BAB III

CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

A. *Cyber Security* Menurut Hukum Positif di Indonesia

Hukum adalah keseluruhan peraturan baik yang tertulis maupun tidak tertulis yang mengatur tata tertib dalam masyarakat dan terhadap pelanggarnya umumnya dikenakan sanksi. Adapun yang dimaksud dengan hukum positif adalah kumpulan asas dan kaidah hukum tertulis yang pada saat ini sedang berlaku dan mengikat secara umum atau khusus dan ditegakkan oleh atau melalui pemerintah atau pengadilan dalam negara Indonesia.

Hukum melekat pada masyarakat, karena hukum diciptakan untuk mengatur masyarakat, maka masyarakat harus ikut serta dalam pelaksanaan peraturan tersebut. Orang-orang diharuskan untuk mengikuti aturan untuk mendapatkan pesanan.[1] Peraturan yang dibuat untuk mengatur masyarakat biasanya berupa undang-undang yang dikeluarkan oleh pemerintah untuk memenuhi kebutuhan masyarakat.

Dasar hukum pengaturan keamanan siber di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun 2008 dan Undang-Undang ITE Perubahan Nomor 19 Tahun 2016. Undang-undang ini memuat ketentuan sejumlah pelanggaran, seperti penyebaran konten ilegal. ,

[1] Satjipto Rahardjo, *Sosiologi Hukum Esai-Esai Terpilih* (Yogyakarta: Genta Publishing, 2010). hlm. 99.

pelanggaran perlindungan data, akses tidak sah ke sistem komputer untuk memperoleh informasi, perampasan ilegal dan tidak sah atau penyadapan sistem komputer komputer atau elektronik lainnya. UU ITE memberikan perlindungan hukum terhadap isi sistem elektronik dan transaksi elektronik. Namun, undang-undang tersebut tidak membahas aspek-aspek penting dari keamanan siber, seperti infrastruktur informasi dan jaringan, serta sumber daya manusia yang memiliki keahlian keamanan siber.

Berdasarkan UU ITE 2016, pemerintah telah mengeluarkan regulasi teknis, khususnya Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PP No 71 Tahun 2019 memuat pemutakhiran terkait penerapan keamanan siber dalam sistem dan transaksi elektronik. Selain sejumlah pasal terkait pelanggaran yang tercakup dalam UU ITE, PP No 71 Tahun 2019 memiliki ketentuan yang lebih ketat tentang perlindungan informasi dan informasi pribadi, serta otentikasi situs web untuk Menghindari situs web palsu atau scam. Selain itu, PP Nomor 71 Tahun 2019 menekankan perlunya pemerintah mencegah kerugian terhadap kepentingan umum melalui penyalahgunaan informasi dan transaksi elektronik serta perlunya mengembangkan strategi keamanan jaringan nasional. Namun, PP No. 71 hanya mencakup kejahatan dunia maya yang terkait dengan transaksi elektronik, seperti penyalahgunaan informasi, tanda tangan elektronik yang tidak sah, dan penyebaran infeksi dan afiliasi. Terbatasnya cakupan UU ITE dan PP No. 71

Tahun 2019 tidak mampu menjawab ancaman siber yang terus berkembang, terutama terhadap infrastruktur kritis pemerintah.. [2]

Selain UU ITE, selama ini *cybersecurity* Indonesia diawasi oleh Indonesia *Internet Infrastructure Security Incident Response Team* (IDSIRTII). Sub Komite Darurat Komputer (IDCERT) dan *cybercrime* Bareskrim Divisi Ekonomi Khusus dan Reserse Kriminal (Dit Tipideksus). Meskipun kebijakan keamanan siber telah diatur dalam UU ITE, Indonesia juga menghadapi masalah pembagian kekuasaan dan lembaga yang diperlukan untuk memerangi *cybercrime*, *cyber terrorism*, *cyber hacktivism*, dan *cyber warfare*. [3]

Undang-Undang yang mengatur untuk perlindungan terhadap keamanan data dan transaksi yang dilakukan konsumen/pengguna jasa/nasabah di Indonesia dikaitkan dengan Undang-Undang Perlindungan Konsumen yang tertuang dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Sedangkan Undang-Undang tentang Informasi dan Teknologi Informasi (ITE) sangat erat kaitannya dengan digitalisasi di Indonesia termasuk perihal perbankan digital yang di dalamnya juga mengatur tentang pentingnya keamanan (*security*) pada transaksi-transaksi digital.

1. Cyber Security pada Bank Digital Menurut Undang-Undang Perlindungan Konsumen

[2] Noor Halimah Anjani, *Ringkasan Kebijakan No. 9 Perlindungan Keamanan Siber di Indonesia, Center For Indonesian Policy Studies (CIPS)*, Maret 2021. hlm.4.

[3] Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara*, Politica Vol. 10 No. 2 November 2019. hlm.119.

Di Indonesia Undang-Undang tentang Perlindungan Konsumen diatur dalam Undang-Undang No. 8 Tahun 1999. Perlindungan Konsumen merupakan istilah yang dipakai untuk menggambarkan adanya hukum yang memberikan perlindungan konsumen. Menurut Pasal 1 angka (1) "Perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberikan perlindungan konsumen".

Perlindungan konsumen mempunyai cakupan yang sangat luas meliputi perlindungan terhadap segala kerugian yang akan, sedang dan telah terjadi akibat penggunaan barang dan jasa.

Dalam transaksi pada bank digital, aspek tanggung jawab berlaku untuk pelaku usaha (bank digital). apabila konsumen (nasabah) menemui barang dan/atau jasa dalam hal ini layanan perbankan yang merugikan pihak nasabah. Aspek tanggung jawab terhadap keamanan/*security* kepada Nasabah dalam Undang-Undang Perlindungan Konsumen diatur dalam Pasal 2 yaitu "Perlindungan Konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan, dan keselamatan konsumen serta kepastian hukum" .

Dan diatur pula dalam pasal 4 bagian a. yaitu "Hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa".

Aspek ini berlaku pada saat pelaku usaha melakukan perbuatan yang menyebabkan kerugian bagi konsumen (nasabah). Kerugian ini berupa kebocoran data nasabah karena kurangnya keamanan/*security* pada bank digital.

2. Cyber Security menurut Undang-Undang Informasi dan Teknologi Elektronik (ITE)

Pengenalan rezim hukum baru (UU ITE) yang dikenal sebagai undang-undang telekomunikasi dapat dilihat sebagai respon positif. Telekomunikasi atau hukum jaringan digunakan secara internasional untuk istilah hukum yang berkaitan dengan penggunaan teknologi informasi dan komunikasi. Demikian pula hukum telekomunikasi merupakan ekspresi dari konvergensi hukum telekomunikasi, hukum telekomunikasi, hukum komunikasi, dan hukum komputer. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*information technology law*), hukum siber (*virtual world law*) dan hukum siber. Istilah ini berasal dari pertimbangan kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik lokal maupun global (Internet) dengan menggunakan teknologi informasi berdasarkan satu sistem.Komputer adalah sistem elektronik yang terlihat secara virtual. [4]

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.

[4] Maskun, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, Kencana Prenada Media Group : Jakarta, 2013, hlm.29.

UU ITE diundangkan pada tahun 2008 dan kemudian direvisi secara terbatas pada tahun 2016, ruang lingkup undang-undang ini adalah “satu untuk semua” dalam hal mengatur segala hal yang berkaitan dengan penggunaan teknologi informasi dan komunikasi termasuk perihal *Cyber Security* namun hanya sedikit pasal yang membahas terkait dengan keharusan adanya *Cyber Security*. Sebagaimana tertuang dalam pasal pasal 15 ayat 1 Undang Undang ITE bahwa “Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.”

Dan tertuang pada pasal 16 ayat (1) point b. Pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang berbunyi :

> “Setiap penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum yaitu dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut”

Cyber Security erat kaitannya dengan Cyber Law. Hukum siber adalah dasar hukum untuk proses penegakan hukum anti kejahatan kejahatan yang menggunakan teknologi digital, termasuk kejahatan pencucian uang dan kejahatan teroris. Fakta bahwa Hukum Jaringan perlu diatasi Kejahatan dunia maya.

Pengaturan Kejahatan Siber (*Cybercrime*) pada Perbankan

Indonesia belum memiliki undang-undang/*cyber law* khusus yang mengatur tentang *cybercrime*. Namun, ada sejumlah hukum positif lainnya yang

diterima secara umum dan dapat diterapkan pada penjahat dunia maya, terutama dalam kasus dimana komputer digunakan sebagai kendaraan, antara lain:[5]

1. Kitab Undang-Undang Hukum Pidana

Ketentuan KUHP sering digunakan lebih dari satu karena berkaitan dengan banyak perbuatan serta ketentuan yang dapat diterapkan dalam KUHP tentang Cybercrime, yaitu:

a) Pasal 362 KUHP berlaku untuk kasus pencurian kartu dimana pelaku mencuri nomor kartu kredit orang lain, bahkan tidak dalam kenyataan, karena nomor kartu hanya diperoleh dengan menggunakan perangkat lunak pembuatan kartu berbasis internet untuk melakukan transaksi *e-commerce* . Setelah menyelesaikan transaksi dan mengirimkan barang, merchant yang ingin menarik uang dari bank ditolak karena pemegang kartu bukanlah orang yang melakukan transaksi.
b) Pasal 378 KUHP dapat dijerat dengan penipuan dengan berpura-pura menawarkan produk atau barang dengan memasang iklan di salah satu situs web agar orang yang berminat membelinya dan kemudian mengirimkan uang kepada pengiklan. Tapi, pada kenyataannya, itu tidak ada. Hal ini diketahui setelah uang dikirim tetapi barang yang dipesan tidak sampai, sehingga pembeli tertipu.

[5] Deris Setiawan, *Sistem Keamanan Komputer*, (Jakarta: PT Elex Media Komputindo, 2005)..hlm. 40

c) Pasal 378 dan 262 KUHP dapat diterapkan pada kasus *carding*, karena pelaku melakukan penipuan seperti ingin membeli barang dan membayar dengan Nomor Kartu Kredit kartu kredit orang yang dicuri.

d) Pasal 406 KUHP dapat berlaku jika terjadi *deface* atau *hacking* yang membuat sistem orang lain, seperti situs web atau program, tidak dapat dioperasikan atau digunakan.

2. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik.

   Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para hacker yang masuk ke jaringan orang lain menurut ketentuan Pasal 22, khususnya: Dilarang keras orang melakukan perbuatan tanpa hak, tidak sah, atau manipulatif: 1. Akses ke jaringan telekomunikasi, 2. Akses ke layanan telekomunikasi, 3. Akses ke jaringan telekomunikasi khusus.

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)".

3. Undang-Undang No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-undang Nomor 15 Tahun 2002 merupakan undang-undang yang paling kuat yang memungkinkan penyidik memperoleh informasi tentang tersangka pelaku penipuan melalui internet, karena tidak memerlukan prosedur administrasi yang panjang dan memakan waktu. Karena tindak pidana pencucian uang (Pasal 2 ayat (1) huruf q). Penyidik dapat meminta kepada bank penerima transfer untuk memberikan identitas tersangka dan rincian perbankan tanpa tunduk pada ketentuan. Dalam undang-undang perbankan, identitas dan data perbankan merupakan bagian dari rahasia perbankan, sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedurnya adalah dengan mengirimkan surat dari Kapolda kepada Kapolri dan diteruskan kepada gubernur. dari Bank Indonesia. Proses ini membutuhkan waktu yang lama untuk mendapatkan data dan informasi yang diinginkan.

Dalam UU Pencucian Uang proses lebih cepat karena Kapolda hanya perlu mengirimkan surat kepada pimpinan Bank Indonesia di daerah beserta tembusannya kepada Kapolri dan Gubernur Bank Indonesia, untuk data dan informasi yang diperlukan Dapat diperoleh lebih lanjut dengan cepat

dan memudahkan penyidikan terhadap pelaku yang ditawarkan oleh pihak bank, berupa: formulir permohonan, nomor rekening kedatangan dan keberangkatan, tanggal dan lokasi transaksi, penyidik dapat menelusuri lokasi pelaku pada data tersebut. Undang-undang ini juga mengatur tentang barang bukti elektronik atau barang bukti digital berdasarkan Pasal 38 huruf b, khususnya alat bukti lain berupa informasi yang diucapkan, dikirim, diterima atau disimpan secara elektronik dengan alat optik atau sejenisnya.[6]

B. Cyber Security menurut Hukum Ekonomi Syariah

Hukum ekonomi syariah adalah kumpulan peraturan yang memiliki kaitannya tentang pemenuhan kebutuhan manusia baik itu bersifat umum maupun khusus berdasarkan ketentuan atau syariat Islam. Secara konseptual hukum ekonomi syariah ini memiliki hubungan yang erat dengan fiqih muamalat, karena kajian mengenai sumber hukum ekonomi syariah telah ada pada fiqih muamalat. Hanya pengembangan dan perluasan gagasannya perlu penjabaran yang sesuai dengan konteks perkembangan zaman khusus dalam bidang ekonomi dan harta benda.

Sumber hukum ekonomi syariah ini merujuk pada muara dari sumbernya. Muara dari hukum ekonomi syariah ini adalah hukum Islam, maka otomatis bahwa sumber hukumnya terbagi menjadi 2 (dua) bagian, yaitu:

1. Sumber hukum primer yaitu sumber hukum yang telah menjadi hujah dan rujukan oleh para ulama untuk mengetahui hukum-hukum Islam

[6] Sofwan Jannah dan M. Naufal, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam,* AL-MAWARID, VOL. XII, NO 1, FEB-AUGUST 2012, hlm. 74-77.

yaitu:

a. Alquran sumber segala hukum yang diturunkan Allah kepada Nabi Muhammad SAW.
b. Sunah yaitu segala perkataan, perbuatan, pengakuan yang berasal dari Nabi Muhammad SAW. Al-Quran dan Sunah menjadi dasar hukum utama dalam Islam. hierarki kedudukannya As-Sunnah merupakan sumber hukum kedua setelah Al-Qur'an.

2. Sumber hukum sekunder adalah hukum yang dikeluarkan melalui teknik berfikir dan penalaran oleh para ulama dengan menyaring kaidah-kaidah dari sumber hukum primer untuk menyelesaikan masalah baru dan belum disebutkan dalam nash yang biasa disebut dengan Usaha Ijtihad. ijtihad dilakukan dengan metode istinbat (menggali dari sumber hukum tertentu). Orang yang melakukan Ijtihad disebut dengan Mujtahid atau *faqih* (ahli fikih). Untuk memudahkan seorang Mujtahid dalam beristinbat hukum terhadap suatu masalah hukum maka diperlukan adanya kaidah fikih atau *qawaid al-fiqhiyah*. Abdullah bin Sa'id Muhammad "Abbadi al-Lahji al-Hadhrami mendefinisikan al-*qawa'id al-fiqhiyyah* sebagai ketentuan yang dapat digunakan untuk mengetahui hukum tentang kasus-kasus yang tidak ada aturan pastinya di dalam Alquran, Sunah maupun Ijma'.[7] Definisi ini mengindikasikan bahwa al-Hadhrami secara tegas meletakkan kaidah fikih dalam

[7] Abdullah bin Sa'id Muhammad al-Lahji al-Hadrami, *Idah al-Qawa'id al-Fiqhiyyah*, (Surabaya : Hidayah. 1410H) hlm. 10.

fungsinya sebagai status hukum tentang kasus-kasus baru yang belum disikapi dengan pasti oleh ketiga sumber hukum yaitu Alquran, Sunnah maupun Ijma'.

Dalam Hukum Ekonomi Syariah yang kaitannya dengan dunia digitalisasi yakni yang berkaitan dengan *Cyber Security* dalam penggunaan internet untuk menangkal serangan dan ancaman dari dunia *Cyber* belum ada ayat Alquran, Sunah dan Ijma' yang secara jelas menerangkan perihal tersebut. Sehingga untuk menjabarkan *Cyber Security* dalam perspektif Hukum Ekonomi Syariah diperlukan adanya Kaidah-kaidah Fikih. Dari hasil penelusuran penulis Kaidah-Kaidah Fiqh adalah sebagai berikut :

الْأَصْلُ فِي الْمُعَامَلَاتِ الْإِبَاحَةِ اِلاَّ اَنْ يَدُلَّ دَلِيْلٌ عَلَى تَحْرِيْمِهَا

"Pada dasarnya segala bentuk muamalah adalah boleh, terkecuali ada dalil yang mengharamkannya".[8]

Kaidah ini menerangkan bahwa Bank Digital dan *Cyber security* merupakan salah satu bentuk kegiatan yang termasuk dalam kajian muamalah kontemporer dan boleh dilakukan. Namun praktik muamalah kontemporer ini bisa saja diharamkan apabila mengandung unsur kezaliman.

Tanpa adanya *cyber security* maka Bank Digital akan menghadapi sebuah bahaya atau ancaman dan serangan kejahatan siber. Maka penerapan *cyber security* harus lebih didahulukan dibanding mengoperasikan Bank Digital. Sebagaimana kaidah fikih bahwa mencegah kemudaratan itu lebih utama daripada menarik datangnya kemaslahatan.

[8] Hendi Suhendi, *Fiqh Muamalah*, (Jakarta : PT Raja Grafindo Persada, 2011). hlm. 2.

دَرْءُ الْمَفَاسِدِ أَوْلَى مِنْ جَلْبِ الْمَصَالِحِ

"Mencegah kemudaratan itu lebih utama daripada menarik datangnya kemaslahatan".[9]

Ancaman dan bahaya serangan dari *cybercrime* merupakan hal yang akan mendatangkan kemudaratan bagi kehidupan manusia yang harus dihilangkan. Dalam kaidah fiqh berkaitan dengan "kemudaratan harus dihilangkan" sebagaimana berbunyi:

الضرار يزال

Menurut Muhammad al-zarqa dalam kitabnya *Syarh al-Qawa'id al-Fiqhiyyah*, kaidah fiqh "al-dhâraru yuzâlu" menunjukkan bahwa menghilangkan kemudaratan adalah wajib.[10]

Menghilangkan kemudaratan harus terus diupayakan walaupun tidak seluruhnya hilang, maka hal ini bersesuaian dengan kaidah fikih:

اَلضَّرَرُ يُدْفَعُ عَلَى قَدرِ الْإِمْكَانِ

"Kemudaratan dihilangkan semaksimal mungkin meskipun tidak seluruhnya hilang".[11]

---

[9] Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah* (Banjarmasin, LKPD, 2015) hlm. 109.

[10] Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008) hlm. 215.

[11] A.Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis* (Jakarta: Kencana, 2007). Hlm. 73.