BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Dewasa ini teknologi informasi dan komunikasi telah mengalami perkembangan yang begitu pesat di dunia, terutama di Indonesia yang tidak mau ketinggalan dalam hal pemanfaatan kemajuan teknologi informasi dan komunikasi, ini dapat dilihat dari banyaknya masyarakat yang menggunakan alat komunikasi dan teknologi seperti *handphone*, *personal computer*, *smartphone, internet* dan banyak sekali macam-macamnya. Di mana kemajuan teknologi ini telah membantu masyarakat dalam berkomunikasi dan memudahkan pekerjaan menjadi lebih sederhana, sehingga hampir seluruh bidang kehidupan manusia menggunakan teknologi.

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat.[1]

Satu hal yang menarik adalah bahwa proses globalisasi dimulai oleh kemajuan teknologi komunikasi dan informasi. Memang awal kehidupan ini sebenarnya adalah komunikasi. Makhluk hidup, khususnya manusia tidak sanggup bertahan hidup tanpa komunikasi. Bahkan para ahli komunikasi

[1] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia,* (Bandung: PT Refika Aditama, 2006), 1.

menekankan, bahwa dalam peradaban kontemporer berkomunikasi merupakan kebutuhan yang paling mendasar bagi makhluk manusia yang melebihi kebutuhan fisik untuk makan dan untuk berlindung dari panas matahari dan hawa dingin.[2]

Dalam hal ini, *internet* sebagai media komunikasi yang paling berkembang saat ini, di mana *internet* saling menghubungkan jutaan manusia di seluruh dunia, tanpa mereka mengetahui keberadaan lawan komunikasinya. Informasi dapat dikirim dalam berbagai bentuk seperti suara, gambar, teks, data, maupun kombinasinya.[3]

Menurut Sutarman, *internet* merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya, di mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi, yaitu protokol TCP/IP.[4]

Saat ini para pengguna *internet* hampir seluruh lapisan masyarakat menggunakannya, terutama negara-negara yang telah maju sebagai media komunikasi yang begitu luas. Dunia *internet* ini biasa disebut dengan dunia maya, atau dunia siber (*cyber space*).

---

[2] Andi Abdul Muis, *Indonesia di Era Dunia Maya Teknologi Informasi dalam Dunia Tanpa Batas,* (Bandung: PT Remaja Rosdakarya Offset, 2001), 3.
[3] Sutarman, *Pengantar Teknologi Informasi,* (Jakarta: Bumi Aksara, 2012), 64.
[4] Ibid., 32.

Cyber space dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini, *cyber space* dianggap sebagai realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal *internet*.[5]

Adanya *cyber space* ini mengakibatkan dunia nyata menjadi tanpa batas (*borderless*), karena kemajuan dari teknologi informasi dan komunikasi ini menyebabkan mudahnya pengguna *internet* dalam mendapatkan segala informasi dari manapun yang ada di dalam *internet* (*cyber space*). Sehingga *cyber space* ini seperti mata pisau ganda, di samping memberikan kemudahan dalam mendapatkan informasi, dapat juga sebagai aksi dalam perbuatan melawan hukum.

Sebagaimana lazimnya *internet* yang menjadi alat dalam media komunikasi yang bersifat netral, jika *internet* digunakan dalam hal kebaikan maka *internet* dapat menjadi manfaat yang baik bagi manusia, namun ketika *internet* digunakan dalam hal kejahatan dengan maksud untuk merugikan orang lain, maka *internet* bisa menjadi alat dalam perbuatan kejahatan tersebut, sehingga *internet* memiliki sisi positif maupun sisi negatif tergantung pengguna *internetnya*.

Kemajuan teknologi informasi (*internet*) dan segala bentuk manfaat di dalamnya membawa konsekuensi negatif tersendiri di mana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin merisaukan masyarakat. Penyalahgunaan yang terjadi dalam *cyber space* inilah yang

[5] Maskun, *Kejahatan Siber (Cyber crime) Suatu Pengantar,* (Jakarta: Prenada Media Group, 2013), 46.

kemudian dikenal dengan *cyber crime* atau dalam literatur lain digunakan istilah *computer crime*.[6]

Namun perbedaan antara *cyber crime* dengan *computer crime* adalah dari objeknya *computer crime* hanyalah perbuatan melawan hukum dengan alat yang berupa komputer sebagai sarana dan juga objek dalam melakukan perbuatannya itu, di mana perbuatannya merugikan orang lain. Sedangkan *cyber crime* adalah sama seperti *computer crime*, hanya saja dalam *cyber crime* dibutuhkan perangkat telekomunikasi berupa *internet*.

Pengertian antara kejahatan komputer (*computer crime*) atau kejahatan dunia maya (*cyber crime*) secara universal adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau tanpa kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[7]

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi (*internet*) dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa bentuk, antara lain:[8]

1. *Unauthorized access to computer system and service,* yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak

[6] Ibid., 47.
[7] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi,* (Bandung: PT Refika Aditama, 2009), 8.
[8] Maskun, *Kejahatan Siber (Cyber crime)...*, 51.

sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal contents,* yaitu kejahatan dengan memasukkan data atau informasi ke *internet* tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Data forgery,* yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui *internet*. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber espionage,* yaitu kejahatan yang memanfaatkan jaringan *internet* untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
5. *Cyber sabotage and extortion,* yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan *internet*. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb,* virus komputer atau suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan

sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6. *Offence against intellectual property,* yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di *internet*. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di *internet* yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
7. *Infringements of privacy,* yaitu kejahatan yang ditujukan terhadap informasi yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara materiil maupun imateriil, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.

Di berbagai literatur, *cyber crime* dideteksi dari dua sudut pandang, yaitu:[9]

1. Kejahatan yang menggunakan teknologi informasi sebagai fasilitas: pembajakan, pornografi, pemalsuan/pencurian kartu kredit, penipuan lewat email (*fraud*), email *spam*, perjudian *online*, pencurian *account internet*, terorisme, isu sara, situs yang menyesatkan, dan sebagainya.

[9] Sutaman, *Pengantar Teknologi...,* 74.

2. Kejahatan yang menjadikan sistem teknologi informasi sebagai sasaran: pencurian data pribadi, pembuatan/penyebaran virus komputer, pembobolan/pembajakan situs, *cyberwar*, *denial of Service* (DOS), kejahatan berhubungan dengan nama domain, dan sebagainya.

Cyber crime adalah jenis tindak pidana yang sulit dideteksi. Tidak seperti kejahatan konvensional biasa, korban kejahatan pada umumnya tidak menyadari bahwa ia telah menjadi korban, umumnya mereka tidak melaporkan karena beranggapan bahwa hukum yang ada belum menjerat pelaku, kurangnya pengetahuan aparat hukum mengenai perkembangan teknologi sehingga kurang dapat mengantisipasi perkembangan kejahatan ini, juga karena menganggap pembuktian telah terjadi kejahatan di depan pengadilan sangatlah sulit.[10]

Cyber crime dalam kategori *infringements of privacy* pernah terjadi di Indonesia, yaitu tindak kejahatan penipuan dengan menggunakan email palsu atau situs *website* palsu yang bertujuan untuk mengelabui *user* sehingga pelaku bisa mendapatkan data pribadi *user* seperti *username,* PIN, nomor rekening bank, atau nomor kartu kredit secara tidak sah. Kejahatan seperti ini dikenal dengan istilah *phising.*

Phising adalah tindakan memperoleh informasi pribadi seperti *user* ID, PIN, nomor rekening bank, atau nomor kartu kredit anda secara tidak sah.

[10] Niniek Suparni, *Cyberspace Problematika dan Antisipasi Pengaturannya,* (Jakarta:Sinar Grafika, 2009), 122.

Informasi ini kemudian akan dimanfaatkan oleh pihak penipu untuk mengakses rekening, melakukan penipuan kartu kredit, atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.[11]

Dalam hal *cyber crime* dalam bentuk *phising* ini pernah terjadi di Indonesia, yaitu kasus perusakan fasilitas *Internet Banking* Bank Central Asia (BCA) pada situs www.klikbca.com dengan cara melahirkan lima nama situs pelesetan yang mirip situs aslinya, adapun nama situs pelesetan yang dibuat *hacker* yaitu *kilkbca.com*, *wwwklikbca.com*, *clikbca.com*, *klickbca.com* dan *klikbac.com*. sehingga apabila nasabah yang menggunakan fasilitas *Internet Banking* BCA salah mengetik nama situsnya (klikbca.com) seperti lima nama situs pelesetan tersebut, yang terjadi adalah nasabah akan dibawa pada situs palsu buatan *hacker* tadi, selanjutnya si nasabah pun tak bisa bertransaksi, sementara *Personal Identification Number* (PIN) milik nasabah terekam di situs palsu tersebut.[12]

Kasus *cyber crime* dalam bentuk *phising* yang terbaru adalah pencurian yang dilakukan oleh seorang *hacker* yang berasal dari Ukraina, *hacker* tersebut berhasil mengambil uang senilai 130 miliar rupiah dari 300 rekening nasabah bank di Indonesia.[13] Di mana *hacker* tersebut melakukan

---

[11] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding,* (Yogyakarta:CV Andi Offset, 2013), 122.
[12] Majalah Tempo, "Rubrik Teknologi Informasi", (24 Juni 2001) dikutip dari Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law...,* 88.
[13] Idr, "*Hacker* Sedot Rp 130 Miliar dari Rekening 300 Nasabah", *Jawa Pos,* (14 April 2015), hlm 1.

kejahatannya dengan cara memanipulasi *website internet banking*, sehingga pengguna aplikasi yang *login* pada *website internet banking* palsu ini, transaksi yang dilakukan oleh nasabah tidak sesuai dengan yang diinginkan oleh nasabah, melainkan diarahkan kepada rekening orang lain yang telah bekerja sama dengan *hacker*, karena *hacker* berasal dari luar negeri sehingga tidak dapat membuka rekening Indonesia.

Untuk mendapatkan korbannya, banyak cara digunakan dan hal ini biasanya terus berkembang sesuai dengan perkembangan yang ada di dalam dunia *internet*. Beberapa metode yang populer digunakan adalah:[14]

1. Email / *SPAM*

   Media yang paling favorit digunakan untuk mencari korban adalah email. Email dipilih karena murah dan mudah untuk digunakan. Pelaku bisa mengirimkan jutaan email setiap harinya tanpa perlu mengeluarkan biaya yang cukup besar. Bahkan pelaku *phising* juga suka menggunakan *server-server* bajakan untuk melakukan aksinya.

2. *Web-based Delivery*

   Pelaku *phising* juga memanfaatkan *website* dalam melakukan aksinya. Pelaku biasanya membuat *website* yang mirip dengan *website-website* terkenal untuk mengelabui korbannya. Membuat *website* yang mirip dengan *website* perusahaan besar sangatlah mudah untuk dilakukan karena pelaku hanya perlu membuat tampilan yang sama, tanpa perlu membuat fungsi atau fasilitas yang sama

[14] S'to, *Certified Ethical Hacker 400% Illegal,* (t.tp.: Jasakom, 2011), 147.

karena tujuannya adalah agar korban memasukkan *username* dan *password* di dalamnya kemudian korban akan dibawa ke situs asli agar tidak curiga.

3. IRC / *Instant Messaging*

   Media *chatting* yang banyak digunakan juga menjadi sasaran pelaku *phising* untuk mengirimkan alamat-alamat yang menjebak kepada korbannya. Biasanya pelaku mengirimkan *link* ini secara acak namun ada juga yang melakukan pendekatan terlebih dahulu sebelum mengirimkan informasi situs palsu ini.

4. *Trojan*

   Pelaku *phising*, terkadang juga menipu korbannya agar *menginstall trojan* dan memanfaatkan *trojan* tersebut untuk mengelabui korbannya. *Trojan* memungkinkan pengontrolan secara penuh komputer korban sehingga korban bisa dialihkan ke situs yang telah disediakan jebakan.

Dalam hal *cyber crime* dalam bentuk *phising* seperti kasus-kasus di atas tadi, bentuk kejahatan tersebut adalah penipuan dengan menggunakan komputer sebagai alat dalam melakukan aksi kejahatannya.

Membahas masalah aturan hukum *cyber crime* yang ada di Indonesia, saat ini telah ada aturan perundang-undangan yang mengatur khusus tentang *cyber crime* yaitu Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Adapun perbuatan *phising* ini secara implisit diatur dalam Pasal 28 ayat (1) jo Pasal 45 ayat (2) dan Pasal 35 jo Pasal 51 ayat (1).

Salah satu Pasal undang-undang tersebut di Bab XI tentang ketentuan pidana, Pasal 45 ayat (2) menyebutkan "setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan penjara paling lama 6 tahun dan/atau denda paling banyak 1 miliar rupiah".

Dalam hukum pidana Islam, pelaku tindak pidana (*jarīmah*) dihukum sesuai dengan adanya aturan, karena ada kaidah bahwa "tidak ada *jarīmah* (tindak kejahatan) dan tidak ada hukuman tanpa adanya *naṣ* (aturan)" kaidah ini seperti asas legalitas yang ada dalam KUHP Pasal 1 ayat (1). [15]

Dalam Alquran juga dijelaskan mengenai asas legalitas ini, dalam surat al-Qashash ayat 59:

وَمَا كَانَ رَبُّكَ مُهْلِكَ ٱلْقُرَىٰ حَتَّىٰ يَبْعَثَ فِىٓ أُمِّهَا رَسُولًا يَتْلُوا۟ عَلَيْهِمْ ءَايَـٰتِنَا ۚ وَمَا كُنَّا مُهْلِكِى ٱلْقُرَىٰٓ إِلَّا وَأَهْلُهَا ظَـٰلِمُونَ ﴿٥٩﴾

> Artinya: Dan tidak adalah Tuhanmu membinasakan kota-kota, sebelum Dia mengutus di ibukota itu seorang rasul yang membacakan ayat-ayat Kami kepada mereka; dan tidak pernah (pula) Kami membinasakan kota-kota; kecuali penduduknya dalam keadaan melakukan kezaliman.

Hukuman dalam hukum pidana Islam bila ditinjau dari segi terdapat atau tidak terdapat *naṣnya* dalam Alquran dan Hadis, dapat dibagi menjadi dua:[16]

---

[15] A. Djazuli, *Hukum Pidana Islam (Fiqih Jināyāh),* (Bandung: Pustaka Setia, 2000), 52.
[16] A. Djazuli, *Fiqh Jināyāh (Upaya Menanggulangi Kejahatan dalam Islam),* (Jakarta: PT RajaGrafindo, 1997), 28.

1. Hukuman yang ada *naṣnya*, yaitu *ḥudūd*, *qiṣāṣ*, dan *kafārat*. Misalnya, hukuman bagi pezina, pencuri, perampok, pembunuh, dan orang yang *mendhihar* istrinya.
2. Hukuman yang tidak ada *naṣnya*, hukuman ini disebut dengan hukuman *ta'zīr*, seperti percobaan melakukan tindak pidana, tidak melaksanakan amanah, saksi palsu dan melanggar aturan lalu lintas.

Cyber crime dalam bentuk *phising* ini adalah identik dengan perbuatan penipuan tradisional, hanya yang membedakan adalah *phising* menggunakan teknologi informasi dan telekomunikasi dalam melakukan kejahatannya. Sedangkan dalam hukum pidana Islam tidak ada *naṣ* yang menjelaskan hukuman bagi kejahatan *phising* tersebut.

Perbuatan *phising* yang identik dengan penipuan tersebut jika dikaitkan dengan pencurian adalah serupa tetapi tidak sama dengan pencurian.[17] Adapun persamaan kedua perbuatan tersebut yaitu pengambilan harta milik orang lain serta memiliki itikad jahat untuk memiliki barang tersebut. Sedangkan perbedaannya yaitu penipuan dalam pengambilan harta tersebut tidak diambil secara diam-diam, sedangkan dalam unsur pencurian harus dengan cara diam-diam. Karena penipuan tersebut mengambil hak orang lain secara licik dengan cara menipu korbannya agar memberikan hartanya kepada pelaku secara tidak disadarinya, sehingga orang lain tersebut menderita kerugian.

[17] Zainuddin Ali, *Hukum Pidana Islam*, (Jakarta: Sinar Grafika, 2009), 62.

Abdul Qadir Audah menjelaskan bahwa sesungguhnya unsur penting dalam *jarīmah* pencurian adalah mengambil (sesuatu) dengan cara sembunyi-sembunyi, sedangkan mengambil (sesuatu) bukan dari tempat penyimpanannya tidak perlu sembunyi-sembunyi sehingga unsur terpenting dalam pencurian tidak terealisasi apabila tidak dapat diambil dari tempat penyimpanannya.[18] Sehingga apabila salah satu syarat atau rukun tidak terpenuhi maka hukuman potong tangan harus dibatalkan dan dialihkan kepada hukum *ta'zīr.*

Dalam tindakan *phising,* cara mengambil hak orang lain dengan mengelabui *user*, sehingga pelaku *phising* bisa mendapatkan data pribadi *user* tersebut seperti PIN, nomor rekening, nomor kartu kredit dan sebagainya karena *user* menjadi korban penipuan. Sehingga tindakan *phising* berbeda dengan pencurian, yang mana dalam pencurian harus mengambil secara diam-diam harta seseorang di dalam tempat penyimpanannya.

Dari berbagai pemaparan di atas, penulis ingin mengkaji terhadap perspektif hukum pidana Islam mengenai sanksi hukum dalam Undang-Undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap pelaku *cyber crime* dalam bentuk *phising*. Karena perbuatan *phising* ini tidak hanya merugikan individu saja, melainkan juga merugikan masyarakat umum dikarenakan banyak yang tidak mengetahui pola kejahatan seperti ini.

[18] Nurul Irfan dan Masyrofah, *Fiqh Jināyāh,* (Jakarta: Amzah, 2013), 116.

B. Identifikasi Masalah

Dalam hal mengenai perspektif hukum pidana Islam, masalah tindak pidana *cyber crime* masih bersifat umum, oleh karena itu yang menjadi perhatian dalam penulisan skripsi ini adalah yang berkaitan dengan *cyber crime* dalam bentuk *phising.*

Adapun identifikasi masalah yang ada dalam latar belakang masalah adalah sebagai berikut:

1. Kemajuan teknologi informasi dan komunikasi mengakibatkan dunia menjadi tanpa batas (*borderless*).
2. Penyalahgunaan kemajuan teknologi informasi dan komunikasi (*internet*) mengakibatkan munculnya kejahatan baru, yaitu *cyber crime.*
3. Bermacam-macam bentuk *cyber crime* yang erat dengan penggunaan teknologi.
4. *Cyber crime* adalah jenis tindak pidana yang sulit untuk dideteksi.
5. Masyarakat beranggapan bahwa hukum yang ada belum mampu menjerat pelaku *cyber crime* dan juga umumnya masyarakat tidak melaporkan kejahatan *cyber crime.*
6. Kurangnya pengetahuan aparat hukum mengenai perkembangan teknologi, sehingga penegak hukum kesulitan dalam hal pembuktian.
7. Kasus *cyber crime* dalam bentuk *phising* terjadi di Indonesia.
8. Berbagai teknik melakukan kejahatan *cyber crime* dalam bentuk *phising*.

9. Aturan hukum untuk *cyber crime* yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
10. Dalam hukum pidana Islam, tidak ada *naṣ* Alquran dan Hadis yang menjelaskan sanksi kejahatan *cyber crime* dalam bentuk *phising.*

C. Batasan Masalah

Batasan masalah dalam penulisan skripsi ini adalah sebagai berikut:

1. Cara melakukan kejahatan *cyber crime* dalam bentuk *phising*.
2. Ketentuan hukum terhadap kejahatan *cyber crime* dalam bentuk *phising* Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
3. Tinjauan hukum pidana Islam terhadap kejahatan *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

D. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dalam penulisan skripsi ini penulis memberikan rumusan masalah sebagai berikut:

1. Bagaimana cara melakukan kejahatan *cyber crime* dalam bentuk *phising* ?
2. Bagaimana ketentuan hukum terhadap kejahatan *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

3. Bagaimana tinjauan hukum pidana Islam terhadap kejahatan *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

E. Kajian Pustaka

Kajian pustaka ini pada intinya untuk mendapatkan gambaran dari hubungan topik yang akan diteliti dengan penelitian yang pernah dilakukan sebelumnya, sehingga tidak terjadi duplikasi dari penelitian yang ada.

Sudah ada beberapa buku yang menjelaskan permasalahan *cyber crime,* di antaranya:

1. "*Kejahatan Siber (Cyber Crime) Suatu Pengantar*", karangan Maskun.
2. "*Cyberlaw Aspek Hukum Teknologi Informasi*", karangan Dikdik M. Arief Mansur dan Elisatris Gulton.
3. "*Cyber Law dan HAKI dalam Sistem Hukum Indonesia*", karangan Ahmad M. Ramli.
4. "*Indonesia di Era Dunia Maya Teknologi Informasi dalam Dunia Tanpa Batas*", karangan Andi Abdul Muis.
5. "*Cyberlaw, Tidak Perlu Takut*", karangan Merry Magdalena dan Maswigrantoro Roes Setiyadi.
6. "*Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*", karangan Budi Suhariyanto.
7. "*Kejahatan Mayantara (Cyber Crime)*", karangan Abdul Wahid dan Mohammad Labib.

8. "*Cyberspace Problematika dan Antisipasi Pengaturannya*", karangan Niniek Suparni.

Adapun penelitian dari beberapa mahasiswa UIN Sunan Ampel Surabaya yang berkaitan dengan *cyber crime* adalah sebagai berikut:

Skripsi yang disusun oleh Khuzaimatus Sholikha yang berjudul "*Hacking Komputer dalam Perspektif Hukum Pidana dan Hukum Islam*" membahas bagaimana perspektif hukum pidana dan hukum Islam terhadap *hacking* komputer, kesimpulannya adalah *hacking* komputer yang merupakan akses atau memasuki suatu sistem komputer tanpa izin dari pemiliknya dapat mengakibatkan kerugian kepada pengguna *internet* maupun pemilik situs komputer. dalam penelitian tersebut *hacking* komputer dijerat dengan Pasal 22 jo. 40 Undang-Undang No. 36 Tahun 1999 dengan ketentuan pidana yang diatur dalam Pasal 50 jo. Pasal 56 UU No. 36 Tahun 1999 tentang Telekomunikasi. Sedangkan dalam hukum pidana Islam dikenai hukuman *ta'zīr* karena sanksinya bukan ditentukan oleh Alquran dan Hadis melainkan ditentukan oleh *Ulil Amri*.

Skripsi selanjutnya berjudul "*Tinjauan Hukum Pidana Islam Terḥadap Cyber Crime dalam Bentuk Spam*" yang disusun oleh Muchammad Nashir, dalam penelitiannya membahas bagaimana tinjauan hukum Islam dan sanksi hukum terhadap *cyber crime* dalam bentuk *spam,* kesimpulan dari penelitian tersebut bahwa yang dimaksud *spam* adalah pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna *website*. Perbuatan

cyber crime dalam bentuk *spam* ini dijerat dengan Pasal 35 jo. Pasal 51 ayat (1) UU ITE No. 11 Tahun 2008. Sedangkan sanksi pidana ditinjau dari hukum Islam maka dapat dikategorikan kepada *ta'zīr* atas pelanggaran-pelanggaran.

Skripsi yang ketiga adalah milik Sylviani yang berjudul "*Studi Komparasi Hukum Pidana Islam dan KUHP* Pasal *362 tentang Tindak Pidana Carding*". Dalam penelitian tersebut menjelaskan mengenai *carding* dan sanksi hukumnya menurut hukum pidana Islam dan KUHP. Bahwa yang dimaksud *carding* adalah aktivitas jual beli melalui *internet* yang sistem pembayarannya dengan menggunakan kartu kredit orang lain. Sedangkan sanksi hukumnya menurut hukum pidana Islam, tindakan *carding* disamakan dengan *sariqah* karena unsur-unsur yang ada pada *sariqah* terdapat pula pada *carding.* Lalu dalam KUHP, tindak pidana *carding* disamakan dengan pencurian pokok atau pencurian biasa karena unsur-unsur yang terdapat pada pencurian juga terdapat pada *carding* dan dikenakan Pasal 362 KUHP.

Dari kajian pustaka di atas, yang membedakan dengan penulisan skripsi ini adalah membahas bagaimana pandangan hukum pidana Islam terhadap sanksi hukum dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap tindakan *cyber crime* dalam bentuk *phising.* Di mana *phising* ini adalah penipuan dengan menggunakan *website* palsu yang menyerupai aslinya dengan tujuan mendapatkan data pribadi dari korbannya seperti *username,* PIN, nomor kartu kredit, *password* dan sebagainya.

F. Tujuan Penelitian

Tujuan yang ingin dicapai dari penulisan skripsi, meliputi hal-hal sebagai berikut:

1. Untuk mengetahui cara melakukan kejahatan *cyber crime* dalam bentuk *phising*.
2. Untuk mengetahui ketentuan hukum terhadap kejahatan *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
3. Untuk mengetahui perspektif hukum pidana Islam terhadap kejahatan *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

G. Kegunaan Hasil Penelitian

Dalam penulisan skripsi ini dapat diharapkan mempunyai nilai kegunaan baik dari segi teoretis maupun praktis sebagai berikut:

1. Dari segi teoretis, hasil penelitian ini dapat bermanfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang teknologi informasi dan hukum yang berkaitan dengan kejahatan dunia maya (*cyber crime*) dalam bentuk *phising*.
2. Dari segi praktis, hasil penelitian ini dapat menambah pemahaman masyarakat terhadap kejahatan dunia maya (*cyber crime*) terutama dalam bentuk *phising*. Di samping

itu, diharapkan dapat menjadi pertimbangan hukum bagi para penegak hukum ketika ada perkara *cyber crime* dalam bentuk *phising*, sehingga dapat menjamin pelaku *cyber crime* mendapat hukuman yang semestinya.

H. Definisi Operasional

Untuk memperjelas dan menghindari terjadinya kesalahpahaman dalam menafsirkan kata-kata yang ada dalam pembahasan penulisan skripsi, maka penulis memandang perlu untuk memberikan penjelasan dalam memahami judul "*Cyber Crime* dalam Bentuk *Phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Menurut Perspektif Hukum Pidana Islam". Adapun yang dimaksud dengan:

1. Hukum Pidana Islam adalah terjemahan dari kata fikih *jināyāh*, dalam skripsi ini menjelaskan khusus kepada *jarīmah ta'zīr*, yaitu *jarīmah* yang diancam dengan hukuman *ta'zīr* (istilah untuk hukuman atas *jarīmah - jarīmah* yang hukumannya belum ditentukan oleh *shara'*).
2. *Cyber crime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama, di mana kejahatan ini memanfaatkan perkembangan teknologi komputer khususnya *internet*.[19]

[19] Roniamardi, "definisi *cybercrime*++", dalam https://roniamardi.wordpress.com/definisi-cybercrime, diakses pada 05 Oktober 2015.

3. *Phising* (*Password Harvesting Fishing*) adalah tindakan penipuan yang menggunakan email palsu atau situs *website* palsu yang bertujuan untuk mengelabui *user* sehingga pelaku bisa mendapatkan data pribadi *user* tersebut seperti PIN, nomor rekening, nomor kartu kredit dan sebagainya.[20]

I. Metode Penelitian

1. Data yang dikumpulkan

   Data yang dikumpulkan adalah data yang terkait dengan tindak pidana *cyber crime* dalam bentuk *phising*, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan hukum pidana Islam beserta ketentuan-ketentuan pidananya.

2. Sumber Data

   Penulisan skripsi ini merupakan hasil dari kajian pustaka. Oleh sebab itu data yang digunakan adalah:

   a. Sumber data primer, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

   b. Sumber data sekunder, yaitu bahan hukum yang diperoleh dari kitab-kitab atau bahan bacaan lain yang memiliki keterkaitan dengan bahan skripsi, yaitu fikih *jināyāh* dari Ahmad Djazuli, CEH *(Certified Ethical Hacker)* 400%

[20] Vyctoria, *Bongkar Rahasia...,* 214.

Illegal, Tindak Pidana Teknologi Informasi (*Cybercrime*) Urgensi Pengaturan dan Celah Hukumnya. Dan buku-buku lain yang membantu penulis dalam menyelesaikan penulisan skripsi ini.

c. Sumber data tersier (penunjang), yaitu bahan hukum yang menunjang dengan pembahasan skripsi, yaitu koran Jawa Pos dan sumber dari *internet*.

3. Teknik Pengumpulan Data

Teknik pengumpulan data yang akan digunakan dalam penelitian ini adalah telaah kepustakaan (*Selected Bibliografie Technique*) yaitu metode pengumpulan data dengan cara mempelajari, memahami buku-buku, peraturan perundang-undangan serta karya tulis ilmiah lainnya yang berhubungan dengan tindak pidana *cyber crime* dalam bentuk *phising.*

4. Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah teknik deskriptif analisis, yaitu teknik analisis dengan cara menjabarkan data sesuai apa adanya, dalam penelitian ini adalah tindak pidana *cyber crime* dalam bentuk *phising* dan menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya di analisis dengan hukum pidana Islam, menggunakan pola pikir deduktif, yaitu pola pikir yang berangkat dari variabel yang bersifat umum

yaitu hukum pidana Islam, lalu ditarik kepada fakta-fakta tentang *cyber crime* dalam bentuk *phising* menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya ditarik kepada kesimpulan yang bersifat khusus menurut hukum pidana Islam.

J. Sistematika Pembahasan

Dalam penulisan skripsi ini penulis membagi 5 (lima) bab secara sistematis, yaitu:

Bab I tentang Pendahuluan yang terdiri dari, Latar Belakang, Identifikasi dan Batasan Masalah, Rumusan Masalah, Kajian Pustaka, Tujuan Penelitian, Kegunaan Hasil Penelitian, Definisi Operasional, Metode Penelitian dan Sistematika Pembahasan.

Bab II tentang landasan teori yang berisi tentang tinjauan umum terhadap *jarīmah ta'zīr* yang memuat pengertian *jarīmah ta'zīr*, unsur-unsur *jarīmah ta'zīr*, macam-macam *jarīmah ta'zīr* dan hukuman *jarīmah ta'zīr*.

Bab III tentang *cyber crime* dalam bentuk *phising* dan sanksi hukumnya. Dalam bab ini akan menerangkan tentang pengertian *cyber crime*, *cyber crime* dalam bentuk *phising,* metode dan teknik serangan *phising*, contoh kasus *cyber crime* dalam bentuk *phising* di Indonesia, dan *cyber crime* dalam bentuk *phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bab IV tentang analisis terhadap *cyber crime* dalam bentuk *phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perspektif hukum pidana Islam, memuat tentang analisis cara melakukan kejahatan *cyber crime* dalam bentuk *phising,* analisis ketentuan hukum terhadap *cyber crime* dalam bentuk *phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan analisis hukum pidana Islam terhadap *cyber crime* dalam bentuk *phising* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Bab V tentang penutup, yang memuat kesimpulan dan saran.