukum kedepannya ketika KUHP baru mulai diberlakukan dan diterapkan. Pasal-pasal lama yang memiliki keterkaitan dengan *phising* akan di gantikan dengan pasal-pasal yang baru, meski istilah *phising* tetap tidak disebutkan namun modus dan substansinya tetap relevan dan lebih modern sehingga harusnya pasal-pasal yang baru akan bersifat lebih sistematis.

Delik *phising* tetap bisa di jerat dengan pasal-pasal baru dalam KUHP baru meski bunyi isinya sedikit berbeda namun unsurnya tetap padanan dengan pasal-pasal yang lama. Berikut pasal-pasal dalam KUHP baru yang menggantikan pasal-pasal KUHP lama. Pasal 492 tentang penipuan (padanan pasal 378 KUHP lama) : Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V.

Pasal 391 tentang pemalsuan surat (padanan pasal 263 KUHP lama) :

ayat (1) Setiap Orang yang membuat secara tidak benar atau memalsu Surat yang dapat menimbulkan suatu hak, perikatan atau pembebasan utang, atau yang diperuntukkan sebagai bukti dari suatu hal, dengan maksud untuk menggunakan atau meminta orang lain menggunakan seolah-olah isinya benar dan tidak palsu, jika penggunaan Surat tersebut dapat menimbulkan kerugian, dipidana karena pemalsuan Surat, dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori VI.

ayat (2) Setiap Orang yang menggunakan Surat yang isinya tidak benar atau yang dipalsu, seolah-olah benar atau tidak dipalsu, jika penggunaan Surat tersebut dapat menimbulkan kerugian dipidana dengan pidana yang sama dengan ayat (1).

Pasal 476 tentang pencurian (padanan pasal 362 KUHP lama) : Setiap Orang yang mengambil suatu Barang yang sebagian atau seluruhnya milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, dipidana karena pencurian, dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak kategori V.

Pidana denda dalam pasal-pasal KUHP baru di klasifikasikan dalam kategori-kategori yang berbeda, pasal 78 KUHP baru menyatakan pidana denda merupakan sejumlah uang yang wajib dibayar oleh terpidana berdasarkan putusan

[15] Aura Nasha Ramadhanti, Tessa Ayuning Tias, Erin Dwi Lestari, Asmak Ul Hosnah, *Jurnal Pendidikan Tambusai* Vol. 8 No. 1, Tahun 2024

pengadilan. Jika tidak ditentukan minimum khusus, pidana denda ditetapkan paling sedikit Rp50.000,00 (lima puluh ribu rupiah).[16]

Pasal 492 KUHP baru tentang penipuan adalah pengganti fungsional pasal 378 KUHP lama, relevansi pasal ini dalam *phising* adalah perbuatan menyesatkan orang lain dengan rangkaian kebohongan dengan identitas palsu untuk menguntungkan diri sendiri yang mengakibatkan kerugian materil, pelaku yang berpura-pura sebagai suatu instansi yang mengirimkan tautan palsu atau pesan manipulatif yang membuat korban menyerahkan data pribadi (*password*, *user id*, dll). Pasal 391 KUHP baru tentang pemalsuan surat yang menggantikan pasal 263 KUHP lama meskipun isinya tidak secara spesifik menyebut "elektronik" namun penafsiran hukum modern menegaskan bahwa surat atau dokumen mencakup bentuk fisik maupun elektronik, contoh surat dan dokumen elektronik seperti email palsu, website tiruan, instansi palsu, dll. Pasal 476 KUHP baru tentang pencurian menggantikan pasal 362 KUHP lama, relevansi dengan *phising* ketika pelaku berhasil menguras atau memindahkan aset digital atau saldo rekening tanpa sepengetahuan korban.

Meskipun KUHP baru akan berlaku dan menggantikan KUHP lama, kejahatan *phising* tetap lebih tepat dijerat menggunakan Undang-Undang Informasi dan Transaksi Elektronik sebagai lex specialis. KUHP baik lama maupun baru, berfungsi sebagai dasar pidana umum terutama dalam aspek penipuan, pencurian, dan pemalsuan.

Undang-Undang Informasi dan Transaksi Elektronik pertama kali disahkan pada tahun 2008 sebagai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian mendapatkan revisi pertama sebagai Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan revisi kedua sebagai Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Meski UU ITE mendapat perubahan sebanyak dua kali, perubahan yang disebut hanya mencakup pengubahan dan penambahan kata kalimat dalam beberapa pasal yang tidak mempengaruhi inti dan unsur dalam pasal tersebut, sehingga pasal-pasal tersebut masih memiliki arti yang sama meski sudah mendapat revisi.

Pasal 28 ayat (1) UU ITE melarang setiap perbuatan yang dapat menimbulkan kerugian bagi konsumen dalam transaksi elektronik melalui tindakan yang menyesatkan. Data pribadi korban yang diperoleh pelaku dapat disalahgunakan sehingga menyebabkan kerugian dalam transaksi elektronik. Dalam kasus *phising*, penekanannya berada pada tindakan penyesatan dalam ranah transaksi elektronik, sehingga pelaku dapat dijerat dengan pasal 45A ayat (1).

Pasal 30 ayat (1) dan (2) UU ITE Melarang setiap perbuatan ilegal yaitu tanpa hak mengakses sistem elektronik orang lain. Dalam konteks kejahatan *phising*, pelaku berarti secara ilegal masuk kedalam akun korban menggunakan data hasil *phising*, akun yang dimaksud bisa berupa akses terhadap rekening, email, dan sosial media. Tindakan tersebut dapat dijerat dengan pasal 46 UU ITE ayat (1) dan (2).

Pasal 32 ayat (1) UU ITE melarang segala bentuk intervensi terhadap data elektronik milik pihak lain secara ilegal, tindakan yang dimaksud mencakup aktivitas peretasan, pengubahan data, penghapusan, hingga pencurian data milik orang lain. Dalam kasus *phising*, penekanannya ada pada tindakan pencurian data elektronik milik orang lain yang dapat dijerat dengan sanksi hukuman sesuai dengan pasal 48 ayat (1).

Pasal 35 UU ITE mengatur larangan mengenai bentuk-bentuk pemalsuan atau rekayasa data elektronik yang dapat menipu dan merugikan korban, sebagai contoh seperti situs websitu palsu yang menyerupai aslinya seperti jasa keuangan atau sosial media, atau pembuatan dokumen palsu untuk menyesatkan korban dalam melakukan transaksi seperti surat keterangan atau bukti pembayaran. Pasal 35 merupakan pasal yang paling relevan dalam kasus *phising* karena pelaku sering menggunakan metode pemalsuan dan rekayasa untuk menipu korban. Pelaku dapat dikenakan sanksi pidana berdasarkan pasal 51 ayat (1).

Terdapat beberapa Undang-Undang khusus lainnya selain UU ITE yang juga berkaitan dengan tindak pidana *phising*, yaitu Undang-Undang Tindak Pidana Pencucian Uang (UU TPPU), Undang-Undang Perbankan (UU Perbankan), dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Setiap undang-undang memiliki alasan relevansi yang berbeda-beda, begitu juga dengan bentuk kontribusinya terhadap kejahatan *phising*.

UU TPPU, UU Nomor 8 Tahun 2010 memiliki bentuk relevansi tahap lanjutan dimana

[16] Zaqiu Rahman, *PASCA DISAHKANNYA UNDANG-UNDANG TENTANG KUHP YANG BARU, APAKAH KETENTUAN PIDANA DI DALAM SEMUA UNDANG-UNDANG ATAU PERATURAN DAERAH HARUS DIREVISI ?*, rechtsvinding.bphn.go.id/?page=artikel&berita=738 (Diakses pada tanggal 3 Desember 2025)

Undang-Undang TPPU akan relevan ketika hasil dari kejahatan *phising* (uang dari rekening atau aset digital) dicuci atau disamarkan, biasanya dengan metode dipindah berlapis atau disamarkan melalui banyak rekening. Adapun pasal yang mengatur dan menjerat kejahatan tersebut, yaitu

a) Pasal 2 ayat (1) : Hasil tindak pidana adalah Harta Kekayaan yang diperoleh dari tindak pidana:
   a. korupsi;
   b. penyuapan;
   c. narkotika;
   d. psikotropika;
   e. penyelundupan tenaga kerja;
   f. penyelundupan migran;
   g. di bidang perbankan;
   h. di bidang pasar modal;
   i. di bidang perasuransian;
   j. kepabeanan;
   k. cukai;
   l. perdagangan orang;
   m. perdagangan senjata gelap;
   n. terorisme;
   o. penculikan;
   p. pencurian;
   q. penggelapan;
   r. penipuan;
   s. pemalsuan uang;
   t. perjudian;
   u. prostitusi;
   v. di bidang perpajakan;
   w. di bidang kehutanan;
   x. di bidang lingkungan hidup;
   y. di bidang kelautan dan perikanan; atau
   z. tindak pidana lain yang diancam dengan pidana penjara 4 (empat) tahun atau lebih, yang dilakukan di wilayah Negara Kesatuan Republik Indonesia atau di luar wilayah Negara Kesatuan Republik Indonesia dan tindak pidana tersebut juga merupakan tindak pidana menurut hukum Indonesia.

b) Pasal 3 : Setiap Orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dengan tujuan menyembunyikan atau menyamarkan asal usul Harta Kekayaan dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

c) Pasal 4 : Setiap Orang yang menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

d) Pasal 5 ayat (1) : Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Phising dalam undang-undang ini memiliki pendekatan sebagai *predicate crime* atau tindak pidana asal. Pasal 3,4,5 adalah bentuk kontribusi yang menjerat kejahatan lanjutan seperti aliran dana hasil *phising* dan memungkinkan perampasan aset serta pembalikan beban pembuktian. UU TPPU berperan dalam mengatur kejahatan lanjutan dari tindak pidana *phising*.

UU Perbankan, UU Nomor 7 Tahun 1992 jo. UU Nomor 10 Tahun 1998. Undang-undang perbankan memiliki relevansi secara sektoral, ini dikarenakan tindak pidana *phising* sering menargetkan nasabah perbankan dalam konteks finansial. Alasan relevansinya adalah ketika dana hasil *phising* masuk ke rekening bank yang bersangkutan tanpa sepengetahuan dan izin pimpinan bank, hal ini juga berkaitan dengan sistem pelayanan perbankan. Adapun pasal-pasal dalam UU Perbankan yang mengatur kejahatan *phising* yang bersifat sektoral, yaitu.

a) Pasal 47 :
   ayat (1) Barang siapa tanpa membawa perintah tertulis atau izin dari Pimpinan Bank Indonesia sebagaimana dimaksud dalam Pasal 41, Pasal 41A, dan Pasal 42, dengan sengaja memaksa bank atau Pihak Terafiliasi untuk memberikan keterangan sebagaimana dimaksud dalam Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 4 (empat) tahun serta denda sekurang-kurangnya Rp 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp 200.000.000.000,00 (dua ratus miliar rupiah).
   ayat (2) Anggota Dewan Komisaris, Direksi,

pegawai bank atau Pihak Terafiliasi lainnya yang sengaja memberikan keterangan yang wajib dirahasiakan menurut Pasal 40, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun serta denda sekurang-kurangnya Rp 4.000.000.000,00 (empat miliar rupiah) dan paling banyak Rp 8.000.000.000,00 (delapan miliar rupiah)."

b) Pasal 47A : Anggota Dewan Komisaris, Direksi, atau pegawai bank yang dengan sengaja tidak memberikan keterangan yang wajib dipenuhi sebagaimana dimaksud dalam Pasal 42A dan Pasal 44a, diancam dengan pidana penjara sekurang-kurangnya 2 (dua) tahun dan paling lama 7 (tujuh) tahun serta denda sekurang-kurangnya Rp4.000.000.000.00 (empat miliar rupiah) dan paling banyak Rp15.000.000.000,00 (lima belas miliar rupiah).
c) Pasal 49 ayat (1) : Anggota Dewan Komisaris, Direksi, atau pegawai bank yang dengan sengaja:
    a. membuat atau menyebabkan adanya pencatatan palsu dalam pembukuan atau dalam proses laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank;
    b. menghilangkan atau tidak memasukkan atau menyebabkan tidak dilakukannya pencatatan dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank;
    c. mengubah, mengaburkan, menyembunyikan, menghapus, atau menghilangkan adanya suatu pencatatan dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank, atau dengan sengaja mengubah, mengaburkan, menghilangkan, menyembunyikan atau merusak catatan pembukuan tersebut, diancam dengan pidana penjara sekurang-kurangnya 5 (lima) tahun dan paling lama 15 tahun serta denda sekurang-kurangnya Rp. 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp200.000.000.000,00 (dua ratus miliar rupiah).

UU Perbankan bukan pasal utama pelaku, tetapi krusial dalam penanganan institusional dan pembuktian. Bentuk kontribusi utama dari Undang-undang ini adalah menjerat pelanggaran terhadap rahasia bank serta menjadi dasar tanggung jawab bank dan perlindungan konsumen perbankan. UU Perbankan berperan dalam konteks finansial.

UU PDP, UU Nomor 27 Tahun 2022 bersifat sangat relevan karena inti kejahatan *phising* adalah pengambilan data pribadi tanpa hak. Unsur yang membuat UU ini relevan adalah karena kejahatan *phising* berkaitan dengan login bank, OTP, PIN, NIK dan nomor kartu yang merupakan data pribadi, *phising* juga melibatkan pengumpulan data secara melawan hukum dan pemalsuan identitas pihak lain. UU PDP memiliki pasal-pasal yang berkaitan dengan kejahatan *phising*, yaitu

a) Pasal 65 :
    ayat (1) Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
    ayat (2) Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
    ayat (3) Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.
    juncto :
    Pasal 67 :
    ayat (1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
    ayat (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
    ayat (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
b) Pasal 66 : Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data

Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.
juncto :
Pasal 68 : Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 .tipidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah).

UU PDP bersifat sebagai *lex specialis* substansi data, UU PDP mengisi kekosongan hukum yang tidak diatur rinci dalam UU ITE, hal ini memungkinkan adanya penuntunan terpisah terhadap penyalahgunaan data pribadi. Bentuk kontribusi UU PDP terhadap kejahatan *phising* adalah melindungi hak korban serta menyasar substansi data (inti atau esensi dari data yang dikumpulkan), bukan hanya unsur elektronik atau alat elektronik saja. Singkatnya UU PDP berperan sebagai perlindungan data dan korban.

B. Penerapan sanksi hukum terhadap pelaku *Phising* pada Putusan Nomor 3006/Pid.Sus/2017/PN Mdn

Sanksi pidana merupakan suatu jenis sanksi yang bersifat nestapa yang diancamkan atau dikenakan terhadap perbuatan atau pelaku perbuatan pidana atau tindak pidana yang dapat mengganggu atau membahayakan kepentingan hukum. Sanksi pidana pada dasarnya merupakan suatu penjamin untuk merehabilitasi perilaku dari pelaku kejahatan tersebut, namun tidak jarang bahwa sanksi pidana diciptakan sebagai suatu ancaman dari kebebasan manusia itu sendiri.[17]

Pembahasan mengenai penerapan sanksi terhadap pelaku pada kasus Putusan No.3006/Pid.Sus/2017/PN Mdn. Berfokuskan dalam membahas unsur kejahatan *phising* yang dilakukan oleh pelaku yang terdapat dalam kasus tersebut dan apa pertimbangan hukumannya. Pembahasan analisis berikut mengandung fakta kasus dan cara kerja *phising* yang digunakan, bagaimana jaksa dalam mengkualifikasi perbuatan secara yuridis, dan bagaimana pertimbangan hakim dalam menilai unsur-unsur tersebut.

Faktanya terdapat tindakan *phising* dalam perkara, berawal dari pelaku yang "memancing" pemilik akun Facebook agar memberikan informasi dan akses dengan tujuan untuk mengambil alih akun Facebook dari pemiliknya serta menggunakan akun tersebut untuk melakukan kejahatan lainnya. Jenis *phising* yang digunakan adalah *clone phising*, dimana pelaku membuat halaman website palsu untuk memperolah data akses akun korban yang kemudian akun tersebut dimanfaatkan untuk menyebarkan materi yang berujung pada tuntutan ITE. Tidak ada dokumen yang menjelaskan secara rinci semua langkah *phising*, misalnya bagaimana secara teknis akun diretas, atau bagaimana korban dipancing.

Pemanfaatan akun yang berujung pada tuntutan ITE adalah mengenai penyebaran ujaran kebencian terhadap suatu instansi negara dan satu tokoh penting negara, hal tersebut pada akhirnya memancing perhatian dan mata hukum hingga berujung pada pelaporan resmi. Pelaku tercatat menggunakan akun palsu yang diperoleh dari hasil kejahatan *phising* sebagai bagian dari operasi, dimana pelaku membuat dan menyebarkan postingan atau unggahan yang berisikan ujaran kebencian dimana pelaku menantang dan mengolok-olok instansi kepolisian serta melakukan pencemaran nama baik terhadap bapak Presiden.

Meskipun telah terbukti bahwa adanya Unsur kejahatan *phising* yang terdapat dalam putusan No.3006/Pid.Sus/2017/Pn Mdn, namun tindak kejahatan tersebut tidak di kualifikasikan sebagai delik khusus yang dapat di jerat dengan Undang-Undang khusus yang telah ada. Jaksa menuntut dengan pasal-pasal dalam UU ITE terkait pencemaran nama baik melalui media elektronik dan menempatkan tindakan *phising* dalam putusan tersebut sebagai bagian dari tindak pidana siber yang luas, serta dakwaan ITE dapat di subtitusi dengan pasal lain bila perlu.

Kejahatan *phising* dan penggunaan akun palsu yang diperoleh dari tindakan *phising* dalam kasus ini dianggap sebagai modus operandi atau cara untuk mencapai delik ITE atau rencana kejahatan pelaku, sehingga tidak dijerat dengan pasal terkait *phising*. Dakwaan serta amar putusan dalam kasus ini menggunakan pasal 27 ayat (3) UU ITE dimana pasal ini mengatur perbuatan dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Akun palsu yang diperoleh pelaku melalui tindakan *phising* di pakai menjadi sarana atau media yang mendistribusikan dan mentransmisikan sehingga dapat diaksesnya informasi tersebut oleh publik. Unsur inilah yang memutuskan bahwa tindakan *phising* dan

[17] Salman Sahrir, Muh. Fadli Faisal Rasyid, Moch Al Fatah Alti Putra, *Jurnal Litigasi Amsir*, Vol 12 No 1, 2024

pengunaan akun palsu yang diperoleh dari *phising* tersebut dikualifikasikan sebagai unsur sarana atau alat bantu untuk melaksanakan perbuatan melawan hukum dan bukan unsur utama atau independen.

Penilaian terhadap unsur *phising* oleh hakim dalam kasus ini dianggap relevan, ini dikarenakan terdapat pembuktian adanya sarana dan metode yang digunakan oleh pelaku dalam melakukan kejahatan dengan pembuatan dan mendistribusikan konten yang memuat unsur ujaran kebencian dan pencemaran nama baik. Tindakan dimana dan bagaimana pelaku memperoleh akun palsu dari korban menjadi bukti perilaku kejahatan siber *phising* yang disengaja.

Fokus utama dalam putusan hakim yang menjadi pertimbangan penjatuhan hukuman adalah pada dampak dari penyebaran konten ujaran kebencian dan pencemaran nama baik melalui media elektronik oleh pelaku. Unsur *phising* diperhitungkan sebagai fakta yang memperkuat unsur tindakan perbuatan kejahatan ITE, *phising* tersebut dipandang sebagai sarana yang memfasilitasi perbuatan pokok dari pelaku dalam melaksanakan kejahatannya.

Unsur perbedaan pengaturan juga berpengaruh dimana pada waktu perkara ini terjadi pengaturan tindak pidana *cyber* dan definisi-definisi yang mengatur mengenai kejahatan *phising* masih dalam tahap berkembang. Unsur demikian juga yang menjadi pertimbangan hakim memutuskan pada delik yang lebih matang yaitu pencemaran nama baik daripada mengisi satu pasal terkhusus yang mengatur tentang kejahatan *phising*.

Putusan dan sanksi yang dijatuhkan kepada pelaku yang dinyatakan bersalah secara sah dan meyakinkan melakukan tindak pidana sesuai dengan pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik setiap orang dengan sengaja dan tanpa hak mentransmisikan atau membuat dapat diaksesnya informasi elektronik yang mengandung pencemaran nama baik, sebagaimana diatur dan diancam dengan pidana dalam Pasal 45 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terdakwa dijatuhkan dengan pidana penjara satu tahun dan enam bulan dan denda sebesar sepuluh juta rupiah dengan ketentuan apa bila denda tersebut tidak dibayar maka akan diganti dengan pidana penjara selama satu bulan.

Putusan yang diberikan sudah sesuai dengan apa yang diatur dalam UU ITE dalam menjerat kejahatan pencemaran nama baik, hanya saja kejahatan *phising* yang terkait tidak dijatuhi hukuman atau jeratan, ini karena menurut hakim *phising* dikatakan hanya sebagai unsur tambahan atau pembantu dari kejahatan setelah *phising*. Pertimbangan ini di putuskan karena pelapor menitikberatkan kejahatan pencemaran nama baik pada satu instansi, sehingga delik *phising* yang terbukti setelah ada penyidikan dikesampingkan dan dianggap sebagai sarana tindak pidana pencemaran nama baik.

Phising pada umumnya tidak serta-merta dapat diproses tanpa adanya laporan dari pihak yang dirugikan, karena dampak utama dari perbuatan tersebut berkaitan dengan kerugian pribadi, baik berupa kerugian immaterial seperti kehormatan dan reputasi, maupun potensi kerugian lainnya. Oleh karena itu, aduan dari korban menjadi pintu awal bagi aparat penegak hukum untuk menelusuri peristiwa pidana yang terjadi di ruang digital. Dalam perkara Nomor 3006/Pid.Sus/2017/PN.Mdn, meskipun *phising* tidak didakwakan sebagai tindak pidana yang berdiri sendiri, keberadaan aduan dari pihak yang dirugikan tetap memiliki arti penting. Aduan tersebut menjadi dasar bagi penyidik untuk melakukan penyelidikan terhadap aktivitas akun palsu dan konten elektronik yang dianggap merugikan. Dengan adanya aduan, aparat penegak hukum dapat mengumpulkan bukti-bukti elektronik seperti tangkapan layar, riwayat unggahan, serta keterangan saksi yang berkaitan dengan penggunaan akun palsu sebagai sarana *phising*.

Aduan yang diajukan juga berfungsi untuk menunjukkan adanya dampak nyata dari perbuatan pelaku. Dalam perkara ini, aduan yang diajukan korban memperlihatkan bahwa tindakan *phising* telah menimbulkan gangguan terhadap kehormatan dan nama baik, sehingga memenuhi unsur kerugian sebagaimana disyaratkan dalam tindak pidana pencemaran nama baik melalui media elektronik. Tanpa adanya aduan, perbuatan tersebut berpotensi dianggap sebagai konflik pribadi atau permasalahan non-pidana, sehingga sulit untuk diproses lebih lanjut dalam ranah hukum pidana. Aduan dari korban menunjukkan bahwa perbuatan terdakwa tidak hanya bersifat teknis atau percobaan semata, melainkan telah menimbulkan akibat yang dirasakan secara langsung oleh pihak yang dirugikan. Hal ini menjadi salah satu dasar pertimbangan hakim dalam menilai tingkat keseriusan perbuatan serta dalam menjatuhkan pidana kepada terdakwa.

Berdasarkan analisis yuridis terhadap penerapan sanksi dalam Putusan Nomor 3006/Pid.Sus/2017/Pn Mdn, penjatuhan pidana kepada terdakwa telah sesuai dengan asas

legalitas sebagaimana diatur dalam hukum pidana Indonesia, karena didasarkan pada ketentuan Pasal 27 ayat (3) jo. Pasal 45 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Unsur perbuatan "dengan sengaja dan tanpa hak" serta tindakan "mendistribusikan dan/atau mentransmisikan informasi elektronik yang bermuatan penghinaan dan/atau pencemaran nama baik" telah terbukti melalui penggunaan akun hasil *phising* untuk menyebarkan konten yang menyerang kehormatan pihak tertentu. Oleh karena itu, sanksi pidana penjara dan denda yang dijatuhkan berada dalam batas ancaman pidana yang ditentukan undang-undang.

Pemahaman secara konseptual terdapat ruang analisis lebih lanjut terhadap tindakan *phising* yang dilakukan terdakwa, karena perbuatan tersebut secara substansial memenuhi karakteristik akses tanpa hak terhadap sistem elektronik. Akan tetapi, mengingat dakwaan penuntut umum lebih menitikberatkan pada delik pencemaran nama baik dan pembuktian difokuskan pada akibat hukum berupa tersebarnya konten penghinaan, maka majelis hakim mengkualifikasikan *phising* sebagai modus operandi atau sarana pendukung tindak pidana utama. Dengan demikian, dapat disimpulkan bahwa penerapan sanksi dalam perkara ini telah tepat secara normatif berdasarkan peraturan perundang-undangan yang berlaku, meskipun dari perspektif pengembangan hukum pidana siber masih dimungkinkan pengaturan dan penegakan yang lebih komprehensif terhadap tindak pidana phising sebagai delik yang berdiri sendiri.

PENUTUP

A. Kesimpulan

1. KUHP belum mengatur secara khusus mengenai kejahatan berbasis teknologi informasi, berlakunya prinsip *lex specialis derogat legi generalis*, menempatkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar hukum utama dalam penanganan kejahatan *phising*. Pasal 35 UU ITE menjadi pasal yang paling relevan dalam kasus *phising*. Undang-undang khusus lainnya yang memiliki alasan relevansi dan kontribusi yang berbeda-beda dalam kasus tindak pidana *phising*, yaitu UU Perlindungan Data Pribadi yang berperan melindungi data dan korban, UU Tindak Pidana Pencucian Uang yang berperan mengatur kejahatan lanjutan, dan UU Perbankan yang berperan dalam konteks finansial. Tindak pidana *phising* tidak dapat ditangani dengan satu instrumen hukum saja, melainkan membutuhkan pendekatan kumulatif. UU ITE menjadi dasar utama, sedangkan UU PDP, UU Perbankan, UU TPPU, serta KUHP lama dan baru berfungsi sebagai pelengkap sesuai karakter dan tahapan kejahatan.
2. Tindak kejahatan *phising* dalam kasus tersebut terbukti digunakan sebagai sarana untuk memperoleh akses akun media sosial orang lain secara tidak sah. Meskipun unsur *phising* terbukti secara faktual, tindakannya tidak dikategorikan sebagai delik khusus yang berdiri sendiri. Jaksa penuntut umum dan majelis hakim menempatkan *phising* sebagai modus operandi atau alat untuk melaksanakan tindak pidana utama, yaitu penyebaran informasi elektronik yang mengandung penghinaan dan/atau pencemaran nama baik. Unsur *phising* dipertimbangkan sebagai faktor pendukung yang memperkuat adanya unsur kesengajaan. Hal ini juga disebabkan karena pada saat perkara tersebut terjadi, pengaturan mengenai tindak pidana *phising* masih dalam tahap perkembangan di Indonesia. Oleh sebab itu, hakim memilih untuk menerapkan pasal yang telah memiliki dasar hukum yang lebih kuat dan jelas, yaitu pasal mengenai pencemaran nama baik melalui media elektronik. Kasus ini menunjukkan bahwa sistem hukum pidana Indonesia masih menghadapi tantangan dalam menjangkau bentuk-bentuk kejahatan siber yang semakin kompleks, termasuk *phising*, karena belum adanya regulasi yang secara spesifik mengaturnya.

B. Saran

1. Pemerintah perlu memperhatikan ketentuan khusus yang secara eksplisit mengatur mengenai tindak pidana *phising* dan kejahatan siber lainnya agar penegakan hukum menjadi lebih efektif dalam menggunakan pasal-pasal umum dalam peraturan-peraturan yang relevan dengan *phising*. Dengan adanya regulasi yang lebih spesifik, aparat penegak hukum akan memiliki dasar hukum yang jelas dan kuat dalam menjerat pelaku *phising*. Penyidik, jaksa, dan hakim perlu mendapatkan pelatihan berkelanjutan mengenai teknologi informasi, forensik digital, serta pembuktian elektronik, sehingga dapat memahami modus operandi kejahatan siber. Pemerintah, lembaga pendidikan, dan sektor swasta perlu bekerja sama dalam memberikan edukasi mengenai pentingnya menjaga keamanan data pribadi serta

mengenali ciri-ciri *phising* dan penipuan daring. Upaya ini akan meningkatkan kesadaran masyarakat agar lebih waspada terhadap ancaman kejahatan siber yang terus berkembang. Selain itu, kerja sama antarnegara juga perlu diperkuat mengingat kejahatan *phising* sering melibatkan jaringan lintas negara. Kerja sama internasional dalam penegakan hukum, pertukaran informasi, dan mekanisme ekstradisi akan membantu mempercepat proses penindakan terhadap pelaku kejahatan siber. Dengan ini diharapkan penanggulangan tindak pidana *phising* di Indonesia dapat berjalan lebih optimal dan efektif.

2. Diperlukan harmonisasi antar undang-undang yang mengatur *cybercrime* guna menghindari kekosongan hukum. Penting juga bagi lembaga peradilan untuk memperluas pemahaman dan adaptasi terhadap dinamika kejahatan siber agar penerapan hukum menjadi lebih responsif dan efektif dengan mempertimbangkan bukti-bukti teknis secara menyeluruh. Penguatan kerja sama antara aparat penegak hukum, penyidik, dan ahli teknologi informasi sangat dibutuhkan guna memastikan validitas bukti digital dalam proses penuntutan tindak pidana *phising*. Di samping itu, penyusunan panduan atau petunjuk teknis dalam penanganan kasus *phising* perlu dilakukan agar aparat penegak hukum memiliki acuan yang konsisten dan dapat memberikan kepastian hukum dalam penanganan kasus serupa. Dalam praktik peradilan, hakim diharapkan tidak hanya fokus pada akibat hukum dari suatu perbuatan, tetapi juga mempertimbangkan metode dan sarana yang digunakan pelaku, seperti *phising*, sebagai bagian penting dalam penilaian unsur tindak pidana. Dengan demikian, penerapan hukum akan menjadi lebih komprehensif dan adaptif terhadap perkembangan teknologi informasi yang terus berkembang pesat.

DAFTAR PUSTAKA

Buku

Amin, F. 2023. *Ilmu Perundang-Undangan.* Banten: PT Sada Kurnia Pustaka.

Bakhrie, S. 2020. *Hukum Sanksi Di Berbagai Praktek Pengadilan.* Tangerang: UM Jakarta Press.

Fajar, M. &. 2019. *Dualisme Penelitian Hukum : Normatif & Empiris.* Yogyakarta: Pustaka Belajar.

Hamzah, A. 1987. *Aspek-aspek Pidana di Bidang Komputer.* Jakarta: Sinar Grafika.

Hamzah, A. 2008. *Asas-Asas Hukum Pidana.* Jakarta: Rineka Cipta.

Hariyadi, D. 2022. *Buku Panduan Dasar Forensik Digital.* Yogyakarta: Baskara Media.

Kadir, A. 2021. *Dasar Logika Pemrograman Komputer (Update Version).* Jakarta: PT Elex Media Komputindo.

Kurniawan, D. 2023. *Ilmu Hacking.* Jakarta: PT Elex Media Komputindo.

Maskun. 2013. *Kejahatan Siber.* Jakarta: Prenada Media.

Naim, N. 2012. *Character Building: Optimalisasi Peran Pendidikan dalam Pengembangan Ilmu & Pembentukan Karakter Bangsa.* Jogjakarta: Ar-Ruzz Media.

Rahmawati, D., Viendyasari, M., Kholifatur, G., Anindhita, W., Bachna, R., & Adiendah, A. 2024. *WASPADA KEJAHATAN Phising ATTACK!* Malang: PT Literasi Nusantara Abadi Grup.

Redi, A. 2022. *Hukum Penyelesaian Sengketa Pertambangan Mineral dan Batubara.* Jakarta Timur: Sinar Grafika.

Rosyadi, I. 2022. *Hukum Pidana.* Surabaya: Revka Prima Media.

Sembiring, T. B., Irmawati, Sabir, M., & Tjahyadi, I. 2024. *Buku Ajar Metodologi Penelitian (Teori Dan Praktik).* Karawang: CV Saba Jaya Publisher.

Soekanto, S. 2004. *Faktor-faktor Yang Mempengaruhi Penegakan Hukum.* Jakarta: Rajawali Pers.

Suhariyanto, B. 2014. *Tindak Pidana Teknologi Informasi (Cybercrime) : Urgensi Pengaturan dan Celah Hukumnya.* Jakarta: Rajawali Pers.

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

Vyctoria. 2013. *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding.* Yogyakarta: Andi.

Wahyuni, F. 2017. *Dasar-Dasar Hukum Pidana Indonesia.* Tangerang: PT Nusantara Persada Utama.

Wicaksono, S. R. 2020. *Fraud dan Scam di Era Digital: Konsep dan Perkembangan.* Malang: CV Seribu Bintang.

Perundang-undangan

Kitab Undang-Undang Hukum Pidana Lama Wetboek van Strafrecht

Kitab Undang-Undang Hukum Pidana Baru Undang-Undang Nomor 1 Tahun 2023

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Jurnal

Ardy, L. A., Istiqomah, I., Ezer, A. E., & Neyman, S. N. 2024. Phising di Era Media Sosial : Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering Vol: 1, No 4*, 1-11.

Gulo, A. S., Lasmadi, S., & Nawawi, K. 2020. Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law Vol. 1 No. 2*, 68-81.

Iman, N., Susanto, A., & Inggi, R. 2020. Analisa Perkembangan Digital Forensik Dalam Penyelidikan Cybercrime di Indonesia. *Jurnal Telekomunikasi dan Komputer*.

Mathar, A. 2023. Aainul Haq. *Jurnal Hukum Keluarga Islam, Vol: 3, Edisi 2*.

Prabhaswara, S. 2023. Analisis Yuridis Terhadap Tindak Pidana Penipuan di dalam Penggunaan Media Sosial. *Jurnal Bevinding Vol 01 No 03*, 62-80.

Purwandari, M. D., Awaliah, A. U., Una, B. K., & Prabowo, H. Y. 2024. STRATEGI PENGUNGKAPAN KASUS PHISHING: STUDI KASUS DI INDONESIA. *Journal of Economic, Bussines, and Accounting*.

Ramadhanti, A. N., Tias, T. A., Lestari, E. D., & Hosnah, A. U. 2024. Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia. *Jurnal Pendidikan Tambusai*.

Sahfitri, A., & Rosmalinda. 2024. PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. *Jurnal Dialektika Hukum Vol 6 No 2*.

Sahrir, S., Rasyid, M. F., & Putra, M. A. 2024. Penerapan Sanksi Hukum: Analisis Kontemporer Berdasarkan Kitab Undang-Undang Hukum Pidana. *Jurnal Litigasi Amsir Vol 12 No 1*.

Website

2019. Diambil kembali dari Binus Library and Knowledge Center: http://library.binus.ac.id/eColls/eThesisdoc/Bab2/BAB%202-ts-r-2019-0038.pdf

A, F. 2023, Desember 4. *Apa Itu Phising? Pengertian, Jenis, dan Cara Mengenalinya*. Diambil kembali dari Hostinger Tutorial: https://www.hostinger.co.id/tutorial/phising-adalah

Admin. 2024, September 9. *Jangan Sampai Terjebak, Pahami Apa Arti Scam dalam Jual Beli*. Diambil kembali dari Penasihat Hukum: https://www.penasihathukum.com/jangan-sampai-terjebak-pahami-apa-arti-scam-dalam-jual-beli

Arti Scam, Ciri-ciri, dan Jenis-jenisnya. 2023, Juli 27. Diambil kembali dari Kumparan: https://kumparan.com/pengertian-dan-istilah/arti-scam-ciri-ciri-dan-jenis-jenisnya-20sEbiy8tYg

Asriansyah, M. F. 2023, Juni 13. *Bahaya Kejahatan Scam*. Diambil kembali dari Kementrian Keuangan Republik Indonesia: https://www.djkn.kemenkeu.go.id/kanwil-sumut/baca-artikel/16202/Bahaya-Kejahatan-Scam.html

Auli, R. C. 2023, desember 7. *Bunyi dan Unsur Pasal 378 KUHP tentang Penipuan*. Diambil kembali dari Hukum Online: https://www.hukumonline.com/klinik/a/pasal-378-kuhp-tentang-penipuan-lt6571693c4c627/

Cloudmatika. 2022, Juli 26. *Memahami Apa itu Second Level Domain serta Tips Memilihnya untuk Website Anda*. Diambil kembali dari Cloudmatika: https://cloudmatika.co.id/blog-detail/second-level-domain-adalah

IDADX. 2023. *Laporan Aktivitas Phising Domain ~ID Quartal 1.* IDADX.

IDADX. 2023. *Laporan Aktivitas Phising Domain ~ID Quartal 2.* IDADX.

IDADX. 2023. *Laporan Aktivitas Phising Domain ~ID Quartal 3.* IDADX.

IDADX. 2023. *Laporan Aktivitas Phising Domain ~ID Quartal 4.* IDADX.

MinBox. 2024, April 25. *Apa Itu CyberSpace? Karakteristik dan Contohnya*. Diambil kembali dari IT Box: https://itbox.id/blog/apa-itu-cyberspace-

karakteristik-dan-contohnya/#cyberspace_adalah

Permatasari, E. 2021, Desember 9. *Jerat Hukum Pelaku Phishing dan Modusnya*. Diambil kembali dari Hukum Online: https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050/

Prayoga, J. 2023, April 6. *Mengenal Bahaya Scam (Scamming) dan Cara Menghindarnya*. Diambil kembali dari Gudang SSL: https://gudangssl.id/blog/scamming-adalah/

Putra, J. S. 2011, Maret 7. *Why Facebook is So Popular in Indonesia*. Diambil kembali dari Techinasia: https://www.techinasia.com/why-facebook-is-so-popular-in-indonesia?

Rahman, Z. 2023, Januari 26. *PASCA DISAHKANNYA UNDANG-UNDANG TENTANG KUHP YANG BARU, APAKAH KETENTUAN PIDANA DI DALAM SEMUA UNDANG-UNDANG ATAU PERATURAN DAERAH HARUS DIREVISI ?* Diambil kembali dari Artikel Hukum: https://rechtsvinding.bphn.go.id/?page=artikel&berita=738

Susela, S. 2022, Desember 31. *Kejahatan Scam (Penipuan) di Media Sosial*. Diambil kembali dari Kalimantan Post: https://kalimantanpost.com/2022/12/kejahatan-scam-penipuan-di-media-sosial/

Wahyuni, W. 2024, Mei 20. *Perbedaan Makna Peraturan dan Peraturan Perundang-Undangan*. Diambil kembali dari Hukum Online: https://www.hukumonline.com/berita/a/perbedaan-makna-peraturan-dan-peraturan-perundang-undangan-lt664b716d7358b/?page=all