

KEJAHATAN DUNIA MAYA (*CYBERCRIME*) DALAM PRESFEKTIF HUKUM ISLAM DAN HUKUM POSITIF INDONESIA

Oleh :

Aidil Fitri

Aidilfitri515@gmail.com

Fakultas Hukum Universitas IBA

Hj. Suryani Yusi

yaniyusi@gmail.com

Fakultas Hukum Universitas IBA

Abstrak

Maraknya tindakan Cyber Crime dengan meningkatnya teknologi yang akan banyak merugikan di masyarakat harus disertai dengan penegakan hukum yang juga lebih masif. Kejahatan siber, atau dikenal pula dengan cybercrime, adalah suatu bentuk kejahatan yang terjadi di jagat maya melalui komputer, perangkat seluler, dan jejaring internet. Kejahatan siber dapat menyerang siapa pun, tidak hanya individu masyarakat, namun juga organisasi pemerintahan sekalipun. Sangat berbahayanya tindakan ini, sehingga tidak hanya diatur dalam undang undang hukum positif Indonesia, dalam Islam tindakan ini merupakan tindakan kejahatan karena merupakan perbuatan kerusakan yang merugikan banyak orang.

Kata Kunci : *Cybercrime*, Hukum Islam, Hukum Positif Indonesia

Abstract

The rise of Cyber Crime with increasing technology which will cause a lot of harm to society must be accompanied by more massive law enforcement. Cybercrime, also known as cybercrime, is a form of crime that occurs in cyberspace via computers, mobile devices and internet networks. Cybercrime can attack anyone, not only individuals in society, but also government organizations. This action is very dangerous, so that it is not only regulated in Indonesian positive law, in Islam this action is a crime because it is an act of damage that harms many people.

Keywords: Cybercrime, Islamic Law, Indonesian Positive Law

A. PENDAHULUAN

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah,

dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.¹

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).² Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *Cybercrime*.

Cybercrime merupakan tindak perilaku kejahatan berbasis komputer dan jaringan internet. Pelaku dari kejahatan siber biasanya akan meretas sistem untuk memperoleh data korban yang bersifat privasi. Keamanan data sangatlah penting, Perusahaan besar seperti Microsoft, Yahoo, TautanedIn, Sony Playstation, Adobe, dan bahkan NASA saja pernah menjadi korban serangan dunia maya, Banyaknya jenis kejahatan siber yang ada, membuat kita harus lebih waspada serta bijak dalam menggunakan media internet. Terlebih pelaku kejahatan siber tidak pandang bulu, sehingga siapa saja dapat menjadi korban kejahatan siber.

Hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam rilis yang berjudul “Penetrasi dan Perilaku Pengguna Internet Indonesia 2017” pengguna internet di Indonesia telah mencapai angka 143,26 juta jiwa atau setara dengan 54,7% total populasi. *Cybercrime* atau kejahatan siber dapat diartikan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana atau alat, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Cybercrime selain bertentangan dengan hukum positif di Indonesia juga merupakan tindakan yang dilarang oleh Allah swt. karena Allah swt. tidak menyukai orang-orang yang membuat kerusakan yang memudharatkan orang lain. Perusakan dalam bentuk apapun tidak dibenarkan, karena perusakan merupakan tindakan yang bertentangan dengan nilai-nilai universal Allah swt.

¹ Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cybercrime)*, Bandung, PT Refika Aditama, hlm. 23.

² Edmon Makarim, 2005, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*, Jakarta PT Raja Grafindo Persada, hlm. 426.

Untuk itu penulis akan membahas lebih mendalam bagaimana *Cybercrime* dalam perspektif hukum Islam dan Hukum Positif di Indonesia.

B. PERMASALAHAN

Bagaimana *Cybercrime* dalam Prespektif Hukum Islam dan Hukum Positif di Indonesia?

C. METODE PENELITIAN

Penelitian dalam tulisan ini adalah penelitian yuridis normatif, yang diteliti hanya bahan pustaka atau data sekunder, yang mungkin mencakup bahan hukum primer, sekunder dan tertier.⁵ Penelitian hukum normatif merupakan penelitian yang dilakukan dengan cara meneliti bahan pustaka. Data yang digunakan dalam penelitian tulisan ini adalah data Sekunder.

D. PEMBAHASAN

1. Pengertian Tindak Pidana *Cybercrime*

Pengertian *Cybercrime* adalah suatu upaya memasuki/ menggunakan fasilitas komputer/ jaringan komputer tanpa ijin dan melawan hukum atau tanpa menyebabkan perubahan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut atau kejahatan yang dengan menggunakan sarana media elektronik internet (merupakan kejahatan dunia alam maya) atau kejahatan dibidang komputer dengan secara ilegal, dan terdapat definisi yang lain yaitu sebagai kejahatan komputer yang ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.

Pengertian *Cybercrime* menurut Prof Widodo adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum. secara material maupun melawan hukum secara formal.³ Kemudian, definisi lain mengenai kejahatan komputer ini dikeluarkan oleh Organization of European Community Development (OECD) yaitu sebagai berikut: “ any illegal, unethical or unauthorized behavior relating to the aouthomathic processing and/or the transmission of

⁵ Beni Ahmad Saebani, *Metode Penelitian Hukum*, CV. Pustaka Setia, Bandung,, 2008, hlm. 39

³ Widodo, *Aspek Hukum Kejahatan Mayantara*, Yogyakarta, Aswindo, 2011, hlm. 7

data”.⁴ Sedangkan Menurut Andi Hamzah, bahwa “kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal”.⁵

Menurut Abdul Wahid dan M. Labib, *Cybercrime* memiliki beberapa karakteristik, yaitu :⁶

- 1) perbuatan yang dilakukan secara illegal, tanpa hak atau tindakan etis terjadi diruang/wilayah siber, sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku terhadapnya;
- 2) perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet;
- 3) perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
- 4) pelakunya adalah orang yang menguasai penggunaan internet dan aplikasinya;
- 5) perbuatan tersebut sering dilakukan secara transnasional.

2. *Cybercrime* dalam Presfektif Hukum Islam

Dalam hukum Islam disyariatkan mengenai pemidanaan dari perbuatan tindak pidana yang merugikan. Adanya hukuman pemidanaan ini bertujuan untuk memperbaiki perilaku dari manusia, dan untuk memberi solusi agar manusia dapat menghindari bentuk-bentuk perilaku yang maksiat. Serta tujuan dari adanya hukuman pemidanaan ini agar semua umat dapat melakukan hal-hal atau perilaku yang sesuai dengan perintah Allah SWT. sehingga dapat menurunkan tingkat kemaksiatan dan kesesatan.

Al-Quran surat al-Mudatsir ayat 38 artinya:

“Tiap-tiap diri bertanggungjawab atas apa yang diperbuatnya”. Al-Quran surat Fatir ayat 18 artinya:

“Dan orang yang berdosa tidak akan memikul dosa orang lain. Dan jika seseorang yang berat dosanya memanggil (orang lain) untuk memikul dosanya itu tidaklah akan dipikulkan untuknya sedikitpun meskipun (yang dipanggil itu) kaum kerabatnya. Sesungguhnya yang dapat kamu beri peringatan hanya orang-orang yang takut kepada azab Tuhannya

⁴ Eddy Djunedji Karnasudiraja, *Yurisprudensi Kejahatan Komputer*, Jakarta, CV Tanjung Agung, 1993, hlm. 3.

⁵ Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta, Sinar Grafika, 1989, hlm. 26.

⁶ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Jakarta: PT. Refika Aditama, 2005, hlm. 76

(sekalipun) mereka tidak melihatNya. dan mereka mendirikan sembahyang. Dan barang siapa yang mensucikan dirinya, sesungguhnya ia mensucikan diri untuk kebaikan dirinya sendiri. Dan kepada Allahlah kembali(mu).

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, sedangkan dalam peristilahan al-Mawardi yaitu hukuman ta'dib (edukatif) yang bersifat mendidik terhadap pelaku, al-man'u (pencegahan/antisipasi), atau tankîf (menakut-nakuti) seperti cyber hoaxes sama dengan kebohongan.

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 harassment (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.⁷

3. *Cybercrime* dalam Prespektif Hukum Positif Indonesia

Dalam undang-undang tersebut terdapat beberapa pasal yang mengatur perbuatan yang dilarang yang termasuk tindak pidana *Cybercrime*. Sebelum ada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini yang digunakan untuk mengancam pidana bagi perbuatan yang dikategorikan dalam tindak pidana *Cybercrime*. Namun undang undang ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana *Cybercrime* yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomodir tindak-tindak pidana yang berkaitan dengan komputer.

⁷ Hendra Gunawan, *Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah*, Jurnal el-Qonuniy, 2020. Hlm 104

“Pasal 22 yang berbunyi: “Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

- 1) Akses ke jaringan telekomunikasi; dan atau
- 2) Akses ke jasa telekomunikasi; dan atau
- 3) Akses ke jaringan telekomunikasi khusus.”

“Pasal 38 yang berbunyi : “Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi”

“Pasal 40 yang berbunyi : “Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun”.

Bentuk-bentuk tindak pidana *Cybercrime* dalam Undang undang Nomor 36 tahun 1999 tentang Telekomunikasi adalah Akses Illegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi. Hal ini merujuk pada pengertian *Cybercrime* yang diberikan oleh Konferensi PBB yang menyatakan *Cybercrime* adalah perbuatan yang tidak sah yang menjadikan komputer atau jaringan komputer, baik pada sistem keamanannya. Telekomunikasi merupakan salah satu bentuk jaringan dan sistem komputer sehingga perbuatan yang dilarang dalam pasal pasal tersebut dapat dikategorikan menjadi tindak pidana *Cybercrime*.

Tindak Pidana *Cybercrime* dalam UU ITE diatur dalam 9 pasal, dari pasal 27 sampai dengan pasal 35.

Dalam 9 pasal tersebut dirumuskan 20 bentuk atau jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Sementara ancaman pidananya ditentukan didalam Pasal 45 sampai Pasal 52. Adapun rumusan pasalpasal tersebut adalah sebagai berikut:

“Pasal 27 yang berbunyi :

- 1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
- 2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

- 3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- 4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

“Pasal 28 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. 2) Setiap Orang dengan sengaja dan 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 (SARA).” “Pasal 29 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.” “Pasal 30 yang berbunyi:
 - 2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
 - 3) Setiap Orang dengan sengaja dan 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.
 - 4) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.”

“Pasal 31 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan 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.
- 2) Setiap Orang dengan sengaja dan 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/ 36 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.
- 3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- 4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.”

“Pasal 32 yang berbunyi:

- 1) Setiap Orang dengan sengaja dan 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.
- 2) Setiap Orang dengan sengaja dan 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.

- 3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) 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.”

“Pasal 33 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

“Pasal 34 yang berbunyi:

1) Setiap Orang dengan sengaja dan 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 37 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
- 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.”

“Pasal 35 yang berbunyi: “Setiap Orang dengan sengaja dan 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.”

“Pasal 36 yang berbunyi: “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.”

“Pasal 37 yang berbunyi: “Setiap Orang 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.”

E. KESIMPULAN

Munculnya berbagai kejahatan di dunia maya juga harus diimbangi oleh penegakan hukum yang sedemikian rupa agar pelaku-pelaku dapat diproses secara hukum agar jera.

Semakin berkembangnya teknologi semakin berkembang pula kejahatan di dunia maya, maka aturan-aturan hukum pun harus terus berkembang mengikutinya.

hukum Islam dan Hukum Positif memandang bahwa *cybercrime* merupakan bagian dari

kejahatan yang merugikan banyak orang harus diberantas agar tercipta ketenangan di masyarakat.

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cybercrime)*, Bandung, PT Refika Aditama

Andi Hamzah, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta, Sinar Grafika, 1989

Beni Ahmad Saebani, *Metode Penelitian Hukum, CV. Pustaka Setia*, Bandung, 2008

Eddy Djunedo Karnasudiraja, *Yurisprudensi Kejahatan Komputer*, Jakarta, CV Tanjung Agung, 1993

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

Hendra Gunawan, *Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah*, Jurnal el-Qonuniy, 2020

Widodo, *Aspek Hukum Kejahatan Mayantara*, Yogyakarta, Aswindo, 2011,