PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE *PHISING* OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

SKRIPSI

Oleh:

Gibran Mahendra Dewantara

No. Mahasiswa: 19410116

PROGRAM STUDI HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2023

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE *PHISING* OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

SKRIPSI

Diajukan Untuk Memenuhi Persyaratan Guna Memperoleh Gelar Sarjana (Strata-1) pada Fakultas Hukum Universitas Islam Indonesia Yogyakarta

Oleh:

Gibran Mahendra Dewantara

No. Mahasiswa: 19410116

PROGRAM STUDI HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2023

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

Telah diperiksa dan disetujui Dosen Pembimbing Tugas Akhir untuk diajukan ke depan TIM Penguji dalam Ujian Tugas Akhir / Pendadaran

pada tanggal 20 Oktober 2023

Yogyakarta, 21 Sepetember 2023
Dosen Pembmbing Tugas Akhir,

Aroma Elmina Martha, Dr., S.H., M.H.

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

Telah Dipertahankan di Hadapan Tim Penguji
dalam Ujian Tugas Akhir / Pendadaran
pada tanggal dan Dinyatakan LULUS

Yogyakarta, 20 Oktober 2023

Tim Penguji			Tanda Tangan
1. Ketua	:	Aroma Elmina Martha, Dr., S.H., M.H.	.....
2. Anggota	:	Ayu Izza Elvany, S.H., M.H.	.....
3. Anggota	:	Fuadi Isnawan, S.H., M.H.	.....

Mengetahui:
Universitas Islam Indonesia
Fakultas Hukum
Dekan,

Prof. Dr. Budi Agus Riswandi, S.H., M.H.
N I K . 0 1 4 1 0 0 1 0 9

PERNYATAAN ORISINALITAS

ORISINALITAS KARYA TULIS ILMIAH BERUPA TUGAS AKHIR MAHASISWA FAKULTAS HUKUM UNIVERSITAS ISLAM INDONESIA

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Yang bertandatangan di bawah ini, saya :

Nama : **Gibran Mahendra Dewantara**

No.Mahasiswa: **19410116**

Adalah benar-benar Mahasiswa Fakultas Hukum Universitas Islam Indonesia Yogyakarta yang telah melakukan Penulisan Karya Tulis Ilmiah (Tugas Akhir) berupa skripsi dengan judul :

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

Karya tulis ini akan saya ajukan kepada Tim Penguji dalam Ujian Tugas Akhir/Pendadaran yang akan diselenggarakan oleh Fakultas Hukum Universitas Islam Indonesia. Sehubungan dengan hal tersebut, dengan ini saya menyatakan :

1. Bahwa karya tulis ilmiah ini adalah benar-benar karya saya sendiri dan dalam penyusunannya tunduk dan patuh terhadap kaidah, etika, dan norma-norma Penulisan sebuah karya ilmiah sesuai dengan ketentuan yang berlaku.
2. Bahwa saya menjamin hasil karya tulis ilmiah ini adalah benar-benar asli (orisinil), bebas dari unsur-unsur yang dapat dikategorikan sebagai melakukan perbuatan ‘penjiplakan karya ilmiah’ (plagiat).

3. Bahwa meskipun secara prinsip hak milik atas karya tulis ilmiah ini ada pada saya, namun demi untuk kepentingan-kepentingan yang bersifat akademik dan pengembangannya, saya memberikan kewenangan kepada perpustakaan Fakultas Hukum Universitas Islam Indonesia dan perpustakaan di lingkungan Universitas Islam Indonesia untuk mempergunakan karya tulis ilmiah saya tersebut.

Selanjutnya berkaitan dengan hal di atas (terutama pernyataan pada butir nomor 1 dan nomor 2), saya sanggup menerima sanksi baik sanksi administratif, akademik, bahkan sanksi pidana, jika saya berbukti secara kuat dan meyakinkan telah melakukan perbuatan yang menyimpang dari pernyataan saya tersebut. Saya juga akan bersikap kooperatif untuk hadir, menjawab, melakukan pembelaan terhadap hak-hak saya, di depan "Majelis" atau "Tim" Fakultas Hukum Universitas Islam Indonesia yang ditunjuk oleh pimpinan Fakultas apabila tanda-tanda plagiasi disinyalir ada atau terjadi pada karya tulis ilmiah say aini oleh pihak Fakultas Hukum Universitas Islam Indonesia.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya, dalam kondisi sehat jasmani dan rohani, dengan sadar serta tidak ada tekanan dalam bentuk apapun oleh siapa pun.

Yogyakarta, 26 September 2023

Yang membuat pernyataan,

Gibran Mahendra Dewantara

19410116

CURRICULUM VITAE

1. Nama Lengkap : Gibran Mahendra Dewantara
2. Tempat Lahir : Sleman
3. Tanggal Lahir : 16 November 2000
4. Jenis Kelamin : Laki-Laki
5. Golongan Darah : -
6. Alamat Terakhir : Gundengan Lor, Rt 01 Rw 15, Margorejo, Tempel, Sleman
7. Alamat Asal : Gundengan Lor, Rt 01 Rw 15, Margorejo, Tempel, Sleman
8. Identitas Orang Tua/Wali
   a. Ayah
      Nama lengkap : Drs.Wahyu Prihatmaka, M.M.
      Pekerjaan : Pensiunan PNS
   b. Ibu
      Nama lengkap : Erni Hastuti, A.Md.
      Pekerjaan : Wiraswasta
9. Riwayat Pendidikan
   a. SD : SD Muhammadiyah Sleman
   b. SMP : SMP N 1 Tempel
   c. SMA : SMA Muhammadiyah 1 Yogyakarta
10. Organisasi : -

Yogyakarta, 25 September 2023

Peneliti

Gibran Mahendra Dewantara

NIM.19410116

HALAMAN MOTTO

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya"
(Al-Baqarah: 286)

"Janganlah kamu bersikap lemah dan janganlah pula kamu bersedih hati, padahal kamulah orang orang yang paling tinggi derajatnya"
(Ali-Imran: 139)

"Seseorang pemenang bukanlah orang yang tidak pernah gagal, tetapi orang yang tidak pernah menyerah"
(Cristiano Ronaldo)

"Hidup yang tidak dipertaruhkan tidak akan pernah dimenangkan"

"Skripsi yang baik adalah skripsi yang selesai"

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk
Bapak dan Ibuku,
Diriku sendiri,
Kekasihku,
Dan Teman-temanku

KATA PENGANTAR

Assalamu'alaikum Warrahmatulahi Wabbarakatuh

Alhamdulillahirabbil'alamin, puji dan syukur atas rahmat, karunia, serta hidayah yang telah diberikan Allah SWT yang Maha Pengasih lagi Penyayang, karena dengan rahmat-Nya peneliti mampu menyelesaikan skripsi yang berjudul "Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyber crime* Metode *Phising* Oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta".

Penyelesaian penelitian ini merupakan kumulasi dari serangkaian upaya peneliti juga ditopang bantuan berbagai pihak dalam berbagai bentuknya. Oleh karenanya tanpa bermaksud mengurangi penghargaan dan rasa terima kasih kepada semua pihak, peneliti menghaturkan rasa terima kasih sebesar-besarnya kepada:

1. Allah SWT yang Maha Pengasih lagi Maha Penyayang yang senantiasa memberikan perlindungan dan kemudahan dalam penelitian ini.
2. Dekan Fakultas Hukum Universitas Islam Indonesia, Bapak Prof. Dr. Budi Agus Riswandi, S.H., M.Hum.
3. Aroma Elmina Martha, Dr., SH., MH., Selaku Dosen Pembimbing yang sangat baik hati meluangan waktu, tenaga, pikiran ditengah Tengah kesibukannya dan dengan penuh kesabaran serta ketulusannya dalam membimbing.
4. Bapak dan Ibu Dosen Fakultas Hukum Universitas Islam Indonesia yang telah membagikan ilmu baik tentang kehidupan ataupun tentang ilmu-ilmu hukum yang sangat bermanfaat pada penulis ke depannya.

5. Kedua orang tua penulis, Bapak Wahyu Prihatmaka, dan Ibu Erni Hastuti, yang selama ini memberikan dukungan moril dan materiil serta doa doa yang tidak putus untuk keberhasilan penulis.
6. Kakek dan Nenek, yang selalu memberikan motivasi dan mendoakan untuk kelancaran dalam proses penulisan Tugas Akhir ini.
7. Nursana'a Aprilliani Triantono selaku sahabat dekat yang selalu sabar dalam membimbing, menemani, mengingatkan, memberikan support penuh dan mendukung pada masa masa sulit dalam proses pengerjaan Tugas Akhir ini, Terima kasih banyak atas usahanya selama ini. Apapun yang terjadi kedepannya, semoga saling mendoakan
8. Sahabat kuliah penulis Athifia Nur Alfa, Salma Wahyu, Raynold Edo Mahendra, Raisa Dara Toyibah, Muhammad Farsha K, Wahyu Ridho Alfiansyah. Terimakasih banyak telah memberikan dukungan penuh, mendengarkan keluh kesah serta memberikan saran dan masukan kepada penulis.
9. Pak Anis Dwi Haryanto selaku perwakilan dari Ditreskrimsus Polda DIY yang telah meluangkan waktunya untuk menjadi narasumber pada penelitian ini.
10. Semua pihak yang telah membantu kelancara Tugas Akhir ini yang tidak bisa penulis sebutkan satu per satu
11. Terakhir yang tak kalah penting, saya ingin berterimakasih kepada diri saya sendiri yang telah berusaha dengan keras dan berjuang sejauh ini, terima kasih telah mampu mengendalikan diri dari berbagai tekanan, terimakasih telah menyelesaikan sebaik dan semaksimal mungkin, ini merupakan kebahagiaan tersendiri.

Selanjutnya, peneliti menyadari akan segala kekurangan dan keterbatasan yang ada dalam penelitian ini, seluruh kritik dan saran yang bersifat konstruktif akan peneliti hargai dan akan indahkan demi terwujudnya sebuah karya ilmiah yang mapan. Selain itu, tulisan ini peneliti harapkan agar dapat menjadi sumbangsih bagi perkembangan hukum di Indonesia ini. Demikian semoga Allah SWT meridhoi.

Yogyakarta, 25 September 2023

Peneliti

Gibran Mahendra Dewantara

NIM.19410116

DAFTAR ISI

ABSTRAK

Penelitian ini dilatar belakangi atas kasus tindak pidana *cyber crime* metode *phising* di Daerah Istimewa Yogyakarta yang mengalami kenaikan setiap tahunnya. Permasalahan yang diangkat dalam penelitian ini pertama, kendala yang dihadapi Polda DIY pada penanganan tindak pidana *cyber crime* metode *phising* dan kedua, upaya yang dilakukan Polda DIY untuk mengatasi kendala penanganan tindak pidana *cyber crime* metode *phising*. Jenis penelitian yang dilakukan oleh penulis adalah penelitian hukum empiris. Pendekatan yang digunakan dalam penelitian ini yakni pendekatan sosiologis. Objek penelitian dalam penelitian ini adalah kendala dan upaya solutif Polda DIY dalam penanganan tindak pidana *cyber crime* metode *phising*. Sumber data yang diperlukan dalam penelitian ini menggunakan data primer dan data sekunder. Hasil penelitian menyatakan bahwa terdapat lima kendala yang dialami oleh Polda DIY terkait penanganan tindak pidana *cyber crime* metode *phising*. Pertama, kurangnya sumber daya manusia dalam mengungkap tindak pidana *cyber crime* metode *phising*. Kedua, kurangnya peralatan. Ketiga, minimnya petunjuk. Keempat, sifatnya tidak terbatas. Kelima, lokasi pelaku di luar perkiraan pihak kepolisian. Upaya dan solusi atas kendala-kendala penanganan tindak pidana *cyber crime* metode *phising* oleh Polda DIY dilakukan melalui tiga cara yaitu upaya pre-emtif, upaya preventif, dan upaya represif.

Kata Kunci: Penegakan Hukum, Tindak Pidana *Cyber Crime, Phising,* Polda DIY.

BAB I

PENDAHULUAN

A. Latar Belakang

Ilmu pengetahuan dan teknologi terus berkembang yang mempengaruhi terhadap gaya hidup dan cara berpikir masyarakat menuju ke era modern di mana teknologi mempermudah aktivitas masyarakat.[1] Hal tersebut dikarenakan ilmu pengetahuan dan teknologi pada dasarnya dikembangkan untuk mempermudah hidup dan meningkatkan kualitas hidup manusia. Praktisnya perkembangan teknologi tidak hanya membawa dampak positif bagi masyarakat namun, juga dampak negatif yang tidak dapat dihindari.[2] Beberapa penelitian menunjukkan bahwa kemajuan teknologi berpengaruh signifikan terhadap peningkatan kriminalitas.[3] Peningkatan kriminalitas dari kemajuan teknologi ini berkaitan dengan ketidakpahaman, keteledoran, ketergantungan, dan kesenjangan masyarakat dalam menggunakan teknologi.[4]

Salah satu perkembangan teknologi yang paling berdampak terhadap kehidupan masyarakat yaitu teknologi informasi yang menyebabkan mudahnya pertukaran informasi, karena tidak terbatas pada ruang, jarak, dan waktu. Perkembangan

---

[1] Muhamad Danuri, Perkembangan dan Transformasi Teknologi Digital, *INFOKAM*, Edisi Nomor 2 Volume 15, 2019, hlm. 117.

[2] Eliasta Ketaren, Cybercrime, Cyber Space, dan Cyber Law, *JTM : Jurnal TIMES*, Edisi No. 02 Vol. 05 2016, hlm. 37.

[3] Widyo Pramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta, 1994, hlm. 28.

[4] *ibid.*

teknologi juga tidak terlepas dari ditemukannya internet pada akhir abad ke-20.[5] Internet merupakan jaringan yang terhubung secara internasional dari dunia digital yang terdapat dalam komputer.[6] Dengan adanya internet, maka batas-batas teritorial antara negara dapat dilampaui. Saat ini, kemudahan yang diberikan oleh internet terhadap kehidupan manusia semakin terasa. Dunia digital menyebabkan ruang dan waktu menjadi tidak terbatas. Terdapat *platform* yang menyediakan fasilitas seperti *e-mail, chatting*, *web-cam*, hingga *zoom meeting*. Sehingga komunikasi jarak jauh dengan biaya yang murah dapat terwujud dalam kehidupan saat ini.[7]

Dampak positif internet juga dirasakan pada dunia bisnis dan perbankan. Transaksi bisnis dan perbankan menjadi lebih mudah tanpa harus pergi ke bank atau dilakukan secara konvensional. Hal tersebut dikarenakan telah dikembangkan *internet banking* yang mengandalkan dunia maya. Begitu pula dengan penggunaan internet dalam penyelenggaraan pemerintahan dan pelayanan publik. Informasi menjadi lebih transparan dan tepat waktu sehingga mencegah terjadinya penyelewengan oleh pejabat publik. Kemudahan dari dimanfaatkannya internet dalam kehidupan memang sangat dirasakan oleh masyarakat saat ini. Namun, harus disadari pula bahwa internet juga dapat dimanfaatkan untuk melakukan tindak kejahatan.

---

[5] Ade Nuriadin dan Yefi Dyan Nofia Harumike, Sejarah Perkembangan dan Implikasi Internet Pada Media Massa dan Kehidupan Masyarakat, *Selasar KPI: Referensi Media Komunikasi dan Dakwah*, Edisi No. 1 Vol 1 2021, Hlm. 7.

[6] Dwi Haryadi, *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*, Penerbit Lima, Yogyakarta, 2013, hlm. 23.

[7] Ahmad M. Ramli, Tasya Safiranita Ramli, dan Ferry Gunawan, *Hukum Telematika*, Universitas Terbuka, Banten, 2020, hlm. 17.

Kriminologi sebagai ilmu yang membahas mengenai kejahatan memandang bahwa teknologi termasuk dalam faktor kriminogen.[8] Kejahatan dengan menggunakan internet sebagai sarananya disebut sebagai *cyber crime*. *Cyber crime* sendiri merupakan kejahatan yang dilakukan pada dunia maya dengan menggunakan internet sebagai media untuk menghubungkan suatu komputer dengan komputer lainnya.[9] *Cyber crime* termasuk dalam dampak negatif dari perkembangan teknologi informasi sejalan dengan perkembangan teknologi informasi, maka bentuk-bentuk dari *cyber crime* juga akan bertambah.

Bentuk-bentuk kejahatan *cyber crime* atau kejahatan di dunia maya kini hampir menyerupai kejahatan di dunia nyata seperti seorang kriminal yang melakukan kejahatan dengan melakukan pencurian dan menggunakan hal yang dicuri tersebut secara ilegal.[10] Namun, terdapat perbedaan pencurian yang dilakukan di dunia maya, di mana umumnya diawali dengan pencurian data.[9] Data yang dicuri ini kemudian digunakan untuk melakukan tindakan yang merugikan korban. Bentuk yang paling umum dari penggunaan data korban ini yakni untuk melakukan pembobolan dana di bank milik korban.[10]

---

[8] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung, 2005), hlm. 25.

[9] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bhakti, Bandung, 2003, hlm. 239.

[10] *ibid.*

[9] Alexander Anggono, Tarjo, dan Moh. Riskiyadi, Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis, *Jurnal Manajemen dan Organisasi (JMO)*, Edisi No. 3 Vol. 12 2021, hlm. 241.

[10] *ibid.*

Data yang dicuri tersebut dapat digunakan oleh pelaku kejahatan untuk melakukan pelanggaran terhadap norma kesusilaan, seperti membuka situs pornografi, prostitusi, dan lain sebagainya. Sementara bentuk kejahatan *cyber crime* dalam lingkup yang lebih luas dapat berbentuk pencurian data yang terintegrasi dalam situs pemerintah atau lembaga negara, pembajakan situs milik perusahaan, melakukan penyebaran virus, dan lain sebagainya.[11] Berdasarkan pada hasil riset yang dirilis tahun 2019 oleh perusahaan keamanan Symantec, ditemukan bahwa Indonesia berada pada urutan ke-7 di antara 157 negara sebagai negara yang mengalami ancaman *cyber crime.*[12]

Berdasarkan data tersebut maka dapat dikatakan bahwa masyarakat Indonesia masih belum mewaspadai *cyber crime*. Salah satu bentuk *cyber crime* yang harus diwaspadai oleh masyarakat yakni metode *phising*. *Cyber crime* metode *phising* adalah *password harvesting fishing* atau penipuan yang dilakukan dengan memalsukan *e-mail* atau situs sehingga seolah-olah asli dengan maksud mengelabui pengguna dan memperoleh data pribadi pengguna tersebut.[15]

Cyber crime metode *phising* memanfaatkan situs palsu atau *e-mail* palsu untuk memperoleh data pengguna internet yang dituju. Pelaku *cyber crime* metode *phising* yang disebut sebagai *pisher* seringkali mengelabui pengguna internet dengan

[11] Andi Hamzah, *Aspek-Aspek Pidana dibidang Komputer*, Sinar Grafika, Jakarta, 1992, hlm. 10.
[12] Symantec, *Internet Security Threat Report Volume 24 February 2019*, California, 2019, hlm. 37.
[15] Dian Rachmawati, *Phising* Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber, *Jurnal Saintkom*, Edisi No. 3 Vol. 13 2014, hlm. 211.

mengirimkan *e-mail* palsu dengan meniru *e-mail* yang dikirimkan oleh perusahaan resmi. *E-mail* tersebut berisi perintah agar pengguna membuka link atau tautan lain yang dikirimkan oleh pisher tersebut. *Cyber crime* metode *phising* umumnya dilakukan dengan melakukan penyamaran sebagai orang lain, baik sebagai situs web palsu maupun dengan tautan palsu. *Situs* palsu dan tautan palsu ini dapat digunakan *pisher* untuk mendapatkan data pengguna yang mengunjungi laman dan mengklik suatu *pop-up* di situs palsu atau tautan palsu tersebut.

Tautan lain yang dikirimkan oleh *pisher* umumnya bertuliskan beberapa baris subjek seperti, "silahkan masukan user ID/password anda" atau dapat pula berisikan, "silahkan kirim kode OTP anda". Dengan data-data yang dikirimkan oleh pengguna, maka *pisher* dapat melakukan kejahatan yang dapat merugikan korban seperti memperoleh keuntungan dengan mengambil uang yang terdapat pada *e-wallet* korban, bank, dan lain sebagainya. *Cyber crime* metode *phising* dapat memakan banyak korban dikarenakan masih banyak masyarakat yang belum memiliki pengetahuan yang memadai mengenai teknologi, sehingga tidak menyadari bahwa tindakan-tindakan seperti membuka tautan dan situs palsu dapat menyebabkan pencurian data.[16]

Selain itu, masyarakat Indonesia juga belum mengetahui bahwa melakukan pemalsuan situs dapat dengan mudah dilakukan. Internet memungkinkan pengguna untuk melakukan *copy* dan *paste*, serta membuat suatu situs mirip dengan aslinya.

[16] Handrini Ardiyanti, Cyber-Security dan Tantangan Pengembangannya di Indonesia, *Jurnal Politica*, Edisi No. 01 Vol. 05 2014, hlm. 98.

Dengan tampilan yang terlihat seperti asli tersebut, maka pengguna tidak mengetahui bahwa *cyber crime* metode *phising* telah terjadi. *Cyber crime* metode *phising* sangat marak terjadi, tercatat secara global, jumlah *cyber crime* metode *phising* adalah 42% dari modus selain *cyber crime* metode *phising* yang dinyatakan dalam website Anti-*Phising* Working Group (APWG) dalam laporan bulannya, mencatat terdapat 12.845 *e-mail* baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana *cyber crime* metode *phising*.[16]

APWG melaporkan sekitar 1.270.883 total serangan *cyber crime* metode *phising* pada kuartal ketiga tahun 2022. Anggota pendiri APWG, OpSec Security mengungkapkan bahwa sektor keuangan termasuk bank, tetap menjadi kelompok serangan terbesar, terhitung 23,2% dalam seluruh *cyber crime* metode *phising*. [17]

Berdasarkan laporan Indonesia Anti *Phising* Data Exchange (IDADX) menunjukkan bahwa pada kuartal pertama tahun 2023, kurang lebih terdapat 26.675 laporan *cyber crime* metode *phising* di Indonesia, dan pada kuartal kedua tahun 2023 sebanyak 20.330 laporan. Angka tersebut merupakan kelanjutan dari kuartal ke 4 tahun 2022 yang hanya terdapat 6.106 laporan *cyber crime* metode *phising*, hal tersebut menandakan adanya peningkatan yang sangat signifikan sebanyak 20.569

[16] Suhardi Rustam, Analisa Clustering *Phising* dengan K-Means dalam Meningkatkan Keamanan Komputer, *Ilkom Jurnal Ilimiah*, Edisi No. 02 Vol. 10 2018, hlm. 175.

[17] Anti-*Phising* Working Group, *Phishing Activity Trends Report 4th Quarter 2022*, 2022, hlm. 5.

laporan. Apabila dilihat dalam kurun waktu lima tahun terakhir sebanyak 69.117 laporan *cyber crime* metode *phising* yang masuk.[18]

Contoh kasus *cyber crime* metode *phising* di Yogyakarta yang baru saja terjadi, pada tanggal 30 April 2023, seorang Pegawai Negri Sipil (PNS) di Yogyakarta tertipu hingga Rp600.000.000,00 (enam ratus juta rupiah) setelah ia diundang masuk ke grup aplikasi telegram, kemudian pelaku meminta korban untuk menyelesaikan beberapa misi di aplikasi tiktok dengan mengikuti dan memberikan *like* beberapa akun yang sudah di tentukan, lalu korban diarahkan untuk melakukan *top up* di situs yang menyerupai aplikasi tiktok, total dana yang di transfer senilai Rp600.000.000,00 (enam ratus juta rupiah) namun, ketika korban ingin melakukan pencairan dana selalu dibuat gagal.[19] Kemudian, pada tanggal 25 Mei 2023, seorang pengusaha yang bertempat tinggal di Malang telah mengaku kehilangan uang di rekening bank miliknya sebesar Rp.1.400.000.000 (satu miliar empat ratus juta rupiah) setelah ia tertipu sebuah *file* undangan pernikahan yang dikirim melalui Whatsapp dari nomor tidak dikenal. [20]

Dengan banyaknya *cyber crime* metode *phising* yang merugikan pengguna internet, maka perlu dilakukan pencegahan dan penegakan terhadap *phiser*.

---

[18] Indonesia Anti-Phishing Data Exchange, *Laporan Aktivitas Phishing Domain .ID Periode Q2 2023*, Jakarta, 2023, hlm. 2-3.

[19] Andi Saputra, Gadaikan SK Ratusan Juta, PNS Ini Malah Jadi Korban *Phising*, terdapat dalam https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-*phising*, diakses tanggal 8 Juli 2023 pukul 18.00 WIB.

[20] Tim detikJatim, Unduh File 'Undangan' di WA, Nasabah Kehilangan Duit Tabungan Rp 1,4 M, terdapat dalam https://www.detik.com/jateng/berita/d-6810966/unduh-file-undangan-di-wa-nasabah-kehilangan-duit-tabungan-rp-14-m., diakses tanggal 8 Juli 2023 pukul 18.00 WIB.

Penegakan hukum *cyber crime* di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE). Berdasarkan UU ITE, maka pelaku *cyber crime* metode *phising* dapat diancam dengan Pasal 35 dikarenakan dilakukan dengan menggunakan situs palsu yang menyerupai asli. Selain itu, *cyber crime* metode *phising* juga dapat diancam dengan Pasal 28 ayat (1) dikarenakan termasuk dalam perbuatan yang dilakukan dengan membohongi pengguna untuk menyesatkan pengguna tersebut. *Pisher* membohongi pengguna dan mengarahkan pengguna menuju situs palsu yang memberikan perintah untuk memberikan data pribadi pengguna kepada *pisher* tersebut.[21] Dengan demikian, *pisher* mendapatkan keuntungan dari data pribadi tersebut dan merugikan pengguna yang mengalami kebocoran data.

Cyber crime metode *phising* tidak hanya melakukan pemalsuan data dengan menyamarkannya sebagai situs asli, namun juga memiliki maksud untuk memperoleh data pribadi pengguna internet untuk digunakan secara ilegal. Sementara, dalam Pasal 35 UU ITE hanya mengandung unsur pemalsuan data tanpa adanya unsur maksud dan tujuan untuk melakukan tindak kejahatan yang merugikan korban.

Berdasarkan hasil pra-riset di Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta (Polda DIY), data yang diperoleh dari wawancara kepada anggota

[21] Ardi Saputra Gulo, Sahuri Lasmadi, dan Khabib Nawawi, *Cyber crime* dalam Bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, PAMPAS: Journal of Criminal Law, Edisi No. 02 Vol. 01 2021, hlm. 70.

Ditreskrimsus Polda DIY, dapat diketahui bahwa kasus tindak pidana *cyber crime* metode *phising* terhitung dari tahun 2019 hingga tahun 2022 mengalami kenaikan setiap tahunnya. Pada tahun 2020, terdapat 28 jumlah laporan kasus *cyber crime* metode *phising*. Kemudian, pada tahun 2021 mengalami kenaikan jumlah kasus yang signifikan, menjadi 54 laporan kasus, kemudian pada tahun 2022 terdapat 55 laporan kasus.

Berdasarkan data kasus yang terus terjadi tersebut maka penelitian ini memiliki urgensi untuk menganalisa kendala Polda DIY dalam penegakan hukum terhadap *cyber crime* metode *phising*. Dengan ditemukan kendala dalam penegakan hukum tersebut maka upaya solutif diharapkan dapat membantu Polda DIY agar melindungi korban serta menegakkan hukum terhadap pelaku tindak pidana *cyber crime* metode *phising*. Berdasarkan permasalahan yang telah dipaparkan di atas, maka peneliti tertarik untuk melakukan penelitian dengan judul, "Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyber crime* Metode *Phising* Oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta"

B. Rumusan Masalah

Berangkat dari latar belakang yang telah dijabarkan, rumusan masalah penelitian adalah:

1. Bagaimana kendala yang dihadapi Polda DIY pada penanganan tindak pidana *cyber crime* metode *phising*?
2. Bagaimana upaya yang dilakukan Polda DIY untuk mengatasi kendala penanganan tindak pidana *cyber crime* metode *phising*?

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian adalah:

1. Untuk mengetahui dan menganalisa kendala yang dihadapi Polda DIY pada penanganan tindak pidana *cyber crime* metode *phising*.
2. Untuk mengetahui dan menganalisa upaya yang dilakukan Polda DIY untuk mengatasi kendala penanganan tindak pidana *cyber crime* metode *phising*.

D. Orisinalitas Penelitian

Penelitian harus dilakukan dengan menjaga orisinalitas penulisan, begitu juga dengan penelitian ini. Untuk menjaga orisinalitas dari hasil penelitian ini, maka penulis memaparkan beberapa contoh dari penelitian yang berkaitan dengan pengaturan *cyber crime* metode *phising* yang pernah dilakukan sebelumnya. Penelitian terdahulu ini akan dibahas lebih lanjut, sehingga akan ditemukan bahwa penulisan penelitian ini memberikan hasil penelitian yang berbeda dengan penelitian yang telah dilakukan sebelumnya yang terdapat pada tabel berikut:

No.	Penelitian Terdahulu	Unsur Pembeda
1.	Skripsi yang ditulis oleh Hilman Mursidi, dengan judul: ‘’Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cyber crime Phising* (Studi Kasus Putusan Pengadilan Negeri Medan Nomor:3006/Pid.Sus/2017/PN.Mdn)”.	Penelitian ini merupakan penelitian yang termasuk dalam tipe penelitian normatif dengan pendekatan peraturan perundang-undangan, pendekatan kasus, dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa pelaku dalam kasus tersebut hanya dapat dikenai pasal mengenai pencemaran nama baik dan pasal penghinaan, meskipun telah jelas pelaku melakukan tindak pidana *phising*. Dari penelitian ini, maka

		dapat dikatakan bahwa peneliti tidak melakukan penelitian mengenai penegakan *cyber crime phising* secara umum berdasarkan pengaturan perundang-undangan, melainkan melakukan penelitian mengenai pertanggungjawaban pidana terhadap pelaku *phising* dalam suatu kasus putusan pengadilan. Oleh karena itu, dapat dikatakan bahwa penelitian tersebut tidak sama dengan yang akan dilakukan oleh peneliti.
2.	Skripsi yang ditulis oleh Zainal Arifin AL-Hakim dalam bentuk skripsi dengan judul: "*Cyber crime* dalam Bentuk *Phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Perspektif Hukum Pidana Islam".	Penelitian dilakukan dengan tujuan yakni mengetahui *cyber crime phising* dalam UU ITE dan dalam perspektif hukum pidana islam. Penelitian termasuk dalam tipologi penelitian nomatif dengan pendekatan konseptual dan peraturan perundang-undangan. Hasil penelitian menunjukkan bahwa pelaku *cyber crime* dalam bentuk *phising* menurut Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat dikenakan Pasal 28 ayat (1) jo Pasal 45 ayat (2) dan Pasal 35 jo Pasal 51 ayat (1). Sementara dalam hukum pidana islam pihak yang berwenang melaksanakan hukuman ta'zir adalah ulil amri, dan telah memenuhi unsur-unsur yang ada dalam jarimah ta'zir. Dengan demikian, dapat dikatakan pokok bahasan dalam penelitian ini berbeda dengan penelitian yang dilakukan oleh peneliti ini. Penelitian tersebut melakukan penelitian mengenai *Phising* dalam UU ITE dan dalam perspektif hukum pidana islam, sehingga pembahasan terbatas pada pengaturan pada UU ITE dan hukum pidana islam. Sementara penelitian

		yang dilakukan oleh peneliti adalah mengenai penegakan hukum terhadap pelaku tindak pidana *phising* di Indonesia. Penelitian yang dilakukan ini tidak hanya menelusuri pada pengaturan dalam UU ITE, namun juga peraturan perundang-undangan lainnya. Selain itu, penelitian ini tidak membahas mengenai *phising* dalam perspektif hukum pidana islam.
3.	Artikel yang ditulis oleh ditulis oleh Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi. dengan judul: "*Cyber crime* dalam Bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik".	Penelitian dilamaksud kan untuk mengetahui lebih lanjut mengenai *phising* dalam UU ITE. Penelitian ini disusun dalam bentuk artikel jurnal. Penelitian ini dilakukan dengan menggunakan pendekatan konseptual dan pendekatan perundang-undangan. Hasil penelitian menunjukkan bahwa pengaturan hukum terhadap *cyber crime* dalam bentuk *phising* berdasarkan Undang-Undang tentang Informasi dan Transaksi Elektronik tidak dapat dikenai Pasal 35 jo Pasal 51 Ayat (1) dan Pasal 28 Ayat (1) jo Pasal 45A Ayat (1). Selain itu, juga menunjukkan hasil bahwa kebijakan hukum terhadap *cyber crime* dilakukan dengan mengubah isi Pasal 35 dalam UU ITE. Dengan demikian, dapat dikatakan bahwa penelitian berbeda dengan yang ditulis oleh peneliti. Penelitian yang dilakukan oleh peneliti melakukan pembahasan mengenai penegakan hukum terhadap pelaku tindak pidana *cyber crime phising.* Dengan demikian, tidak hanya mengatur mengenai pengaturan *phising* dalam peraturan perundang-undangan, melainkan juga pertanggungjawaban pidananya dalam penegakannya

Berdasarkan penelitian terdahulu, dapat dikatakan bahwa belum terdapat penelitian yang membahas mengenai penegakan hukum terhadap pelaku tindak pidana *cyber crime* metode *phising* di Polda DIY. Dari tinjauan penelitian terdahulu ini, maka originalitas penulisan penelitian ini telah dibuktikan. Selain itu, penelitian ini tidak mengandung plagiasi serta mencantumkan sumber dalam pengutipan-pengutipan teori dan konsep yang digunakan dalam penelitian.

E. Tinjauan Pustaka

1. Tindak Pidana *Cyber Crime*

Tindak pidana *cyber crime* merupakan kejahatan yang berbeda dengan kejahatan konvensional. Tindak pidana *cyber crime* muncul sebagai akibat lahirnya revolusi teknologi informasi. Dengan interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan sosial menyesuasikan bentuk dn karakter baru dalam kejahatan.[22]

Sehingga, tindak pidana *cyber crime* dapat dimaknai secara luas dan sempit. Dalam arti sempit, tindak pidana *cyber crime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer. Sedangkan, dalam arti luas tindak pidana *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan pada komputer baik dari jaringan maupun penggunanya serta kejahatan konvensional yang menggunakan teknologi komputer.

[22] Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005, hlm. 25.

Tindak pidana *cyber crime* dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi. Terdapat suatu definisi tindak pidana *cyber crime* sebagai berikut, computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain. Hal tersebut dapat diartikan sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.[23]

2. *Cyber Crime* Metode *Phising*

Berdasarkan keterangan Iptu Anis Dwi Haryanto, *phising* bukan merupakan suatu tindak pidana namun, sebuah metode dalam tindak pidana *cyber crime*.[24] Tindak pidana *cyber crime* metode *phising* merupakan kejahatan dunia maya dengan seseorang menyamar sebagai lembaga yang sah menghubungi target atau korban melalui email, telepon, atau pesan teks, agar ia memberikan data sensitif seperti informasi identitas pribadi, detail perbankan atau kartu kredit serta kata sandi. Setelah korban atau target memberikan informasi tersebut kemudian

[23] Andi Hamzah, *Hukum Pidana yang berkaitan dengan komputer*, Sinar Grafika Offset, Jakarta, 1993, hlm. 18.

[24] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

nantinya akan digunakan untuk mengakses akun penting yang dapat mengakibatkan pencurian identitas dan kerugian finansial.[25]

Phising sendiri berasal dari kata "fishing" yang memiliki arti memancing. Seperti halnya kegiatan memancing, *phising* adalah kejahatan dengan cara memanfaatkan umpan. Umpan yang tepat sasaran adalah faktor penentu keberhasilan *phising*. Kehadiran akun *phising* adalah kunci, sebab menyerupai akun resmi. Apabila dilihat dari definisinya, *phising* adalah kejahatan yang menggunakan rekayasa sosial dan dalih teknis mencuri data identitas pribadi dan akun keuangan dengan skema memangsa korban yang tidak waspada atau lalai dengan membodohi mereka agar mereka percaya bahwa mereka berurusan dengan pihak terpercaya dan sah, seperti menggunakan alamat email yang menipu, hal ini direncanakan untuk mengarahkan korban ke situs web palsu yang menipu korbannya sehingga data akun yang berhubungan dengan keuangan, nama pengguna serta kata sandi itu dibocorkan.[13]

Ketika terdapat celah pada sistem keamanan, disitulah peretas memanfaatkan momen yang sering didengar dengan sebutan hacking ataupun hacker. Kemudian, terdapat juga istilah cracking dan cracker yang mana kejahatan yang dilakukan oleh cracking salah satunya adalah *phising* karena memiliki tujuan

[25] Erizka Permatasari, Jerat Hukum Pelaku Phishing dan Modusnya, terdapat dalam https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050, diakses tanggal pada tanggal 17 Juli 2023 pukul 21:32 WIB.

[13] Anti-*Phising* Working Group, *Loc. Cit.*

yaitu untuk menguntungkan diri sendiri dan tentunya akan ada pihak yang dirugikan dan menjadi korban dari tindak pidana *cyber crime* ini.[14]

Phising merupakan salah satu kejahatan elektronik dalam lingkup penipuan, dimana proses *phising* ini memiliki tujuan untuk mengambil informasi yang sangat sensitif seperti username, password, dan detail kartu kredit dalam bentuk meniru sebagai sebuah lembaga yang dipercaya dan biasanya berkomunikasi secara elektronik.[15]

3. Penegakan Hukum

Penegakan hukum merupakan suatu proses dilakukannya upaya untuk tegaknya norma-norma hukum secara nyata sebagai pedoman perilaku dalam hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.[16] Penegakan hukum juga merupakan suatu bentuk pelaksanaan hukum secara nyata dengan usaha mewujudkan ide keadilan, kepastian hukum, kemanfaatan sosial dan keadilan menjadi kenyataan.[17]

Konsep dasar penegakan hukum pidana membutuhkan adanya unsur moral terkait hubungan moral dengan penegakan hukum yang dapat menentukan keberhasilan atau ketidakberhasilan suatu penegakan hukum yang menjadi

---

[14] Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi, Cyber crime dalam Bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, *PAMPAS: Journal of Criminal*, Edisi No. 02 Vol. 01 2020, hlm. 70.

[15] Dian Rachmawati, *Loc. Cit.*

[16] Jimly Asshiddiqie, Penegakan Hukum, terdapat dalam http://www.jimly.com/makalah/namafile/56/Penegakan_Hukum.pdf, diakses tanggal 18 Juli 2023 pukul 19:21 WIB.

[17] Satjipto Raharjo, *Hukum dan Masyarakat*, Angkasa, Bandung, 1980, hlm. 15.

harapan tujuan hukum. Kemudian, terkait aspek moral dan etika, merupakan hal yang berkaitan dengan penegakan hukum pidana, dikarenakan proses penemuan fakta tidak memihak dan penuh dengan pemecahan masalah yang harus dilakukan dengan adil dan patut.[18]

Upaya penegakan hukum dapat dilakukan dengan cara pencegahan atau preventif dan penindakan atau represif. Upaya represif dan preventif tersebut dapat dilakukan melalui jalur hukum pidana dan diluar jalur hukum pidana. Upaya preventif diluar jalur hukum pidana dilakukan sebagai bentuk pencegahan tanpa penerapan pidana maupun pengendalian sebelum tindak pidana terjadi yang dapat dilakukan oleh masyarakat umum ataupun penegak hukum. Sedangkan, upaya represif jalur hukum pidana dilakukan sebagai bentuk penanganan atau penindakan yang dilakukan setelah tindak pidana terjadi.

F. Definisi Operasional

Judul penelitian ini adalah Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cyber crime* Metode *Phising* Oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, terdapat beberapa penjelasan untuk memberikan penjelasan yang akan diteliti dalam penelitian ini, antara lain:

1. Penegakan Hukum

   Penegakan hukum yang dimaksud dalam penelitian ini adalah penegakan hukum tindak pidana *cyber crime* metode *phising* seperti yang diatur dalam Pasal

[18] Muladi, *Hak Asasi Manusia*, Refika Aditama, Bandung, 2009, hlm. 4.

45A ayat (1) dengan ketentuan pidana Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Tindak Pidana *Cyber crime* Metode *Phising*

   Tindak pidana *cyber crime* metode *phising* yang dimaksud dalam penelitian ini adalah kelompok kejahatan siber yang menggunakan komputer sebagai alat utama pada wilayah Daerah Istimewa Yogyakarta.

3. Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta

   Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta yang dimaksud dalam penelitian ini adalah para anggota kepolisian terutama yang bertugas pada Direktorat Reserse Kriminal Khusus (Ditreskrimsus).

G. Metode Penelitian

Adapun metode penelitian yang digunakan dalam menyusun skripsi ini, diuraikan lebih rinci sebagai berikut:

1. Jenis Penelitian

   Jenis penelitian yang dilakukan oleh penulis adalah penelitian hukum empiris. Penelitian empiris adalah penelitian hukum terkait pemberlakuan ataupun implementasi pada setiap peristiwa hukum tertentu yang terjadi dalam masyarakat.[19]

2. Pendekatan Penelitian

[19] Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, 2004, hlm. 134.

Adapun pendekatan yang digunakan dalam penelitian ini yakni pendekatan sosiologis. Pendekatan sosiologis adalah suatu pendekatan yang pembahasannya atas suatu objek yang dilandaskan pada masyarakat yang ada pada pembahasan tersebut dan pendekatan ini berdasarkan data lapangan untuk memperoleh data primer.

3. Objek Penelitian

Objek penelitian dalam penelitian ini adalah kendala yang dihadapi Polda DIY pada penanganan tindak pidana *cyber crime* metode *phising*, serta upaya yang dilakukan Polda DIY untuk mengatasi kendala penanganan tindak pidana *cyber crime* metode *phising*.

4. Subjek Penelitian

Subjek penelitian dalam penelitian ini adalah Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Polda DIY.

5. Sumber Data Penelitian

Sumber data yang diperlukan dalam penelitian ini menggunakan data primer dan data sekunder dengan bahan-bahan hukum sebagai berikut:

a. Data Primer

Data Primer merupakan data yang diperoleh terutama dari hasil penelitian secara empiris, yaitu penelitian yang dilakukan oleh peneliti untuk melakukan wawancara dengan narasumber yang ahli pada bidangnya. Narasumber pada penelitian ini adalah dari pihak Ditreskrimsus Polda DIY.

b. Data Sekunder

Data sekunder adalah data yang diperoleh dari hasil penelaahan kepustakaan atau penelaahan terhadap berbagai literatur atau bahan pustaka yang berkaitan dengan masalah atau materi penelitian yang sering disebut bahan hukum.[20]

1) Bahan Hukum Primer
   a) Undang-Undang Negara Republik Indonesia 1945;
   b) Kitab Undang-Undang Hukum Pidana (KUHP);
   c) Kitab Undang-Undang Hukum Acara Pidana (KUHAP);
   d) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2) Bahan Hukum Sekunder

   Bahan hukum sekunder dalam penelitian ini meliputi bahan-bahan yang dapat menjelaskan lebih lanjut terhadap bahan hukum primer, seperti buku-buku hukum, jurnal-jurnal hukum, karya tulis atau pandangan ahli hukum.
3) Bahan Hukum Tersier

   Bahan hukum tersier merupakan bahan-bahan hukum yang memberikaan informasi tentang bahan hukum primer dan bahan hukum sekunder berupa pencarian data di internet, Kamus Besar Bahasa Indonesia, Kamus Inggris-Indonesia, serta kamus hukum.

[20] Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris,* Pustaka Pelajar, Yogyakarta, 2009, hlm. 156.

6. Teknik Pengumpulan Data

Dalam pengumpulan data, peneliti melakukan wawancara untuk mendapatkan data yang valid terkait penelitian, melakukan studi kepustakaan yang dilakukan dengan cara mempelajari buku-buku, artikel dan jurnal ilmiah yang berhubungan dengan masalah yang diteliti.

7. Analisis Bahan Hukum

Analisa data merupakan kegiatan dalam penelitian yang berupa melakukan kajian atau telaah terhadap hasil pengolahan data yang dibantu dengan teori-teori yang telah didapatkan sebelumnya. Data yang telah diperoleh dari penelitian kepustakaan maupun penelitian lapangan, kemudian dianalisis dengan menggunakan deskriptif kualitatif, yaitu dengan cara mengumpulkan data yang kemudian diolah dan dianalisis dengan dengan permasalahan yang diperoleh dari penelitian lapangan maupun kepustakaan menurut kualitas dan kebenarannya kemudian hasil analisis tersebut disusun secara sistematis, yang selanjutnya dikaji dan di analisis kemudian dibuat kesimpulan guna untuk menjawab rumusan masalah dalam penelitian ini.[21]

H. Kerangka Skripsi

Untuk mempermudah pembahasan dalam penulisan, penelitian ini disusun menggunakan sistematika sebagai berikut:

BAB I PENDAHULUAN

[21] Abdul Kadir Muhammad, *Op. Cit.,* hlm. 50.

Bab ini memuat pendahuluan yang meliputi latar belakang masalah, rumusan masalah, tujuan penelitian, orisinalitas penelitian, manfaat penelitian, tinjauan pustaka, definisi operasional, dan metode penelitian.

BAB II TINJAUAN UMUM

Bab ini memuat penjelasan atas tindak pidana, penegakan hukum, tindak pidana *cyber crime*, tindak pidana *cyber crime* metode *phising*, dan hukum pidana islam.

BAB III ANALISA DAN PEMBAHASAN

Bab ini memuat hasil penelitian mengenai kendala dan upaya solutif Polda DIY dalam penanganan tindak pidana *cyber crime* metode *phising*.

BAB IV PENUTUP

Bab ini memuat kesimpulan dari pembahasan bab-bab sebelumnya dan juga berisi saran sebagai acuan guna memanfaatkan maupun mengembangkan penelitian dalam skripsi ini agar lebih baik dan sempurna.

BAB II

TINJAUAN UMUM TENTANG TINDAK PIDANA CYBER CRIME, PENEGAKAN HUKUM, DAN TINDAK PIDANA CYBER CRIME METODE PHISING MENURUT HUKUM PIDANA ISLAM

A. Tindak Pidana *Cyber crime*

1. Pengertian Tindak Pidana

Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia telah mengatur terkait tindak pidana yang memiliki arti berupa pelanggaran norma baik dilakukan dengan sengaja maupun tidak oleh seseorang. Hukuman berupa sanksi tersebut diperlukan agar hukum di Indonesia terpelihara dan terjaminnya kepentingan umum.[35] Tindak pidana sendiri dapat disamakan dengan perbuatan pidana, dimana perbuatan yang dilarang oleh suatu aturan hukum, larangan yang disertai sanksi berupa pidana tertentu, dan bagi barang siapa yang melanggar larangan tersebut.[22]

Tindak pidana merupakan suatu perbuatan yang bertentangan dengan Peraturan Perundang-undangan. Hal tersebut dikarenakan tindak pidana merupakan suatu perbuatan yang bersifat melawan hukum dan perbuatan tersebut

[35] P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997, hlm.182.

[22] Moeljatno*, Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2008, hlm. 9.

berlawanan dengan norma yang dikehendaki dalam masyarakat yang adil yang dapat dijatuhi hukuman pidana.[23]

KUHP membagi tindak pidana menjadi dua yaitu, kejahatan dan pelanggaran. Keduanya telah termuat dalam Buku II KUHP dan Buku III KUHP, dimana kejahatan merupakan perbuatan yang bertentangan dengan keadilan sehingga ada atau tidaknya perbuatan tersebut diancam dengan pidana yang dimuat dalam Peraturan Perundang-undangan. Sementara, pelanggaran adalah perbuatan yang disadari oleh masyarakat sebagai suatu tindak pidana, Peraturan Perundang-undangan menyebut perbuatan tersebut adalah delik sehingga disebut sebagai pelanggaran.[24]

Seseorang dapat dianggap berbuat tindak pidana apabila perbuatan tersebut telah telah memenuhi dua unsur pokok yaitu unsur subyektif dan obyektif sebagai berikut:

a. Unsur Subjektif

Unsur ini merupakan unsur yang berkaitan dengan pribadi pelaku yang terdiri dari, adanya kesengajaan atau ketidaksengajaan, maksud dalam suatu percobaan, macam-macam dari maksud seperti tindak pidana penipuan, merencanakan terlebih dahulu seperti tindak pidana pembunuhan

[23] R. Abdoel Djamali, *Pengantar Hukum Indonesia*, Raja Grafindo Persada, Jakarta, 2014, hlm. 175.

[24] Dani Krisnawati, Eddy O.S. Hiariej, Marcus Priyo Gunarto, Sigid Riyanto, dan Supriyadi, *Bunga Rampai Hukum Pidana Khusus*, Pena Ilmu dan Amal, Jakarta, 2006, hlm. 6.

berencana, terdapat perasaan takut seperti tindak pidana Pasal 308 KUHP, dan orang tersebut bertanggung jawab.[25]

b. Unsur Objektif

Unsur ini merupakan unsur yang tidak terlepas dari suatu keadaan tertentu yang menentukan dalam keadaan apa tindakan dari pelaku yang terdiri dari sifat melawan hukum dan kualitas pelaku. Kualitas pelaku tersebut seperti dalam hal kejahatan jabatan yang menggambarkan keadaan pelaku merupakan seorang pegawai negeri sipil. Sementara, kausalitas yang dimaksud adalah hubungan kausalitas keterkaitan antara tindak pidana sebagai penyebab dengan kenyataan sebagai akibat.[26]

Kemudian, unsur-unsur tindak pidana menurut pandangan Moeljatno meliputi, perbuatan yang dilakukan manusia, memenuhi ketentuan Undang-Undang, dan bersifat melawan hukum.[27] Memenuhi ketentuan Undang-Undang merupakan suatu keharusan yang berkenaan dengan asas legalitas. Sementara, bersifat melawan hukum merupakan syarat mutlak untuk dapat dikatakan sebagai tindak pidana. Konsekuensi atas asas legalitas sudah seharusnya menetapkan suatu perbuatan yang dapat dijatuhi hukuman pidana sebab, perbuatan tersebut

[25] P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997, hlm. 193.

[26] Adami Chazawi, *Pelajaran Hukum Pidana 1*, Raja Grafindo Persada, Jakarta, 2005, hlm. 79.

[27] Moeljatno, *Op. Cit.*, hlm. 54.

dapat dirasakan oleh masyarakat sebagai perbuatan yang tidak semestinya. Sudah seharusnya setiap perbuatan pidana tertuang dalam aturan hukum yang ada.[28]

2. Pengertian Tindak Pidana *Cyber crime*

Tindak pidana *cyber crime* merupakan kejahatan yang berbeda dengan kejahatan konvensional. Tindak pidana *cyber crime* muncul sebagai akibat lahirnya revolusi teknologi informasi. Dengan interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan sosial menyesuasikan bentuk dn karakter baru dalam kejahatan.[29]

Sehingga, tindak pidana *cyber crime* dapat dimaknai secara luas dan sempit. Dalam arti sempit, tindak pidana *cyber crime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer. Sedangkan, dalam arti luas tindak pidana *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan pada komputer baik dari jaringan maupun penggunanya serta kejahatan konvensional yang menggunakan teknologi komputer.

Tindak pidana *cyber crime* dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi. Terdapat suatu definisi tindak pidana *cyber crime* sebagai berikut, *computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a*

[28] *ibid.*, hlm. 5.
[29] Didik M. Arief Mansur dan Elisatris Gultom, *Loc. Cit.*

perpetrator by intention made or could have gain.[30] Hal tersebut dapat diartikan sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.[31]

Tindak pidana *cyber crime* merupakan perbuatan melawan hukum yang memanfaatkan media komputer yang terhubung ke internet dan mengeksploitasi komputer lain, adapun bentuk-bentuk kejahatan *cyber crime* sebagai berikut:[32]

a. Tindak pidana *cyber crime* berdasarkan sifat kejahatan

   Terdapat dua klasifikasi tindak pidana *cyber crime* berdasarkan sifat kejahatan. Pertama, tindak pidana *cyber crime* sebagai tindakan kriminal yang merupakan kejahatan yang dilakukan dengan motif kriminalitas. Kedua, tindak pidana *cyber crime* sebagai kejahatan abu-abu karena sulit menentukan apakah tindakan ini merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan.

b. Tindak pidana *cyber crime* berdasarkan modus kejahatan

   Terdapat tujuh klasifikasi tindak pidana *cyber crime* berdasarkan modus kejahatan. Pertama, *unauthorized access to computer system and service* yang

[30] Suresh T. Viswanathan, *The Indian Cyber Laws with Cyber Gl*ossary, Bharat Law House, New Delhi, 2001, hlm. 81.

[31] Andi Hamzah, *Loc. Cit.*

[32] Florida Mathilda, Cyber crime dalam Sistem Hukum Indonesia, *Sigma-Mu*, Edisi No. 04 Vol. 04 2012, hlm. 35.

terjadi ketika seseorang menyusup ke dalam suatu sistem jaringan komputer milik orang lain secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Kedua, *illegal contents* yang memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar dan dapat dianggap melanggar hukum.

Ketiga, *data forgery* yang dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Keempat, *cyber espionage, sabotage, and extortion* yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata pada pihak lain. Kelima, *data theft* yang mengambil data komputer milik orang lain secara tidak sah, baik untuk digunakan sendiri atau digunakan untuk orang lain.

Keenam, *infringements of privacy* yang biasanya ditujukan kepada keterangan pribadi seseorang pada formulir data pribadi yang tersimpan secara *computerized*. Ketujuh, *cyber terrorism* yang merupakan suatu tindakan tindak pidana *cyber crime* yang mengancam pemerintah atau warga negara.

c. Tindak pidana *cyber crime* berdasarkan sasaran kejahatan

Terdapat lima klasifikasi tindak pidana *cyber crime* berdasarkan sasaran kejahatan. Pertama, *cyber crime* yang menyerang individu yang ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Kedua, *cyberstalking* yang dilakukan

untuk mengganggu atau melecehkan seseorang dengan masuk menggunakan *e-mail* yang dilakukan secara berulang-ulang.

Ketiga, *cyber-trespass* yang dilakukan melanggar area privasi orang lain. Keempat, *cyber crime* menyerang hak milik yang mengganggu atau menyerang hak milik orang lain, seperti mengakses komputer secara tidak sah. Kelima, *cyber crime* menyerang pemerintah yang memiliki tujuan khusus penyerangan terhadap pemerintah, seperti mengancam melalui situs resmi pemerintah.

Kemudian, terdapat juga beberapa jenis-jenis tindak pidana *cyber crime* apabila dilihat dari aktivitasnya sebagai berikut:[33]

b. *Carding*

Merupakan aktifitas berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet.

c. *Hacking*

Merupakan aktifitas menerobos program komputer milik pihak lain.

d. *Cracking*

Merupakan aktifitas hacking untuk tujuan jahat. Sebutan untuk *cracker* adalah *hacker* bertopi hitam. Berbeda dengan *carder* yang hanya mengintip kartu kredit, *cracker* mengintip simpanan para nasabah di berbagai bank atau

[33] Nunuk Sulisrudatin, Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit, *Jurnal Ilmiah Hukum Dirgantara*, Edisi No. 01 Vol. 09 2018, hlm. 31.

pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, *hacker* lebih fokus pada prosesnya. Sedangkan *cracker* lebih fokus untuk menikmati hasilnya.

e. *Defacing*

Merupakan aktifitas mengubah halaman situs pihak lain. Tindakan *deface* ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat mencuri data dan dijual kepada pihak lain.

f. *Phising*

Merupakan aktifitas memancing pemakai komputer di internet agar mau memberikan informasi data diri pemakai dan kata sandinya pada suatu situs yang sudah di-*deface*. *Phising* biasanya diarahkan kepada pengguna *online banking*.

g. *Spamming*

Merupakan aktifitas pengiriman berita atau iklan lewat *e-mail* yang tidak dikehendaki.

h. *Malware*

Merupakan program komputer yang mencari kelemahan dari suatu *software*. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau operating system. *Malware* terdiri dari berbagai macam seperti *virus, worm, trojan horse, adware,* hingga *browser hijacker*.

Terdapat berbagai pengaturan dan dasar hukum dari tindak pidana *cyber crime*. Berikut merupakan dasar hukum yang mengatur tentang tindak pidana *cyber crime*.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi telah mengatur perbuatan yang dilarang terkait tindak pidana *cyber crime*. Adapun beberapa pasal tersebut yakni sebagai berikut.

1) Pasal 22

Pasal ini mengatur larangan untuk melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi, akses ke jaringan telekomunikasi, dan atau akses ke jasa telekomunikasi, dan atau akses ke jaringan telekomunikasi khusus.

2) Pasal 38

Pasal ini mengatur larangan untuk melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi.

3) Pasal 40

Pasal ini mengatur larangan untuk melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

c. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas 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 telah mengatur perbuatan yang dilarang terkait tindak pidana *cyber crime*. Adapun beberapa pasal tersebut yakni sebagai berikut.

1) Pasal 27 ayat (1)

   Pasal ini mengatur larangan bagi seseorang yang dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan.

2) Pasal 27 ayat (2)

   Pasal ini mengatur larangan bagi seseorang yang dengan sengaja tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

3) Pasal 27 ayat (3)

   Pasal ini mengatur larangan bagi seseorang yang tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atauDokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

4) Pasal 27 ayat (4)

   Pasal ini mengatur larangan bagi seseorang tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi

Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

5) Pasal 28 ayat (1)

   Pasal ini mengatur larangan bagi seseorang tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

6) Pasal 28 ayat (2)

   Pasal ini mengatur larangan bagi seseorang tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan.

7) Pasal 29

   Pasal ini mengatur larangan bagi seseorang yang tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

8) Pasal 30 ayat (1)

   Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

9) Pasal 30 ayat (2)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

10) Pasal 30 ayat (3)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

11) Pasal 31ayat (1)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

12) Pasal 31 ayat (2)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan,

dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

13) Pasal 31 ayat (3)

Pasal ini mengatur larangan bagi seseorang yang melakukan intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

14) Pasal 32 ayat (1)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

15) Pasal 32 ayat (2)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

16) Pasal 32 ayat (3)

Pasal ini mengatur larangan bagi seseorang yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik

yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

17) Pasal 33

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

18) Pasal 34 ayat (1)

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

19) Pasal 34 ayat (2)

Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem

Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

20) Pasal 35

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

21) Pasal 36

Pasal ini mengatur larangan bagi seseorang yang tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

22) Pasal 37

Pasal ini mengatur larangan bagi seseorang yang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

3. Pengertian Tindak Pidana *Cyber crime* Metode *Phising*

Berdasarkan keterangan Iptu Anis Dwi Haryanto, *phising* bukan merupakan suatu tindak pidana namun, sebuah metode dalam tindak pidana *cyber crime*.[34] Tindak pidana *cyber crime* metode *phising* merupakan kejahatan dunia maya dengan seseorang menyamar sebagai lembaga yang sah menghubungi target atau korban melalui email, telepon, atau pesan teks, agar ia memberikan data sensitif seperti informasi identitas pribadi, detail perbankan atau kartu kredit serta kata sandi. Setelah korban atau target memberikan informasi tersebut kemudian nantinya akan digunakan untuk mengakses akun penting yang dapat mengakibatkan pencurian identitas dan kerugian finansial.[35]

Phising sendiri berasal dari kata *fishing* yang memiliki arti memancing. Seperti halnya kegiatan memancing, *phising* adalah kejahatan dengan cara memanfaatkan umpan. Umpan yang tepat sasaran adalah faktor penentu keberhasilan *phising*. Kehadiran akun *phising* adalah kunci, sebab menyerupai akun resmi. Apabila dilihat dari definisinya, *phising* adalah kejahatan yang menggunakan rekayasa sosial dan dalih teknis mencuri data identitas pribadi dan akun keuangan dengan skema memangsa korban yang tidak waspada atau lalai dengan membodohi mereka agar mereka percaya bahwa mereka berurusan dengan pihak terpercaya dan sah, seperti menggunakan alamat *e-mail* yang

[34] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

[35] Erizka Permatasari, *Loc. Cit.*

menipu, hal ini direncanakan untuk mengarahkan korban ke situs palsu yang menipu korbannya sehingga data akun yang berhubungan dengan keuangan, nama pengguna serta kata sandi itu dibocorkan.[36]

Ketika terdapat celah pada sistem keamanan, disitulah peretas memanfaatkan momen yang sering didengar dengan sebutan *hacking* ataupun *hacker*. Kemudian, terdapat juga istilah *cracking* dan *cracker* yang mana kejahatan yang dilakukan oleh *cracking* salah satunya adalah *phising* karena memiliki tujuan yaitu untuk menguntungkan diri sendiri dan tentunya akan ada pihak yang dirugikan dan menjadi korban dari tindak pidana *cyber crime* ini.[37]

Phising merupakan salah satu kejahatan elektronik dalam lingkup penipuan, dimana proses *phising* ini memiliki tujuan untuk mengambil informasi yang sangat sensitif seperti *username*, *password*, dan detail kartu kredit dalam bentuk meniru sebagai sebuah lembaga yang dipercaya dan biasanya berkomunikasi secara elektronik.[38]

Tindak pidana *cyber crime* metode *phising* sendiri pada dasarnya dapat dikenakan Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Hal tersebut dikarenakan termasuk dalam tindakan penipuan yang mengarahkan sang korban untuk mengakses situs palsu. Adapun Pasal 378 KUHP tersebut berbunyi sebagai berikut, barangsiapa dengan maksud untuk menguntungkan diri sendiri

[36] Anti *Phising* Working Group, *Loc. Cit.*
[37] Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi, *Loc. Cit.*
[38] Dian Rachmawati, *Loc. Cit.*

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 empat tahun.

Kemudian, tindak pidana *cyber crime* metode *phising* juga dapat dikenakan Pasal 28 ayat (1) dan Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal tersebut dikarenakan pelaku tindak pidana *cyber crime* metode *phising* melakukan kebohongan untuk menyesatkan orang lain dimana mengarahkan orang yang dibohongi untuk mengakses sebuah link yang ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbaharui informasi pribadinya yang rahasia ke dalam situs palsu tersebut sehingga informasi pribadinya itu dapat diketahui oleh pelaku dan menyebabkan orang tersebut mengalami kerugian.

Adapun bunyi Pasal 28 ayat (1) dan Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut.

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Pasal 45A

(1) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam

Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Selain itu, tindak pidana *cyber crime* metode *phising* dapat dikenakan Pasal 35 dengan ketentuan pidana Pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal tersebut dikarenakan tindak pidana *cyber crime* metode *phising* merupakan kejahatan siber yang memanipulasi korbannya dengan membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. Adapun bunyi kedua pasal tersebut sebagai berikut.

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/atau dokumen elektronik dengan tujuan agar Informasi Elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data otentik.

Pasal 51

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah).

B. Penegakan Hukum

1. Pengertian Penegakan Hukum

Penegakan hukum merupakan suatu proses dilakukannya upaya untuk tegaknya norma-norma hukum secara nyata sebagai pedoman perilaku dalam hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.[39]

[39] Jimly Asshiddiqie, *Loc. Cit.*

Penegakan hukum juga merupakan suatu bentuk pelaksanaan hukum secara nyata dengan usaha mewujudkan ide keadilan, kepastian hukum, kemanfaatan sosial dan keadilan menjadi kenyataan.[40]

Konsep dasar penegakan hukum pidana membutuhkan adanya unsur moral terkait hubungan moral dengan penegakan hukum yang dapat menentukan keberhasilan atau ketidakberhasilan suatu penegakan hukum yang menjadi harapan tujuan hukum. Kemudian, terkait aspek moral dan etika, merupakan hal yang berkaitan dengan penegakan hukum pidana, dikarenakan proses penemuan fakta tidak memihak dan penuh dengan pemecahan masalah yang harus dilakukan dengan adil dan patut.[41]Upaya penegakan hukum dapat dilakukan dengan tiga cara, pre-emtif, preventif dan represif.

a. Upaya Pre-Emtif

   Upaya pre-emtif merupakan upaya awal yang dilakukan oleh pihak kepolisian untuk mencegah terjadinya tindak pidana, tujuan dari upaya ini adalah menghilangkan faktor niat oleh pelaku meskipun ada kesempatan.[42]

b. Upaya Preventif

   Upaya preventif merupakan upaya untuk mencegah terjadinya atau timbulnya kejahatan yang pertama kali, upaya ini bertujuan untuk mencegah

[40] Satjipto Raharjo, *Loc. Cit.*
[41] Muladi, *Loc. Cit.*
[42] Maya Indah, *Perlindungan Korban: Suatu Perspektif Viktimologi dan Kriminologi*, Kencana Prenada, Jakarta, 2014, hlm. 134.

bertemunya niat dan kesempatan seseorang yang hendak melakukan suatu kejahatan.[43]

c. Upaya Represif

Upaya represif merupakan suatu upaya dalam penanggulangan tindak kejahatan secara konsepsional yang ditempuh setelah terjadinya suatu tindak kejahatan. Upaya ini bertujuan untuk membuat pelaku tidak akan mengulanginya dan orang lain juga tidak akan melakukannya mengingat sanksi yang akan ditanggungnya sangat berat.[44]

Upaya represif dan preventif tersebut dapat dilakukan melalui jalur hukum pidana dan diluar jalur hukum pidana. Upaya preventif diluar jalur hukum pidana dilakukan sebagai bentuk pencegahan tanpa penerapan pidana maupun pengendalian sebelum tindak pidana terjadi yang dapat dilakukan oleh masyarakat umum ataupun penegak hukum. Sedangkan, upaya represif jalur hukum pidana dilakukan sebagai bentuk penanganan atau penindakan yang dilakukan setelah tindak pidana terjadi.

Terdapat suatu gagasan baru yaitu sistem keadilan restoratif yang muncul sebagai alternatif dalam proses penegakan hukum yang digunakan oleh para penegak hukum dalam merespon suatu tindak pidana yang terjadi guna mewujudkan tujuan dari penegakan hukum itu sendiri yaitu untuk tercapainya

[43] Airi Safrijal dan Riza Chatias Pratama, *Asas-Asas Hukum Pidana dan Delik-delik Tertent*u, Fakultas Hukum Universitas Muhammadiyah Aceh Press, Banda Aceh, 2017, hlm. 42.

[44] Maya Indah, *Loc. Cit.*

keadilan, kemanfaatan, dan kepastian. Hal tersebut dikarenakan dalam mewujudkan tujuan penegakan hukum tidak hanya terpaku pada Peraturan Perundang-undangan yang tertulis saja.

Sehingga penegakan hukum melalui sistem peradilan, tidak hanya bertolak pada cara berpikir legisme yang hanya bersandar pada Peraturan Perundang-undangan, tetapi melihat hal-hal lain seperti kesabaran, kejujuran, empati, dedikasi, komitmen, keberanian dan hati nurani menjadi bagian penting peran penegakan hukum.[45]

Pasal 2 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia, fungsi kepolisian adalah salah satu fungsi pemerintahan Negara dibidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat. Kemudian, dalam melaksanakan tugas pokok sebagaimana dimaksud dalam Pasal 13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia, Kepolisian Republik Indonesia bertugas:

a. Melaksanakan pengaturan, penjagaan, pengawalan, dan patroli terhadap kegiatan masyarakat dan pemerintah sesuai kebutuhan;
b. Menyelenggarakan segala kegiatan dalam menjamin keamanan, ketertiban dan kelancaran lalu lintas di jalan;

[45] Mahrus Ali, Sistem Peradilan Pidana Progresif: Alternatif dalam Penegakan Hukum Pidana, *Jurnal Hukum*, Edisi Nomor 2 Volume 14, Yogyakarta, 2007, hlm. 1.

c. Membina masyarakat untuk meningkatkan partisipasi masyarakat, kesadaran hukum masyarakat serta ketaatan warga masyarakat terhadap hukum dan peraturan perundang-undangan;
d. Turut serta dalam pembinaan hukum nasional;
e. Memelihara ketertiban dan menjamin keamanan umum;
f. Melakukan koordinasi, pengawasan dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa;
g. Melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya;
h. Menyelenggarakan identifikasi kepolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian;
i. Melindungi keselamatan jiwa raga, harta benda, masyarakat, dan lingkungan hidup dari gangguan ketertiban dan/atau bencana termasuk memberikan bantuan dan pertolongan dengan menjunjung tinggi hak asasi manusia;
j. Melayani kepentingan warga masyarakat untuk sementara sebelum ditandatangani oleh instansi dan/atau pihak yang berwenang;
k. Memberikan pelayanan kepada masyarakat sesuai dengan kepentingannya dalam lingkup tugas kepolisian; dan
l. Melaksanakan tugas lain sesuai dengan peraturan perundang-undangan.

2. Efektivitas Penegakan Hukum

Penegakan hukum merupakan upaya untuk berdiri dan berfungsinya norma hukum secara nyata sebagai pedoman berperilaku dalam hubungan hukum kehidupan masyarakat dan bernegara guna terjaminnya tegaknya hukum. Apabila diperlukan daya paksa oleh penegak hukum maka dapat diperkenankan.[46]

Menurut Soerjono Soekanto, penegakan hukum merupakan suatu kegiatan untuk menyelaraskan hubungan nilai-nilai yang terjabarkan dalam kaidah-kaidah yang mantap dan mewujudkan sikap penegakan hukum untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.[47] Berdasarkan pendapat Lawrence Friedman, dalam sistem hukum memiliki cakupan yang luas dari hukum itu sendiri. Arti kata hukum sendiri sering adanya pengacuan pada aturan dan pengaturan. Menurut Lawrence M. Friedman sistem hukum membedakan antara aturan dan peraturan, struktur, serta lembaga, dan proses yang ada di dalam sistem hukum tersebut.[48] Menurut Lawrence M. Friedman suatu sistem yang berjalan dengan baik memiliki 3 (tiga) unsur, yaitu struktur hukum *(legal structure),* substansi hukum *(legal substance),* dan budaya hukum *(legal culture)*.[49]

---

[46] Jimly Asshiddiqie, *Loc.Cit.*

[47] Soerjono Soekanto, *Penegakan Hukum*, Bina Cipta, Bandung, 1983, hlm. 80.

[48] Lawrence M. Friedman, *The Legal System: A Social Scince Prespective*, Russel Sage Foundation, New York, 1975, hlm 14.

[49] *Ibid.* Lihat juga Lawrence M. Friedman dan Grant M. Hayden, *American Law an Introduction*, Ctk. Ketiga, Oxford University Press, New York, 2017, hlm. 6.

Struktur hukum *(legal structure)* merupakan hal yang memberikan definisi dan bentuk bagi bekerjanya sistem yang ada dengan batasan yang telah ditentukan.[50] Substansi hukum *(legal substance)* merupakan sebuah aturan, norma, dan pola pada perilaku manusia yang berada di dalam sistem hukum tersebut.[51] Sedangkan budaya hukum *(legal culture)* merupakan sikap manusia terhadap hukum dan sistem hukum.[52]

Dalam sistem peradilan pidana *(criminal justice system)* struktur hukum *(legal structure)* yang menjalankan proses peradilan pidana adalah kepolisian, kejaksaan, kehakiman, dan lembaga permasyarakatan. Substansi hukum *(legal substance)* adalah sebuah aturan, norma, dan pola perilaku manusia dalam sistem hukum. Budaya hukum *(legal culture)* sebuah sikap manusia berdasarkan pada hukum dan sistem hukum. Sikap yang dimaksud seperti kepercayaan, nilai-nilai, ide-ide serta harapan masyarakat terhadap hukum dan sistem hukum.

C. Tindak Pidana *Cyber crime* Metode *Phising* menurut Hukum Pidana Islam

1. Pengertian dan Jenis-Jenis Jarimah

Berdasarkan hukum pidana islam, tindak pidana memiliki istilah *jinayah* atau *jarimah*. Menurut bahasa, kata *jarimah* berasal dari kata *jarama* kemudian menjadi bentuk *masdar jaramatan* yang berarti perbuatan dosa atau perbuatan yang salah atau kejahatan. Pelakunya tindak pidana berdasarkan hukum pidana

[50] Lawrence M. Friedman, *The Legal System: A Social Scince Prespective*, *Loc. Cit.*
[51] Lawrence M. Friedman, *American Law an Introduction*, *Loc. Cit.*
[52] *Ibid.*

islam dinamakan dengan *jarim* dan yang dikenai perbuatan itu adalah *mujarom a'alaihi*.[53] *Jarimah* merupakan larangan-larangan *syara'* yang diancam dengan hukuman *had* atau *ta'zir*.[54]

Pengertian mengenai larangan adalah mengabaikan tindakan atau perbuatan yang dilarang atau mengabaikan perintah yang telah ditetapkan. *Syara'* sendiri merupakan sebuah ketetentuan yang berasal dari *nash* berupa wahyu Allah atau teks yang ada dalam Al-Quran yang langsung diterima oleh Nabi Muhammad SAW dan hadist Nabi Muhammad SAW. *Had* sendiri merupakan ketetentuan yang telah ditetapkan hukuman oleh Allah. Sedangkan, *ta'zir* merupakan hukuman yang besar maupun kecil yang ditetapkan oleh penguasa atau pemerintahan.[55]

Pengertian *jarimah* atau disebut dengan peristiwa pidana atau tindak pidana atau delik dalam hukum positif.[56] Namun, hukum positif saat ini membedakan antara kejahatan atau pelanggaran yang berat dan ringan, sedangkan *syari'at* tidak membedakan semuanya sama dengan *jarimah* karena sifatnya merupakan tindak pidana.

Jarimah dapat terjadi apabila dapat merugikan aturan yang telah dibuat oleh masyarakat atau kepercayaan-kepercayaan yang ada di masyarakat, atau yang

---

[53] Marsum, *Fiqih Jinayat (Hukum Pidana Islam),* Penerbitan FH UII, Yogyakarta, 1991, hlm. 2.
[54] Abdul Qadir Audah, *Al Tasyri' al Jina'iy al Islami*, Muamalah al Risalah, Beirut, 1992, hlm. 65.
[55] *Ibid*, hlm. 78.
[56] Ahmad Hanafi, *Asas-Asas Hukum Pindana Islam*, Bulan Bintang, Jakarta, 1996, hlm. 1.

merugikan anggota masyarakat maupun individu yang harusnya dihormati dan dipelihara.[57] Dalam hukum pidana islam dijelaskan bahwa adanya larangan yang harus ditaati agar menjadikan masyarakat yang lebih tertib termasuk juga mengenai perkara jarimah atau tindak pidana Islam. Adapun jenis-jenis *jarimah* terbagi atas: [58]

d. Berdasarkan berat dan ringannya hukuman

Berdasarkan berat dan ringannya hukuman, *jarimah* dapat dibagi menjadi tiga bagian antara lain:

1) *Jarimah hudud*

Merupakan sebuah *jarimah* atau tindak pidana yang memiliki ancaman dengan hukuman *had* yang merupakan hukuman yang telah ditentukan oleh *syara'* dan sudah menjadi hak Allah. Yang termasuk dalam *jarimah hudud* adalah *jarimah zina*, *jarimah* menuduh *zina*, *jarimah jarimah* jarimah perampokan, *jarimah* pencurian, *jarimah* pemberontakan, dan *jarimah* minuman keras.

2) *Jarimah qishash* dan *had*

Merupakan *jarimah* yang diancam dengan hukuman *qishash* atau *diat*. *Qishash* atau *diat* merupakan hukuman yang telah ditentukan oleh *syara'*. Yang termasuk dalam *jarimah qishash* dan *had* adalah pembunuhan

[57] *Ibid*, hlm. 3.
[58] A. Djazuli*, Fiqih Jinayah*, Raja Grafinfo Persada, Jakarta, 2000, hlm. 23-25.

sengaja, pembunuhan karena kesalahan, pembunuhan yang menyerupai sengaja, penganiyaan sengaja, dan penganiyaan tidak sengaja.

3) *Jarimah ta'zir*

Merupakan sebuah hukuman yang belum ditetapkan oleh *syara'* melainkan diserahkan kepada *ulil amri*, baik penentuannya maupun pelaksanaanya.

b. Berdasarkan niatnya

Berdasarkan niatnya, *jarimah* dapat dibagi menjadi dua bagian antara lain:

1) *Jarimah* sengaja

Adalah pelaku yang melakukan tindak pidana sudah memiliki niat untuk melakukan atau sudah direncanakan. Contohnya, seseorang memiliki niat untuk masuk kerumah orang lain dengan memiliki maksud untuk mengambil sesuatu dari rumah tersebut.

2) *Jarimah* tidak sengaja

Adalah pelaku yang tidak sengaja untuk melakukan perbuatan yang dilarang dan perbuatan tersebut terjadi akibat adanya kelalaiannya. Contohnya, seseorang melempar batu untuk mengusir binatang yang membahayakan, tetapi batu tersebut mengenai orang lain bukan mengenai binatang yang membahayakan tersebut.

c. Berdasarkan objeknya

Berdasarkan objeknya, *jarimah* dapat dibagi menjadi dua yaitu:

1) *Jarimah* perseorangn

Merupakan suatu *jarimah* dimana hukuman terhadap pelakunya dijatuhkan untuk melindungi hak perseorangan seperti penghinaan, penipuan, dan sebagainya.

2) *Jarimah* masyarakat

Merupakan suatu *jarimah* di mana hukuman terhadap pelakunya dijatuhkan untuk melindungan kepentingan masyarakat. Contohnya seperti korupsi.

d. Berdasarkan cara melakukannya

Berdasarkan cara melakukannya, *jarimah* dapat dibagi menjadi dua bagian yaitu:

1) *Jarimah* negatif

Merupakan *jarimah* yang terjadi dikarenakan meninggalkan perbuatan yang sudah diperintahkan. Seperti tidak mau melakukan sholat dan puasa.

2) *Jarimah* positif

Merupakan *jarimah* yang terjadi karena adanya perbuatan yang dilarang. Seperti melakukan *zina*.

e. Berdasarkan motifnya

Berdasarkan motifnya, *jarimah* dapat dibagi menjadi dua bagian yaitu:

1) *Jarimah* biasa

Merupakan sebuah *jarimah* yang dilakukan oleh individu tanpa mengaitkannya dengan tujuan tertentu. Seperti mencuri ayam.

2) *Jarimah* politik

Merupakan *jarimah* yang adanya pelanggaran terhadap adanya peraturan pemerintah atau pejabat pemerintah. Contohnya seperti: pemberontakan.

2. Tindak Pidana *Cyber crime* Metode *Phising* menurut Hukum Pidana Islam

Phising merupakan salah satu kejahatan elektronik dalam lingkup penipuan, dimana proses *phising* ini memiliki tujuan untuk mengambil informasi yang sangat sensitif seperti *username, password*, dan detail kartu kredit dalam bentuk meniru sebagai sebuah lembaga yang dipercaya dan biasanya berkomunikasi secara elektronik.[59]

Berdasarkan *syaria*t agama islam, menipu adalah membohongi yang termasuk dalam bentuk orang yang munafik. Sehingga, dalam perbuatan membohongi terdapat unsur munafik, yang mana unsur itu adalah mengelabuhi ataupun menipu korban. Terdapat ayat Al-Qur'an mengenai orang yang munafik yang dinyatakan dalam surah An-Nisaa' ayat 145 sebagai berikut:

إِنَّ ٱلْمُنَٰفِقِينَ فِى ٱلدَّرْكِ ٱلْأَسْفَلِ مِنَ ٱلنَّارِ وَلَن تَجِدَ لَهُمْ نَصِيرًا

Artinya: Sesungguhnya orang-orang munafik itu (ditempatkan) pada tingkatan yang paling bawah dari neraka. Dan kamu sekali-kali tidak akan mendapat seorang penolongpun bagi mereka.

Ayat tersebut di atas memberikan pengertian kepada orang munafik yang lebih membahayakan daripada orang kafir. Apabila merampas atau merampok harta maka hukumannya seperti hukuman orang kafir yaitu hukuman mati, maka

[59] Dian Rachmawati, *Loc. Cit.*

hukuman terhadap orang munafik minimal sama dengan hukuman yang ditentukan terhadap perampok.

Terdapat pula hadist yang diriwayatkan oleh Jabir RA tentang hukuman bagi pelaku tindak pidana penipuan sebagai berikut, *Jabir RA menceritakan, Nabi Muhammad SAW bersabda: tidak ada hukuman potong tangan atas penghianat, pencopet dan perampok di jalan." (HR. Ahmad, Abu Daud, An-Nasa-y, At-Turmudzy dan Ibnu Majah).*[60]

Berdasarkan hadist tersebut di atas, maka dapat disamakan antara penghianat dengan penipuan yang dalam hadis di atas dapat ditarik kesimpulan hukuman terhadap penghianat, pencopet dan perampok di jalan tidak dapat dipotong tanganya seperti pada hukuman *sariqah* atau pencurian. Sehingga, hukuman yang dapat diberikan terhadap pelaku kejahatan penipuan ini adalah *jarimah ta'zir*. Pengertian *ta'zir* sendiri merupakan hukuman atas dosa-dosa yang telah dilakukan oleh pelaku *jarimah* yang belum bisa ditentukan hukumannya oleh syarat.[61] Dalam *ta'zir*, terdapat beberapa hukuman yaitu: [62]

1. Pidana mati

   Imam Hanafi berpendapat bahwa memperbolehkan dalam hukuman *ta'zir* dengan hukuman mati tetapi memiliki syarat apabila kesalahan tersebut dilakukan berulang-ulang. Imam Malik juga berpendapat bahwa

[60] Imam Az-Zabid, *Ringkasan Shahih Al-Bukhari*, Mizan Pustaka, Bandung, 2008, hlm. 540.
[61] Ahmad Azhar, *Kamus Istilah Hukum Islam*, Fakultas Hukum UII, Yogyakarta, 1987, hlm. 53.
[62] A. Jazuli, *Op. Cit.,* hlm. 188.

memperbolehkan hukuman mati sebagai sanksi tertinggi dalam *ta'zir*, dan Imam Syafi'e juga memperbolehkan adanya hukuman mati dalam *ta'zir*.

2. Pidana dera atau cambuk

   Hukuman ini merupakan hukuman terendah dalam *ta'zir* misalnya seperti melakukan *zina*. Hukuman dera bukanlah sebuah hukuman mati tetapi hukuman yang meninggalkan bekas luka.

3. Pidana penjara

   Dalam hukum islam, pidana penjara dibagi menjadi dua yaitu pidana penjara yang terbatas yang artinya memiliki batas waktunya dan pidana penjara yang tidak memiliki batas waktu.

BAB III

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA *CYBER CRIME PHISING* OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

A. Kendala yang Dihadapi Polda DIY pada Penanganan Tindak Pidana *Cyber Crime* Metode *Phising*

Penegakan hukum merupakan suatu proses dilakukannya upaya untuk tegaknya norma-norma hukum secara nyata sebagai pedoman perilaku dalam hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.[63] Penegakan

[63] Jimly Asshiddiqie, *Loc.Cit.*

hukum juga merupakan suatu bentuk pelaksanaan hukum secara nyata dengan usaha mewujudkan ide-ide keadilan, kepastian hukum, kemanfaatan sosial dan keadilan menjadi kenyataan.[64] Konsep dasar penegakan hukum pidana membutuhkan adanya unsur moral terkait hubungan moral dengan penegakan hukum yang dapat menentukan keberhasilan atau ketidakberhasilan suatu penegakan hukum yang menjadi harapan tujuan hukum.

Berdasarkan Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, ruang lingkup tugas dan fungsi lembaga kepolisian memiliki tugas pokok memelihara keamanan dan ketertiban masyarakat, menegakan hukum, dan memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat.[65] Pada penelitian ini penegakan hukum terfokus pada instansi kepolisian yang memiliki fungsi penegakan hukum pada penyelidikan dan penyidikan. Upaya penyelidikan dan penyidikan dalam penegakan hukum yang dilakukan oleh Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta (Polda DIY) berpedoman pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sebelum melakukan analisa terhadap kendala yang Dihadapi Polda DIY pada penanganan tindak pidana *cyber crime* metode *phising*, peneliti akan memaparkan proses penegakan hukumnya. Berdasarkan keterangan Iptu Anis Dwi Haryanto, penegakan hukum dimulai dari proses penerimaan laporan korban tindak pidana

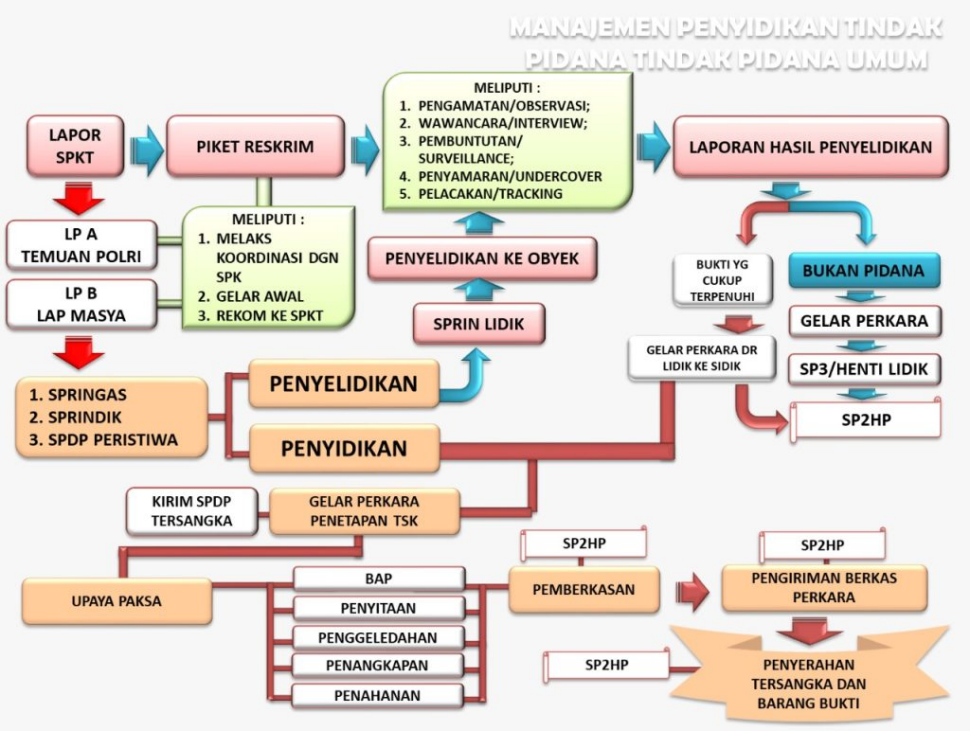
[64] Satjipto Raharjo, *Loc.Cit.*

[65] Pasal 13 Undang-Undang Nomor 2 Tahun 2002. Lihat juga Andi Hamzah, *Masalah Penegakan Hukum Pidana*, Rineka Cipta, Jakarta 1994, hlm. 27.

cyber crime metode *phising* pada Sentra Pelayanan Kepolisian Terpadu (SPKT). Kemudian, setelah laporan masuk maka akan diterima oleh pimpinan untuk dilakukan disposisi atau tanggapan atau intruksi yang diberikan oleh atasan kepada bawahannya untuk segera di tindak lanjuti.[66]

Setelah itu laporan tersebut akan dilakukan *profiling* seperti pengamatan atau observasi. Setelah melakukan tahapan profiling maka didapati laporan hasil penyelidikan dan akan dilakukan gelar perkara.[67] Laporan hasil penyelidikan tersebut berfungsi untuk menyimpulkan apakah perkara tersebut dapat dilanjutkan atau tidak.[68] Apabila dapat dilanjutkan maka dapat dilakukan upaya paksa seperti pemanggilan, penyitaan, penangkapan, dan penahanan. Agar lebih mudah dipahami peneliti akan menyajikan infografis terkait proses manajemen penyidikan tindak pidana sebagai berikut.

[66] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.
[67] *Ibid.*
[68] *Ibid.*



Gambar 1.0: Bagan Mekanisme Penyidikan Tindak Pidana.[69]

Dalam berbagai upaya tersebut tentu Polda DIY mengalami hambatan-hambatan dalam peranan sebagai aparatur penegakan hukum. Berdasarkan keterangan Iptu Anis Dwi Haryanto, laporan yang diterima pihak kepolisian terkait tindak pidana *cyber crime* metode *phising* hanya berdasarkan petunjuk bukti nomor telefon serta rekening bank.[70] Hal tersebut menyulitkan pihak kepolisian dalam melakukan tahapan penyelidikan *profiling*. Spesifiknya, pada tahapan pengamatan dan

[69] Kepolisian Resor Tuban, Mekanisme Penyidikan Tindak Pidana, terdapat dalam https://tribratanews.tuban.jatim.polri.go.id/alur-manajemen-penyidikan-tindak-pidana/, Diakses tanggal 25 September 2023 pukul 17:29 WIB.

[70] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

observasi terhadap tidak terdapatnya data dan petunjuk membuat kasus tidak dapat dilakukan naik sidik.

Terlebih, bukti petunjuk berupa rekening bank tidak dapat diungkap apapun alasannya meskipun oleh pihak kepolisian kecuali, apabila kasus tersebut telah pada tahap naik sidik atau telah menetapkan tersangka.[71] Sepanjang tahun 2021 hingga tahun 2023 Polda DIY mendapat laporan 133 kasus tindak pidana *cyber crime* metode *phising* yang terbagi menjadi modus tautan palsu (*Link*) dan *One-Time Password* (OTP) atau kata sandi sekali pakai palsu.[72] Adapun rekapitulasi data pengaduan tindak pidana *cyber crime* metode *phising* pada tahun 2021 hingga tahun 2023 peneliti sajikan pada tabel-tabel berikut.[73]

NO	BULAN	MODUS OPERANDI	
		LINK	OTP
1	JANUARI	2	1
2	FEBRUARI	4	3
3	MARET	1	1
4	APRIL	2	2
5	MEI		1
6	JUNI	2	1
7	JULI	5	2
8	AGUSTUS	2	1
9	SEPTEMBER	9	2
10	OKTOBER	4	3
11	NOVEMBER	1	1
12	DESEMBER	3	1
JUMLAH		35	19

Tabel 1.0: Rekapitulasi data pengaduan tindak pidana *cyber crime* metode *phising* pada tahun 2021 di Polda DIY.

[71] *ibid.*
[72] *ibid.*
[73] *ibid.*

NO	BULAN	MODUS OPERANDI	
		LINK	OTP
1	JANUARI	2	1
2	FEBRUARI	1	
3	MARET	3	1
4	APRIL	2	
5	MEI		2
6	JUNI	2	1
7	JULI		4
8	AGUSTUS	5	2
9	SEPTEMBER	3	2
10	OKTOBER	8	1
11	NOVEMBER	4	1
12	DESEMBER	10	
JUMLAH		40	15

Tabel 2.0: Rekapitulasi data pengaduan tindak pidana *cyber crime* metode *phising* pada tahun 2022 di Polda DIY.

NO	BULAN	MODUS OPERANDI	
		LINK	OTP
1	JANUARI	4	
2	FEBRUARI	2	
3	MARET	4	
4	APRIL	1	
5	MEI	4	
6	JUNI	7	
7	JULI	2	
8	AGUSTUS		
9	SEPTEMBER		
10	OKTOBER		
11	NOVEMBER		
12	DESEMBER		
JUMLAH		24	0

Tabel 3.0: Rekapitulasi data pengaduan tindak pidana *cyber crime* metode *phising* pada tahun 2023 di Polda DIY.

Berbagai kasus tindak pidana *cyber crime* metode *phising* tersebut di atas kebanyakan terhambat pada proses penyelidikan tahapan *profiling*.[74] Hal tersebut dikarenakan sulitnya menentukan pelaku akibat data petunjuk yang tidak dapat diungkap.[75] Berbagai kasus tindak pidana *cyber crime* metode *phising* tersebut di atas juga memiliki berbagai latar belakang faktor pelaku seperti faktor ekonomi hingga faktor manusia dengan menguji kemampuan.[76] Faktor manusia tersebut dilakukan dengan tujuan harapan setelah melakukan tindakan sang pelaku akan meminta sejumlah uang atau pekerjaan pada perusahaan yang ditujunya.[77] Adapun modus pelaku yaitu mengaku dari pihak yang resmi seperti perbankan, kepolisian, instansi pemerintahan, hingga modus aplikasi berformat *apk*. Para pelaku menggunakan kelemahan psikologis korban agar panik dan kemudian menggunakan kepanikannya tersebut untuk mengikuti langkah-langkah jebakan yang telah di rencanakan oleh pelaku.[78]

Tidak seluruh 133 kasus tindak pidana *cyber crime* metode *phising* tersebut di atas terhambat. Terdapat contoh tiga kasus yang berhasil ditangani oleh Polda DIY. Berikut merupakan identifikasi data kasus terbaru yang ditangani oleh Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Polda DIY:[79]

1. Kasus penipuan yang mengaku pihak PT Telekomunikasi Indonesia Tbk

[74] *ibid.*
[75] *ibid.*
[76] *ibid.*
[77] *ibid.*
[78] *ibid.*
[79] *ibid.*

Kasus ini terjadi ketika para pelaku yang mengaku-ngaku merupakan pihak dari PT Telekomunikasi Indonesia Tbk. Korban atas kasus ini beragam mulai pelajar hingga para orang yang berpendidikan. Kasus ini memiliki modus melalui telefon rumah yang mana pelaku menyampaikan bahwa identitas korban telah digunakan atas tunggakan tagihan yang belum dibayarkan berbulan-bulan.

Bahkan, pelaku mengatakan identitas korban telah digunakan oleh pelaku sindikat Narkotika dan Obat-Obatan Berbahaya (Narkoba). Korban yang panik dimanfaatkan oleh para pelaku yang kemudian memberikan solusi padahal, hal tersebut merupakan jebakan. Kerugian atas kasus ini berkisar Rp430.000.000,00 (empat ratus tiga puluh juta rupiah).

2. Kasus pemalsuan website pihak PT Karya Beton Sudhira

   Kasus ini dialami oleh PT Karya Beton Sudhira yang beralamat pada Jalan Solo KM 1, Krajan, Tirtomartani, Kecamatan Kalasan, Kabupaten Sleman, Daerah Istimewa Yogyakarta. Akibat dari pemalsuan website ini, seorang korban mengalami kerugian sebesar Rp50.000.000,00 (lima puluh juta rupiah). Polda DIY menangani kasus ini dengan menggunakan dasar hukum Pasal 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Kasus penipuan yang mengaku pihak perbankan

   Kasus yang melibatkan berbagai pihak perbankan Indonesia seperti Bank Negara Indonesia (BNI), Bank Central Asia (BCA), hingga Bank Rakyat Indonesia (BRI). Berbagai kerugian telah dialami oleh para korban bahkan,

terdapat korban yang kerugiannya mencapai Rp500.000.000,00 (lima ratus juta rupiah). Polda DIY menduga bahwa kasus yang dialami oleh nasabaha perbankan tersebut diawali dengan tindak pidana *cyber crime* metode *phising* namun, terdapat faktor internal dari perbankan itu sendiri yaitu kebocoran data yang menyebabkan para pelaku dengan mudah menghubungi korban dan meminta OTP dari para korban.

Berdasarkan kasus-kasus tersebut di atas serta berdasarkan keterangan Iptu Anis Dwi Haryanto, para pelaku merupakan jaringan internasional yang melakukan modusnya dari luar negeri.[80] Peneliti kemudian mewawancarai Iptu Anis Dwi Haryanto mengenai kendala upaya penegakan hukum terhadap tindak pidana *cyber crime* metode *phising* yang diproses pada Polda DIY. Berdasarkan wawancara tersebut peneliti mendapatkan dua faktor internal dan faktor eksternal mengenai hal-hal yang menghambat upaya penegakan hukum tersebut sebagai berikut.

1. Faktor Internal

   Terdapat dua kendala internal yang dialami Polda DIY terkait tindak pidana *cyber crime* metode *phising.* Pertama, kendala akan kurangnya personil atau kekurangan sumber daya manusia dalam mengungkap tindak pidana *cyber crime* metode *phising.* Kedua, kurangnya peralatan. Hal tersebut dikarenakan tindak pidana *cyber crime* metode *phising* membutuhkan kerjasama berbagai instansi dari seluruh Indonesia. Namun, saat ini yang mumpuni dalam menangani

[80] *ibid.*

hanyalah Polda Metro Jaya, Polda DIY, dan Polda Jatim. Hal tersebut dikarenakan ketiga Polda tersebut memiliki lab digital forensik yang mumpuni dalam mengatasi tindak pidana *cyber crime* metode *phising.* Hal tersebut dikarenakan ketiga Polda tersebut memiliki laboratorium digital forensik yang mumpuni dalam mengatasi tindak pidana *cyber crime* metode *phising.* Laboratorium tersebut telah meraih ISO 17025:2018 sebagai laboratorium uji dan kalibrasi dalam bidang komputer forensik yang memenuhi standard mutu dalam hal manajerial dan teknis pemeriksaan barang bukti digital.[81]

2. Faktor Eksternal

Terdapat tiga kendala eksternal yang dialami Polda DIY terkait tindak pidana *cyber crime* metode *phising.* Pertama, minimnya petunjuk. Hal tersebut dikarenakan ketika melaporkan tindak pidana *cyber crime* metode *phising,* para pelapor hanya melaporkan nomor telefon dan rekening bank, ketika nomor telefon tersebut tidak dapat dilacak maka otomatis pihak kepolisian akan melakukan penyidikan terhadap rekening bank. Namun, tidak sembarang orang dapat membuka rekening bank tersebut dikarenakan berbagai syarat seperti tahap penyidikan telah menetapkan tersangka hingga memiliki izin dari Otoritas Jasa Keuangan (OJK).

[81] Direktorat Tindak Pidana Siber Bareskrim Polri, "Tentang Direktorat Tindak Pidana Siber (Dittipidsiber)", terdapat dalam https://patrolisiber.id/about, Diakses tanggal 22 Oktober 2023 pukul 19:40 WIB.

Kedua, sifatnya tidak terbatas. Hal tersebut dikarenakan terdapat kasus yang pelakunya melakukan tindak pidana *cyber crime* metode *phising* yang berasal dari Lembaga Pemasyarakatan (Lapas). Hal tersebut patut tidak terduga dikarenakan berbagai macam teknologi dibatasi di Lapas. Ketiga, lokasi pelaku di luar perkiraan pihak kepolisian. Hal tersebut dikarenakan para pelaku yang memiliki jaringan internasional melakukan tindak pidana *cyber crime* metode *phising* di luar negeri. Tidak terbatas negara mana saja. Bahkan, ketika melakukan pelacakan nomor telefon, lokasi pelaku dapat berganti-ganti seiring waktu akibat teknologi yang mereka miliki.

Berdasarkan analisa tersebut di atas, dapat disimpulkan bahwa terdapat lima kendala yang dialami oleh Polda DIY terkait penanganan tindak pidana *cyber crime* metode *phising.* Pertama, kurangnya sumber daya manusia dalam mengungkap tindak pidana *cyber crime* metode *phising.* Kedua, kurangnya peralatan. Ketiga, minimnya petunjuk. Keempat, sifatnya tidak terbatas. Kelima, lokasi pelaku di luar perkiraan pihak kepolisian

B. Upaya yang Dilakukan Polda DIY untuk Mengatasi Kendala Penanganan Tindak Pidana *Cyber Crime* Metode *Phising*

Setelah menganalisa terhadap kendala yang dialami oleh Polda DIY terkait penanganan tindak pidana *cyber crime* metode *phising* maka, pembahasan berikutnya mengenai upaya dan solusi atas kendala-kendala tersebut. Berdasarkan pendapat Lawrence M. Friedman, bekerjanya hukum dalam suatu sistem ditentukan oleh tiga unsur, yaitu struktur hukum (*legal strukture*), substansi hukum (*legal*

substance), dan budaya hukum (*legal culture*).[82] Struktur hukum merupakan kerangka berpikir yang memberikan definisi dan bentuk bagi bekerjanya sistem yang ada pada batasan yang telah ditentukan.

Struktur hukum dapat disebut sebagai lembaga yang menjalankan fungsi penegakan hukum dengan segala prosses yang ada pada lembaga tersebut.[83] Adapun teori terkait faktor-faktor yang mempengaruhi penegakan hukum berdasar pendapat Lawrence M. Friedman tersebut sebagai berikut:

1. Faktor Struktur Hukum

   Struktur hukum *(legal structure)* merupakan hal yang memberikan definisi dan bentuk bagi bekerjanya sistem yang ada dengan batasan yang telah ditentukan.[84] Terhadap kendala dalam penanganan tindak pidana *cyber crime* metode *phising* oleh Polda DIY, hambatan dalam struktur hukum terdapat pada kurangnya sumber daya manusia dan kurangnya peralatan dalam mengungkap tindak pidana *cyber crime* metode *phising.*

   Kedua hal tersebut dikarenakan tindak pidana *cyber crime* metode *phising* membutuhkan kerjasama berbagai instansi dari seluruh Indonesia. Namun, saat ini yang mumpuni dalam menangani hanyalah Polda Metro Jaya, Polda DIY, dan Polda Jatim. Hal tersebut dikarenakan ketiga Polda tersebut memiliki lab digital

[82] Lawrence M. Friedman, *The Legal System: A Social Scince Prespective*, Russel Sage Foundation, New York, 1975, hlm. 14.
[83] *ibid.*
[84] *ibid.*

forensik yang mumpuni dalam mengatasi tindak pidana *cyber crime* metode *phising.*

2. Faktor Substansi Hukum

Substansi hukum *(legal substance)* merupakan sebuah aturan, norma, dan pola pada perilaku manusia yang berada di dalam sistem hukum tersebut.[85] Terhadap kendala dalam penanganan tindak pidana *cyber crime* metode *phising* oleh Polda DIY, kendala terkait substansi hukum terdapat pada minimnya petunjuk. Hal tersebut dikarenakan ketika melaporkan tindak pidana *cyber crime* metode *phising,* para pelapor hanya melaporkan nomor telefon dan rekening bank, ketika nomor telefon tersebut tidak dapat dilacak maka otomatis pihak kepolisian akan melakukan penyidikan terhadap rekening bank. Namun, tidak sembarang orang dapat membuka rekening bank tersebut dikarenakan regulasi yang ketat dan berbagai syarat seperti tahap penyidikan telah menetapkan tersangka hingga memiliki izin dari OJK.

3. Faktor Budaya Hukum

Faktor budaya hukum *(legal culture)* merupakan sikap manusia terhadap hukum dan sistem hukum.[86] Budaya hukum juga merupakan kekuatan sosial yang menentukan bagaimana hukum dilaksanakan, dihindari atau bahkan

[85] Lawrence M. Friedman, *American Law an Introduction)*, W. W. Norton and Company, New York, 1984, hlm. 4.
[86] *ibid.*

bagaimana hukum disalahgunakan.[87] Terhadap kendala dalam penanganan tindak pidana *cyber crime* metode *phising* oleh Polda DIY, hambatan dalam budaya hukum dikarenakan tindak pidana *cyber crime* metode *phising* yang sifatnya tidak terbatas.

Hal tersebut dikarenakan lokasi pelaku di luar perkiraan pihak kepolisian. Terdapat pelaku yang berasal dari Lapas hingga pelaku yang memiliki jaringan internasional. Hal tersebut menuntut pihak kepolisian untuk melakukan kerja sama secara internasional.

Berdasarkan keterangan Iptu Anis Dwi Haryanto, peneliti mendapati bahwa terdapat tiga upaya dan solusi untuk mengatasi kendala dalam tindak pidana *cyber crime* metode *phising* yang dilakukan oleh Polda DIY. Ketiga upaya tersebut adalah upaya pre-emtif, upaya preventif, dan upaya represif. Berikut merupakan hasil analisa yang dilakukan oleh peneliti.

1. Upaya Pre-Emtif

Upaya pre-emtif merupakan upaya awal yang dilakukan oleh pihak kepolisian untuk mencegah terjadinya tindak pidana, tujuan dari upaya ini adalah menghilangkan faktor niat oleh pelaku meskipun ada kesempatan.[88] Upaya pre-

[87] Any Ismawati, Pengaruh Budaya Hukum Terhadap Pembangunan Hukum di Indonesia (Kritik Terhadap Lemahnya Budaya Hukum di Indonesia), *Pranata Hukum*, Edisi Nomor 1 Volume 6, 2011, hlm. 57

[88] Maya Indah, *Perlindungan Korban: Suatu Perspektif Viktimologi dan Kriminologi*, Kencana Prenada, Jakarta, 2014, hlm. 134.

emtif yang dilakukan oleh Polda DIY terhadap tindak pidana *cyber crime* metode *phising* berupa sosialisasi.

Upaya sosialisasi kepada masyarakat tersebut dapat melalui media sosial resmi kepolisian maupun melalui Bhayangkara Pembina Keamanan dan Ketertiban Masyarakat (Bhabinkamtibmas) agar disampaikan langsung kepada masyarakat mengenai pencegahan tindak pidana *cyber crime* metode *phising.* Upaya sosialisasi bertujuan agar masyarakat memahami tentang pentingnya menjaga data pribadi yang termasuk OTP.[89]

2. Upaya Preventif

Upaya preventif merupakan upaya untuk mencegah terjadinya atau timbulnya kejahatan yang pertama kali, upaya ini bertujuan untuk mencegah bertemunya niat dan kesempatan seseorang yang hendak melakukan suatu kejahatan.[90] Upaya preventif yang dilakukan oleh Polda DIY berupa mengungkap kasus tindak pidana *cyber crime* metode *phising.* Dengan mengungkap kasus maka kesempatan terjadinya tindak pidana *cyber crime* metode *phising* menjadi minim. Upaya tersebut juga bertujuan untuk memberikan efek jera kepada pelaku.[91]

3. Upaya Represif

[89] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

[90] Airi Safrijal dan Riza Chatias Pratama, *Asas-Asas Hukum Pidana dan Delik-delik Tertent*u, Fakultas Hukum Universitas Muhammadiyah Aceh Press, Banda Aceh, 2017, hlm. 42.

[91] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

Upaya represif merupakan suatu upaya dalam penanggulangan tindak kejahatan secara konsepsional yang ditempuh setelah terjadinya suatu tindak kejahatan. Upaya ini bertujuan untuk membuat pelaku tidak akan mengulanginya dan orang lain juga tidak akan melakukannya mengingat sanksi yang akan ditanggungnya sangat berat.[92]

Upaya represif yang dilakukan oleh Polda DIY terhadap tindak pidana *cyber crime* metode *phising* berupa pemenuhan ketentuan Peraturan Perundang-undangan. Polda DIY menggunakan dasar hukum utama Pasal 378 KUHP dalam menangani tindak pidana *cyber crime* metode *phising.* Selain itu Polda DIY juga menggunakan Pasal 28 ayat (1) dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[93]

Berdasarkan ketiga upaya tersebut, serta berdasarkan keterangan Iptu Anis Dwi Haryanto, upaya yang paling efektif dilakukan terhadap masyarakat adalah upaya pre-emtif. Upaya tersebut berupa memberikan sosialisasi kepada masyarakat melalui media sosial maupun melalui bhabinkamtibmas mengenai pencegahan tindak pidana *cyber crime* metode *phising.*

Sehubungan dengan upaya represif, tindak pidana *cyber crime* metode *phising* yang dalam hukum pidana islam merupakan penipuan maka hukuman yang dapat

[92] Maya Indah, *Loc. Cit.*

[93] Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

diberikan terhadap pelaku kejahatan penipuan ini adalah *jarimah ta'zir*. Pengertian *jarimah ta'zir* sendiri merupakan hukuman atas dosa-dosa yang telah dilakukan oleh pelaku *jarimah* yang belum bisa ditentukan hukumannya oleh syarat.[94] Dalam *ta'zir*, terdapat beberapa hukuman yaitu: [95]

1. Pidana Mati

   Imam Hanafi berpendapat bahwa memperbolehkan dalam hukuman ta'zir dengan hukuman mati tetapi memiliki syarat apabila kesalahan tersebut dilakukan berulang-ulang. Imam Malik juga berpendapat bahwa memperbolehkan hukuman mati sebagai sanksi tertinggi dalam *ta'zir*, dan Imam Syafi'e juga memperbolehkan adanya hukuman mati dalam *ta'zir*.

2. Pidana Dera atau Cambuk

   Hukuman ini merupakan hukuman terendah dalam *ta'zir* misalnya seperti melakukan *zina*. Hukuman dera bukanlah sebuah hukuman mati tetapi hukuman yang meninggalkan bekas luka.

3. Pidana Penjara

   Dalam hukum islam, pidana penjara dibagi menjadi dua yaitu pidana penjara yang terbatas yang artinya memiliki batas waktunya dan pidana penjara yang tidak memiliki batas waktu.

Berdasarkan analisa tersebut di atas, maka dapat disimpulkan bahwa upaya dan solusi atas kendala-kendala penanganan tindak pidana *cyber crime* metode *phising*

[94] Ahmad Azhar, *Loc. Cit*
[95] A. Jazuli, *Loc. Cit*

oleh Polda DIY dilakukan melalui tiga cara. Pertama, upaya pre-emtif berupa sosialisasi melalui media sosial resmi kepolisian maupun melalui Bhabinkamtibmas yang bertujuan agar masyarakat memahami tentang pentingnya menjaga data pribadi.

Kedua, upaya preventif berupa mengungkap kasus tindak pidana *cyber crime* metode *phising* yang bertujuan untuk memberikan efek jera kepada pelaku. Ketiga, upaya represif dengan Polda DIY menggunakan dasar hukum utama Pasal 378 KUHP. Selain itu Polda DIY juga menggunakan Pasal 28 ayat (1) dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

BAB IV

PENUTUP

A. Kesimpulan

1. Kendala Polda DIY dalam penegakan hukum tindak pidana *cyber crime* metode *phising* terdapat pada tahapan penyelidikan *profiling* dikarenakan tidak terdapatnya data dan petunjuk yang membuat kasus tidak dapat dilakukan naik sidik. Berdasarkan hal tersebut, terdapat lima kendala yang dialami oleh Polda DIY. Pertama, kurangnya sumber daya manusia dalam mengungkap tindak pidana *cyber crime* metode *phising.* Kedua, kurangnya peralatan. Ketiga, minimnya petunjuk. Keempat, sifatnya tidak terbatas. Kelima, lokasi pelaku di luar perkiraan pihak kepolisian.
2. Upaya dan solusi atas kendala-kendala penanganan tindak pidana *cyber crime* metode *phising* oleh Polda DIY dilakukan melalui tiga cara. Pertama, upaya pre-emtif berupa sosialisasi melalui media sosial resmi kepolisian maupun melalui Bhabinkamtibmas yang bertujuan agar masyarakat memahami tentang pentingnya menjaga data pribadi. Kedua, upaya preventif berupa mengungkap kasus tindak pidana *cyber crime* metode *phising* yang bertujuan untuk memberikan efek jera kepada pelaku. Ketiga, upaya represif dengan Polda DIY menggunakan dasar hukum utama Pasal 378 KUHP. Selain itu Polda DIY juga menggunakan Pasal 28 ayat (1) dan Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Saran

1. Polda DIY dapat melakukan kerja sama dengan instansi perguruan tinggi untuk meminimalisir kendala, terutama terkait kurangnya sumber daya manusia dan kurangnya peralatan.
2. Polda DIY dapat memaksimalkan upaya pre-emtif dengan meningkatkan sinergi antara instansi seperti dengan Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta.

DAFTAR PUSTAKA

Buku

A. Djazuli*, Fiqih Jinayah*, Raja Grafinfo Persada, Jakarta, 2000.

Abdul Qadir Audah, *Al Tasyri' al Jina'iy al Islami*, Muamalah al Risalah, Beirut, 1992.

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung, 2005.

Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, 2004.

Adami Chazawi, *Pelajaran Hukum Pidana 1*, Raja Grafindo Persada, Jakarta, 2005.

Ahmad Azhar, *Kamus Istilah Hukum Islam*, Fakultas Hukum UII, Yogyakarta, 1987.

Ahmad Hanafi, *Asas-Asas Hukum Pindana Islam*, Bulan Bintang, Jakarta, 1996.

Ahmad M. Ramli, Tasya Safiranita Ramli, dan Ferry Gunawan, *Hukum Telematika*, Universitas Terbuka, Banten, 2020.

Airi Safrijal dan Riza Chatias Pratama, *Asas-Asas Hukum Pidana dan Delik-delik Tertent*u, Fakultas Hukum Universitas Muhammadiyah Aceh Press, Banda Aceh, 2017.

Andi Hamzah, *Aspek-Aspek Pidana dibidang Komputer*, Sinar Grafika, Jakarta, 1992.

Andi Hamzah, *Hukum Pidana yang berkaitan dengan komputer*, Sinar Grafika Offset, Jakarta, 1993.

Andi Hamzah, *Masalah Penegakan Hukum Pidana*, Rineka Cipta, Jakarta 1994.

Anti-*Phising* Working Group, *Phishing Activity Trends Report 4th Quarter 2022*, 2022.

Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bhakti, Bandung, 2003.

Dani Krisnawati, Eddy O.S. Hiariej, Marcus Priyo Gunarto, Sigid Riyanto, dan Supriyadi, *Bunga Rampai Hukum Pidana Khusus*, Pena Ilmu dan Amal, Jakarta, 2006.

Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005.

Dwi Haryadi, *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*, Penerbit Lima, Yogyakarta, 2013.

Imam Az-Zabid, *Ringkasan Shahih Al-Bukhari*, Mizan Pustaka, Bandung, 2008.

Indonesia Anti-Phishing Data Exchange, *Laporan Aktivitas Phishing Domain .ID Periode Q2 2023*, Jakarta, 2023.

J.E Sahetapy, *Bunga Rampai Viktimisasi*, Eresco, Bandung, 1995.

Lawrence M. Friedman, *American Law an Introduction)*, W. W. Norton and Company, New York, 1984.

Lawrence M. Friedman, *The Legal System: A Social Scince Prespective*, Russel Sage Foundation, New York, 1975.

Marsum, *Fiqih Jinayat (Hukum Pidana Islam),* Penerbitan FH UII, Yogyakarta, 1991.

Maya Indah, *Perlindungan Korban: Suatu Perspektif Viktimologi dan Kriminologi*, Kencana Prenada, Jakarta, 2014.

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

Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris,* Pustaka Pelajar, Yogyakarta, 2009.

Muladi, *Hak Asasi Manusia*, Refika Aditama, Bandung, 2009.

P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997.

R. Abdoel Djamali, *Pengantar Hukum Indonesia*, Raja Grafindo Persada, Jakarta, 2014.

Satjipto Raharjo, *Hukum dan Masyarakat*, Angkasa, Bandung, 1980.

Soerjono Soekanto, *Penegakan Hukum*, Bina Cipta, Bandung, 1983.

Suresh T. Viswanathan, *The Indian Cyber Laws with Cyber Gl*ossary, Bharat Law House, New Delhi, 2001.

Symantec, *Internet Security Threat Report Volume 24 February 2019*, California, 2019.

Widyo Pramono, *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta, 1994.

Jurnal Penelitian

Ade Nuriadin dan Yefi Dyan Nofia Harumike, Sejarah Perkembangan dan Implikasi Internet Pada Media Massa dan Kehidupan Masyarakat, *Selasar KPI: Referensi Media Komunikasi dan Dakwah*, Edisi No. 1 Vol 1 2021.

Alexander Anggono, Tarjo, dan Moh. Riskiyadi, Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis, *Jurnal Manajemen dan Organisasi (JMO)*, Edisi No. 3 Vol. 12 2021.

Any Ismawati, Pengaruh Budaya Hukum Terhadap Pembangunan Hukum di Indonesia (Kritik Terhadap Lemahnya Budaya Hukum di Indonesia), *Pranata Hukum*, Edisi Nomor 1 Volume 6, 2011.

Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi, Cyber crime dalam Bentuk *Phising* Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik, *PAMPAS: Journal of Criminal*, Edisi No. 02 Vol. 01 2020.

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

Eliasta Ketaren, Cybercrime, Cyber Space, dan Cyber Law, *JTM : Jurnal TIMES*, Edisi No. 02 Vol. 05 2016.

Florida Mathilda, Cyber crime dalam Sistem Hukum Indonesia, *Sigma-Mu*, Edisi No. 04 Vol. 04 2012.

Handrini Ardiyanti, Cyber-Security dan Tantangan Pengembangannya di Indonesia, Jurnal Politica, Edisi No. 01 Vol. 05 2014.

Mahrus Ali, Sistem Peradilan Pidana Progresif: Alternatif dalam Penegakan Hukum Pidana, *Jurnal Hukum*, Edisi Nomor 2 Volume 14, Yogyakarta, 2007.

Muhamad Danuri, Perkembangan dan Transformasi Teknologi Digital, *INFOKAM*, Edisi Nomor 2 Volume 15, 2019.

Nunuk Sulisrudatin, Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit, *Jurnal Ilmiah Hukum Dirgantara*, Edisi No. 01 Vol. 09 2018.

Suhardi Rustam, Analisa Clustering *Phising* dengan K-Means dalam Meningkatkan Keamanan Komputer, *Ilkom Jurnal Ilimiah*, Edisi No. 02 Vol. 10 2018.

Peraturan Perundang-undangan

Undang-Undang Negara Republik Indonesia 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

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

Internet

Andi Saputra, Gadaikan SK Ratusan Juta, PNS Ini Malah Jadi Korban *Phising*, terdapat dalam https://news.detik.com/berita/d-6696948/gadaikan-sk-ratusan-juta-pns-ini-malah-jadi-korban-*phising*, diakses tanggal 8 Juli 2023 pukul 18.00 WIB.

Erizka Permatasari, Jerat Hukum Pelaku Phishing dan Modusnya, terdapat dalam https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050, diakses tanggal pada tanggal 17 Juli 2023 pukul 21:32 WIB.

Jimly Asshiddiqie, Penegakan Hukum, terdapat dalam http://www.jimly.com/makalah/namafile/56/Penegakan_Hukum.pdf, diakses tanggal 18 Juli 2023 pukul 19:21 WIB.

Tim detikJatim, Unduh File 'Undangan' di WA, Nasabah Kehilangan Duit Tabungan Rp 1,4 M, terdapat dalam https://www.detik.com/jateng/berita/d-6810966/unduh-file-undangan-di-wa-nasabah-kehilangan-duit-tabungan-rp-14-m., diakses tanggal 8 Juli 2023 pukul 18.00 WIB.

Wawancara

Wawancara dengan Iptu Anis Dwi Haryanto selaku perwakilan Ditreskrimsus Kepolisian Daerah Provinsi Daerah Istimewa Yogyakarta, di Yogyakarta, tanggal 14 Juli 2023.

Lampiran

FAKULTAS HUKUM
Gedung Fakultas Hukum
Universitas Islam Indonesia
Jl. Kaliurangkm 14,5 Yogyakarta 55584
T. (0274) 7070222
E. fh@uii.ac.id
W. law.uii.ac.id

SURAT KETERANGAN BEBAS PLAGIASI

No. : 396/Perpus-S1/20/H/IX/2023

Bismillaahhirrahmaanirrahaim

Yang bertanda tangan di bawah ini:

Nama	: **M. Arief Satejo Kinady, A.Md.**
NIK	: **001002450**
Jabatan	: **Kepala Divisi Adm. Akademik Fakultas Hukum UII**

Dengan ini menerangkan bahwa :

Nama	: Gibran Mahendra Dewantara
No Mahasiswa	: 19410116
Fakultas/Prodi	: Hukum
Judul karya ilmiah	: PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA.

Karya ilmiah yang bersangkutan di atas telah melalui proses uji deteksi plagiasi dengan hasil **16**.%

Demikian surat keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 27 September 2023 M
12 Rabbiul Awwal 1445 H

Kepala Divisi Adm. Akademik

M. Arief Satejo Kinady, A.Md

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

by 19410116 Gibran Mahendra Dewantara

Submission date: 27-Sep-2023 10:13AM (UTC+0700)
Submission ID: 2178172956
File name: g_Oleh_Kepolisian_Daerah_Wilayah_Daerah_Istimewa_Yogyakarta.docx (655.07K)
Word count: 13455
Character count: 86794

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE *PHISING* OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

SKRIPSI

Oleh:

Gibran Mahendra Dewantara

No. Mahasiswa: 19410116

PROGRAM STUDI HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2023

PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA CYBER CRIME METODE PHISING OLEH KEPOLISIAN DAERAH PROVINSI DAERAH ISTIMEWA YOGYAKARTA

ORIGINALITY REPORT

16%	18%	8%	15%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.uksw.edu Internet Source	3%
2	eprints.umm.ac.id Internet Source	2%
3	core.ac.uk Internet Source	2%
4	jurnal.uii.ac.id Internet Source	2%
5	dspace.uii.ac.id Internet Source	1%
6	Submitted to Universitas Negeri Semarang Student Paper	1%
7	digilib.uinsa.ac.id Internet Source	1%
8	Submitted to Universitas Islam Indonesia Student Paper	1%

9	Submitted to UIN Sunan Gunung DJati Bandung Student Paper	1 %
10	Submitted to Surabaya University Student Paper	1 %
11	id.123dok.com Internet Source	1 %
12	fh.upnvj.ac.id Internet Source	1 %
13	repository.uinjkt.ac.id Internet Source	1 %
14	Submitted to Universitas Jember Student Paper	1 %

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		