"Jurnal Pilar Keadilan"
Prodi Magister Ilmu Hukum – Sekolah Tinggi Ilmu Hukum Painan

KEBIJAKAN HUKUM PIDANA SEBAGAI REGULASI DALAM PENANGGULANGAN CYBER CRIME DI INDONESIA

Oleh :

Maya Sri Novita
Universitas Sultan Ageng Tirtayasa, Banten.
Email : mayasrinovita11@gmail.com

ABSTRAK

Globalisasi teknologi informasi telah membawa dunia memasuki era dunia maya, dimana fasilitas Internet menghadirkan dunia maya dengan realitas virtualnya dan menawarkan berbagai harapan dan peluang kepada masyarakat. Namun terdapat permasalahan berupa kejahatan yang disebut cybercrime. Kejahatan ini tidak mengenal batas negara (no borders) maupun waktu, karena seringkali korban dan pelaku berada di negara yang berbeda. Kejahatan dunia maya dapat dilakukan melalui sistem jaringan komputer yang sama sebagai target dan komputer itu sendiri sebagai sarana untuk melakukan kejahatan. Pesatnya perkembangan teknologi informasi harus diperhitungkan dengan peraturan perundang-undangan yang mengaturnya. Dampak negatif tersebut harus diantisipasi dan diatasi melalui pengaturan hukum penggunaan teknologi informasi dan komunikasi. Berdasarkan permasalahan tersebut maka dilakukan penelitian mengenai kebijakan kriminal untuk memberantas kejahatan siber di Indonesia. Tujuan dari penelitian ini adalah untuk memahami kebijakan hukum pidana berdasarkan KUHP untuk memberantas kejahatan siber di Indonesia dan mempelajari kebijakan hukum pidana berdasarkan UU ITE untuk memberantas kejahatan siber di Indonesia. Pendekatan sentral dalam penelitian ini bersifat hukum normatif, karena pembahasannya didasarkan pada peraturan hukum dan asas-asas hukum yang berlaku pada topik cybercrime. Pendekatan hukum bertujuan untuk melakukan penelitian di bidang hukum khususnya hukum pidana. Upaya penegakan hukum tidak hanya sebatas peningkatan kapasitas, sarana dan prasarana penegakan hukum, namun juga dibarengi dengan kesadaran masyarakat terhadap hukum yang didukung dengan kerjasama dengan penyedia layanan Internet.

Kata Kunci : Kebijakan Hukum Pidana, Penanggulangan, Cyber Crime

PENDAHULUAN

Kebijakan pidana adalah kebijakan negara melalui badan-badan yang berwenang, yang ditujukan untuk melaksanakan ketentuan-ketentuan yang diinginkan yang dimaksudkan untuk mengungkapkan apa yang terkandung dalam masyarakat dan mencapai tujuan yang telah ditetapkan. Upaya dan upaya mewujudkan hukum pidana yang baik pada umumnya tidak dapat dilepaskan dari tujuan pencegahan kejahatan. Kebijakan penal dengan demikian juga mencakup kebijakan atau kebijakan hukum pidana. Dari sudut pandang hukum pidana, kebijakan penal identik dengan "kebijakan pencegahan kejahatan dengan hukum pidana". Pemberantasan kejahatan melalui hukum pidana biasanya merupakan bagian dari penegakan hukum. Kebijakan yang bersifat menghukum merupakan bagian dari kebijakan yang represif. Penggunaan cara-cara hukum, termasuk hukum pidana, untuk menyelesaikan permasalahan sosial merupakan kebijakan yang represif. Selain itu, kebijakan sosial ditujukan untuk mencapai kebaikan masyarakat secara keseluruhan dan juga mencakup kebijakan represif, yaitu segala upaya rasional yang bertujuan untuk mencapai kebaikan masyarakat. Dalam kaitannya dengan kebijakan peradilan pidana, salah satu dimensi kehidupan masyarakat saat ini yang memerlukan kebijakan peradilan pidana adalah dampak dari teknologi informasi yang berkembang sangat pesat dan menyebabkan banyak perubahan pada aspek kehidupan sosial masyarakat, baik ekonomi maupun sosial. rasa hormat politik. Sistem komunikasi dan interaksi, pendidikan, termasuk hukum. Teknologi informasi atau internet pada awalnya dikembangkan secara eksklusif untuk memungkinkan masyarakat dapat hidup normal.

1. Teknologi informasi diyakini membawa manfaat yang sangat besar bagi negara- negara di dunia.

2. Telah muncul sistem hukum baru yang disebut cyber law, istilah hukum yang berkaitan dengan penggunaan teknologi informasi. Istilah lain yang digunakan adalah hukum teknologi informasi dan hukum dunia maya. Istilah-istilah ini berasal dari aktivitas internet dan keunggulan teknologi informasi di pasar

virtual. Istilah "Hukum Siber" yang digunakan dalam artikel ini didasarkan pada asumsi bahwa jika diidentikkan dengan "Dunia Siber", Siber akan mempunyai masalah yang cukup besar ketika diperlukan pembuktian suatu masalah yang dapat disebut sebagai "virtual". Jadi tak kasat mata dan tak kasat mata itu semu.

3. Pergeseran paradigma ini juga diiringi dengan perubahan cara pandang perspektif baru yang dipermasalahkan adalah dokumentasi, yang awalnya berbentuk kertas dan kemudian menjadi elektronik. Hal ini menjadi jelas ketika melakukan perdagangan melalui pasar online (Internet). Dalam transaksi ini Anda akan melihat bahwa semuanya dilakukan secara elektronik seperti: tanda tangan digital, email. Teknologi informasi mempunyai dampak terhadap masyarakat secara keseluruhan, baik positif maupun negatif. Dampak positifnya adalah dapat diperolehnya berbagai informasi dalam dan luar negeri untuk transaksi jarak jauh. Sedangkan dampak negatifnya adalah membuka peluang terjadinya berbagai kejahatan seperti penipuan, pencurian, pencemaran nama baik, amoralitas, perjudian, pengancaman, pengrusakan, dan terorisme yang semuanya disebut sebagai kejahatan siber (cybercrime). Cybercrime adalah kejahatan yang dilakukan oleh seseorang, sekelompok orang, dan suatu perusahaan (badan hukum) dengan menggunakan atau menyasar suatu komputer, sistem komputer, atau jaringan komputer. Kejahatan ini terjadi di dunia maya (virtual) sehingga memiliki karakteristik yang berbeda dengan kejahatan tradisional. Hasil berbagai penelitian menunjukkan bahwa karakteristik penjahat dunia maya benar- benar unik dan termasuk dalam kategori yang berbeda dibandingkan penjahat lainnya. Meskipun hukum pidana konvensional yang berlaku di Indonesia dapat digunakan oleh hakim sebagai landasan hukum untuk mengadili pelaku kejahatan siber, namun dalam praktiknya hukum tersebut mempunyai banyak keterbatasan, baik dari segi unsur pidananya maupun pertanggungjawaban pidananya. Akibatnya, banyak penjahat yang lolos dari hukum. Berdasarkan hasil penelitian yang dilakukan Widodo dalam "Sistem Penalti dalam Kejahatan Dunia Maya", seluruh pelaku divonis penjara. Ditinjau dari segi

filosofis, teoritis, normatif, dan empiris, pidana penjara merupakan salah satu jenis pemidanaan yang mempunyai banyak kelemahan, karena penerapan pidana penjara belum memadai khususnya di Indonesia. Kejahatan baru ini berdampak besar pada dunia bisnis. Banyak yang percaya bahwa hukum pidana tidak dapat mencakup kejahatan-kejahatan baru ini, itulah sebabnya pemerintah mulai membuat undang-undang kejahatan dunia maya. Berdasarkan dokumen yang ada, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) adalah Undang-Undang Nomor 19 Tahun 2016, perubahan atas Undang-Undang Nomor 11 Tahun 2008. Menurut Widodo, menjatuhkan hukuman penjara kepada pelaku kejahatan siber merupakan tindakan yang tidak bijaksana. Hal ini disebabkan adanya kesenjangan antara karakteristik pelanggar dengan sistem pembinaan narapidana di lembaga pemasyarakatan sehingga menyebabkan tidak tercapainya tujuan pemidanaan yang ditetapkan dalam UU Pemasyarakatan. Menurut Widodo, pidana pelayanan sosial atau tindak pidana pengawasan bisa menggantikan hukuman tersebut. Karena karakteristik pelaku kejahatan dunia maya konsisten dengan paradigm pemidanaan untuk kejahatan yang berkaitan dengan pekerjaan sosial atau pengawasan, maka tujuan pemidanaan dapat tercapai. Sejalan dengan pandangan Widodo, rancangan undang- undang KUHP tentang Kejahatan Dunia Maya (RUU KUHP) bertujuan untuk memperluas cakupan konsep untuk dapat mendeteksi dan mencatat kejahatan tersebut. Sementara itu, menurut Barda Nawawi Arief, dari sudut pandang hukum pidana, upaya pemberantasan cybercrime dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (rumusan pidana), aspek pertanggungjawaban atau sanksi pidana (termasuk aspek pembuktian) dan aspek kompetensi. Sehubungan dengan itu, rumusan pidana dalam KUHP masih bersifat konvensional dan tidak berkaitan langsung dengan perkembangan cybercrime. Selain itu, mempunyai berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan kejahatan teknologi tinggi yang sangat beragam. Misalnya untuk mengatasi permasalahan penipuan kartu kredit dan transfer dana elektronik, tidak ada ketentuan khusus dalam KUHP mengenai pembuatan kartu kredit,

hanya ketentuan mengenai pernyataan palsu tercantum dalam Bab IX Pasal 242 KUHP, pemalsuan uang logam dan uang kertas berdasarkan Bab X Pasal 244- 252 KUHP, tentang pemalsuan pada Bab XI Pasal 253-262 KUHP, pemalsuan surat pada Bab XII Pasal 263-276 KUHP. 8 Indonesia berupaya mengupayakan harmonisasi kebijakan dengan negara lain, khususnya di lingkungan Asia dan ASEAN, dalam isu kejahatan siber. Permasalahan cybercrime tidak hanya diantisipasi melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun juga upaya antisipasinya dalam kerangka kerja RUU KUHP. Dalam Buku I RUU KUHP Indonesia pada Pasal 174 dalam Ketentuan Umum, disebutkan tentang pengertian "barang", yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon,telekomunukasi, atau jasa komputer. Adapun redaksi teks Pasal 174 sebagai berikut: "Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasatelepon, jasa telekomunikasi, atau Pidana kerja sosial dan pidana pengawasan termasuk jenis-jenis pemidanaan yang tercantum dalam RUU KUHP Tahun 2007 pada Pasal 65 ayat 1. Dalam Buku I RUU KUHP Indonesia Pasal 188 juga dicantumkan tentang pengertian "surat", mencakup data tertulis atau tersimpan dalam disket, pita magnetik, media penyimpan komputer atau penyimpan data elektronik lainnya. Dalam pasal tersebut dinyatakan: "Surat adalah selain surat yang tertulis di atas kertas, juga surat atau data yang tertulis atau tersimpan dalam disket, pita magnetik, atau media penyimpan komputer atau media penyimpan data elektronik lain". Pengertian "surat" menggambarkan makna materi (tertulis) dan tidak berwujud (virtual) dari sebuah surat. Yang dimaksud dengan surat tidak berwujud dapat berupa email, pesan chat/buku tamu, komentar tertulis pada suatu website dalam bentuk aplikasi, short message service (SMS) atau WhatsApp (WA) termasuk software. Berdasarkan 2 (dua) pasal tersebut dapat menjadi contoh bagaimana cybercrime dilihat dari perspektif KUHP. Tujuannya untuk mencegah dan mengurangi kejahatan di dunia maya. Selain itu, pelaku kejahatan yang berkaitan dengan kemajuan teknologi dapat dimintai

pertanggungjawaban berdasarkan undang-undang ini. Aspek utama aktivitasnya adalah kejahatan dunia maya, dengan penekanan pada penyerangan terhadap konten, sistem komputer, dan sistem komunikasi orang lain, baik secara pribadi maupun di dunia maya secara umum. Untuk alasan ini, Anda perlu melindungi sistem Anda dari kerusakan. Pemberantasan kejahatan dunia maya dilakukan melalui pencegahan dan penerapan hukum dengan tujuan menjamin supremasi hukum. Jika dibiarkan, hal itu dapat membahayakan keamanan nasional dan internasional. Faktanya, kejahatan dunia maya telah mengancam keamanan nasional dan luar negeri, dan penegak hukum harus mengambil langkah - langkah strategis untuk mengatasinya. Kejahatan dunia maya terjadi karena lemahnya kontrol pribadi dan kontrol sosial. Padahal, kejahatan ini bersifat virtual, dimana pelakunya tidak terlihat secara fisik. Dalam pendekatan regulasi, kejahatan dunia maya merupakan kejahatan tradisional, namun juga mencakup bentuk-bentuk baru seperti pornografi, penipuan, pencemaran nama baik, dan lain- lain, yang menggunakan media online sebagai sarana untuk melakukan kejahatan dan oleh Cyber crime bersifat nyata (real) tetapi maya (virtual) adalah kenyataan suatu peristiwa hukum yang terjadi dalam ruang maya (cyber space) atau internet. Secara yuridis aktivitas tersebut tidak dapat dideteksi dengan ukuran dan kualifikasi hukum konvensional, karena apabila cara ini yang ditempuh akan banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Oleh karena itu, hal ini perlu dilengkapi fasilitas aturan hukum yang serupa dan sepadan. Seperti halnya Undang-Undang RI Nomor 11 Tahun 2008 tentang ITE yang mencoba menjangkau ruang maya tersebut. karena itu dapat dihukum berdasarkan KUHP, sedangkan kejahatan komputer jenis baru, seperti pembajakan komputer tidak tunduk pada ketentuan apa pun dalam KUHP. Hal ini menimbulkan kekosongan hukum (rechts vacuum). Diakui bahwa dengan berlakunya Undang-Undang Republik Indonesia Nomor 19 Tahun 2016, perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dapat memberantas jenis kejahatan yang mencakup perkembangan kejahatan tentang media Online. Selain itu, undang-undang ini

juga diharapkan dapat memberikan jawaban konkrit terhadap permasalahan penegakan hukum. Berdasarkan penjelasan yang telah diuraikan di atas, penulis ingin mengkaji dan menganalisa mengenai kebijakan hukum pidana dalam penanggulangan cyber crime di Indonesia.

METODE PENELITIAN

Penelitian normatif dalam bidang hukum digunakan, yang menganalisis permasalahan berdasarkan peraturan perundang-undangan yang berlaku, serta literatur yang berhubungan dengan permasalahan yang dibahas. Oleh karena penelitian ini merupakan penelitian hukum normatif yang menitikberatkan pada data sekunder, maka pengumpulan data primer dilakukan melalui penelitian kepustakaan dan kajian dokumen-dokumen yang berkaitan dengan topik yang diteliti.

PEMBAHASAN

1. Kasus cyber crime di Indonesia

a. Defacing

Situs milik KPU (Komisi Pemilihan Umum) Defacing oleh hacker. Peristiwa tersebut terjadi pada tanggal 17 April 2004 dengan target situs http://tnp.kpu.go.id.Lambang 24 partai tersebut diganti dengan nama lucu "Pesta Jambu Biji", "Pesta Cucak Rowo", "Pesta Warna Ijo" dan lain-lain. Pelakunya adalah Dani Firmansyah, mahasiswi berusia 24 tahun asal Yogyakarta yang kemudian ditangkap Polda Metro Jaya. Motivasi penulis hanya ingin menguji sistem keamanan server KPU yang dibelinya dengan harga mahal dan tahan terhadap serangan hacker, ujarnya saat itu. Namun ternyata Dani berhasil kabur. 13 Undang-Undang Republik Indonesia No. 19 Tahun 2019 tentang Informasi dan Transaksi Elektronik (ITE) selanjutnya disebut Undang-Undang ITE siber di Indonesia mengakibatkan Dani Firmansyah dijerat pasal UU Telekomunikasi No. 36 Tahun 1999 yang mengatur sanksi pidana terhadap: "Manipulasi akses jaringan telekomunikasi yang mengakibatkan interferensi fisik

dan elektromagnetik dalam penyelenggaraan telekomunikasi". Dani Firmansyah juga didakwa melakukan tindak pidana yang bertentangan dengan 22 huruf a, b, c, Pasal 38 dan Pasal 50 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Pasal 22 UU Telekomunikasi menyatakan: "Setiap orang dilarang melakukan perbuatan yang dilarang atau melawan hukum atau memanipulasi akses jaringan telekomunikasi dan/atau akses terhadap layanan telekomunikasi; dan/atau akses terhadap jaringan telekomunikasi khusus. Sedangkan Pasal 50 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur: "Barangsiapa melanggar ketentuan Pasal. 22 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)."

b. Phising

Kasus klik BCA melibatkan nama domain yang memanfaatkan kesalahan ketik yang mungkin dilakukan pelanggannya. Steven Haryanto membeli 5 domain permainan kata dari landing site www.klikbca.com yaitu www.klikbca.com, kilkbca.com, klikbca.com, klikbca.com, iklikbca.com. Steven Haryanto menyasar nasabah BCA yang salah ketik pada tulisan Klikbca. Beranda permainan kata itu sama persis dengan BCA. Pengguna masuk ke situs phishing ini dan nama pengguna serta PIN online korban dikirimkan ke pemilik situs. Steven Haryanto meminta maaf dan memberikan seluruh user ID dan PIN kepada BCA. Kasus ini tidak dibawa ke pengadilan karena Steven melaporkan bahwa pengamanan BCA masih lemah. Saat itu, BCA mempertimbangkan alternatif lain selain melaporkan Steven ke polisi. Steven Haryanto adalah salah satu contoh ciri-ciri "WHITE HAT HACKER".

c. Pornografi

Larangan melakukan perbuatan yang melanggar kesusilaan diatur dalam Pasal 27 Bab 1 dan dikenakan sanksi pidana sesuai Pasal 45 ayat (1). Pasal 27 ayat (1) angka 1 yang mengatur: Barangsiapa dengan sengaja dan melawan hukum menyebarkan informasi elektronik dan/atau dokumen elektronik dan/atau

mentransmisikan dan/atau menyediakan konten yang bertentangan dengan praktik yang baik. Ancaman pidana terhadap pelaku pelanggaran Pasal 27 ayat (1) diatur dalam Pasal 45 ayat (1) sebagai berikut: Barangsiapa yang memenuhi unsur-unsur sebagaimana diatur dalam Pasal 27 ayat (1), ayat (2), ayat (5), atau ayat (4) diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Awal Juni 2010, publik dihebohkan dengan beredarnya tiga video cabul yang dilakukan tiga artis ibu kota, yakni Nazriel Irham (Ariel), Luna Maya, dan Cut Tari. Dalam keterangannya, Ariel mengatakan ia yakin telah meninggalkan dokumen pribadi yang dimaksudkan untuk penggunaan pribadi. Namun hukum juga harus bertindak. Ariel didakwa berdasarkan pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi dan Informasi Elektronik yang menyatakan: "Barangsiapa dengan sengaja dan melawan hukum menyebarkan nomor dan/atau mentransmisikan dan/atau menyediakan informasi elektronik dan/atau dokumen komputer yang mengandung muatan yang bertentangan dengan kesusilaan". Ariel juga didakwa berdasarkan Pasal 29 UU Pornografi: setiap orang yang memproduksi, menciptakan, memperbanyak, menggandakan, mengedarkan, menyebarkan, mengimpor, mengekspor, menawarkan, menjual, menyewakan, atau untuk tujuan yang dimaksudkan, menyediakan materi pornografi. Majelis hakim Pengadilan Negeri Bandung memvonis Ariel 3,5 tahun

penjara dalam satu dakwaan membuat video tidak senonoh. Actus reus adalah perbuatan yang dapat berupa melakukan perbuatan tertentu yang dilarang oleh undang-undang atau "melakukan" atau "bertindak" atau berdiam diri atau tidak melakukan suatu perbuatan atau "kelalaian" yang ditentukan oleh undang-undang yaitu membungkam tindak pidana Pasal 27 ayat (1) jo. Pasal 45 ayat (1) terdiri dari menyebarkan, mentransmisikan dan/atau membuat dapat diaksesnya "mens rea" (sikap hati) atau unsur bersalah dari delik tersebut. Pelanggaran tersebut melibatkan informasi komputer dan/atau dokumen komputer yang mengandung konten yang melanggar kesusilaan umum.

d. Kasus Pencemaran Nama Baik

Larangan penghinaan dan/atau pencemaran nama baik melalui penggunaan sistem TI diatur dalam Pasal 27 ayat (3) dan dikenai sanksi pidana sesuai Pasal 45 ayat (1). Pasal 27 ayat (3) menyatakan: Setiap orang yang dengan sengaja dan tidak patut menggunakan informasi elektronik dan/atau mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya dokumen elektronik yang mengandung muatan ofensif dan/atau pencemaran nama baik. Ancaman pidana terhadap pelaku pelanggaran Pasal 27 ayat (3) didefinisikan dalam Pasal 45 ayat (1) sebagai berikut: Barangsiapa memenuhi unsur-unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Prita Mulyasari adalah pasien di Rumah Sakit Internasional Omni Alam Sutra Tangerang. Peristiwa itu terjadi saat Prita dirawat di rumah sakit, dimana Prita tidak kunjung sembuh namun penyakitnya semakin parah. Pihak rumah sakit tidak memberikan informasi yang jelas mengenai penyakit Prita atau memberikan catatan medis yang dibutuhkan Prita. Prita Mulyasari kemudian menyampaikan pengaduan terkait pelayanan rumah sakit tersebut melalui email yang kemudian dikirimkan ke milis berbeda di dunia maya. Rumah Sakit Omni Internasional marah dan yakin Pita telah mencemarkan nama baik mereka.RS Omni Internasional telah mengajukan tuntutan pidana terhadap Prita Mulyasari. Prita diangkat berdasarkan UU No. 11 Tahun 2008, Pasal 27 ayat (3) tentang Informasi dan Transaksi Elektronik (UU ITE). Pasal ini menyatakan: "Barangsiapa dengan sengaja dan kasar menyebarkan dan/atau mentransmisikan dan/atau menyediakan informasi elektronik dan/atau dokumen komputer yang mengandung muatan yang menyinggung dan/atau memfitnah." Pasal 27 ayat (3) disebut sebagai pasal karet oleh para ahli hukum dan praktisi TIK. Dua kata kunci dalam artikel ini adalah "TUJUAN" dan "TANPA HUKUM". Menurut banyak ahli. Tersangka tidak bermaksud menghina atau mencemarkan nama baik siapa pun karena ia hanya mengeluhkan pengalamannya. Undang-undang ini juga diatur dalam Undang-Undang Perlindungan Konsumen. Prita berhak mengeluh atas pengalamannya. Karena Prita adalah konsumen, ia dirawat di rumah sakit. Adanya permasalahan

tersebut akan memberikan dampak yang sangat negatif dan membuat masyarakat menjadi takut untuk menyampaikan pendapat, kritik, saran atau komentarnya di dunia maya. Pasal UU ITE ini perlu direvisi, setidaknya belum bisa dijadikan acuan hukum hingga terbitnya PP (Peraturan Pemerintah) dan Keputusan Menteri/Kepmen Kominfo yang merupakan turunan hukumnya.

e. Peretasan Situs Negara

Meretas komputer dan/atau sistem elektronik tidak hanya untuk mendapatkan akses tetapi juga untuk memanipulasi keamanan sistem komputer yang diakses. Larangan dilakukannya undang-undang ini diatur dalam Pasal 30 ayat (3) yang menyatakan: Setiap orang yang dengan sengaja dan tidak patut memperoleh akses terhadap suatu komputer dan/atau sistem elektronik dengan cara apapun dengan cara melanggar, mengabaikan atau melanggar sistem keamanan. Pelanggaran terhadap larangan sesuai Pasal 30 ayat (3) diancam dengan sanksi sesuai Pasal 46 ayat (3) sebagai berikut: Barangsiapa menggabungkan unsur-unsur tersebut dalam Pasal. 30 Ayat 3 diancam dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah). Actus reus dari kejahatan di atas adalah "akses". Mens rea yang dibahas di atas adalah "disengaja". Pokok bahasan actus reus kejahatan ini sesuai dengan pokok bahasan actus reus dalam pengertian Pasal 30 ayat (l) dan ayat (2) atau "komputer dan/atau sistem elektronik". Namun di bagian bawah terdapat logo dan teks putih "Jemberhacker Team". Wildan ditangkap setelah mencemarkan nama baik situs SBY www.presidensby.info. Wildan Yani S (22 tahun), hacker website SBY, lulusan SMK pada tahun 2010. Wildan tidak melanjutkan studi karena alasan keuangan. Wildan bekerja sebagai operator warung internet di Jember.Wildan ditangkap pada 25 Januari dengan ancaman melanggar seni. 50 tahun. Pasal 22(b) UU Telekomunikasi Nomor 36 Tahun 1999. Wildan terancam hukuman maksimal 6 tahun penjara dan/atau denda paling banyak Rp600 juta. Wildan juga dinyatakan bersalah melanggar Pasal 46 Ayat (1), (2), dan (3) jo. Pasal 30 Ayat (1), (2), dan (3) serta Pasal 48 Ayat (1) juncto Pasal 32 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang

Informasi dan Transaksi Elektronik, Wildan terancam hukuman penjara 6 hingga 10 tahun dan denda paling banyak Rp5 miliar. Namun, polisi yakin tujuan Wildan hanyalah mengubah tampilan situs tersebut, tanpa maksud politik apa pun. Bareskrim Polri mencatat Wildan akan dipekerjakan sebagai petugas cybercrime di Mabes Polri. Meski demikian, polisi masih mendalami kasus Wildan. Kasus tersebut saat ini sedang diselesaikan. Penangkapan Wildan memicu reaksi keras dari kelompok hacker internasional terkemuka ANONYMOUS. Mereka meminta Wildan melepaskan diri dari tuntutan apapun karena tindakan Wildan tidak merusak sistem maupun data, namun mereka perlu menginformasikan dan mengingatkan bahwa pengelolaan fasilitas penting milik pemerintah telah gagal menjamin keamanan yang optimal. Jika tuntutan mereka tidak dipenuhi, mereka akan menyatakan "perang" terhadap situs-situs pemerintah Republik Indonesia dan menghancurkannya dengan domain "go.id". Website yang dapat diakses oleh penyandang disabilitas tersebut mencakup beberapa subdomain di website KPPU, BPS, KBRI Tashkent, Kementerian Hukum dan Hak Asasi Manusia, Kementerian Sosial dan Kementerian Pariwisata dan Industri Kreatif, bahkan Indonesia.go.id.

2. Kebijakan cyber crime melalui pendekatan KUHP

Hukum pidana adalah bagian dari hukum umum yang berlaku di suatu negara tertentu, yang menetapkan dasar dan aturan mengenai perbuatan apa yang tidak boleh dilakukan dan kapan serta dalam hal apa orang yang melanggar larangan tersebut dapat dihukum atau dihukum 15 Arifiyadi Teguh. 2008. Menjerat Pelaku Cyber Crime dengan KUHP. Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 27 september 2019 dari www. depkominfo.go.id dengan sanksi pidana yang diberikan. Ancaman menentukan bagaimana suatu kejahatan dapat dilakukan jika ada yang diduga melanggarnya. Tindak pidana juga mencakup kejahatan yang didefinisikan sebagai berikut: "perbuatan yang dilarang oleh suatu larangan yang sah dan disertai ancaman (sanksi) berupa sanksi khusus terhadap siapa saja yang melanggar larangan tersebut".

Saat ini Indonesia telah memiliki undang-undang untuk mengatur kejahatan siber. RUU tersebut telah ada sejak tahun 2000, dan perubahan terakhir UU Cybercrime pada tahun 2016 disampaikan oleh Kementerian Komunikasi dan Informatika kepada Sekretariat Negara RI dan diteruskan ke DPR, namun dikirim kembali ke Kementerian Komunikasi dan Informatika untuk koreksi. Kitab Undang-undang Hukum Pidana (KUHP) merupakan hukum nasional yang menjadi sumber hukum dan kerangka hukum dalam menindak berbagai jenis kejahatan yang dilakukan di Indonesia. Dalam kaitannya dengan persoalan cybercrime, peraturan perundang- undangan dalam KUHP Nasional dapat dibagi menjadi dua bagian, yaitu peraturan perundang- undangan yang bersifat umum/tidak langsung dan peraturan perundang-undangan yang bersifat khusus/langsung. Regulasi langsung mengacu pada regulasi eksplisit atas pelanggaran yang berkaitan dengan kejahatan dunia maya. Arahan kriminalisasi cybercrime yang tertuang dalam rancangan Undang-Undang Penggunaan Teknologi Informasi (RUU-PTI) terdapat pada Bab XIV yang berjudul "Ketentuan Sanksi" pasal 35-40. Undang-Undang tentang Penggunaan Teknologi Informasi (RUU-PTI) pada umumnya memuat kata-kata delik seperti yang terdapat dalam Konvensi Dewan Eropa tentang Kejahatan Komputer 2001 (Council of Europe Convention on Computer Crime), yaitu:

Pasal 35: • Mengunggah Frasa Terlarang Terkait "Penggunaan Nama Domain yang Bertentangan dengan Hak Kekayaan Intelektual Orang Lain";

• Dalam Konvensi Cyber Crime, delik serupa ini termasuk "infringement ofcopyright".

Pasal 36: • Berisi kata-kata pelanggaran yang berkaitan dengan "penggunaan data komputer/sarana elektronik lainnya secara tidak sah";

• Dalam Konvensi Cyber Crime, delik ini disebut dengan istilah "illegalaccess".

Pasal 37: • Ayat (1) memuat ketentuan melawan hukum yang berkaitan dengan "interupsi atau penyadapan yang melanggar hukum terhadap transmisi data melalui komputer/alat elektronik lainnya"; dan Ayat (2) memuat susunan kata

delik yang berkaitan dengan perbuatan. "secara melawan hukum menyadap transmisi data pada komputer/media elektronik dan mencegah komunikasi dalam sistem komputer/jaringan komputer/sistem komunikasi lainnya";

• Dalam Konvensi Cyber Crime, delik dalam Pasal 37 di atas, disebut "illegal interception" untuk ayat (1) dan termasuk "interference system" untuk ayat (2).

Pasal 38: • Ayat (1) memuat bunyi delik "perampasan, pengubahan, penambahan, penghapusan atau pemusnahan secara melawan hukum atas data komputer/program komputer/data elektronik lainnya". Kejahatan sebagaimana dimaksud dalam ayat (1) menjadi lebih serius jika "mengakibatkan kerugian finansial bagi orang lain" yang tertuang di ayat (2) dan "menyebabkan gangguan terhadap pengoperasian sistem komputer atau sistem multimedia elektronik lainnya pada ayat (3); • Dalam Konvensi Cyber Crime, delik dalam ayat (1) dan ayat (2) tergolong "data interference" dan ayat (3) termasuk "system interference".

Pasal 39: • Berisi kata-kata delik yang berkaitan dengan penggunaan secara tidak sah kartu kredit/alat pembayaran elektronik lainnya milik orang lain sebagai bagian dari suatu transaksi elektronik.

• Delik ini dalam Konvensi Cyber Crime termasuk "computer related offences", khususnya "computer related fraud".

Pasal 40: • Ayat (1) memuat ketentuan mengenai perbuatan "membuat, menyebarluaskan, mentransmisikan, menyebarluaskan data/catatan/gambar/rekaman yang isinya melanggar kelaziman yang baik melalui penggunaan komputer/media elektronik lainnya". Pelanggaran sebagaimana dimaksud dalam ayat (1) diperberat dengan pidana sebagaimana dimaksud dalam ayat (2) apabila pelanggaran tersebut melibatkan anak di bawah umur. • Dalam Konvensi Cyber Crime, hanya disebutkan adanya "child pornography" seperti pada ayat (2) di atas. Tindak pidana di atas diancam dengan pidana penjara (maksimumnya berkisar antara 1 (satu) sampai dengan 5 (lima) tahun dan/atau pidana denda (maksimumnya berkisar antara Rp.

100.000.000,00 (seratus juta rupiah) sampai dengan Rp. 500.000.000,00 (lima ratus juta rupiah). Dalam memproses kasus-kasus yang ada, khususnya terkait cybercrime, penyidik (khususnya kepolisian) menggunakan analogi atau perumpamaan dan kemiripan dengan pasal- pasal KUHP, antara lain:

a. KUHP (Kitab Undang-Undang Hukum Pidana), pasal-pasal yang terkait:

1. Pasal 362 KUHP tentang pencurian (Kasus carding) Carding sendiridalam versi

Polri meliputi:

a) Mendapatkan nomor kartu kredit dari tamu hotel, khususnya orang asing;

b) Mendapatkan nomor kartu kredit melalui kegiatan chatting di Internet;

c) Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet;

d) Mengambil dan memanipulasi data di Internet;

e) Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman;

f) Carding (pelakunya biasa disebut carder), adalah melakukan transaksi

perdagangan elektronik menggunakan nomor kartu kredit yang dipalsukan atau

dicuri. Penyerang tidak perlu mencuri atau memalsukan kartu kredit secara fisik,

mereka hanya perlu mengetahui nomor kartu dan tanggal kedaluwarsa;

g) Pasal 378 KUHP tentang Penipuan (Penipuan melalui website seolah-olah

menjual barang);

h) Pasal 311 KUHP Pencemaran nama Baik (melalui media internet dengan mengirim

email kepada Korban maupun teman-teman korban);

i) Pasal 303 KUHP Perjudian (permainan judi online);

j) Pasal 282 KUHP Pornografi (Penyebaran pornografi melalui media internet).

2. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software

3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomukasi, (penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi).

4. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-Undang No.15 Tahun 2002 tentang Pencucian Uang.

5. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme. Untuk memerangi kejahatan dunia maya, perlu mengambil beberapa langkah penting, yaitu: a. Melaksanakan modernisasi hukum pidana dan acara nasional sesuai dengan konvensi internasional mengenai kejahatan tersebut.

b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

c. Meningkatkan pemahaman dan keahlian penegak hukum dalam mencegah, menyelidiki, dan menuntut kasus kejahatan dunia maya.

d. Meningkatkan kesadaran masyarakat mengenai masalah kejahatan dunia maya dan pentingnya mencegah terjadinya kejahatan dunia maya.

e. Memperkuat kerja sama bilateral, regional, dan multilateral antar negara dalam memerangi kejahatan dunia maya, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan hukum timbal balik.

3. Kebijakan cyber crime melalui pendekatan UU ITE

Kejahatan merupakan fenomena yang selalu menjadi bagian dari dinamika perkembangan peradaban manusia. Kejahatan yang digambarkan oleh Saparinah Sadli sebagai penyimpangan selalu ada dan melekat pada semua lapisan

masyarakat; Tidak ada masyarakat yang kebal terhadap kejahatan. Oleh karena itu, upaya pencegahan kejahatan sebenarnya merupakan upaya yang berkelanjutan dan berkesinambungan. Dengan kemajuan peradaban manusia, sebagai konsekuensi dari berkembangnya ilmu pengetahuan dan teknologi, bermunculan berbagai jenis kejahatan dengan dimensi baru, termasuk cybercrime. Oleh karena itu, tindakan penanggulangan diperlukan untuk menjamin ketertiban dalam masyarakat. Secara hukum, upaya ini dilaksanakan melalui hukum pidana. KUHP harusnya mampu menjamin ketertiban umum. Namun seiring berkembangnya masyarakat, hukum pidana tidak selalu mampu memerangi dampak negatif kejahatan. Hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang sangat cepat, sedangkan hukum pidana merupakan produk sejarah tertentu yang berfungsi menurut logika sejarah yang mendasarinya, meskipun dengan tingkat prediktabilitas tertentu dalam kaitannya dengan perkembangan masyarakat. Dua isi utama UU ITE menyangkut pengaturan transaksi elektronik dan kejahatan dunia maya. Isi UU ITE merupakan implementasi beberapa prinsip hukum internasional. UU ITE mencakup perbuatan-perbuatan yang dilarang oleh Pasal 27 sampai Pasal 36. Pasal 42 UU ITE juga mengatur ketentuan mengenai penyidikan, yang menyatakan: "Penyidikan berdasarkan Undang-undang ini dilakukan berdasarkan ketentuan KUHAP dan Peraturan Undang-Undang." Oleh karena itu, sistem pembuktian yang digunakan adalah sistem/teori pembuktian negatif yang berdasarkan hukum, yaitu sistem yang dianut dalam KUHAP dan berdasarkan Pasal 183 KUHAP, yang menyatakan: "Hakim dapat melakukan tindak pidana terhadap seseorang hanya jika terdapat paling sedikit dua unsur penting yang menjamin bahwa kejahatan itu benar-benar terjadi dan bahwa terdakwa bersalah." Artinya pembuktian harus berdasarkan ketentuan hukum, yaitu terhadap pembuktian yang sah menurut pengertian Pasal 184 KUHAP, disertai kepastian hakim atas pembuktian itu. Berikut beberapa bukti yang diatur dalam Pasal 184 KUHAP sebagai acuan untuk membuktikan kejahatan komputer, yaitu:

a. Syarat formil keterangan saksi yang diatur dalam KUHAP antara lain keterangan di persidangan dan sumpah atau janji di hadapan keterangan saksi. Syarat materiil seorang saksi untuk memberikan kesaksian saat ini antara lain:

1) Pernyataan tersebut mengenai fakta-fakta yang didengar, dilihat, dan dialaminya sendiri serta membenarkan pengetahuannya

2) Bukan pendapat, rekaan, maupun keterangan ahli

3) Ada lebih dari satu orang saksi yang sesuai asas unus testis nullus testis bukan keterangan yang dia peroleh dari orang lain (testimonium de auditu)

4) Adanya konsistensi antara keterangan saksi yang satu dengan keterangan saksi yang lain, serta antara keterangan saksi yang satu dengan alat bukti yang lain

5) Dalam kejahatan dunia maya, karena sifatnya yang virtual, tidak mungkin memperoleh bukti secara langsung berdasarkan keterangan saksi. Kesaksian seorang saksi hanya dapat berupa hasil percakapan atau sekedar mendengarkan orang lain. Pernyataan ini disebut testimonium de auditum atau bukti desas-desus. Sekalipun kesaksian semacam ini tidak dapat diterima sebagai alat bukti, namun dalam praktiknya tetap dapat menjadi bahan refleksi bagi hakim untuk memperkuat keyakinannya sebelum mengambil keputusan. Kemungkinan penggunaan testimoni muncul dari hasil interaksi di dunia cyber, seperti: Obrolan dan email antar pengguna Internet, atau bisa juga berdasarkan kesaksian administrator sistem komputer bersertifikat.

b. Pasal 186 KUHAP mengatur tentang syarat formal laporan, yaitu pendapat ahli adalah apa yang dijelaskan oleh ahli di pengadilan. Para ahli tersebut disebut ahli patologi forensic dan ahli lainnya. Penggunaan kesaksian ahli menjadi penting ketika jaksa menyajikan bukti elektronik untuk membuktikan kesalahan penjahat dunia maya. Tugas ahli dalam hal ini adalah menjelaskan di persidangan bahwa dokumen/data elektronik yang diserahkan adalah sah dan dapat dipertanggungjawabkan secara hukum.

c. Alat bukti surat (Pasal 184 huruf c dan Pasal 187 KUHAP)

Surat yang diterima sebagai alat bukti adalah surat yang disampaikan di bawah sumpah jabatan atau dengan sumpah sesuai dengan Pasal 187 KUHAP. "Surat" dalam kasus kejahatan dunia maya tidak lagi tertulis, melainkan tidak tertulis dan tersedia di Internet. Ada dua kategori bukti komputer bersertifikat. Pertama, jika sistem komputer telah tersertifikasi oleh lembaga resmi, maka dapat dipastikan bahwa hasil cetakan computer tersebut adalah asli. Misalnya saja kwitansi yang diterbitkan bank untuk transaksi ATM. Bukti ini akan mempunyai nilai pembuktian meskipun informasi lebih lanjut diperlukan selama persidangan. Kedua, sertifikat yang diterbitkan oleh lembaga yang disetujui dapat dianggap sebagai bukti dokumenter karena dibuat dan/atau disetujui oleh pejabat yang berwenang. Jenis bukti dokumenter lainnya dapat mencakup bukti elektronik, yang dapat dicetak, yang dapat dilihat pada layar jaringan komputer. Sepanjang kedua alat bukti tersebut dikeluarkan/dibuat oleh pihak yang berwenang dalam sistem jaringan computer tersebut dapat dipercaya, maka surat tersebut mempunyai nilai pembuktian yang sama dengan alat bukti surat berdasarkan KUHAP.

d. Pembuktian informasi (Pasal 184 Ayat 1 Huruf d dan Pasal 188 KUHAP) mengatur sumber informasi hanya sebatas tertentu, yaitu keterangan hanya dapat diperoleh berdasarkan keterangan saksi, surat, dan keterangan sah terdakwa. Agar ketiga alat bukti tersebut dapat dijadikan petunjuk, maka harus sahih, sehingga petunjuk yang dihasilkan juga sahih. Dalam kasus kejahatan dunia maya, akan sulit mengumpulkan bukti fisik. Cara termudah untuk mengumpulkan bukti adalah dengan mencari tanda-tanda niat jahat dalam bentuk akses tidak sah. Misalnya melihat dan mendengarkan keterangan saksi pengadilan, email atau print out data, serta keterangan terdakwa di pengadilan.

e. Keterangan terdakwa (Pasal 184 huruf e dan Pasal 189 KUHAP) adalah keterangan terdakwa di persidangan tentang perbuatan yang dilakukannya yang diketahui atau dialaminya sendiri. Agar keterangan tergugat dianggap sah, harus dipenuhi syarat formil, yaitu dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik Pasal 5 ayat 1 dan 2 menjelaskan

bahwa dokumen dan informasi elektronik merupakan alat bukti yang sah. Selanjutnya, Pasal 44 Undang-Undang yang sama menyatakan: "Pembuktian untuk keperluan penyidikan, persidangan, dan persidangan menurut ketentuan Undang-undang ini adalah sebagai berikut":

1) alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan.

2) alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik

sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). Informasi dan dokumen elektronik mungkin merupakan alat bukti yang sah menurut UU Teknologi Informasi dan Perdagangan Elektronik, namun sulit untuk menganggapnya sebagai alat bukti yang sah menurut Pasal 184 ayat (1) KUHAP. Informasi elektronik dan/atau dokumen elektronik dianggap sah apabila menggunakan sistem elektronik sesuai dengan ketentuan UU ITE.

KESIMPULAN

Pedoman hukum pidana berdasarkan pendekatan KUHP dalam pemberantasan

kejahatan siber di Indonesia masih mengandung ketentuan yang tumpang tindih dan belum sepenuhnya tercermin dalam produk KUHP. Ada banyak persamaan terkait dengan penangkapan hukum tersangka kejahatan dunia maya, seperti kasus berkas yang terkait dengan pasal pencurian, yaitu Pasal 368 KUHP. Hal serupa juga terjadi pada pendekatan UU ITE yang belum sepenuhnya mengatur berbagai tindak pidana terkait kejahatan siber, sehingga kerangka hukum yang ditetapkan belum ada.

DAFTAR PUSTAKA

Arifiyadi Teguh. 2008. Menjerat Pelaku Cyber Crime dengan KUHP. Pusat DataDepartemen Komunikasi dan Informatika.

Barda Nawawi Arief. 2016. Pembaharuan Hukum Pidana dalam Perspektif Kajian

Perbandingan. Jakarta: Prena Media Group.

Budi Suhariyanto. 2012. Tindak Pidana Teknologi Informasi (Cybercrime). Jakarta: RajaGrafindo Persada.

Hardianto Djanggih, ” Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan”. Jurnal Media Hukum. Vol. 1 No. 2, September 2013.

Kitab Undang-Undang Hukum Pidana (KUHP) Rudi Hermawan, “Kesiapan aparatur pemerintah dalam menghadapi cyber crime di Indonesia”. Jurnal Media Hukum. Vol. 6 No. 1 , 25 September 2019.

Sehatapy, J.E. 2004. Pisau Analisis Kriminologi. Bandung: PT Citra Aditya Bakti.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disebut 17 Sehatapy, J.E. 2004. Pisau Analisis Kriminologi. Bandung: PT Citra Aditya Bakti.

Undang-Undang ITE Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi

Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme Widodo. 2013. “Sistem Pemidanaan dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime”