



TINDAK KEJAHATAN CYBER CRIME DALAM PERSPEKTIF FIKIH JINAYAH

Oleh

Hendra Gunawan

Dosen Fakultas Syariah dan Ilmu Hukum IAIN Padangsidimpuan

Email: hendragunawan@iain-padangsidimpuan.ac.id

Abstrac

Technological progress is an inevitable growth along with the progress of human civilization to make humans integrate without space and time limit in cyberspace, but this technological progress is boarded by people who are not responsible for committing crimes in cyberspace termed cyber crime, then this paper tries to discuss cyber crime from the perspective of Jurisprudence. The main problem in this article is how the jurisprudence perspective of cyber crime, from here the authors formulate a sub-issue namely how the terminology of cyber crime according to jurisprudence jinayah. The method used in this article is descriptive qualitative, sourced from fiqh books and books related to the topics discussed in this article with the method of collecting data using literature studies.

The author's findings in this article, that the current form of cyber crime is not spared from jinayah fiqh studies because even though cyber crime is a new crime model, but it has similarities with the cases discussed in jurisprudence, one of the cyber crime crimes is hacking (stealing data) or breaking into an ATM is the same as Syariqah (stealing) only that distinguishes it is the way to do it, so if Syariqah is done in the real world while cyber crime is done in cyberspace. For more details, please look at the next discussion.

Kata Kunci; *cyber, crime, perspektif, fikih, dan jinayah*

A. Pendahuluan

Seiring dengan perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) telah mengantarkan insan manusia kepada sebuah peradaban yang gemilang dengan munculnya internet sebagai produk perkembangan teknologi saat ini,¹ membuat dunia berubah menjadi mengglobal hingga bumi terasa *borderless* (tidak memiliki batas),² sebab sekalipun berbeda negara tetapi lewat teknologi *smartphone* bisa berkomonikasi lewat *chat* (berbincang-bincang), *voice call* (telepon suara), maupun langsung menggunakan *video call* (telepon gambar) dengan bertatap muka secara langsung membuat terasa behadapan langsung sehingga siyar Islam untuk menyambung silaturahmi pun semakin mudah diamalkan. Begitu juga ibadah haji pergi ke Makkah yang dulunya terasa sangat jauhi hingga membutuhkan



waktu berbulan-bulan untuk bisa sampai kesana, tetapi sekarang ini dengan kemajuan Iptek saat ini apabila naik *burung besi* (pesawat) sudah terasa sangat dekat hanya dengan hitungan jam saja sudah bisa sampai ke sana. Namun disisi lain ternyata dengan kemajuan Iptek ternyata membawa dampak negatif karena lewat perkembangan internet kejahatan-kejahatan versi baru pun banyak bermunculan salah satunya adalah *cyber crime* (teknologi informasi). Kemajuan teknologi informasi ini bagaikan dua sisi mata uang yang satu sisi memberikan manfaat untuk kemaslahatan umat dan sisi lainnya menghancurkan umat termasuk munculnya *cyber crime prostitution* (prostitusi online) dan lain sebagainya.³

Cyber crime ini tidak dapat dipandang sebelah mata, sebab para pelakunya bukan orang biasa-biasa yang hanya bermain-main di tingkat masyarakat *awam* (biasa) saja, tetapi mereka adalah orang-orang hebat yang menguasai internet beserta aplikasinya yang dapat mempropogandakan website milik pemerintah sebagaimana pada tahun 1999 tercatat dalam koran Kompas bahwa website Negara Kesatuan Republik Indonesia (NKRI) dirusak pelaku *cyber crime*. Tidak hanya di Indonesia, di Amerika Serikat praktek *cyber crime* ini juga telah berhasil menembus database America Online (AOL) sebuah perusahaan yang bergerak dibidang *e-commerce* (Perdagangan elektronik) padahal database pengguna jasa AOL ini sudah memiliki *proteksi* (pelindung) tingkat tinggi. Bahkan situs Federal Bureau of Investigation (FBI) pun diserang oleh *cyber crime* sehingga situs FBI sempat tidak berfungsi beberapa waktu.

Kejahatan *cyber crime* ini, adalah merupakan bagian dari kejahatan *transnasional* (internasional) sebab tindakan kejahatan ini terjadi di *cyberspace* (dunia maya) sehingga sulit untuk menentukan yurisdiksi hukum negara mana yang harus diterapkan kepada pelakunya.⁴ Untuk itu, semua kita harus menyoroti *cyber crime* ini dari berbagai aspek termasuk dari kacamata fikih jinayah mengingat dampak yang dapat ditimbulkan dari kejahatan *cyber crime* ini begitu luas baik materil maupun immateril berupa uang, barang, harga diri, martabat, dan rahasia pribadi sebagaimana tujuan dari teori *maqasid al-syari'ah* (tujuan hukum) yaitu mewujudkan kemaslahatan manusia baik di dunia maupun di akhirat dengan melindungi *al-masalih al-khamsah* (lima kebutuhan pokok dalam kehidupan manusia) mencakup *hifz al-din* (pemeliharaan agama), *hifz al-nafs* (jiwa), *hifz al-nasl* (keturunan atau kehormatan), *hifz al-mal* (harta), dan *hifz al-'aql* (akal) sebab *cyber crime* dapat mencederai lima pokok yang harus di jaga ini.



B. Pengertian Cyber Crime

Kata *cyber crime* adalah berasal dari kata *cyber* yang berarti internet atau dunia maya sedangkan kata *crime* berarti kejahatan,⁵ maka sederhananya dapat disimpulkan bahwa *cyber crime* adalah semua bentuk kejahatan-kejahatan yang dilakukan oleh seseorang, kelompok maupun korporasi di *dunia maya* (internet) dengan memanfaatkan perkembangan teknologi informasi internet yang semakin canggih.⁶ Adapun bentuk *cyber crime* paling tidak ada tujuh yaitu ;

Pertama, *unauthorized access to computer system and service* yaitu suatu tindakan kejahatan yang dilakukan dengan cara *menyusup* (memasuki tanpa izin) sebuah sistem jaringan komputer tanpa sepengetahuan pemilik sistem jaringan komputer tersebut⁷ dengan maksud tujuan *sabotase* (mencuri data rahasia) walaupun oleh sebagian pelaku ada juga yang hanya sekedar *iseng-iseng* (mencoba) keahliannya menyusup sistem yang memiliki proteksi tingkat tinggi. Model yang satu ini semakin hari semakin meningkat seiring dengan perkembangan teknologi internet, yang mana para pelaku kejahatan seperti ini sering disebut *hacker* (penyusup).

Kedua, *illegal contents* yaitu tindak kejahatan dengan cara memasukkan data atau informasi ke internet mengenai suatu informasi yang *tidak etis* (tidak benar) yang dapat mengganggu ketertiban umum, seperti pemuatan suatu informasi palsu terkait kerahasiaan negara untuk memancing propaganda melawan pemerintah. Atau memuat suatu, fitnah, pornografi yang dapat mendiskreditkan *martabat* (harga diri) orang lain atau memuat berita bohong. Model *illegal contents* dapat digunakan pelaku untuk menipu dengan cara menawarkan suatu produk dalam sebuah iklan di website seolah-olah barang tersebut ada dan nyata sehingga orang yang melihatnya tertarik kemudian membelinya dengan mentranferkan bayarnya lewat ATM kepada *pengiklan* (pelaku) lalu setelah uang dikirimkan oleh korban namun barang yang dipesankan pembeli tidak kunjung-kunjung datang alhasil korban bersedih karena sudah tertipu.

Ketiga, *data forgery* yaitu tindak kejahatan dengan cara memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Model *cyber crime* ini biasanya ditujukan terhadap dokumen-dokumen *e-commerce* dengan cara membuat pada data tersebut seolah-olah terjadi salah ketik yang pada ujungnya pelaku mendapatkan untung dari kesalahan ini.

Keempat, *cyber espionage* yaitu tindak kejahatan dengan cara memata-matai orang lain dengan memanfaatkan jaringan internet pada *computer network system* (sistem jaringan



komputer). Kejahatan ini biasanya ditujukan kepada saingan bisnisnya dengan memata-matai dokumen atau data-data penting yang tersimpan di sistem *computerized* miliknya. Apabila data-data penting termasuk data yang paling rahasia, maka pelaku bisa saja melanjutkannya kepada pemerasan dengan mengancam para korban melalui e-mail untuk memaksa korban supaya melakukan sesuatu yang diinginkan pelaku.

Kelima, *cyber sabotage and extortion* atau *cyber terrorism* yaitu tindak kejahatan yang dilakukan dengan cara menciptakan virus untuk mengganggu, merusak atau menghancurkan data, program komputer yang terhubung dengan internet. Pelaku kejahatan ini biasanya dilakukan dengan cara menyusupkan *logic bomb* (semacam *malware*) baik dalam bentuk virus, *worm*, *trojan horse*, *adware*, *browser hijacker* dan lain sebagainya sehingga *operating system* (software) pada program komputer tersebut tidak dbisa difungsikan lagi seperti biasanya, tetapi komputer tersebut dikendalikan pelaku⁸ sehingga berjalan sesuai dengan kehendak pelaku. Maka apabila pelaku telah mengendalikan komputer korban tersebut pelaku pun akan menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut untuk diperbaiki dengan bayaran tertentu.

Keenam, *offense against intellectual property* yaitu tindak kejahatan di internet terhadap Hak Atas Kekayaan Intelektual (HAKI) yang dimiliki seseorang seperti meniru secara *ilegal* (tanpa izin pemilik) atas sebuah tampilan web page seseorang padahal sudah dihakikan pemilik web page tersebut. Atau menyiarkan informasi tentang rahasia dagang orang lain di internet. Dengan kata lain, mencemarkan nama baik sebuah perusahaan seseorang baik lewat media sosial WhatsApp (WA), fecebook, twitter, instagram, skype, camfrog, mirc maupun menyebarkannya lewat *mailing list* email sehingga semua mengetahui rahasia penting perusahaan tersebut.

Ketujuh, *infringements of privacy* yaitu tindakan kejahatan terhadap data pribadi seseorang yang sangat rahasia yang tersimpan didalam *computerized* yang mana apabila data pribadi tersebut sampai diketahui oleh orang lain maka yang bersangkutan akan mengalami kerugian materiil maupun immateriil. Adapun contoh data pribadi yang sangat rahasia itu antara lain nomor kartu kredit, nomor pin ATM atau informasi penyakit yang dirahasiakan dan sebagainya. Sekalipun pelaku tidak mendapatkan fisik kartu kredit korban tetapi pelaku sudah mengantongi nomor kartu kredit korban lewat *software card generator* di internet maka akan terjadi kasus *carding* dan akan merugikan banyak orang tidak hanya pemilik kartu tapi orang lain juga akan penjadi korban, dimana pelaku pencuri nomor kartu kredit tersebut



melakukan transaksi di *e-commerce* lalu setelah transaksi itu barang pun dikirimkan oleh penjual dan sampailah ke tangan pelaku. Hironisnya ketika penjual yang telah mengirimkan barang ingin mencairkan uangnya di bank ternyata ditolak pihak bank karena pemilik kartu kredit tersebut bukanlah orang yang melakukan transaksi dengan si penjual.

C. Cyber Crime Ditinjau dari Fikih Jinayah

Dari paparan pengertian *cyber crime* tdi atas, dapat dipahami bahwa *cyber crime* merupakan bentuk kejahatan modern karena selalu berkaitan dengan internet sementara pada masa ulama fikih klasik belum tren teknologi internet namun bukan berarti tidak ada keterkaitannya dengan fikih jinayah, sebab semua aspek kehidupan diatur dalam ajaran Islam termasuk segala bentuk kejahatan mulai dari kejahatan modus kuno sampai kepada modus yang terbaru. Sekalipun secara terminologi tidak ada ditegaskan dalam al-Qur'an dan sunnah maupun pendapat ulama klasik namun *cyber crime* ini bisa saja diselidiki atau diidentifikasi lewat metode *qiyas* (mempersamakan) dengan kasus yang mirip atau hampir sama dengan kasus-kasus terdahulu yang sudah *dijabarkan* (dijelaskan) secara tuntas di dalam fikih jinayah. Misalnya, pencurian yang dilakukan dengan memasuki rumah korban lalu *menggasap* (mengambil tanpa sisa) uang yang ada di lemari sama saja dengan pencurian yang dilakukan hacker dengan membobol pin ATM korban lewat internet lalu *menggasap* uang korban.

Disini terlihat bahwa kedua kejahatan di atas sama-sama masuk kedalam kategori pencurian hanya cara dan modusnya saja yang berbeda, begitu juga dengan kasus pembunuhan baik ala orang dahulu kala dengan pedang maupun ala zaman naw dengan *tembak elektronik* (pistol listrik) tetap sama-sama menghilangkan nyawa seseorang sehingga harus dikenai sanksi hukuman.

No	Terminologi		Analisis	
	Cyber Crime	Fikih Jinayah	Persamaan	Perbedaan
1	<u>Unauthorized access to computer system and service;</u> "kejahatan yang dilakukan dengan cara memasuki tanpa izin sebuah	<u>Syariqah (pencurian);</u> "Tindakan mengambil barang orang lain atau sesuatu tanpa	Sama-sama mencuri	<i>Unauthorized access to computer system and service</i> terjadi di dunia maya termasuk <i>carding</i> (mensabotase kartu kredit orang lain dan membelanjakannya secara illegal). Sedangkan <i>syariqah</i> di dunia nyata; <i>Pada unauthorized access to computer</i>



	sistem jaringan komputer yang bertujuan mensabotase data rahasia”	izin secara diam-diam daari tempat penyimpanan untuk menguasai barang tersebut”		<i>system and service</i> yang diambil adalah data sedangkan pada <i>syariqah</i> yang diambil adalah uang atau barang; <i>Unauthorized access to computer system and service</i> pelakunya disebut hacker sedangkan pelaku <i>syariqah</i> disebut pencuri.
2	<u><i>Illegal contents;</i></u> “kejahatan yang dilakukan dengan cara memasukkan data atau informasi ke internet tidak benar sehingga mengganggu ketertiban umum”	<i>Kadzib (berbohong);</i> “Perbuatan dusta yaitu tindakan yang tidak sesuai antara ucapan dengan hati nurani dan kenyataan yang sebenarnya”	Sama-sama berbohong.	<i>Illegal contents</i> terdapat di dunia maya sedangkan <i>kadzib</i> terjadi di dunia nyata; <i>Illegal contents</i> sering disebut <i>hoax</i> s. Menurut Budi Suhariyanto <i>hoax</i> s merupakan tindakan penyebaran berita bohong dan penyesatan dapat dikategorikan sebagai penipuan. ⁹ Bahkan terkadang berita <i>hoax</i> s tersebut ditujukan untuk menghinakan seseorang sehingga sering juga disebut sebagai <i>cyber bullying</i> (prilaku merendahkan harga diri dan mental orang lain). Sedangkan <i>kajib</i> sering diartikan kebohongan.
3	<u><i>Data forgery;</i></u> “kejahatan yang dilakukan dengan cara memalsukan dokumen-dokumen penting yang tersimpan di internet lalu membuat data tersebut seolah-olah terjadi salah ketik agar pelaku bisa mendapatkan untung dari keslahan itu”	<i>altazif (pemalsuan)</i> “ <i>tindakan pemalsuan terhadap barang atau dokumen untuk mengelabui orang lain seperti surat palsu yang dapat menimbulkan sesuatu hak, perikatan atau pembebasan hutang, dan lain</i>	Sama-sama memalsukan.	<i>Data forgery</i> terjadi di dunia maya sedangkan <i>altazif</i> terjadi didunia nyata seperti sumpah palsu, saksi palsu, atau merekayasa sebuah dokumen dengan menambah-nambahi maupunmengurang-ngurangi dokumen tersebut.



		sebagainya.		
4	<p><i>Cyber espionage;</i></p> <p>“kejahatan yang dilakukan dengan cara memata-matai orang lain lewat <i>computer network system</i> untuk memata-matai data penting saingan bisnis di <i>computerized</i>”.</p>	<p><i>tajasus</i></p> <p>(<i>memata-matai</i>)</p> <p>“Tindakan memata-matai atau mencari tahu tentang sesuatu hal dengan cara sembunyi-sembunyi”</p>	Sama-sama memata-matai.	<p><i>Cyber espionage</i> terjadi di internet bisa saja bertujuan untuk <i>impersonation</i> (meniru) produk atau mencari kelemahan pesaing bisnis agar semakin <i>merosot</i> (bangkrut). sedangkan <i>tajasus</i> terdapat di kehidupan <i>real</i> (nyata).</p>
5	<p><i>Cyber terrorism;</i></p> <p>“kejahatan yang dilakukan dengan virus komputer untuk <i>hacking</i> (mengendalikan) program komputer berfungsi sesuai dengan kehendak pelaku. Kemudian menawarkan diri untuk memperbaikinya dengan bayaran yang fantastis”.</p>	<p><i>tahdid</i></p> <p>(ancaman)</p> <p>“tindakan mengancam atau menakut-nakuti seseorang sehingga korban merasa tidak tenang atau ketakutan”</p>	Sama-sama mengancam.	<p>Ancaman yang terdapat pada <i>cyber terrorism</i> secara halus dilakukan seorang <i>hacker</i> (orang yang memiliki keahlian di bidang program komputer yang suka mengoprek program komputer orang lain. Sedangkan pada <i>tahdid</i> terang-terangan;</p> <p>Objek pada <i>cyber terrorism</i> mengenai hal yang berkaitan dengan internet sedang <i>tahdid</i> tidak begitu bersinggungan dengan internet.</p>
6	<p><i>Offense against intellectual property;</i></p> <p>“kejahatan yang dilakukan terhadap Hak Atas Kekayaan Intelektual (HAKI) seseorang seperti meniru tampilan web page yang sudah dihakikan pemiliknya”</p>	<p><i>alaintihal</i></p> <p>(palagiat atau memanipulasi)</p> <p>“Tindakan mengambil karya orang lain yang kemudian menjadikannya seolah-olah karangannya sendiri atau meniplak karya tulis</p>	Sama-sama meniru.	Kejahatan pada <i>offense against intellectual property</i> mengklaim milik orang lain menjadi miliknya lewat internet sedangkan <i>alaintihal</i> mengklaim milik orang lain menjadi miliknya pada realita suatu barang.



		orang lain” <i>aintihal alhuia</i> (penipuan atau peniruan) “sebuah tindakan tipu muslihat untuk mendapatkan keuntungan <u>pribadi</u> dengan merugikan orang lain”.	Sama-sama menipu	Kejahatan pada <i>offense against intellectual property</i> melakukan penipuan lewat ponsel dengan mengirimkan pesan singkat kepada korbannya dengan mengaku sebagai papa, mama, adik ataupun kerabat lainnya yang pada akhirnya meminta dikirimkan pulsa kepada korbannya. Sedangkan <i>aintihal alhuia</i> tindakan <i>trickery</i> (penipuan) di dunia nyata seperti mengurangi timbangan.
7	<u><i>Infringementsof privacy;</i></u> “kejahatan terhadap data pribadi seseorang yang sangat rahasia seperti nomor pin ATM sehingga dapat merugikan banyak pihak”.	<u><i>Hirabah</i></u> (perampokan); “yaitu tindakan mengambil harta atau pemindahan hak kepemilikan harta orang lain dengan transaksi yang tidak sah disertai dengan pemaksaan”	Sama-sama merampok milik orang lain dan sama-sama <i>meresahkan</i> (mengganggu) keamanan masyarakat.	<i>Infringementsof privacy</i> merupakan cara merampok dengan cara bijak lewat internet sedangkan <i>hirabah</i> masih menggunakan cara kuno <i>pes tu pes</i> (kontak fisik) antara perampok dan korban saling berhadapan. <i>Infringementsof privacy</i> bisa saja dipandang sebagai tindakan pengrusakan dokumen elektronik seseorang yang paling rahasia, sedangkan <i>hirabah</i> juga tindakan pengrusakan rasa kenyamanan di masyarakat.

Selain tujuh terminologi *cyber crime*, ada beberapa model *cyber crime* lain yang terdapat di internet antara lain perjudian online, calo online, dan penyebaran pornografi lewat situs-situs porno yang mudah diakses para penikmat internet. Semua model kejahatan *cyber crime* yang diuraikan di sini masih belum final sebab masih banyak lagi modelnya yang tidak memungkinkan untuk dipaparkan pada artikel ini, bahkan semakin hari maka semakin banyak bermunculan model *cyber crime* yang baru.

Disini terlihat bahwa kedua kejahatan di atas sama-sama masuk kedalam kategori pencurian hanya cara dan modusnya saja yang berbeda, begitu juga dengan kasus pembunuhan baik ala orang dahulu kala dengan pedang maupun ala zaman now dengan



tembak elektronik apabila dianalogikan tetap sama yaitu sama-sama menghilangkan nyawa seseorang sehingga harus dikenai sanksi hukuman.

Mengenai hukuman dalam hukum Islam diatur pada fikih jinayah yang membahas rangkaian *jarimah* (semua hal yang dilarang ajaran Islam) baik perbuatan maupun tindakan yang dilarang dalam syariat Islam. Adakalanya *jarimah* itu disebut *jarimah hudud* karena larangan tersebut dibarengi dengan ancaman hukuman langsung ditentukan Allah SWT di dalam al-Qur'an dan sunnah¹⁰ seperti kejahatan zina, *qozaf* (tujuan palsu tentang perzinaan), *sariqah* (pencurian), *hirabah* (perampokan), *riddah* (murtad), *al-baghy* (pemberontakan), dan *syurb al-khamr* (minum-minuman keras).¹¹

Namun adakalanya *jarimah* itu disebut *jarimah ta'zir* atau sebab Allah SWT tidak menentukan hukumannya secara tegas di dalam al-Qur'an maupun sunnah tentang *kadar* (besar kecil) hukuman bagi pelakunya.¹² Maksud *ta'zir* disini, ketentuan hukuman bagi pelakunya ditetapkan oleh *ulil amri* (penguasa atau hakim) yang memiliki kredibilitas untuk memberikan rasa jera kepada pelaku dalam rangka menghentikan kejahatan sehingga tercipta rasa aman dan ketenteraman di masyarakat.¹³

Mengingat *cyber crime* adalah merupakan tindak kejahatan yang relatif baru maka sudah pasti dapat dikategorikan sebagai *jarimah ta'zir* yang menurut Wahbah Zuhaili yaitu suatu hukuman bagi suatu kemaksiatan atau kejahatan yang tidak ditetapkan hukumannya secara tegas dalam nash,¹⁴ sedangkan dalam peristilahan al-Mawardi yaitu hukuman *ta'dib* (edukatif) yang bersifat mendidik terhadap pelaku,¹⁵ *al-man'u* (pencegahan/ antisipasi), atau *tankif* (menakut-nakuti)¹⁶ seperti *cyber hoaxes* sama dengan kebohongan.¹⁷ Kecuali beberapa model *cyber crime* yang dapat diqiyaskan dengan *jarimah hudud* (hukuman yang sudah ditetapkan secara jelas dalam nash al-Qur'an dan sunnah) salah satunya adalah *unauthorized access to computer system and service* seperti *carding* (pembobolan kartu kredit) apalagi sampai mencapai lebih dari seperempat dirham maka sudah dapat diqiyaskan dengan *syariqah* (pencurian) maka yang bersangkutan bisa saja dikenahi hukuman potong tangan apabila yang bersangkutan mencuri mencapai nisabnya (batasnya) yaitu lebih dari seperempat dirham. Termasuk juga kejahatan *Illegal contents* seperti *cyber seks* (prostitusi online) yang pada akhirnya akan menjerumus insan manusia kedalam kasus *harasement* (kesusilaan), pornografi, atau perzinaan, maka apabila pelaku sampai kepada perzinaan maka mereka yang melakukan perzinaan tersebut dapat dijatuhi hukuman *dera* (cambuk) buat pelaku yang belum menikah dan bisa saja dijatuhi hukuman *rajam* (dilempari batu sampai meninggal) terhadap pelaku yang sudah menikah.¹⁸



Sekalipun hukuman ta'zir merupakan pembelajaran bagi pelaku, tetapi hukuman ta'zir memiliki variasi mulai yang paling ringan sampai yang paling berat sesuai dengan tingkat kejahatan yang dilakukan pelaku. Dalam kitab *Al-Fiqh 'Ala Al-Madzahib Al-'Arba'ah* Abdurrahman Al-Jaziri menyebutkan ada beberapa macam hukuman ta'zir sebagai berikut :¹⁹

6	Hukuman mati Terhadap <i>cyber terrorism</i> (pengancaman) dan <i>infringements of privacy</i> (perampokan) mengganggu ketentraman umum dapat dikenakan hukuman mati.
5	Hukuman pengasingan Terkait dengan <i>cyber data forgery</i> (pemalsuan) khalifah Umar bin Khattab pernah menghukum pelaku pemalsuan stempel Baitul Mal dengan hukuman pengasingan selama 1 tahun dan dicambuk sebanyak 100 kali.
4	Hukuman penjara : Terhadap <i>crime offense against intellectual property</i> (penipuan) tidak dijelaskan mengenai hukuman bagi pelakunya sehingga hakim bisa saja menjatuhkan hukuman penjara.
3	Hukuman cambuk : Terhadap <i>cyber data forgery</i> (pemalsuan) hukuman cambuk sebanyak 100 kali serta diasingkan selama 1 tahun.
2	Hukuman denda : Terhadap <i>crime offense against intellectual property</i> (palagiat) tidak dijelaskan mengenai hukuman bagi pelakunya sehingga hakim bisa saja menjatuhkan hukuman denda sesuai dengan besarnya kerugian yang dialami korbannya.
1	Hukuman pengucilan : Terhadap <i>crime offense against intellectual property</i> (hoax) tidak dijelaskan mengenai hukuman bagi pelakunya sehingga hakim bisa saja menjatuhkan pengucilan atau sanksi sosial berupa himbauan supaya yang bersangkutan dijauhi masyarakat.
	Hukuman <i>tahdid</i> (ancaman), <i>tanbih</i> (teguran), dan <i>al-Wadh'u</i> (peringatan) : Terhadap <i>cyber espionage</i> (memata-matai) tidak ada hukuman yang telah ditentukan maka para hakim bisa saja menjatuhi pelakunya berupa <i>tahdid</i> , <i>tanbih</i> , atau <i>al-Wadh'u</i> .

Sebagai hukuman ta'zir, maka seorang hakim tidak salah apabila menjatuhkan hukuman ta'zir bersesuaian dengan aturan-aturan yang sudah ada di dalam hukum positif,



terkhusus pada tindak kejahatan yang memang tidak dijelaskan secara tegas dalam al-Qur'an maupun sunnah termasuk mengenai kejahatan *cyber crime* ini, maka seorang hakim dapat menjatuhkan hukuman dengan mensinergikannya dengan sanksi-sanksi yang sudah ada dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang antara lain sebagai berikut :

Pasal 322 ayat 1 dan 2 KUHP menyatakan bahwa barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama 9 (sembilan) bulan atau pidana denda paling banyak Rp. 9.000,- (sembilan ribu rupiah).

Pasal 269 ayat 1 dan 2 KUHP menyatakan bahwa barang siapa membuat surat palsu atau memalsu surat keterangan tanda kelakuan baik, kemiskinan, kecacatan atau keadaan lain, dengan maksud supaya diterima dalam pekerjaan atau pertolongan diancam dengan pidana penjara paling lama 1 (satu) tahun 4 (empat) bulan.

Pasal 406 ayat 1 dan 2 KUHP menyatakan bahwa barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tidak dapat dipakai atau menghilangkan sesuatu barang yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama 2 (dua) tahun 8 (delapan) bulan atau denda paling banyak Rp. 300.000,- (tiga ratus rupiah).

Pasal 45 ayat 3 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan penghinaan atau pencemaran nama baik akan dipidana dengan pidana penjara paling lama 4 (empat) tahun atau denda paling banyak Rp. 750.000.000,- (tujuh ratus lima puluh juta rupiah).

Pasal 45b Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mengirimkan informasi elektronik atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi akan dipidana dengan pidana penjara paling lama 4 (empat) tahun atau denda paling banyak Rp. 750.000.000,- (tujuh ratus lima puluh juta rupiah).”

Pasal 362 ayat 1 dan 2 KUHP menyatakan bahwa barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki



secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp. 900.000,- (sembilan ratus rupiah).

Pasal 45 ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya Informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan akan dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).

Pasal 45 ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya Informasi elektronik atau dokumen elektronik yang memiliki muatan perjudian akan dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).

Pasal 45 ayat 4 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan pemerasan atau pengancaman akan dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).

Pasal 45a ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik akan dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).

Pasal 45a ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu atau kelompok masyarakat tertentu berdasarkan atas Suku, Agama, Ras, dan Antargolongan (SARA) akan dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Pasal 263 ayat 1 dan 2 KUHP menyatakan bahwa barang siapa membuat surat palsu atau memalsukan surat diancam dengan pidana penjara paling lama 6 (enam) tahun.



Pasal 242 ayat 1, 2, 3, dan 4 KUHP menyatakan bahwa barang siapa dengan sengaja memberi keterangan palsu baik dengan lisan atau tulisan diancam dengan pidana penjara paling lama 7 (tujuh) tahun. Apabila keterangan palsu itu merugikan seseorang mengenai pidana maka pelaku diancam pidana penjara paling lama 9 (sembilan) tahun.

Pasal 264 ayat 1 dan 2 KUHP menyatakan bahwa barang memalsukan surat akta-akta otentik atau sertifikat yayasan diancam dengan pidana penjara paling lama 8 (delapan) tahun.

D. Penutup

Hampir disetiap aktivitas yang kita lakukan sehari-hari di dunia maya semuanya memberikan peluang untuk terjadi kejahatan *cyber crime*, padahal saat ini kita hampir setiap hari selalu berhubungan ke internet sehingga sangat tidak memungkinkan buat kita yang hidup di zaman now ini untuk *gaptek* (beralih atau meninggalkan internet). Tetapi kita harus selalu waspada dan berhati-hati dengan memperdalam semaksimal mungkin pengetahuan kita tentang fitur-fitur yang kita gunakan di internet terutama hal-hal yang berkaitan dengan *celal-cela* (kemungkinan-kemungkinan) yang dapat dimanfaatkan pelaku *cyber crime* untuk menyalahgunakan teknologi digital kepada kita.

Menurut fikih jinayah, kejahatan *cyber crime* (kriminal berteknologi tinggi) ini dapat digolongkan sebagai *jarimah* (hal-hal yang dilarang syariat Islam) ada yang diqiyaskan dengan *syariqah, kadzib, tajasus, altazif, tahdid, alaintihal, dan hirabah*. Maka dalam aturan-aturan di dalam fikih jinayah bahwa setiap pelaku *cyber crime* dapat dijatuhi hukuman ta'zir bahkan hukuman *hudud* apabila memiliki illat (kesamaan) dengan *jarimah hudud*.

End Note :

¹ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara; Cybercrime*, (Jakarta: Refika Aditama, 2005), hlm. 39-103.

² Hinca IP Panjaitan dkk, *Membangun Cyber Law Indonesia yang Demokratis*, (Jakarta : IMLPC, 2005) hlm. 56-58.

³ Maskun, *Kejahatan Cyber Crime : Suatu Pengantar*, (Jakarta : Kencana, 2013), hlm. 64. Lihat juga Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta : Raja Grafindo Persada, 2006), hlm.179.

⁴ Dian Purnamawati, *Mengenal Dunia Cyber*, (Surakarta : CV. Mediatama, 2007) , hlm. 68. Lihat juga Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw; Tinjauan Aspek Hukum Pidana*, (Jakarta: Tatanusa, 2012), hlm. 309-310.

⁵ Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, cet ke-1, (Yogyakarta: Laksbang Pressindo, 2007), hlm. 1-64.

⁶ Widodo, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi*, (Yogyakarta: Aswaja Pressindo, 2013), hlm. 1.

⁷ Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyberlaw Aspek Hukum Teknologi Informasi*, cet ke-2, (Bandung: Refika Aditama, 2009), hlm. 4.

⁸ Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, (Yogyakarta: Graha Ilmu, 2014), hlm. 12-13.



-
- ⁹ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi; Cybercrime; Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012), hlm. 124.
- ¹⁰ Zainuddin Ali, *Hukum Pidana Islam*, (Jakarta: Sinar Grafika, 2009), hlm. 1-60.
- ¹¹ Makhrus Munajat, *Hukum Pidana Islam; Fiqih Jinayat*, (Yogyakarta: Pesantren Nawasea Press, 2010), hlm. 105.
- ¹² Nurul Irfan, *Hukum Pidana Islam*, (Jakarta: Amzah, 2016), hlm. 1-57. Lihat juga Mustofa Hasan dan Beni Ahmad Saebani, *Hukum Pidana Islam; Fiqh Jinayah*, (Bandung: Pustaka Setia, 2013), hlm. 27.
- ¹³ Makhrus Munajat, *Reaktualisasi Pemikiran Hukum Pidana Islam*, (Yogyakarta: Cakrawala, 2006), hlm. 13. Lihat juga M. Nurul Irfan dan Masyrofah, *Fiqh Jinayat*, cet ke-1, (Jakarta: Amzah, 2013), hlm. 188.
- ¹⁴ Wahbah Zuhaili, *Al-Fiqh Al-Islami wa Adillatuhu*, juz VI, (Damaskus: Dar Al-Fikr, 1989), hlm. 197.
- ¹⁵ Abu Al-Hasan Ali Al-Mawardi, *Kitab Al-Ahkam As-Sulthaniyah*, (Beirut : Dar Al-Fikr, 1996), hlm. 236.
- ¹⁶ Sofwan Jannah & M. Naufal, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam*, Jurnal Al-Mawarid Fakultas Ilmu Agama Islam UII Yogyakarta, Volume XII Nomor 1 Edisi Februari-Agustus Tahun 2012, hlm. 82.
- ¹⁷ Muhammad Arsad Nasution, *Hoax Sebagai Bentuk Hudud*, Jurnal Yurispudentia; Jurnal Hukum Ekonomi Syariah Fakultas Syariah dan Ilmu Hukum IAIN Padangsimpuan, Volume 3 Nomor 1, Edisi Januari-Juni Tahun 2017, hlm. 1-28.
- ¹⁸ Ahmad Wardi Muslich, *Hukum Pidana Islam*, (Jakarta : Sinar Grafika, 2005), hlm. 6-29. Lihat pula Topo Santoso, *Membumikan Hukum Pidana Islam; Penegakan Syariat dalam Wacana dan Agenda*, cet ke-1, (Jakarta : Gema Insani Press, 2003), hlm. 25.
- ¹⁹ Abdurrahman Al-Jaziri, *Al- Fiqh 'Ala Al-Madzahib Al-'Arba'ah*, jilid V, (Beirut: Dar Al-Fikr Al-'Arabi, 1989), hlm. 2234.



DAFTAR PUSTAKA

- Ali, Zainuddin,. *Hukum Pidana Islam*, Jakarta: Sinar Grafika, 2009.
- Al-Jaziri, Abdurrahman ., *Al- Fiqh 'Ala Al-Madzahib Al- 'Arba 'ah*, jilid V, Beirut: Dar Al-Fikr Al-'Arabi, 1989.
- Al-Mawardi, Abu Al-Hasan Ali,. *Kitab Al-Ahkam As-Sulthaniyah*, Beirut : Dar Al-Fikr, 1996.
- Arief, Barda Nawawi,. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta : Raja Grafindo Persada, 2006.
- Hasan, Mustofa dan Saebani, Beni Ahmad,. *Hukum Pidana Islam; Fiqh Jinayah*, Bandung: Pustaka Setia, 2013.
- Indrajit, Richardus Eko,. *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta: Graha Ilmu, 2014.
- Irfan, M. Nurul dan Masyrofah,. *Fiqh Jinayat*, cet ke-1, Jakarta: Amzah, 2013.
- ,. *Hukum Pidana Islam*, Jakarta: Amzah, 2016.
- Jannah, Sofwan & Naufal, M.,. *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam*, Jurnal Al-Mawarid Fakultas Ilmu Agama Islam UII Yogyakarta, Volume XII Nomor 1 Edisi Februari-Agustus Tahun 2012.
- Labib, Abdul Wahid dan Mohammad,. *Kejahatan Mayantara; Cybercrime*, Jakarta: Refika Aditama, 2005.
- Mansur, Dikdik M. Arief dan Gultom, Elisatris, *Cyberlaw Aspek Hukum Teknologi Informasi*, cet ke-2, Bandung: Refika Aditama, 2009.
- Maskun, *Kejahatan Cyber Crime : Suatu Pengantar*, Jakarta : Kencana, 2013.
- Munajat, Makhrus,. *Hukum Pidana Islam; Fiqh Jinayat*, Yogyakarta: Pesantren Nawasea Press, 2010.
- ,. *Reaktualisasi Pemikiran Hukum Pidana Islam*, Yogyakarta: Cakrawala, 2006.
- Muslich, Ahmad Wardi,. *Hukum Pidana Islam*, Jakarta : Sinar Grafika, 2005.
- Nasution, Muhammad Arsad,. *Hoax Sebagai Bentuk Hudud*, Jurnal Yurispudentia; Jurnal Hukum Ekonomi Syariah Fakultas Syariah dan Ilmu Hukum IAIN Padangsimpunan, Volume 3 Nomor 1, Edisi Januari-Juni Tahun 2017.
- Panjaitan, Hinca IP dkk,. *Membangun Cyber Law Indonesia yang Demokratis*, Jakarta: IMLPC, 2005.
- Purnamawati, Dian,. *Mengenal Dunia Cyber*, Surakarta : CV. Mediatama, 2007.
- Santoso, Topo, *Membumikan Hukum Pidana Islam; Penegakan Syariat dalam Wacana dan Agenda*, cet ke-1, Jakarta : Gema Insani Press, 2003.
- Sitompul, Josua,. *Cyberspace, Cybercrimes, Cyberlaw; Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa, 2012.
- Suhariyanto, Budi,. *Tindak Pidana Teknologi Informasi; Cybercrime; Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers, 2012.
- Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, cet ke-1, Yogyakarta: Laksbang Pressindo, 2007.
- Widodo, *Memerangi Cybercrime Karakteristik Motivasi dan Strategi Penanganannya dalam Perspektif Kriminologi*, Yogyakarta: Aswaja Pressindo, 2013.
- Zuhaili, Wahbah,. *Al-Fiqh Al-Islami wa Adillatuhu*, juz VI, Damaskus: Dar Al-Fikr, 1989.