Pertanggungjawaban Pidana Terhadap Kejahatan Siber *Phishing* Dalam Sistem Hukum Indonesia Berdasarkan Putusan Pengadilan Banjarbaru

Khairul Saleh Harahap*, Achmad Yusuf, Dimas Arya Aziza

Fakultas Hukum, Universitas Krisnadwipayana, Jakarta
Email: khairul_2533007004@unkris.ac.id

ABSTRAK

Perkembangan teknologi informasi telah melahirkan berbagai bentuk kejahatan siber yang semakin kompleks, salah satunya adalah *phishing*, yaitu metode penipuan digital yang bertujuan memperoleh data pribadi korban melalui manipulasi sistem elektronik dan rekayasa sosial. Fenomena ini menimbulkan tantangan serius bagi sistem hukum karena tidak semua bentuk kejahatan digital diatur secara eksplisit dalam peraturan perundang-undangan. Penelitian ini bertujuan untuk menganalisis konstruksi pertanggungjawaban pidana terhadap kejahatan *phishing* dalam sistem hukum Indonesia serta mengkaji penerapan norma hukum dalam Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb.

Penelitian ini menggunakan metode penelitian hukum yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Data penelitian diperoleh melalui studi kepustakaan yang mencakup bahan hukum primer berupa peraturan perundang-undangan dan putusan pengadilan, serta bahan hukum sekunder berupa literatur akademik terkait kejahatan siber dan pertanggungjawaban pidana. Seluruh bahan hukum dianalisis secara kualitatif melalui analisis isi hukum untuk memahami konstruksi norma serta penerapannya dalam praktik peradilan.

Hasil penelitian menunjukkan bahwa meskipun istilah *phishing* belum diatur secara khusus dalam hukum positif Indonesia, perbuatan yang terkandung di dalamnya dapat dijerat melalui kombinasi ketentuan dalam Kitab Undang-Undang Hukum Pidana, Undang-Undang Informasi dan Transaksi Elektronik, dan Undang-Undang Tindak Pidana Pencucian Uang. Analisis terhadap putusan pengadilan menunjukkan bahwa pengembang perangkat lunak *phishing toolkit* dapat dimintai pertanggungjawaban pidana karena secara sadar memproduksi sarana yang memfasilitasi terjadinya kejahatan siber.

Penelitian ini menyimpulkan bahwa sistem hukum Indonesia pada dasarnya mampu menjerat pelaku *phishing* melalui interpretasi norma yang ada. Namun, penguatan regulasi khusus, peningkatan kapasitas forensik digital, serta penguatan perlindungan korban diperlukan untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan siber di masa depan.

Kata Kunci: *Cybercrime*; *Phishing*; Pertanggungjawaban Pidana; Hukum Siber; Tindak Pidana Teknologi Informasi; Putusan Pengadilan.

ABSTRACT

The rapid development of information technology has generated increasingly complex forms of cybercrime, one of which is phishing, a digital fraud technique aimed at obtaining victims' personal data through manipulation of electronic systems and social engineering. This phenomenon poses significant challenges for the legal system because not all forms of digital crime

are explicitly regulated in statutory law. This study aims to analyze the construction of criminal liability for phishing crimes within the Indonesian legal system and to examine the application of legal norms in Decision of the Banjarbaru District Court Number 85/Pid.Sus/2022/PN.Bjb.

This research employs a normative juridical legal research method using statutory, conceptual, and case approaches. Research data were collected through library research consisting of primary legal materials such as legislation and court decisions, as well as secondary legal materials including academic literature on cybercrime and criminal liability. All legal materials were analyzed qualitatively using legal content analysis to understand the construction of legal norms and their application in judicial practice.

The results indicate that although the term phishing is not explicitly regulated in Indonesian positive law, the conduct associated with phishing can be prosecuted through a combination of provisions within the Criminal Code, the Electronic Information and Transactions Law, and the Anti-Money Laundering Law. The analysis of the court decision demonstrates that developers of phishing toolkit software may be held criminally liable because they intentionally produce technological tools designed to facilitate cybercrime.

This study concludes that the Indonesian legal system is capable of prosecuting phishing offenses through the interpretation of existing legal provisions. However, stronger regulatory frameworks, improved digital forensic capabilities, and enhanced victim protection mechanisms are necessary to strengthen cybercrime law enforcement in the future.

Keywords: *Cybercrime; Phishing; Criminal Liability; Cyber Law; Information Technology Crime; Court Decision.*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar dalam berbagai aspek kehidupan manusia, termasuk dalam aktivitas ekonomi, sosial, dan hukum. Digitalisasi yang semakin luas memungkinkan masyarakat untuk mengakses informasi dengan cepat, melakukan transaksi secara daring, serta memanfaatkan berbagai layanan berbasis teknologi yang semakin efisien.[1] Teknologi pada dasarnya diciptakan sebagai sarana untuk memecahkan berbagai permasalahan manusia serta meningkatkan efektivitas dan efisiensi dalam berbagai aktivitas kehidupan.[2] Melalui pemanfaatan teknologi, manusia dapat mengolah, memproses, menyusun, dan mengelola data sehingga menghasilkan informasi yang akurat dan dapat digunakan untuk mendukung pengambilan keputusan dalam berbagai sektor kehidupan. Kemajuan ini pada satu sisi memberikan kontribusi positif terhadap pembangunan ekonomi dan kesejahteraan masyarakat, namun pada sisi lain juga memunculkan tantangan baru yang berkaitan dengan keamanan sistem digital dan perlindungan data pribadi.

Di tengah pesatnya perkembangan teknologi tersebut, muncul pula

---

1 Listiyono Listiyono dkk., "Perlindungan Hukum Nasabah Atas Kerugian Transaksi Pinjaman Online Ilegal Dihubungkan Dengan Undang-Undang Informasi dan Transaksi Elektronik," *Binamulia Hukum* 12, no. 1 (2023): 109–19, https://doi.org/10.37893/jbh.v12i1.348.

2 Nudirman Munir, *Pengantar Hukum Siber Indonesia* (Rajawali Pers, 2017).

fenomena kejahatan baru yang memanfaatkan sistem elektronik dan jaringan internet sebagai sarana maupun sasaran tindak pidana. Kejahatan semacam ini dikenal sebagai *cybercrime*, yaitu segala bentuk kejahatan yang terjadi di dunia maya atau *cyberspace* yang melibatkan komputer dan jaringan sebagai instrumen utama dalam melakukan perbuatan melawan hukum.[3] Fenomena ini tidak dapat dilepaskan dari kompleksitas interaksi sosial manusia dalam masyarakat modern yang semakin bergantung pada teknologi digital. Dalam perspektif hukum pidana, *cybercrime* dipandang sebagai salah satu sisi gelap dari perkembangan teknologi modern yang memiliki dampak luas terhadap berbagai aspek kehidupan masyarakat.[4] Oleh karena itu, perkembangan teknologi informasi tidak hanya menuntut inovasi dalam bidang ekonomi dan komunikasi, tetapi juga menuntut kesiapan sistem hukum dalam mengantisipasi dan menanggulangi berbagai bentuk kejahatan digital yang terus berkembang.

Salah satu bentuk *cybercrime* yang semakin sering terjadi dalam praktik adalah tindak pidana *phishing*. *Phishing* merupakan bentuk penipuan elektronik yang bertujuan untuk memperoleh informasi sensitif milik korban seperti *username*, *password*, dan data kartu kredit dengan cara menyamar sebagai entitas yang terpercaya melalui komunikasi elektronik.[5] Modus operandi *phishing* berkembang sangat cepat seiring dengan meningkatnya penggunaan layanan digital oleh masyarakat. Pelaku biasanya memanfaatkan teknik rekayasa sosial (*social engineering*) dengan mengirimkan tautan palsu, email penipuan, atau membuat situs web tiruan yang menyerupai layanan resmi suatu institusi. Ketika korban mengakses tautan tersebut, mereka secara tidak sadar memasukkan data pribadi yang kemudian digunakan oleh pelaku untuk melakukan berbagai tindakan kejahatan, seperti pencurian identitas, pembobolan rekening bank, atau penyalahgunaan informasi keuangan.

Perkembangan modus *phishing* semakin kompleks dengan munculnya berbagai perangkat lunak khusus yang dikenal sebagai *phishing toolkit*. Perangkat ini memungkinkan pelaku kejahatan untuk membuat situs web palsu secara massal dengan tampilan yang menyerupai situs resmi lembaga keuangan atau layanan digital lainnya.[6] Dengan memanfaatkan perangkat tersebut, pelaku dapat menyasar ribuan korban dalam waktu singkat dengan tingkat anonimitas yang tinggi. Fenomena ini menunjukkan bahwa kejahatan *phishing* tidak lagi dilakukan secara sederhana oleh individu dengan kemampuan teknologi

---

3 Robert Moore, *Investigating High-Technology Computer Crime. Cybercrime: Investigating High-Technology Computer Crime* (Abingdon, 2014).

4 Barda Nawawi Arief, *Tindak Pidana Mayantara (Cyber Crime)* (RajaGrafindo Persada, 2006).

5 Dian Rachmawati, "Phishing Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," *Jurnal Saintkom* 13, no. 3 (2014).

6 Erry Fitrya Primadhany dkk., *Pengantar Hukum Siber Indonesia* (Sada Kurnia Pustaka, 2025).

terbatas, tetapi telah berkembang menjadi aktivitas kriminal yang terorganisasi dengan memanfaatkan teknologi digital secara sistematis.

Secara normatif, sistem hukum Indonesia sebenarnya telah memiliki berbagai instrumen hukum yang dapat digunakan untuk menjerat pelaku *phishing*. Pengaturan tersebut antara lain terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mengatur berbagai bentuk perbuatan yang dilarang dalam sistem elektronik, seperti akses ilegal, manipulasi data elektronik, dan penyalahgunaan informasi elektronik. Selain itu, ketentuan mengenai penipuan dalam Kitab Undang-Undang Hukum Pidana juga dapat digunakan untuk menjerat pelaku kejahatan berbasis penipuan digital. Dalam beberapa kasus, ketentuan mengenai tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 juga digunakan untuk menindak pelaku yang memanfaatkan hasil kejahatan *phishing* melalui mekanisme pencucian uang.

Meskipun kerangka regulasi tersebut secara normatif terlihat cukup memadai, praktik penegakan hukum terhadap tindak pidana *phishing* masih menghadapi berbagai kendala. Salah satu persoalan utama adalah belum adanya pengaturan yang secara khusus dan eksplisit mengatur mengenai *phishing* sebagai bentuk tindak pidana tersendiri. Akibatnya, aparat penegak hukum sering kali harus menafsirkan berbagai ketentuan yang ada untuk menjerat pelaku berdasarkan perbuatan yang dilakukan. Kondisi ini dapat menimbulkan ketidakpastian hukum, baik bagi aparat penegak hukum maupun bagi korban kejahatan digital. Selain itu, perlindungan hukum terhadap korban *phishing* juga masih relatif terbatas karena belum adanya mekanisme pemulihan kerugian yang secara jelas diatur dalam sistem hukum pidana Indonesia.[7]

Dalam konteks akademik, berbagai penelitian sebelumnya telah mencoba menjelaskan fenomena *cybercrime* dan mekanisme pertanggungjawaban pidana terhadap pelaku kejahatan digital. Widodo menjelaskan bahwa *cybercrime* merupakan aktivitas yang dilakukan oleh individu atau kelompok dengan memanfaatkan komputer sebagai sarana maupun sebagai objek kejahatan yang bertentangan dengan peraturan perundang-undangan.[8] Sementara itu, Budi Suhariyanto menegaskan bahwa *phishing* merupakan salah satu bentuk penipuan digital yang memanfaatkan teknik rekayasa sosial untuk memperoleh

---

[7] Rafi Septia Budianto Pansariadi dan Noenik Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (2023): 287–98, https://doi.org/10.37893/jbh.v12i2.605.

[8] Edmon Makarim, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)* (Raja Grafindo Persada, 2005).

informasi sensitif milik korban melalui media elektronik.[9] Dalam perspektif hukum pidana, pertanggungjawaban pidana terhadap pelaku kejahatan digital tetap didasarkan pada prinsip umum bahwa seseorang hanya dapat dipidana apabila memenuhi unsur tindak pidana dan memiliki kesalahan (*schuld*) atas perbuatan yang dilakukannya.

Di sisi lain, teori sistem hukum yang dikemukakan oleh Lawrence M. Friedman memberikan kerangka analisis yang penting dalam memahami efektivitas penegakan hukum terhadap kejahatan siber. Friedman menjelaskan bahwa keberhasilan penegakan hukum sangat dipengaruhi oleh tiga unsur utama, yaitu struktur hukum, substansi hukum, dan budaya hukum.[10] Struktur hukum berkaitan dengan institusi dan aparat penegak hukum, substansi hukum berkaitan dengan peraturan perundang-undangan yang berlaku, sedangkan budaya hukum berkaitan dengan sikap dan perilaku masyarakat terhadap hukum. Dalam konteks penanggulangan *phishing*, ketiga unsur tersebut harus berjalan secara sinergis agar sistem hukum mampu memberikan perlindungan yang efektif bagi masyarakat.

Meskipun berbagai kajian akademik telah membahas *cybercrime* dan pertanggungjawaban pidana pelaku kejahatan digital, masih terdapat kesenjangan penelitian yang berkaitan dengan penerapan norma hukum terhadap kasus *phishing* secara konkret dalam praktik peradilan. Banyak penelitian lebih menekankan pada aspek konseptual atau regulasi hukum secara umum, sementara kajian yang menganalisis secara mendalam putusan pengadilan terkait tindak pidana *phishing* masih relatif terbatas. Padahal, analisis terhadap putusan pengadilan sangat penting untuk memahami bagaimana norma hukum diterapkan oleh hakim dalam memutus perkara serta bagaimana pertanggungjawaban pidana pelaku kejahatan siber ditafsirkan dalam praktik peradilan.[11]

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana atas kejahatan siber berbasis *phishing* dalam sistem hukum Indonesia serta mengkaji penerapan norma hukum dalam Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb sebagai studi kasus. Penelitian ini memiliki kebaruan pada pendekatan analisis yang mengintegrasikan kajian normatif mengenai pengaturan hukum *cybercrime* dengan analisis yuridis terhadap putusan pengadilan yang berkaitan dengan tindak pidana *phishing*. Dengan demikian, penelitian ini diharapkan dapat

[9] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime)* (Raja Grafindo Persada, 2014).

[10] Lawrence M. Friedman, *Sistem Hukum Perspektif Ilmu Sosial* (Nusa Media, 2009).

[11] Listiyono dkk., "Perlindungan Hukum Nasabah Atas Kerugian Transaksi Pinjaman Online Ilegal Dihubungkan Dengan Undang-Undang Informasi dan Transaksi Elektronik."

memberikan kontribusi akademik dalam pengembangan kajian hukum pidana siber serta memberikan rekomendasi bagi penguatan sistem penegakan hukum terhadap kejahatan digital di Indonesia.

B. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum yang bersifat yuridis normatif, yaitu penelitian yang berfokus pada kajian terhadap norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, serta putusan pengadilan yang relevan dengan permasalahan yang diteliti. Pendekatan ini digunakan untuk menelaah secara komprehensif pengaturan hukum mengenai tindak pidana *phishing* dalam sistem hukum Indonesia serta untuk menganalisis penerapan norma hukum tersebut dalam praktik peradilan. Penelitian ini juga bersifat deskriptif kualitatif, yang berarti bahwa hasil penelitian disajikan dalam bentuk uraian sistematis dan analitis melalui penjelasan naratif terhadap konsep, prinsip, dan aturan hukum yang berkaitan dengan pertanggungjawaban pidana atas kejahatan siber berbasis *phishing*. Melalui pendekatan ini, penelitian berupaya menggambarkan secara jelas bagaimana pengaturan hukum yang berlaku serta bagaimana norma tersebut diinterpretasikan dalam putusan pengadilan yang menjadi objek kajian penelitian.

Dalam penelitian hukum normatif, analisis dilakukan dengan menelaah berbagai sumber hukum yang relevan untuk menjawab permasalahan penelitian. Pendekatan utama yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif, yaitu pendekatan yang menempatkan hukum sebagai sistem norma yang dianalisis berdasarkan ketentuan peraturan perundang-undangan serta doktrin hukum yang berkembang dalam literatur akademik.[12] Selain itu, penelitian ini juga menggunakan beberapa pendekatan pendukung, yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan digunakan untuk menelaah berbagai ketentuan normatif yang berkaitan dengan tindak pidana *phishing*, khususnya dalam Undang-Undang Informasi dan Transaksi Elektronik serta peraturan hukum pidana lainnya. Pendekatan konseptual digunakan untuk mengkaji teori-teori hukum yang berkaitan dengan *cybercrime* dan pertanggungjawaban pidana. Sementara itu, pendekatan kasus digunakan untuk menganalisis penerapan norma hukum dalam praktik peradilan melalui studi terhadap putusan pengadilan yang relevan dengan tindak pidana *phishing*.

---

[12] Amirudin Amirudin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum* (Raja Grafindo Persada, 2004).

Pengumpulan data dalam penelitian ini dilakukan melalui metode penelitian kepustakaan (*library research*), yaitu dengan mengkaji berbagai bahan hukum yang relevan dengan objek penelitian. Metode ini digunakan karena penelitian hukum normatif pada dasarnya bertumpu pada analisis terhadap sumber-sumber hukum tertulis. Bahan hukum yang dikumpulkan meliputi peraturan perundang-undangan, literatur akademik, jurnal ilmiah, serta putusan pengadilan yang berkaitan dengan pertanggungjawaban pidana atas kejahatan siber berbasis *phishing*. Seluruh bahan hukum tersebut kemudian dianalisis secara sistematis untuk memperoleh pemahaman yang komprehensif mengenai konstruksi hukum yang mengatur tindak pidana *phishing* dalam sistem hukum Indonesia. Proses analisis dilakukan secara kualitatif dengan menelaah substansi norma hukum serta interpretasi yang berkembang dalam praktik hukum.

Sumber data dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer merupakan sumber hukum yang bersifat mengikat dan menjadi dasar hukum positif dalam sistem hukum Indonesia. Dalam penelitian ini, bahan hukum primer meliputi berbagai peraturan perundang-undangan yang berkaitan dengan kejahatan siber, antara lain 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 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana, serta Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Selain itu, penelitian ini juga menggunakan Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb sebagai objek studi kasus untuk menganalisis penerapan norma hukum dalam praktik peradilan.

Bahan hukum sekunder terdiri atas berbagai literatur hukum yang memberikan penjelasan dan interpretasi terhadap bahan hukum primer, seperti buku teks hukum pidana, jurnal ilmiah, artikel akademik, serta pendapat para ahli hukum yang relevan dengan kajian *cybercrime* dan pertanggungjawaban pidana. Sementara itu, bahan hukum tersier digunakan sebagai sumber penunjang yang membantu memahami konsep dan terminologi hukum yang digunakan dalam penelitian, seperti kamus hukum dan sumber referensi lainnya. Seluruh bahan hukum tersebut dianalisis secara normatif kualitatif melalui teknik analisis isi hukum (*legal content analysis*), yaitu dengan menelaah isi peraturan perundang-undangan, doktrin hukum, dan putusan pengadilan yang berkaitan dengan permasalahan penelitian, kemudian menarik kesimpulan secara sistematis dan argumentatif.

C. HASIL PENELITIAN DAN PEMBAHASAN

Para Pihak dalam Perkara

Perkara tindak pidana siber yang dianalisis dalam penelitian ini melibatkan beberapa pihak yang memiliki peran berbeda dalam proses peradilan pidana. Pertama adalah Jaksa Penuntut Umum (JPU) yang bertindak sebagai pihak yang mengajukan dakwaan terhadap terdakwa berdasarkan alat bukti yang diperoleh dalam proses penyidikan. Dalam perkara ini, Jaksa Penuntut Umum mengajukan dua dakwaan utama. Dakwaan pertama adalah pelanggaran terhadap Pasal 34 ayat (1) huruf a jo. Pasal 50 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mengatur mengenai larangan memproduksi, menjual, atau menyediakan perangkat keras atau perangkat lunak komputer yang secara khusus dirancang untuk memfasilitasi tindak pidana siber. Dakwaan kedua adalah pelanggaran terhadap Pasal 3 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang yang berkaitan dengan pengelolaan harta kekayaan yang berasal dari tindak pidana.[13]

Pihak kedua dalam perkara ini adalah terdakwa Riswanda Noor Saputra, seorang pemuda berusia sekitar 22 tahun yang berdomisili di Kota Banjarbaru. Meskipun tidak memiliki pendidikan formal di bidang teknologi informasi, terdakwa mempelajari pemrograman secara autodidak melalui internet. Pengetahuan tersebut kemudian digunakan untuk mengembangkan perangkat lunak yang berfungsi sebagai *phishing toolkit* yang diberi nama 16Shop. Dalam proses persidangan, terdakwa didampingi oleh penasihat hukum yang berusaha membangun argumentasi bahwa terdakwa tidak secara langsung melakukan tindak pidana *phishing*, melainkan hanya membuat perangkat lunak yang kemudian digunakan oleh pihak lain. Selain itu, persidangan juga menghadirkan dua saksi ahli, yaitu ahli di bidang teknologi informasi dan transaksi elektronik serta ahli di bidang analisis transaksi keuangan dan kripto yang memberikan keterangan terkait karakteristik teknis perangkat lunak dan aliran dana yang berkaitan dengan tindak pidana tersebut.

Objek Perkara

Objek utama dalam penelitian ini adalah Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb yang berkaitan dengan tindak pidana siber berbasis *phishing*. Dalam perkara tersebut, terdakwa didakwa sebagai pengembang dan distributor perangkat lunak *phishing toolkit* bernama 16Shop yang digunakan oleh berbagai pihak untuk melakukan pencurian data

[13] Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb.

pribadi secara ilegal. Perangkat lunak tersebut dirancang sedemikian rupa sehingga mampu meniru tampilan situs resmi berbagai layanan digital seperti Apple, Amazon, dan PayPal. Melalui sistem tersebut, pelaku kejahatan dapat memperoleh data login, informasi kartu kredit, serta data pribadi korban yang kemudian dapat digunakan untuk berbagai tindakan kejahatan lanjutan.

Dalam dakwaan yang diajukan oleh Jaksa Penuntut Umum, terdakwa dianggap telah memproduksi dan mendistribusikan perangkat lunak yang secara khusus dirancang untuk memfasilitasi tindak pidana siber. Selain itu, terdakwa juga didakwa melakukan tindak pidana pencucian uang karena menerima dan menyamarkan hasil penjualan perangkat lunak tersebut melalui berbagai mekanisme transaksi keuangan, termasuk melalui rekening bank dan mata uang kripto. Dengan demikian, perkara ini tidak hanya berkaitan dengan kejahatan siber dalam bentuk pencurian data, tetapi juga mencakup aspek kejahatan keuangan yang dilakukan untuk menyembunyikan asal-usul hasil kejahatan.[14]

Kronologi dan Duduk Perkara

Kasus ini bermula ketika Direktorat Tindak Pidana Siber Bareskrim Polri menerima informasi dari National Central Bureau (NCB) Interpol serta Kedutaan Besar Amerika Serikat mengenai keberadaan situs web 16.shop yang diduga menyediakan layanan *phishing toolkit*. Informasi tersebut menunjukkan bahwa situs tersebut digunakan sebagai layanan *phishing as a service* yang memungkinkan pelaku kejahatan siber melakukan penipuan dengan menargetkan pengguna layanan digital seperti Apple, Amazon, PayPal, dan American Express. Perangkat tersebut dapat digunakan untuk mengirimkan email *phishing* dalam berbagai bahasa serta mengarahkan korban ke halaman login palsu yang dirancang untuk mencuri informasi sensitif.

Melalui proses investigasi digital, aparat penegak hukum melakukan analisis terhadap domain situs, aktivitas transaksi keuangan, serta jejak digital yang berkaitan dengan pengelolaan situs tersebut. Hasil penelusuran menunjukkan bahwa situs tersebut terhubung dengan terdakwa Riswanda Noor Saputra yang berdomisili di Kota Banjarbaru. Dari catatan transaksi keuangan yang ditemukan, penyidik menemukan adanya aliran dana dalam jumlah besar yang masuk ke rekening bank terdakwa serta transaksi mata uang kripto yang terkait dengan penjualan perangkat lunak tersebut. Dana yang diperoleh kemudian digunakan untuk berbagai keperluan pribadi, termasuk pembelian kendaraan dan barang elektronik.

[14] Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb.

Dalam pemeriksaan lebih lanjut, diketahui bahwa terdakwa merupakan pengembang utama perangkat lunak 16Shop. Ia membuat skrip perangkat lunak tersebut dengan menggunakan bahasa pemrograman seperti HTML, PHP, JavaScript, dan CSS. Terdakwa juga memanfaatkan teknik inspect element untuk menyalin tampilan situs resmi sehingga halaman yang dihasilkan terlihat identik dengan situs asli. Setelah perangkat lunak tersebut selesai dikembangkan dan diuji, terdakwa kemudian menjualnya kepada berbagai pembeli melalui situs 16.shop dengan harga sekitar satu juta rupiah per lisensi. Pembayaran dilakukan melalui transfer bank maupun melalui mata uang kripto Bitcoin yang kemudian ditukarkan menjadi rupiah.[15]

Fakta Persidangan dan Pembuktian

Dalam persidangan, majelis hakim mempertimbangkan berbagai alat bukti yang diajukan oleh penuntut umum, termasuk keterangan saksi, keterangan ahli, dokumen elektronik, serta barang bukti digital yang diperoleh dari perangkat milik terdakwa. Dari hasil pemeriksaan forensik digital, ditemukan berbagai file yang berkaitan dengan operasi perangkat lunak *phishing*, seperti skrip program, database yang berisi data korban, serta catatan transaksi pembayaran dari pembeli perangkat lunak tersebut. Temuan ini memperkuat dugaan bahwa perangkat lunak yang dikembangkan oleh terdakwa memang dirancang secara khusus untuk melakukan pencurian data pribadi melalui metode *phishing*.

Selain itu, keterangan ahli di bidang teknologi informasi menjelaskan bahwa perangkat lunak yang dikembangkan oleh terdakwa bukan sekadar tampilan tiruan situs web, melainkan sebuah sistem lengkap yang mampu menangkap dan menyimpan data korban secara otomatis. Hal ini menunjukkan bahwa perangkat lunak tersebut memiliki fungsi yang secara langsung memfasilitasi terjadinya tindak pidana akses ilegal terhadap data elektronik. Dengan demikian, unsur perbuatan memproduksi perangkat lunak yang dirancang untuk memfasilitasi tindak pidana sebagaimana diatur dalam Pasal 34 ayat (1) huruf a Undang-Undang ITE dinilai terpenuhi.

Di sisi lain, keterangan ahli dari Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) menjelaskan bahwa transaksi keuangan yang dilakukan oleh terdakwa menunjukkan pola yang mencurigakan. Analisis terhadap rekening bank dan transaksi kripto menunjukkan adanya aliran dana yang tidak sesuai dengan profil pekerjaan terdakwa. Selain itu, ditemukan pula bahwa terdakwa menukarkan mata uang kripto melalui jalur yang tidak resmi untuk menghindari deteksi oleh lembaga keuangan. Pola transaksi tersebut

[15] Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb.

menunjukkan adanya upaya untuk menyamarkan asal-usul dana yang diperoleh dari penjualan perangkat lunak *phishing*.

Analisis Penerapan Pasal dalam Putusan

Majelis hakim dalam perkara ini mempertimbangkan beberapa ketentuan hukum yang diajukan oleh penuntut umum, termasuk Pasal 35 jo. Pasal 51 Undang-Undang ITE serta Pasal 34 jo. Pasal 50 Undang-Undang ITE. Setelah mempertimbangkan fakta persidangan dan keterangan ahli, majelis hakim menilai bahwa perbuatan terdakwa lebih tepat dikualifikasikan sebagai perbuatan memproduksi perangkat lunak yang dirancang untuk memfasilitasi tindak pidana sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf a. Hal ini karena terdakwa tidak hanya membuat tampilan situs palsu, tetapi juga mengembangkan sistem perangkat lunak yang secara aktif menjalankan fungsi pencurian data korban.

Selain itu, majelis hakim juga menilai bahwa unsur tindak pidana pencucian uang sebagaimana diatur dalam Pasal 3 Undang-Undang TPPU telah terpenuhi. Hal ini didasarkan pada fakta bahwa terdakwa menerima pembayaran dari penjualan perangkat lunak *phishing*, kemudian menukarkan mata uang kripto tersebut menjadi rupiah dan menggunakan dana tersebut untuk berbagai transaksi pribadi.[16] Pola transaksi tersebut menunjukkan adanya upaya untuk menyembunyikan atau menyamarkan asal-usul dana yang diperoleh dari tindak pidana.

Putusan Majelis Hakim

Berdasarkan seluruh fakta hukum yang terungkap dalam persidangan, majelis hakim menyatakan bahwa terdakwa Riswanda Noor Saputra terbukti secara sah dan meyakinkan melakukan tindak pidana memproduksi perangkat lunak yang dirancang untuk memfasilitasi tindak pidana sebagaimana diatur dalam Pasal 34 ayat (1) huruf a jo. Pasal 50 Undang-Undang ITE. Selain itu, terdakwa juga dinyatakan terbukti melakukan tindak pidana pencucian uang sebagaimana diatur dalam Pasal 3 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Sebagai konsekuensi dari putusan tersebut, majelis hakim menjatuhkan pidana kepada terdakwa berupa pidana penjara selama dua tahun enam bulan serta denda sebesar Rp500.000.000 dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama tiga bulan. Selain itu, berbagai barang bukti yang berkaitan dengan tindak pidana tersebut, termasuk perangkat elektronik, kendaraan, serta akun digital yang digunakan dalam operasi kejahatan siber, dirampas untuk negara. Putusan ini

[16] Pansariadi dan Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya."

menunjukkan bahwa pengadilan memandang serius peran pengembang perangkat lunak dalam memfasilitasi kejahatan siber dan menegaskan bahwa pertanggungjawaban pidana tidak hanya berlaku bagi pelaku langsung kejahatan, tetapi juga bagi pihak yang menyediakan sarana yang memungkinkan terjadinya kejahatan tersebut.

Konstruksi Pertanggungjawaban Pidana terhadap Kejahatan *Phishing* dalam Sistem Hukum Indonesia

Phishing merupakan salah satu bentuk kejahatan siber yang berkembang pesat seiring dengan kemajuan teknologi informasi dan komunikasi. Dalam literatur hukum siber, *phishing* dipahami sebagai tindakan memperoleh data pribadi korban dengan cara menyamar sebagai entitas yang sah atau terpercaya melalui media komunikasi elektronik seperti surat elektronik, pesan instan, maupun situs web tiruan.[17] Metode ini pada dasarnya merupakan bentuk penipuan berbasis rekayasa sosial (*social engineering*) yang memanfaatkan kepercayaan korban untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau data identitas lainnya. Informasi tersebut kemudian dapat dimanfaatkan secara langsung oleh pelaku untuk melakukan transaksi ilegal ataupun diperjualbelikan kepada pihak lain.

Dalam praktiknya, *phishing* dilakukan melalui tahapan yang sistematis. Pelaku terlebih dahulu melakukan pengumpulan informasi mengenai target melalui berbagai platform digital seperti media sosial atau jaringan profesional. Informasi tersebut digunakan untuk membangun skenario komunikasi yang meyakinkan sehingga korban mempercayai pesan atau tautan yang dikirimkan oleh pelaku. Selanjutnya korban diarahkan untuk mengakses halaman web palsu atau memasukkan data pribadi melalui formulir elektronik yang tampak autentik. Proses ini menunjukkan bahwa *phishing* merupakan kombinasi antara manipulasi psikologis terhadap korban dan manipulasi teknis terhadap sistem elektronik.[18]

Dalam perspektif hukum pidana, suatu perbuatan dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur-unsur perbuatan melawan hukum, kesalahan, serta ancaman pidana yang diatur dalam undang-undang. Unsur kesalahan dalam hukum pidana umumnya terdiri dari dua bentuk, yaitu kesengajaan (*dolus*) dan kealpaan (*culpa*). Dalam konteks kejahatan *phishing*, unsur kesengajaan relatif mudah dibuktikan karena pelaku secara sadar merancang sistem atau skenario yang bertujuan untuk memperoleh data pribadi

---

[17] Maskun Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Kencana Prenada Media Group, 2013).

[18] Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional* (Refika Aditama, 2015).

korban secara ilegal. Hal ini menunjukkan bahwa *phishing* merupakan kejahatan yang memerlukan tingkat pengetahuan teknis tertentu serta perencanaan yang matang.[19]

Dalam hukum positif Indonesia, istilah *phishing* tidak diatur secara eksplisit sebagai jenis tindak pidana tersendiri. Namun demikian, perbuatan yang terkandung dalam praktik *phishing* sebenarnya telah diatur dalam berbagai ketentuan hukum pidana, baik dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Dalam hal ini, sistem hukum Indonesia menggunakan pendekatan kombinasi antara hukum pidana umum dan hukum pidana khusus dalam menanggulangi kejahatan siber.[20]

Pendekatan tersebut didasarkan pada prinsip bahwa hukum pidana tidak selalu mengatur secara spesifik setiap bentuk kejahatan baru, melainkan lebih menekankan pada unsur-unsur perbuatan yang dilakukan oleh pelaku. Oleh karena itu, untuk menentukan apakah suatu perbuatan dapat dipidana, perlu dilakukan analisis terhadap unsur-unsur delik yang terdapat dalam peraturan perundang-undangan yang berlaku.[21] Dalam konteks *phishing*, unsur-unsur tindak pidana yang relevan dapat ditemukan dalam beberapa ketentuan hukum yang mengatur mengenai penipuan, manipulasi informasi elektronik, akses ilegal terhadap sistem elektronik, serta pemindahan data elektronik tanpa hak.

Pertama, *phishing* dapat dikualifikasikan sebagai bentuk penipuan sebagaimana diatur dalam Pasal 378 KUHP. Unsur utama dalam pasal ini adalah adanya maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan tipu muslihat atau rangkaian kebohongan. Dalam praktik *phishing*, penggunaan situs web palsu, email tiruan, maupun akun digital yang menyerupai institusi resmi merupakan bentuk nyata dari tipu muslihat yang digunakan untuk menggerakkan korban menyerahkan data pribadi atau akses ke sistem elektronik. Dengan demikian, unsur penipuan sebagaimana diatur dalam KUHP dapat terpenuhi apabila tindakan tersebut mengakibatkan korban mengalami kerugian atau kehilangan akses terhadap data atau asetnya (Andi Hamzah, 2017).

Kedua, *phishing* juga mengandung unsur manipulasi informasi elektronik. Dalam tahap ini, pelaku menciptakan atau memodifikasi informasi elektronik sehingga tampak seolah-olah berasal dari sumber yang sah. Perbuatan tersebut

---

19 Moeljatno Moeljatno, *Asas-Asas Hukum Pidana* (Rineka Cipta, 2008).

20 Arief, *Tindak Pidana Mayantara (Cyber Crime)*.

21 Romli Atmasasmita, *Pengantar Hukum Pidana Internasional dan Nasional* (Refika Aditama, 2010).

dapat dijerat dengan Pasal 35 jo. Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang mengatur tentang penciptaan atau manipulasi informasi elektronik agar dianggap sebagai data yang autentik. Unsur utama dalam pasal ini adalah adanya kesengajaan untuk menciptakan informasi elektronik palsu yang berpotensi menyesatkan pihak lain.

Ketiga, tahap lanjutan dalam *phishing* biasanya melibatkan akses ilegal terhadap sistem elektronik korban. Setelah memperoleh data autentikasi korban, pelaku dapat menggunakan informasi tersebut untuk masuk ke dalam sistem elektronik tanpa izin. Perbuatan ini memenuhi unsur akses tanpa hak sebagaimana diatur dalam Pasal 30 ayat (3) jo. Pasal 46 ayat (3) Undang-Undang ITE. Dalam konteks ini, meskipun korban secara sadar memasukkan data pribadi ke dalam sistem palsu, tindakan tersebut tetap dikategorikan sebagai akses ilegal karena persetujuan korban diperoleh melalui tipu muslihat. Dengan demikian, unsur melawan hukum tetap terpenuhi.

Keempat, *phishing* juga dapat melibatkan perbuatan memindahkan atau mentransfer informasi elektronik milik korban kepada pihak yang tidak berhak. Perbuatan ini diatur dalam Pasal 32 ayat (2) jo. Pasal 48 ayat (2) Undang-Undang ITE yang melarang pemindahan atau transfer informasi elektronik tanpa hak. Dalam banyak kasus *phishing*, data yang diperoleh dari korban tidak hanya digunakan oleh pelaku, tetapi juga diperjualbelikan di pasar gelap atau digunakan oleh pihak lain untuk melakukan kejahatan lanjutan. Oleh karena itu, unsur pemindahan informasi elektronik secara melawan hukum dapat dianggap terpenuhi.[22]

Meskipun secara normatif berbagai ketentuan hukum telah tersedia untuk menjerat pelaku *phishing*, tantangan utama dalam praktik terletak pada proses penegakan hukum. Kejahatan *phishing* memiliki karakter lintas batas, menggunakan teknologi yang kompleks, serta melibatkan alat bukti elektronik yang memerlukan keahlian khusus untuk dianalisis. Proses penyelidikan dan penyidikan sering kali memerlukan waktu yang panjang karena aparat penegak hukum harus melakukan analisis terhadap log server, alamat IP, serta berbagai jejak digital lainnya yang dapat dengan mudah dihapus atau disamarkan oleh pelaku.[23]

Selain itu, keterbatasan sumber daya manusia yang memiliki keahlian di bidang forensik digital juga menjadi kendala dalam penanganan kasus kejahatan siber. Dalam banyak kasus, aparat penegak hukum masih menghadapi keterbatasan dalam hal peralatan laboratorium forensik digital serta kemampuan teknis untuk mengidentifikasi bukti elektronik yang relevan.

---

[22] Edmon Makarim, *Pengantar Hukum Telematika* (Raja Grafindo Persada, 2014).
[23] Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*.

Kondisi ini menunjukkan bahwa efektivitas penegakan hukum terhadap kejahatan siber tidak hanya bergantung pada keberadaan regulasi, tetapi juga pada kapasitas institusi penegak hukum dalam memanfaatkan teknologi secara optimal.

Analisis Pertimbangan Hakim dalam Putusan Nomor 85/Pid.Sus/2022/PN Banjarbaru

Pertimbangan hakim merupakan bagian yang sangat penting dalam suatu putusan pengadilan pidana karena pada bagian ini hakim menilai fakta-fakta yang terungkap di persidangan dan menghubungkannya dengan ketentuan hukum yang berlaku. Pertimbangan tersebut mencerminkan proses penalaran hukum (*judicial reasoning*) yang digunakan oleh hakim untuk menentukan apakah unsur-unsur tindak pidana yang didakwakan kepada terdakwa telah terpenuhi atau tidak.[24]

Dalam perkara yang dianalisis, majelis hakim terlebih dahulu menilai fakta hukum yang berkaitan dengan identitas dan peran terdakwa. Berdasarkan alat bukti yang diajukan di persidangan, hakim menyimpulkan bahwa terdakwa merupakan pihak yang secara aktif membuat, mengembangkan, dan menjual perangkat lunak *phishing toolkit* bernama 16Shop. Fakta ini diperkuat oleh keterangan saksi, keterangan terdakwa, serta barang bukti berupa server, akun penjualan, dan panel lisensi yang dikendalikan oleh terdakwa. Dengan demikian, hakim menilai bahwa terdakwa bukan sekadar pengguna atau perantara, melainkan pelaku utama yang memproduksi sarana kejahatan siber.

Selanjutnya, hakim mempertimbangkan fungsi teknis perangkat lunak yang dibuat oleh terdakwa. Berdasarkan hasil pemeriksaan forensik digital dan keterangan ahli teknologi informasi, perangkat lunak 16Shop merupakan sistem yang terdiri dari berbagai komponen teknis seperti skrip HTML, PHP, JavaScript, sistem penyimpanan data, serta fitur pengalihan otomatis yang memungkinkan pencurian data korban secara sistematis. Sistem tersebut juga dilengkapi dengan fitur anti-bot dan mekanisme penyamaran yang bertujuan untuk menghindari deteksi oleh sistem keamanan digital. Berdasarkan fakta tersebut, majelis hakim menyimpulkan bahwa perangkat lunak tersebut tidak memiliki fungsi legal yang wajar dan secara khusus dirancang untuk memfasilitasi tindak pidana *phishing*.[25]

Dalam menilai unsur kesengajaan, hakim mempertimbangkan bahwa terdakwa mengetahui tujuan penggunaan perangkat lunak tersebut serta secara aktif menambahkan berbagai fitur yang memperkuat kemampuan sistem untuk melakukan pencurian data. Terdakwa juga memperoleh keuntungan ekonomi

[24] Sudikno Mertokusumo, *Penemuan Hukum* (Liberty, 2009).

[25] Listiyono dkk., "Perlindungan Hukum Nasabah Atas Kerugian Transaksi Pinjaman Online Ilegal Dihubungkan Dengan Undang-Undang Informasi dan Transaksi Elektronik."

dari penjualan perangkat lunak tersebut kepada berbagai pembeli. Fakta-fakta ini menunjukkan bahwa terdakwa memiliki pengetahuan dan kehendak terhadap akibat dari perbuatannya, sehingga unsur kesengajaan sebagai maksud (*dolus directus*) dianggap telah terpenuhi.

Majelis hakim juga menilai alat bukti yang diajukan oleh penuntut umum, termasuk bukti transaksi keuangan, tangkapan layar situs web, data server, serta catatan transaksi mata uang kripto yang menunjukkan adanya aliran dana dari hasil penjualan perangkat lunak *phishing*. Bukti-bukti tersebut menunjukkan bahwa terdakwa menerima pembayaran melalui rekening bank maupun melalui mata uang kripto yang kemudian ditukarkan menjadi rupiah. Berdasarkan analisis terhadap pola transaksi tersebut, hakim menyimpulkan bahwa terdakwa telah melakukan tindakan yang memenuhi unsur tindak pidana pencucian uang sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 2010.

Dalam tahap penentuan pidana, majelis hakim mempertimbangkan keadaan yang memberatkan dan meringankan terdakwa. Keadaan yang memberatkan antara lain bahwa terdakwa telah menikmati hasil kejahatan, menggunakan kemampuan teknologinya untuk merugikan orang lain, serta perbuatannya menimbulkan keresahan masyarakat bahkan hingga lintas negara. Sementara itu, keadaan yang meringankan adalah bahwa terdakwa belum pernah dihukum sebelumnya serta mengakui kesalahannya di persidangan. Berdasarkan pertimbangan tersebut, hakim menjatuhkan pidana penjara selama dua tahun enam bulan serta denda sebesar lima ratus juta rupiah kepada terdakwa.

Secara keseluruhan, putusan tersebut menunjukkan bahwa sistem hukum Indonesia telah mampu menjerat pelaku kejahatan *phishing* melalui kombinasi ketentuan dalam Undang-Undang ITE dan Undang-Undang Tindak Pidana Pencucian Uang. Namun demikian, perkembangan teknologi yang semakin pesat menuntut adanya pembaruan regulasi yang lebih komprehensif agar sistem hukum dapat merespons berbagai bentuk kejahatan siber secara lebih efektif. Selain itu, peningkatan kapasitas aparat penegak hukum di bidang teknologi informasi dan forensik digital juga menjadi faktor penting dalam memastikan keberhasilan penegakan hukum terhadap kejahatan siber di masa mendatang.

D. KESIMPULAN

Penelitian ini menunjukkan bahwa kejahatan siber berbasis *phishing* merupakan bentuk kejahatan digital yang memiliki kompleksitas tinggi karena memadukan manipulasi teknologi dan rekayasa sosial untuk memperoleh data pribadi korban secara ilegal. Meskipun istilah *phishing* belum diatur secara eksplisit sebagai jenis tindak pidana tersendiri dalam sistem hukum Indonesia, penelitian ini menemukan bahwa konstruksi pertanggungjawaban pidana

terhadap pelaku *phishing* tetap dapat diterapkan melalui interpretasi berbagai ketentuan yang terdapat dalam hukum pidana umum dan hukum pidana khusus. Ketentuan dalam Kitab Undang-Undang Hukum Pidana mengenai penipuan serta berbagai pasal dalam Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Tindak Pidana Pencucian Uang dapat digunakan secara komplementer untuk menjerat pelaku kejahatan digital tersebut. Dengan demikian, sistem hukum Indonesia secara normatif telah memiliki dasar hukum yang memadai untuk menindak pelaku *phishing*, meskipun masih memerlukan penguatan dari sisi regulasi dan implementasi.

Analisis terhadap Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb menunjukkan bahwa pengadilan tidak hanya menilai tindakan pelaku yang secara langsung melakukan penipuan digital, tetapi juga memperluas pertanggungjawaban pidana kepada pihak yang memproduksi atau menyediakan sarana yang secara khusus dirancang untuk memfasilitasi kejahatan siber. Dalam perkara tersebut, terdakwa dinyatakan terbukti secara sah dan meyakinkan telah memproduksi serta mendistribusikan perangkat lunak *phishing toolkit* yang digunakan oleh berbagai pihak untuk melakukan pencurian data elektronik, serta terbukti melakukan tindak pidana pencucian uang atas hasil kejahatan tersebut. Putusan ini menegaskan bahwa pengembang teknologi yang secara sadar menciptakan perangkat lunak untuk tujuan kejahatan dapat dimintai pertanggungjawaban pidana, meskipun mereka tidak secara langsung melakukan tindakan penipuan terhadap korban.

Secara akademik, penelitian ini memberikan kontribusi penting dalam pengembangan kajian hukum pidana siber di Indonesia, khususnya terkait konstruksi pertanggungjawaban pidana terhadap pelaku *phishing* serta analisis penerapan norma hukum dalam praktik peradilan. Temuan penelitian ini memperkaya literatur hukum mengenai bagaimana sistem hukum merespons perkembangan teknologi yang melahirkan bentuk-bentuk kejahatan baru di ruang digital. Selain itu, penelitian ini juga menegaskan pentingnya penguatan kapasitas aparat penegak hukum dalam bidang forensik digital serta pembaruan regulasi yang lebih komprehensif agar mampu mengantisipasi dinamika kejahatan siber yang terus berkembang. Penelitian lanjutan diperlukan untuk mengkaji lebih dalam mengenai perlindungan hukum terhadap korban *phishing*, mekanisme pemulihan kerugian korban, serta harmonisasi regulasi nasional dengan rezim hukum internasional dalam penanggulangan kejahatan siber lintas negara.

DAFTAR PUSTAKA

Amirudin, Amirudin, dan Zainal Asikin. *Pengantar Metode Penelitian Hukum*. Raja Grafindo Persada, 2004.

Arief, Barda Nawawi. *Tindak Pidana Mayantara (Cyber Crime)*. RajaGrafindo Persada, 2006.

Atmasasmita, Romli. *Pengantar Hukum Pidana Internasional dan Nasional*. Refika Aditama, 2010.

Friedman, Lawrence M. *Sistem Hukum Perspektif Ilmu Sosial*. Nusa Media, 2009.

Listiyono, Listiyono, Deny Guntara, Muhamad Abas, dan Farhan Asyahadi. "Perlindungan Hukum Nasabah Atas Kerugian Transaksi Pinjaman Online Ilegal Dihubungkan Dengan Undang-Undang Informasi dan Transaksi Elektronik." *Binamulia Hukum* 12, no. 1 (2023): 109–19. https://doi.org/10.37893/jbh.v12i1.348.

Makarim, Edmon. *Pengantar Hukum Telematika*. Raja Grafindo Persada, 2014.

Makarim, Edmon. *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*. Raja Grafindo Persada, 2005.

Maskun, Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Kencana Prenada Media Group, 2013.

Mertokusumo, Sudikno. *Penemuan Hukum*. Liberty, 2009.

Moeljatno, Moeljatno. *Asas-Asas Hukum Pidana*. Rineka Cipta, 2008.

Moore, Robert. *Investigating High-Technology Computer Crime. Cybercrime: Investigating High-Technology Computer Crime*. Abingdon, 2014.

Munir, Nudirman. *Pengantar Hukum Siber Indonesia*. Rajawali Pers, 2017.

Pansariadi, Rafi Septia Budianto, dan Noenik Soekorini. "Tindak Pidana Cyber Crime dan Penegakan Hukumnya." *Binamulia Hukum* 12, no. 2 (2023): 287–98. https://doi.org/10.37893/jbh.v12i2.605.

Primadhany, Erry Fitrya, Adwi Mulyana Hadi, Astrid Rasyid, Hanugrah Titi Habsari, dan Indira Swasri Gama Bhakti. *Pengantar Hukum Siber Indonesia*. Sada Kurnia Pustaka, 2025.

Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb.

Rachmawati, Dian. "Phishing Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber." *Jurnal Saintkom* 13, no. 3 (2014).

Rosadi, Sinta Dewi. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Refika Aditama, 2015.

Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cyber Crime)*. Raja Grafindo Persada, 2014.