

ASPEK HUKUM PIDANA TELEMATIKA TERHADAP KEMAJUAN TEKNOLOGI DI ERA INFORMASI

Besse Sugiswati

Fakultas Hukum Universitas Wijaya Kusuma Surabaya
e-mail: kietaw53@yahoo.com

ABSTRAK

Kejahatan di dunia maya adalah persoalan baru dan perbuatan pidana yang berdimensi baru. Undang-Undang Informasi dan Transaksi Elektronik diharapkan bisa memayungi bidang telematika. Namun, Undang-Undang tersebut masih memiliki kendala yuridis dan kendala penanganan tersangka. Banyak ketentuan-ketentuan yang menyangkut perbuatan yang dapat dihukum belum masuk dalam Undang-Undang tersebut.

Kata Kunci: kejahatan dunia maya, telematika, teknologi informasi

ABSTRACT

Crime in cyberspace is a new problem and new dimensions of criminal acts. Information Act and Electronic Transaction is expected to be an umbrella for the field of telematics. However, the Act still has the legal obstacles and constraints handling of suspects. Many of the provisions relating to actions that can be punished yet in the Act.

Keywords: cyber crime, telematics, information technology

PENDAHULUAN

Masyarakat modern cenderung berkembang makin kompleks dan rumit. Pesatnya perkembangan telematika mengakibatkan perubahan demi perubahan juga berlangsung secara cepat dan menjangkau lapisan yang luas dan mendalam. Istilah telematika merupakan adopsi dari bahasa asing. Kata telematika berasal dari kata dalam bahasa Prancis, yaitu *telematique*. Istilah ini pertama kali digunakan pada tahun 1978 oleh Simon Nora dan Alain Minc dalam bukunya yang berjudul *L'informatisation de la Societe* (<http://www.beritanet.com/Technology/Communication/seluk-beluk-telematika.htm>, 2001:1).

Istilah telematika merujuk pada perkembangan konvergensi antara teknologi telekomunikasi, media, dan informatika yang semula masing-masing berkembang secara terpisah. Konvergensi telematika kemudian dipahami sebagai sistem elektronik berbasis digital atau the net (<http://www.law.ui.ac.is/lama/telematika/index.htm>.) Selain itu, mengacu kepada penggunaan di kalangan masyarakat telematika Indonesia (MASTEL), istilah telematika berarti perpaduan atau pembauran (*konvergensi*) antara teknologi informasi (teknologi komputer), teknologi telekomunikasi, termasuk siaran radio maupun televisi dan multimedia (Wawan Wardiana, 2002: 234).

Dalam perkembangannya, teknologi telematika

ini telah menggunakan kecepatan dan jangkauan transmisi energi elektromagnetik, sehingga sejumlah besar informasi dapat ditransmisikan dengan jangkauan, menurut keperluan, sampai seluruh dunia, bahkan ke seluruh angkasa, serta terlaksana dalam sekejap. Kecepatan transmisi elektromagnetik adalah (hampir) 300.000 km/detik, sehingga langsung dikirim begitu sampai, memungkinkan orang berdialog langsung, atau komunikasi interaktif.

Berdasarkan pendapat-pendapat tersebut, maka dapat disarikan pemahaman tentang telematika sebagai berikut (Wawan Wardiana, 2002: 239-240): *Pertama*, Telematika adalah sarana komunikasi jarak jauh melalui media elektromagnetik; *Kedua*, Kemampuannya adalah mentransmisikan sejumlah besar informasi dalam sekejap, dengan jangkauan seluruh dunia, dan dalam berbagai cara, yaitu dengan perantaraan suara (telepon, musik), huruf, gambar dan data atau kombinasi-kombinasinya. Teknologi digital memungkinkan hal tersebut terjadi. *Ketiga*, Jasa telematika ada yang diselenggarakan untuk umum (online, internet), dan ada pula untuk keperluan kelompok tertentu atau dinas khusus (intranet).

Dengan demikian, dapat diambil kesimpulan bahwa telematika merupakan teknologi komunikasi jarak jauh, yang menyampaikan informasi satu arah, maupun timbal balik, dengan sistem digital.

Jika dikaitkan dengan peraturan perundang-undangan yang sudah ada saat ini maka cakupan hukum telematika meliputi Undang-undang Pers (media cetak), Undang-Undang Perfilman (media film), dan Undang-Undang Informasi dan Transaksi Elektronik (media komputer).

Permasalahan yang paling kompleks saat ini mengenai hukum telematika adalah mengenai media komputer atau lebih tepatnya media internet sebagai dunia maya (*cyber space*). Masalah-masalah yang dihadapi pada hukum telematika khususnya masalah *cyber space* sangat luas, karena tidak lagi dibatasi oleh teritori suatu negara, dan dapat diakses kapanpun dimanapun. Salah satu contoh yaitu kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelian di internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit, sehingga perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Hukum dari waktu ke waktu mengalami perkembangan. Sejak jaman Yunani dan Romawi sampai sekarang hukum mengalami perkembangan yang luar biasa yang mungkin saja orang Yunani dan Romawi dahulu tidak akan dapat memperkirakan hal-hal yang terjadi sekarang dalam bidang hukum. Perkembangan ini tidak bisa dilepaskan dari sifat hukum yang selalu berada di tengah-tengah masyarakat sedangkan masyarakat itu sendiri senantiasa mengalami perkembangan.

Dualisme pendapat mengenai bagaimana hukum berkembang memang menjadi perdebatan yang hangat di kalangan praktisi hukum. Ada yang berpendapat bahwa hukum itu berkembang mengikuti perkembangan masyarakat atau sebaliknya masyarakat berkembang karena adanya campur tangan hukum. Jika diikuti jalan pikiran yang pertama maka yang akan dipakai sebagai dasar pijakan adalah ajaran von Savigny mengenai hukum tumbuh, hidup dan berkembang dalam masyarakat dan jika yang dipakai adalah jalan pikiran yang

kedua maka pendekatannya lebih mengarah kepada apa yang telah dikemukakan oleh John Austin yang memandang hukum sebagai perintah dari penguasa yang berdaulat. Austin memisahkan hukum dan keadilan, ini adalah kekeliruan besar karena bagaimanapun inti hukum adalah keadilan. Pemisahan ini tidak didasarkan pada pengertian baik atau buruk akan tetapi didasarkan pada kekuasaan dari sesuatu yang lebih kuat (*the power of a superior*) (W. Friedmann, 1993: 149)

Berdasarkan hal tersebut dapat diketahui bahwa aliran hukum imperatif dari Austin tidak menghendaki hukum yang tumbuh, hidup dan berkembang dalam masyarakatnya sendiri. Hukumnya adalah hukum penguasa yang superior untuk kepentingan penguasa itu sendiri. Apa yang dikemukakan mengenai dualisme pendapat mengenai bagaimana hukum itu berkembang hanyalah merupakan suatu gambaran adanya dua sisi yang berbeda dalam pandangan mengenai hukum yang berangkat dari dua sisi yang berbeda pula.

Cepatnya proses perkembangan telematika, maka untuk menjamin agar proses perubahan yang terjadi dapat dikendalikan secara teratur, sehingga muncul kebutuhan yang makin meningkat untuk membuat aturan demi aturan. Akibatnya, aturan itu tumbuh cepat sekali di semua sektor dan di semua lapisan kehidupan bermasyarakat, berbangsa dan bernegara dan bahkan dalam hubungan antar masyarakat, antar bangsa dan antar negara. Dengan demikian, tepat kiranya bahwa dasar pijakan untuk mengetahui bagaimana hukum berkembang adalah ajaran Von Savigny yang menyatakan hukum tumbuh, hidup dan berkembang dalam masyarakat.

Untuk mengatasi segala kerumitan yang timbul dalam dinamika masyarakat itu sendiri, mau tidak mau, masyarakat membutuhkan segala macam aturan-aturan yang memang dibutuhkan dengan adanya perkembangan jaman. Makin cepat perkembangan telematika itu berlangsung, makin cepat pula berkembangnya tuntutan kebutuhan untuk mengadakan pembaruan terhadap berbagai produk peraturan yang ada. Semakin berkembang telematika, maka makin kompleks pula perkembangan yang terjadi dalam masyarakat, sehingga memicu banyaknya terjadi persengketaan yang perlu diputuskan oleh hakim. Di samping itu, makin kompleks perubahan terjadi dan makin rumit permasalahan yang dihadapi, makin berkembang pula kebutuhan untuk membuat aturan-aturan

guna mengendalikan dinamika perubahan itu. Karena itu, sebagai akibat terjadinya revolusi teknologi komunikasi, media dan informatika dan makin cepatnya dinamika perubahan terjadi, maka makin meningkat pula kecenderungan untuk memproduksi peraturan-peraturan baru, baik dalam bentuk putusan-putusan hakim maupun dalam bentuk peraturan tertulis (peraturan perundang-undangan). Bagaimanakah kendala kebijakan hukum telematika dalam menghadapi pesatnya perkembangan telematika saat ini? Bagaimanakah mengatasi kendala-kendala yuridis yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya ditulis UU ITE) dalam penanganan berbagai bentuk kejahatan dunia maya?

KENDALA KEBIJAKAN HUKUM TELEMATIKA DALAM MENGHADAPI PESATNYA PERKEMBANGAN TELEMATIKA SAAT INI

Teori dari Marc Ancel yang memberikan pengertian bahwa kebijakan hukum merupakan suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif yang dirumuskan secara lebih baik. Peraturan hukum positif di sini diartikan sebagai peraturan perundang-undangan hukum pidana. Karena itu istilah *penal policy* menurut Ancel, sama dengan istilah “kebijakan atau politik hukum pidana” (Barda Nawawi Arief, 1996: 2).

Mengenai kebijakan hukum, ada pula teori lainnya dikemukakan oleh Lilik Mulyadi yang menyatakan bahwa kebijakan hukum hakikatnya merupakan “usaha untuk mewujudkan peraturan perundang-undangan agar sesuai dengan keadaan pada waktu tertentu saat ini (*ius constitutum*) dan masa mendatang (*ius constituendum*)”. Konsekuensi logisnya, kebijakan hukum identik dengan penal reform dalam arti sempit. Sebab, sebagai suatu sistem, hukum terdiri dari budaya (*cultural*), struktur (*structural*), dan substansi (*substantive*) hukum (Lilik Mulyadi, 2009: 1).

Setiap bangsa di dunia mempunyai kebijakan hukumnya sendiri-sendiri yang bisa berbeda dengan hukum bangsa lain. Kebijakan hukum berarti peraturan dan cara atau tata tertib hukum di suatu negara, atau lebih dikenal dengan tatanan berupa tata hukum. Tata hukum atau susunan hukum adalah hukum yang berlaku pada waktu tertentu dalam suatu wilayah negara tertentu yang disebut hukum positif, dalam bahasa latinnya *Ius*

Constitutum lawannya adalah *Ius Constituendum* atau hukum yang dicita-citakan atau hukum yang belum membawa akibat hukum. Dalam kaitannya di Indonesia, yang ditata itu adalah hukum positif yang berlaku di Indonesia. Hukum yang sedang berlaku artinya apabila ketentuan-ketentuan hukum itu dilanggar maka bagi si pelanggar akan dikenakan sanksi yang datangnya dari badan atau lembaga berwenang (http://pojokhukum.blogspot.com/2008/03/ilmu_hukum_sebuahpengantar.html, diakses tanggal 20 November 2009 tulisan Muliadi, Ilmu Hukum)

Mengenai *Ius constituendum*, terdapat tiga hal yakni: *Pertama*, perombakan hukum lama menjadi hukum baru, perubahan-perubahan hukum terhadap hukum yang berlaku dan pembentukan hukum. Mengenai perombakan hukum lama menjadi hukum baru, terjadi ketika hal itu diinginkan oleh seluruh rakyat Indonesia. Misalnya jaman dulu ketika seluruh rakyat menginginkan perombakan dari hukum kolonial menjadi hukum nasional; *Kedua*, perubahan hukum dilakukan dengan selalu meninjau kembali hukum positif atau peraturan perundangan yang diberlakukan yang diharapkan dengan hal ini akan menjadikan hukum lebih dinamis dan tidak berhenti pada satu persoalan kehidupan bangsa dan negara. Dan yang terakhir adalah mengenai pembentukan hukum yang akan terjadi jika para pakar hukum dapat memahami dan mendeskripsikan setepat-tepatnya hukum positifnya sendiri. Melalui suatu penemuan hukum (*rechtsvinding*) hakim dapat juga mewujudkan *ius constituendum*. (Moempoeni Moelatiningsih Maemoenah, 2003: 26).

Hukum mempunyai berbagai fungsi yaitu sebagai sarana pengendalian masyarakat (*a tool of social control*), sarana pemelihara masyarakat (*a tool of social maintenance*), sarana untuk menyelesaikan konflik (*a tool of dispute settlement*), sarana pembaharuan atau alat merekayasa masyarakat (*a tool of social engineering*) (Soetandyo Wignjo soebroto, 1994:234).

Dari fungsi-fungsi hukum tersebutlah pemerintah sebagai penjamin kebijakan hukum dapat menjadi sarana pemanfaatan teknologi yang modern dan aman. Sebagai salah satu bukti nyata dibuatnya kebijakan hukum telematika adalah dibuatnya UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Di Indonesia, persoalan kejahatan dalam hukum telematika atau lebih khususnya mengenai

cybercrime sebenarnya bukan hal baru, akan tetapi aturan untuk mengkriminalisasi pelaku *cybercrime* dengan perangkat aturan khusus berupa *cyberlaw* (UU ITE) adalah persoalan yang baru, karena baru pada tahun 2008 Indonesia benar-benar mempunyai kebijakan hukum khusus dalam persoalan *cybercrime* (Barda Nawawi Arief, 2005: 126 : lihat juga dalam Barda Nawawi Arief, 2006: 90; lihat juga pengertian kriminalisasi dari Sudarto, 1986: 32 dan 151).

Persoalan pemidanaan tersebut timbul karena dihadapan masyarakat terdapat perbuatan yang berdimensi baru, sehingga di masyarakat banyak muncul pertanyaan adakah hukumnya untuk perbuatan tersebut (Tb. Ronny R. Nitibaskara, 2000: 2-5). Kesan yang muncul kemudian adalah terjadinya kekosongan hukum yang akhirnya mendorong kriminalisasi terhadap perbuatan tersebut. Hal tersebut sesuai dengan apa yang dikemukakan oleh von Savigny bahwa hukum tumbuh, hidup dan berkembang karena menyesuaikan kebutuhan masyarakat (W. Friedmann, 1993: 150).

Salah satu kunci agar sistem hukum tidak tertinggal dengan perkembangan telematika yang semakin pesat maka aturan yang dibuat harus bisa holistik, fleksibel dan antisipatif terhadap perubahan zaman. UU ITE mengandung pendekatan *futuristic* karena pada masa yang akan datang teknologi semakin berkembang sehingga hukum harus mengatur tentang perubahan yang ada di masyarakat termasuk perubahan dalam bidang teknologi supaya tercapai kepastian hukum dalam Undang-Undang ITE tercemin kaidah-kaidah bahwa hukum dapat menjangkau perkembangan zaman sehingga Undang-Undang ITE ini bersifat fleksibel sepanjang tidak bertentangan dengan Undang-Undang yang lain (<http://www.scribd.com/doc/24106593/Smtr-Sejarah-Hukum>, tanggal 14 Desember 2009, tulisan Muslim Heri Kiswanto, Cyber crime dan Transaksi Elektronik dalam UU No. 11 Tahun 2008 tentang ITE, h. 15). Akan tetapi walaupun hukum dibuat antisipatif atau preventif dan seholistik mungkin agar dapat memayungi setiap kegiatan khususnya bidang telematika akan tetapi Undang-Undang ITE ini tetap memiliki kendala-kendala antara lain:

KENDALA YURIDIS UNDANG-UNDANG ITE

Undang-Undang ITE tidak mengatur secara khusus hal-hal yang menyangkut *cybercrime*.

Di dalam Bab Ketentuan Umum tidak secara jelas digambarkan tentang penjelasan kejahatan-kejahatan dengan menggunakan komputer. Kejahatan-kejahatan komputer yang dikenal dalam dunia maya tidak tergambar secara jelas. Pemerintah dalam membentuk Undang-Undang ITE ini masih menggunakan pendekatan politis-pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan, sehingga tidak heran kalau UU ITE ini hanya sepotong-sepotong mengatur pemanfaatan teknologi yang sudah begitu luas penggunaannya di berbagai aspek kehidupan manusia. UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapapun tahu bahwa dunia siber (*cyberword*) lebih luas dari sekedar transaksi elektronik.

Banyak ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang ITE seperti hal-hal yang diatur dalam buku I KUHP tidak ada dalam Undang-Undang ITE. Seperti kelalaian atau khilaf, di mana lalai atau khilaf adalah kalimat yang sering dilakukan oleh manusia dalam melakukan kegiatannya. Apabila kelalaian itu dilakukan oleh manusia di dunia nyata dan menimbulkan kerugian bagi dirinya sendiri dan orang lain, diatur secara tersendiri dengan menggunakan pasal-pasal tertentu, bahkan kadang pula si pembuat lalai ini juga akan mendapatkan ancaman hukuman seperti banyak ditemukan kasus-kasus pelanggaran lalu lintas. Namun di dalam dunia maya (*cyberspace*) kelalaian adalah tindakan fatal yang bisa menimbulkan kerugian yang tidak sedikit, bahkan bisa menghancurkan sebuah negara sekalipun. Dalam Undang-Undang ITE tidak menyebutkan sedikitpun tentang kelalaian yang dibuat oleh pembuat situs sehingga hacker bisa masuk dengan leluasa. Kegiatan yang lain yang sama pentingnya dengan kelalaian adalah percobaan melakukan perbuatan jahat dan turut serta melakukan. Dalam Undang-Undang ITE ini tidak diatur apakah percobaan melakukan dan juga turut serta kejahatan *hacking* dapat dipidana atau tidak. Kemudian Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan *hacking*. Semua kegiatan kejahatan tersebut diatur pada Bab tentang perbuatan perbuatan apa saja yang dilarang, sehingga terkesan seperti pasal keranjang sampah, pokoknya semua kegiatan yang melanggar aturan telematika di

Indonesia itulah yang dilarang.

Dari sekian banyak sisi gelap yang ada dalam *cyberspace*, yang paling banyak mendapat perhatian adalah perbuatan yang dilakukan oleh Hacker Hitam (*Cracker*). Pada umumnya reaksi yang diberikan oleh korban *Cracker* adalah merasa kaget, kesal dan terakhir mencela ulah *Cracker* ini. Akibat ulah *Cracker* ini bukan hanya uang yang seharusnya dapat diinvestasikan untuk keperluan lain menjadi terhambat, melainkan keuntungan seperti dijanjikan ketika memasuki *cyberspace* untuk sementara tidak terwujud. Para korban umumnya menganggap serangan *Cracker* ini sebagai sebuah kecelakaan dan mereka tidak mau mempublikasikan atau melaporkan apa yang dideritanya kepada polisi meskipun sebenarnya tahu apa yang dilakukan oleh *Cracker* itu merupakan tindak kejahatan.

Internet sebagai hasil revolusi teknologi memungkinkan transfer data secara cepat dan efisien pada skala global, namun tampaknya sumber daya aparatur belum sepenuhnya menyadari betapa hebatnya teknologi informasi dan komunikasi yang menyebabkan perubahan paradigma dalam kehidupan berbangsa dan bernegara. Ketidamampuan polisi dalam menangani aktivitas *Hacking* juga menjadi sorotan dari para korban *Cracker*. Ketidamampuan ini telah mengubah paradigma teori labeling yang mengasumsikan tindakan penangkapan merupakan proses awal dari labeling. Polisi belum dapat menangkap *Cracker* yang menghack sebuah situs (termasuk ketidakmampuan menangkap *Cracker* yang menyerang situs Polri sendiri) sehingga langkah awal dari proses labeling berupa penangkapan tidak ada. Proses awal dari labeling justru terdapat dari laporan-laporan media massa yang secara gencar memberitahukan aktivitas *Hacking*.

Indonesia menjadi tampak tertinggal dan sedikit terkucilkan di dunia internasional, karena negara lain misalnya Malaysia, Singapura dan Amerika Serikat sudah sejak 10 tahun yang lalu mengembangkan dan menyempurnakan *Cyberlaw* yang mereka miliki. Malaysia punya *Computer Crime Act* (Akta Kejahatan Komputer) 1997, *Communication and Multimedia Act* (Akta Komunikasi dan Multimedia) 1998, dan *Digital Signature Act* (Akta Tandatangan Digital) 1997. Singapura juga sudah punya *The Electronic Act* (Akta Elektronik) 1998, *Electronic Communication Privacy Act* (Akta Privasi Komunikasi Elektronik) 1996. Amerika Serikat intens untuk memerangi *child*

pornography dengan: *US Child Online Protection Act (COPA)*, *US Child Pornography Protection Act*, *US Child Internet Protection Act (CIPA)*, *US New Laws and Rulemaking* (Romi Satria Wahono, Analisa Undang-Undang ITE, diunduh dari <http://romisatriawahono.net/2008/04/24/analisa-uu-ite/>, tanggal 24 Desember 2009).

Lahirnya Undang-Undang ITE ini belum dibarengi oleh peraturan yang mengatur tentang hukum formilnya. Perangkat hukum yang ada di Indonesia belum memadai untuk menjerat kejahatan dunia maya (*cybercrime*) pada umumnya dan kejahatan hacking pada khususnya. Indonesia saat ini pun baru mempunyai sebuah Undang-Undang baru yang mengatur tentang perilaku kegiatan di dunia siber (*cyberspace*), namun Undang-Undang ITE yang ada saat ini masih menggunakan model *umbrella provision* sehingga ketentuan *cybercrime* tidak diatur dalam peraturan perundang-undangan tersendiri, sedangkan peraturan perundang-undangan yang ada sebelum Undang-Undang ITE ini lahir juga ada mengatur tentang kegiatan di dunia siber (I) meskipun itu hanya beberapa pasal saja. Kitab Undang-Undang Hukum Pidana yang dipunyai Indonesia juga harus dilakukan perubahan revolusioner untuk mengatur kegiatan di dunia siber (*cyberspace*) dengan memperluas pengertian-pengertian yang terkait dengan kegiatan-kegiatan di *cyberspace*.

KENDALA PROSES PENANGANAN TER-SANGKA

Kendala yuridis lain terkait dengan pemberrantasan kejahatan dunia maya (*Cyber Crime*) adalah masalah penanganan tersangka. Kendala-kendala tersebut antara lain adalah (Petrus Reinhard Golose, 2006:tanpa halaman); *Pertama*, Penyelidikan, Tahap penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dalam melakukan penyelidikan tindak pidana serta tahap tersulit dalam proses penyidikan. Hal tersebut dikarenakan dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebab-sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Dalam penyelidikan kasus-kasus *cybercrime* yang modusnya seperti kasus *carding*. Metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkoba terutama dalam *undercover* dan *control delivery*. Petugas setelah menerima informasi atau

laporan dari Interpol atau *merchant* yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang (Petrus Reinhard Golose, 2006: tanpa halaman).

Permasalahan yang ada dalam kasus seperti ini adalah laporan yang masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, di samping adanya kerjasama antara *carder* dengan karyawan *shipping* sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu. Untuk kasus *hacking* atau memasuki jaringan komputer orang lain secara ilegal dan melakukan modifikasi (*deface*), penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan SDM serta peralatan komputer forensik yang baik.

Dalam hal kasus-kasus lain seperti situs porno maupun perjudian para pelaku melakukan hosting. Pendaftaran di luar negeri yang memiliki yurisdiksi yang berbeda dengan negara Indonesia, sebab pornografi secara umum dan perjudian bukanlah suatu kejahatan di Amerika dan Eropa walaupun alamat yang digunakan berbahasa Indonesia dan operator website ada di Indonesia sehingga kepolisian tidak dapat melakukan tindakan apapun terhadap mereka sebab website tersebut bersifat universal dan dapat diakses dimana saja. Banyak rumor beredar yang menginformasikan adanya penjabolan bank-bank swasta secara online oleh hacker tetapi korban menutup-nutupi permasalahan tersebut. Hal ini berkaitan dengan kredibilitas bank bersangkutan yang takut apabila kasus ini tersebar akan merusak kepercayaan terhadap bank tersebut oleh masyarakat. Dalam hal ini penyidik tidak dapat bertindak lebih jauh sebab untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan; *Kedua*, Penindakan, Penindakan kasus *cybercrime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kepolisian tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer

yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung.

Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kepolisian tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana. Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor sangat lambat dalam melakukan pelaporan, hal tersebut membuat data serangan di *log server* sudah dihapus biasanya terjadi pada kasus *deface*, sehingga penyidik menemui kesulitan dalam mencari log statistik yang terdapat di dalam server sebab biasanya secara otomatis server menghapus log yang ada untuk mengurangi beban server. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data log statistik merupakan salah satu bukti vital dalam kasus *hacking* untuk menentukan arah datangnya serangan; *Ketiga*, Pemeriksaan, Pemeriksaan terhadap saksi dan korban banyak mengalami hambatan, hal ini disebabkan karena pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (*testimonium de auditu*). Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking*.

Untuk kasus *carding*, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Apakah mungkin nantinya hasil berita acara pemeriksaan (BAP) dari luar negeri yang dibuat oleh kepolisian setempat dapat dijadikan kelengkapan isi berkas perkara atau tidak.

Untuk kasus pornografi, internet sebagai sarana untuk melakukan penghinaan dan pelecehan sangatlah efektif sekali untuk “pembunuhan karakter”. Penyebaran gambar porno atau email yang mendiskreditkan seseorang sangatlah sering sekali terjadi. Permasalahan yang ada adalah, mereka yang menjadi korban jarang sekali mau menjadi saksi karena berbagai alasan. Apabila

hanya berupa tulisan atau foto yang tidak terlalu vulgar penyidik tidak dapat bersikap aktif dengan langsung menangani kasus tersebut melainkan harus menunggu laporan dari mereka yang merasa dirugikan karena kasus tersebut merupakan delik aduan (pencemaran nama baik dan perbuatan tidak menyenangkan).

Peranan saksi ahli sangatlah besar sekali dalam memberikan keterangan pada kasus *cyber crime* sebab apa yang terjadi di dunia maya membutuhkan ketrampilan dan keahlian yang spesifik. Saksi ahli dalam kasus *cyber crime* dapat melibatkan lebih dari satu orang saksi ahli sesuai dengan permasalahan yang dihadapi, misalnya dalam kasus deface, disamping saksi ahli yang menguasai desain grafis juga dibutuhkan saksi ahli yang memahami masalah jaringan serta saksi ahli yang menguasai program; *Keempat*, Penyelesaian berkas perkara, Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena belum samanya persepsi diantara aparat penegak hukum karena penafsiran yang berbeda mengenai isi undang-undang, serta barang bukti digital adalah barang bukti dalam kasus *cyber crime* yang perumusannya dan pengumpulan barang buktinya membutuhkan keahlian khusus sebab digital *evidence* tidak selalu dalam bentuk fisik yang nyata. Misalnya untuk kasus pembunuhan sebuah pisau merupakan barang bukti utama dalam melakukan pembunuhan sedangkan dalam kasus *cyber crime* barang bukti utamanya adalah komputer tetapi komputer tersebut hanya merupakan fisiknya saja sedangkan yang utama adalah data di dalam hard disk komputer tersebut yang berbentuk file, yang apabila dibuat nyata dengan print membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut dalam bentuk *compact disc* saja, hingga saat ini mengenai bentuk dari pada barang bukti digital (*digital evidence*) yang masih membutuhkan penafsiran dari ahli untuk menentukan keabsahannya.

Mengatasi kendala-kendala yang terdapat dalam Undang-Undang ITE dalam penanganan berbagai bentuk kejahatan dunia maya. Upaya revisi Undang-Undang ITE. Redefinisi pengertian dan peristilahan, Untuk menghindari beragam penafsiran perlu dilakukan redefinisi mengenai pengertian atau peristilahan dalam peraturan perundang-undangan ITE, sehingga terdapat batasan dan kejelasan makna serta tidak menimbulkan celah hukum

(*loopholes*), seperti pengertian mengenai: *Pertama*, Membobol sistem keamanan. Sehubungan dengan itu, redefinisi pengertian mengenai dengan sengaja dan tanpa hak menjebol sistem pengamanan dari sebuah sistem elektronik mutlak diperlukan karena untuk mengetahui sejauh mana sebuah produk baru dari sistem elektronik akan dibiarkan produk tersebut dibobol oleh para hacker. Seperti halnya group microsoft meluncurkan produk elektroniknya akan membiarkan produk tersebut dibobol untuk mengetahui sampai sejauhmana sistem keamanan dari sistem tersebut. Dengan demikian, apakah tindakan para hacker tersebut dapat dikategorikan sebagai pembobol sistem keamanan seperti yang dimaksud dalam pasal tersebut. Apabila jawabannya adalah termasuk kategori pembobolan berarti Undang-Undang ITE mengabaikan proses yang berlaku secara tak tertulis di dunia *cyber* khususnya di kalangan para *hacker*; *Kedua*, Melakukan tindakan apapun yang berakibat terganggunya sistem elektronik. Sehubungan dengan hal itu juga mutlak harus dilakukan redefinisi dari setiap orang yang melakukan tindakan apapun yang berakibat terganggunya sistem elektronik karena banyak kegiatan-kegiatan di dunia nyata yang secara nyata tidak ada hubungannya dengan *cybercrime* namun karena kalimat dari pasal ini kegiatan tersebut dapat dikategorikan kejahatan. Seperti halnya seringnya dilakukan pemadaman listrik di suatu daerah, maka sedikit banyaknya akan berdampak terhadap sebuah sistem elektronik suatu perusahaan; *Ketiga*, Masyarakat dapat mengajukan gugatan. Pasal 33 Undang-Undang ITE menyebutkan bahwa masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan sistem elektronik. Apakah kalimat ini berlaku juga bagi nasabah yang uangnya ada di dalam bank yang menjadi korban *hacking*? Itu yang menjadi permasalahannya dan membutuhkan definisi penjelasan lebih dalam.

Penyempurnaan rumusan delik *cybercrime*, Rumusan kriminalisasi perbuatan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan sebuah sistem elektronik masih terlalu banyak unsur yang harus dibuktikan. Dalam Pasal 30 ayat (3) Undang-Undang ITE di dalam Undang-Undang ITE tidak dijelaskan tentang definisi *cybercrime*, jadi tidak diketahui sampai sejauhmana yang dinyatakan dengan unsur *cybercrime*, apakah akan melakukan atau percobaan melakukan kejahatan *cybercrime* dapat dikategorikan kejahatan

belum jelas tertulis di dalamnya.

Selain itu dalam Undang-Undang ITE tidak mengatur mengenai pemidanaan bagi pelaku-pelaku yang perbuatan pidananya seharusnya masuk dalam kategori kejahatan siber, antara lain: data *leakage and espionage* (membocorkan data dan memata-matai), *identity theft and fraud*. Oleh karena itu, revisi Undang-Undang ITE diperlukan agar payung hukum atas tindak pidana siber (*cybercrime*) bisa lebih komplis dan konkrit dalam menyelesaikan masalah-masalah *cybercrime*.

Penyempurnaan hukum acara pemeriksaan *cybercrime*, Untuk lebih meningkatkan efektifitas dan keberhasilan penegakkan hukum dunia siber, maka ketentuan yang mengatur mengenai hukum acara *cybercrime* atau pemeriksaan dalam setiap tingkatan perlu lebih diperjelas dan diperkuat. Kedudukan dan hubungan antara Undang-Undang ITE dan peraturan perundang-undangan terkait lainnya harus jelas dan harmonis agar tidak menimbulkan penafsiran yang berbeda-beda sehingga menimbulkan keragu-raguan dari aparat penegak hukum dalam mengambil tindakan. Mengacu kepada Undang-Undang Tindak Pidana Pencucian Uang yang menerapkan prinsip sistem pembuktian terbalik, maka hukum acara *cybercrime* diharapkan dapat juga menerapkan prinsip yang sama agar dapat lebih menjerat kepada pelaku kejahatan dunia siber.

Perspektif terhadap alternatif penanganan pelaku kejahatan telematika berupa pidana kerja sosial. Menjawab tuntutan dan tantangan komunikasi global lewat internet, undang-undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

RUU KUHP yang merupakan *ius constituendum* diharapkan akan memperkaya aturan yuridis telematika khususnya dalam hal penanganan *cyber crime* dan memberikan efek yang signifikan dalam pemberantasan tindak pidana di bidang *cyber crime*. Saat ini, berdasarkan hasil studi dalam hukum pidana di 56 negara asing, diperoleh kesimpulan bahwa pidana penjara adalah jenis pidana pokok yang paling banyak diancamkan terhadap pelaku *cybercrime* (Widodo, 2009:147, selanjutnya disebut Widodo I).

Dalam rangka mencari alternatif pengganti pidana penjara (*alternative to custodial sentence*), seyogyanya didasarkan pada pertimbangan-pertimbangan yang realistis dalam masyarakat. Pandangan sebagian ahli hukum yang ingin menghapus pidana penjara merupakan ide yang tidak mungkin terwujud (Muladi, 1995:133) Menurut penulis penjatuhan pidana penjara terhadap pelaku *cybercrime* di Indonesia perlu dibatasi. Alasan perlunya pembatasan tersebut adalah sebagai berikut: *Pertama*, Pelaksanaan pidana penjara di Indonesia belum optimal. Pada tahun 1984, Lamintang menyatakan bahwa dalam praktik di Indonesia, gagasan tujuan pidana penjara sebagai upaya pemasyarakatan tidak didukung oleh konsepsi yang jelas dan sarana yang memadai (PAF Lamintang, 1984: 181); *Kedua*, Meskipun demikian, sejak tahun 1995 di Indonesia sudah mempunyai Undang-Undang Pemasyarakatan yang dapat digunakan sebagai pedoman pelaksanaan pidana penjara; *Ketiga*, Karakteristik pelaku *cybercrime* antara lain berusia relatif muda, terdidik, orang-orang terhormat, terampil mengoperasikan komputer beserta program aplikasinya, menyukai tantangan teknologi, kreatif, dan ulet. Karakteristik tersebut berbeda dengan karakteristik pelaku kejahatan yang bukan tergolong dalam *cybercrime*. Karena itu, perlu penanganan tersendiri yang berbeda dengan pelaku tindak pidana lainnya. Hal ini didasarkan pada konsep individualisasi pemidanaan, bahwa pidana harus sesuai dengan kondisi terpidana dengan memperhatikan asas keseimbangan monodualistik; *Keempat*, Fasilitas pendidikan dan pembinaan narapidana di dalam Lembaga Pemasyarakatan relatif terbatas. Hasil penelitian Widodo menyebutkan bahwa di LAPAS Anak Blitar, sarana fisik dan peralatan tertentu yang mengarah pada upaya individualisasi pembinaan belum tersedia (Widodo, 2001: 163, selanjutnya disebut Widodo II). (5) Berdasarkan hasil identifikasi kasus kejahatan dan penelitian, ternyata tidak semua *cybercrime* mempunyai dampak yang sangat serius bagi korban dan masyarakat, dan banyak pelaku yang masih pertama kali melakukan kejahatan (*first offenders*) (Widodo I: 151).

Menurut penulis jenis pidana yang layak menggantikan pidana penjara terhadap pelaku *cybercrime* di Indonesia adalah pidana kerja sosial. Meskipun demikian, bukan berarti setiap pelaku *cybercrime* di Indonesia dapat dijatuhi pidana kerja sosial. Dalam perkara tertentu, pidana

penjara masih relevan dijatuhkan. Penentuan jenis pidana yang dijatuhkan tergantung dari kondisi pelaku kejahatan, kerugian yang ditimbulkan, dan perasaan hukum dalam masyarakat. Pidana kerja sosial adalah jenis pidana baru dalam hukum pidana di Indonesia karena belum diatur dalam Pasal 10 KUHP atau Undang-Undang di luar KUHP yang berlaku saat ini.

Penjelasan mengenai pidana kerja sosial diatur dalam Pasal 83 RUU KUHP. Akan tetapi pengertian dari pidana kerja sosial tidak dijelaskan. Menurut Widodo pengertian pidana kerja sosial adalah: Jenis pidana berupa pelaksanaan pekerjaan tertentu oleh terpidana di masyarakat tanpa mendapatkan upah, berdasarkan persyaratan yang diatur oleh peraturan perundang-undangan dan Putusan Pengadilan. Dalam putusan pengadilan pengadilan tersebut terkandung suatu perintah (*orders*) terhadap terpidana, yaitu tentang jangka waktu pidana dan tempat pelaksanaan pidana (Widodo I: 153).

Pidana kerja sosial dapat digunakan sebagai alternatif pengganti penjatuhan pidana jangka pendek. Uraian di atas didasarkan pada ketentuan Pasal 83 dan Penjelasan Pasal 83 RUU KUHP diuraikan sebagai berikut: Pidana kerja sosial dapat diterapkan sebagai alternatif pidana penjara jangka pendek dan denda yang ringan. Salah satu pertimbangan yang harus diperhatikan dalam penjatuhan pidana kerja sosial adalah harus ada persetujuan terdakwa sesuai dengan ketentuan dalam *Forced Labour Convention (Geneva Convention 1930)*, *The Convention for the Protection of Human Rights and Fundamental Freedom (Treaty of Rome 1950)*, *the Abolition of Forced Labour Convention (the Geneva Convention. 1957)* dan *the International Covenant on Civil and Political Rights (the Yew York Convention, 1966)*. Pidana kerja sosial ini tidak dibayar karena sifatnya sebagai pidana (*work as a penalty*), oleh karena itu pelaksanaan pidana ini tidak boleh mengandung hal-hal yang bersifat komersial. Riwayat sosial terdakwa diperlukan untuk menilai latar belakang terdakwa serta kesiapan yang bersangkutan baik secara fisik maupun mental dalam menjalani pidana kerja sosial. Pelaksanaan pidana kerja sosial dapat dilakukan di rumah sakit, rumah panti asuhan, panti Lansia, sekolah, atau lembaga sosial lainnya, dengan sebanyak mungkin disesuaikan dengan profesi terpidana.

Pidana Kerja Sosial dapat dijatuhkan jika dalam keputusan musyawarah majelis hakim menjelang

vonis, terdakwa akan dijatuhi pidana penjara yang lamanya tidak lebih dari 6 (enam) bulan atau pidana denda tidak lebih dari denda Kategori I. Hal ini didasarkan pada ketentuan Pasal 83 ayat (1) dan (2) RUU KUHP. Selain itu, dalam penjatuhan pidana kerja sosial, hakim wajib mempertimbangkan hal-hal berikut: *Pertama*, pengakuan terdakwa terhadap tindak pidana yang dilakukan; *Kedua*, usia layak kerja dari terdakwa berdasarkan peraturan perundang-undangan yang berlaku; *Ketiga*, persetujuan terdakwa terhadap kerja sosial, yaitu sesudah dijelaskan mengenai tujuan dan segala yang berhubungan dengan pidana kerja sosial; *Keempat*, riwayat sosial terdakwa; *Kelima*, perlindungan keselamatan terdakwa; *Keenam*, keyakinan agama dan politik terdakwa; *Ketujuh*, kemampuan terdakwa membayar denda

Selanjutnya, berdasarkan ketentuan Pasal 83 ayat (3), (4), (5), (6), dan (7) RUU KUHP, diatur bahwa pelaksanaan pidana kerja sosial tidak boleh dikomersialkan.

Pelaksanaan pidana kerja sosial dapat diangsur dalam waktu paling lama 12 (dua belas) bulan dengan memperhatikan kegiatan terpidana dalam menjalankan mata pencahariannya dan/atau kegiatan lain yang bermfaat. Jika terpidana tidak memenuhi seluruh atau sebagian kewajiban menjalankan pidana kerja sosial tanpa alasan yang sah, maka terpidana diperintahkan: *Pertama*, mengulangi seluruh atau sebagian pidana kerja sosial tersebut; *Kedua*, menjalani seluruh atau sebagian pidana penjara yang diganti dengan pidana kerja sosial tersebut; atau *Ketiga*, membayar seluruh atau sebagian pidana denda yang diganti dengan pidana kerja sosial atau menjalani pidana penjara sebagai peng-ganti denda yang tidak dibayar.

Berdasarkan ketentuan tentang pengertian dan pelaksanaan pidana (*strafmodus*) pidana kerja sosial di atas, penulis berpendapat bahwa karena tidak ada ketentuan dalam RUU KUHP yang mengatur tentang tindak pidana apa saja yang dapat dijatuhi pidana kerja sosial, maka putusan untuk menjatuhkan pidana kerja sosial mutlak ditentukan oleh hakim berdasarkan pedoman pemidanaan dalam RUU KUHP. Meskipun demikian, jika berdasarkan ketentuan Pasal 52 RUU KUHP majelis hakim sepakat untuk menjatuhkan pidana penjara yang jangka waktunya tidak melebihi 6 bulan terhadap pelaku *cybercrime* maka pidana kerja sosial lebih tepat dijatuhkan dari pada menjatuhkan pidana penjara.

Pidana kerja sosial sudah diterapkan sebagai alternatif pengganti pidana penjara jangka pendek di beberapa negara kawasan Eropa, misalnya Denmark, Jerman, Inggris, Perancis, Belanda, Norwegia, dan Portugal (Tongat, 2001: 8). Selain itu, Swis dan Italia memberlakukan pidana kerja sosial (Andi Hamzah, 1993: 24).

Barda Nawawi Arif menyatakan bahwa pada hakikatnya masalah kebijakan hukum pidana bukanlah semata-mata pekerjaan teknik perundang-undangan yang dapat dilakukan secara yuridis normatif dan sistematis dogmatik. Di samping pendekatan yuridis faktual juga dapat berupa pendekatan sosiologis, historis dan komperatif, bahkan memerlukan pula pendekatan komprehensif dari berbagai disiplin ilmu sosial lainnya dan pendekatan integral dengan kebijakan sosial dan pembangunan nasional pada umumnya (Andi Hamzah, 1993: 24).

Oleh karena itu dasar-dasar pertimbangan penulis menganalisa dan merekomendasikan mengenai kebijakan hukum pidana berupa penjatuhannya pidana berupa kerja sosial terhadap pelaku *cybercrime* di Indonesia adalah sebagai berikut: *Pertama*, Dasar Pertimbangan Filosofis, Pidana kerja sosial selaras dengan sila ke lima Pancasila, yaitu keadilan sosial bagi seluruh rakyat Indonesia, yang di dalamnya terkandung nilai bekerja keras. Dalam menjalankan pidana kerja sosial, terpidana dituntut bekerja keras dalam menjali pembedaan (Made Sahi Astuti, 1997: 157). Kerja keras adalah salah satu sarana utama untuk menuju keadilan sosial (keadilan masyarakat). Selain itu, menurut penulis, pidana kerja sosial juga sesuai dengan nilai-nilai sila ke-2, yaitu kemanusiaan yang adil dan beradab. Dalam sila ke-2 tersebut terkandung nilai-nilai pengakuan terhadap martabat manusia, karena manusia Indonesia adalah bagian dari warga masyarakat dunia yang berharkat dan bermartabat sama sebagai hamba Tuhan. Manusia dituntut berlaku adil dan menghormati hak asasi manusia lainnya, dan mengandung nilai penghormatan terhadap hak dan kewajiban asasi manusia. Kesesuaian ini tampak pada proses pelaksanaan pidana, yaitu terpidana ditempatkan di tempat kerja yang sesuai dengan keterampilan dan bakat narapidana, tidak merampas kemerdekaan narapidana, diintegrasikan dengan kelompok nonkriminal, dibimbing ke jalan yang benar oleh petugas yang kompeten. Dalam pidana kerja sosial juga terkandung nilai pengayoman, yaitu mengayomi narapidana dari pergaulan dengan

kelompok kriminal lain yang dapat mengakibatkan narapidana bertambah jahat, mengayomi narapidana agar dapat hidup layak di kemudian hari, dan mengayomi narapidana dari balas dendam masyarakat atau korban kejahatan. Pidana kerja sosial merupakan budaya asli bangsa Indonesia. Sedangkan pidana penjara yang diancamkan terhadap pelaku *cybercrime* sebagaimana diatur dalam RUU KUHP bukan merupakan budaya asli bangsa Indonesia. Menurut Made Sahi Astuti dalam hukum adat Indonesia tidak dikenal pidana perampasan kemerdekaan, yaitu pidana penjara dan pidana kurungan. Kesesuaian nilai-nilai yang dianut oleh bangsa Indonesia dengan nilai-nilai pidana kerja sosial ini merupakan pendorong keberhasilan pelaksanaan pidana kerja sosial (Made Sahi Astuti, 1997: 157). *Kedua*, Dasar Pertimbangan Teoretis, Pidana Kerja Sosial Sesuai dengan Ajaran Teori Gabungan. Teori gabungan, dalam penjatuhannya pidana perlu adanya pemilahan dan pembedaan antara tahap-tahap pembedaan narapidana, dan berat ringannya tindak pidana karena teori ini menggabungkan antara unsur pembalasan dengan unsur tujuan (*prevensi*). Golongan ke tiga dalam teori gabungan, bahwa pidana yang dijatuhkan dapat memenuhi keharusan pembalasan dan keharusan melindungi masyarakat, memberikan titik berat yang sama antara pembalasan dengan perlindungan masyarakat. Tujuan pidana bertalian erat dengan jenis kejahatan yang dilakukan dan nilai-nilai budaya bangsa yang bersangkutan (Made Sahi Astuti, 1997: 136). Berpijak pada konsep teori gabungan tersebut, menurut penulis pidana kerja sosial sudah memenuhi konsep 5 unsur dalam teori gabungan: (i) Pembedaan Pidana Berdasarkan Berat Ringannya Kejahatan dan Pembinaan Narapidana Sebagaimana penulis kemukakan di atas bahwa pidana kerja sosial dapat dijatuhkan terhadap pelaku kejahatan yang menjadikan komputer sebagai sasaran. Pidana ini merupakan alternatif pengganti pidana penjara jangka pendek. Uraian ini menunjukkan tentang perlunya mempertimbangkan berat ringannya tindak pidana sebelum hakim menjatuhkan pidana kerja sosial. Dalam pidana kerja sosial terkandung unsur rehabilitasi, reedukasi, dan resosialisasi. Se-lama menjalankan pidana, narapidana dibina dan dibimbing dan dibina dari sisi pembentukan sikap dan tingkah laku oleh Petugas Kemasyarakatan, wali narapidana, pamong narapidana (dari pegawai tempat pelaksanaan pidana), dari lembaga khusus yang dibentuk

pemerintah (misalnya dari sukarelawan). Selama menjalankan pidana, perkembangan pekerjaan dan kepribadian terpidana selalu diawasi dan dipantau oleh petugas kemasyarakatan. Hasil pengawasan dan pengamatan tersebut dapat digunakan sebagai sarana membimbing narapidana agar dapat berperilaku baik dan aktif berpartisipasi dalam pembangunan. (ii) Mengandung Unsur Pembalasan Berupa Penderitaan. Pidana kerja sosial dijatuhkan oleh pengadilan melalui putusan hakim. Pengumuman putusan hakim tersebut sudah merupakan unsur penderitaan berupa rasa malu bagi narapidana, karena masyarakat umum mengetahuinya. Proses pembinaan dan pengawasan narapidana di tempat pidana kerja sosial juga merupakan penderitaan, karena selalu diawasi dan dinilai. Pembebanan kewajiban narapidana untuk memenuhi segala persyaratan sebagaimana ditentukan oleh pengadilan, Balai Pemasyarakatan (BAPAS), penanggung jawab tempat pidana kerja sosial juga dapat merupakan penderitaan. Jika terpidana tidak memenuhi kewajiban tersebut, akan diperintahkan melakukan perbuatan sebagaimana diatur dalam RUU KUHP Pasal 10 ayat (7). Melakukan pekerjaan untuk kepentingan pihak lain selama berpuluh-puluh jam dengan tidak mendapatkan upah juga merupakan penderitaan. Bahkan, pada saat terpidana membaur dengan kelompok nonkriminal di tempat pidana kerja sosial juga merupakan penderitaan, karena sebagian besar orang yang ada di tempat kerja tersebut mengetahui tentang status dan keberadaan nara pidana; (iii) Perlindungan Masyarakat, Melalui pidana kerja sosial, terpidana akan berusaha tidak mengulangi kejahatan sebagaimana yang pernah dilakukan karena jika melakukan tindak pidana lagi, maka pengadilan kemungkinannya besar akan menjatuhkan pidana penjara dan denda dan tidak lagi menjatuhkan pidana kerja sosial untuk kedua kalinya. Anggota masyarakat lain yang berpotensi melakukan *cybercrime* juga akan menahan diri untuk tidak melakukan perbuatan, karena mengetahui bahwa pelaku kejahatan dapat dijatuhi pidana. Jika terpidana dijatuhi pidana tidak mengulangi kejahatan dan anggota masyarakat lain takut melakukan kejahatan, maka masyarakat akan merasa terlindung karena ada kemungkinan terjadinya penurunan jumlah kejahatan yang berhubungan dengan dunia maya (*cybercrime*) sehingga masyarakat tidak akan menjadi korban. Sesuai dengan Nilai Budaya Bangsa Indonesia

Pidana kerja sosial mempunyai nilai luhur, yaitu melakukan perbuatan yang bernilai sosial karena dilakukan di organisasi kemasyarakatan yang tidak mengutamakan perolehan keuntungan. Ini sesuai dengan sila ke dua dan ke lima Pancasila yang mengandung nilai kemanusiaan dan keadilan. Pada jaman dahulu atau mungkin juga sampai saat ini di beberapa daerah, meskipun perkara tersebut tidak diputus oleh pengadilan, para pelaku kejahatan sudah biasa dijatuhi pidana kerja sosial. Perintah pidana kerja sosial tersebut diberikan oleh kepala desa atau kepala adat atau tetua adat dalam masyarakat tersebut, misalnya membersihkan selokan, memperbaiki jalan. Perbuatan-perbuatan yang dapat dijatuhi pidana kerja sosial, misalnya orang yang lalai menjaga Pos Sistem Keamanan Lingkungan (Kamling). Keputusan tersebut terjadi karena Kepala Desa pernah mempunyai kedudukan sebagai hakim perdamaian desa.

Pidana Kerja Sosial sesuai dengan Aliran Modern dan Konsep Individualisasi Pidana. Individualisasi pidana merupakan konsekuensi logis dari munculnya aliran modern (positif) dalam hukum pidana, yang mengajarkan bahwa pidana terhadap pelaku tindak pidana perlu dilakukan dengan prinsip medis, dengan memperhatikan narapidana dari sisi biologis, psikologis dan sosiologis. Individualisasi pidana adalah menjatuhkan pidana sesuai dengan kondisi pelaku tindak pidana dengan mengabaikan prinsip keseimbangan monodualistis. Barda Nawawi Arief berpendapat, bahwa keseimbangan tersebut adalah keseimbangan antara kepentingan umum dengan kepentingan individu, antara unsur objektif dengan unsur subjektif, antara kriteria formal dengan materiel, antara kepastian hukum dengan kelenturan dan keadilan (Barda Nawawi Arief, 2005: 14).

Selain itu, juga harus ada keseimbangan antara nilai-nilai nasional dengan nilai-nilai global. Konsepsi ini mengandung 3 karakteristik utama, yaitu pertanggungjawaban pidana bersifat pribadi (asas personalitas), pidana hanya akan dijatuhkan terhadap orang yang bersalah (asas kulpabilitas), dan pidana disesuaikan dengan karakteristik dan kondisi si pelaku. Pidana kerja sosial memenuhi kriteria individualisasi pidana, karena dijatuhkan terhadap pelaku tindak pidana yang bersalah, dan jenis pidana tersebut dapat diubah oleh hakim berdasarkan permohonan pihak terpidana. Jenis pidana juga sesuai dengan karakteristik pelaku *cybercrime* di Indonesia, dan karakteristik

masyarakat Indonesia. Secara medis, agar pengobatan efisien dan efektif obat yang diberikan oleh dokter harus sesuai dengan kondisi pasien, begitu pula kondisi perawat dan perawatan harus menunjang. Metode pengobatan klinis tersebut sesuai dengan penjatuhan pidana kerja sosial. Ini tampak dalam ilustrasi berikut. Kesesuaian antara jenis pidana (ibarat obat) dan jenis kondisi penjahat (ibarat pasien) akan memudahkan hakim (ibarat dokter) dalam memutuskan langkah penanganan untuk penyembuhan, berdasarkan hasil pemantauan pegawai BAPAS, wali narapidana, pamong narapidana, dan sukarelawan (ibarat perawat). Kondisi dan fasilitas yang ada dalam masyarakat nonkriminal (ibarat suasana rumah sakit) sehingga secara psikologis dan sosiologis dapat menunjang percepatan penyembuhan dan penyehatan mentalitas penjahat.

Pidana Kerja Sosial dapat Digunakan sebagai Sarana Pencapaian Tujuan Teori Pidanaan Integratif. Dalam KUHP yang berlaku saat ini tidak ditemukan ketentuan tentang tujuan pidanaan. Untuk mengetahui tujuan pidanaan, penulis menggunakan hasil temuan penelitian Muladi, yaitu teori pidanaan integratif. Berdasarkan hasil penelitian Muladi, pidanaan mempunyai tujuan intergratif yaitu perlindungan masyarakat, pemeliharaan solidaritas masyarakat, pencegahan umum dan khusus, dan pengimbangan atau pengimbangan. Teori integratif memungkinkan untuk mengadakan artikulasi terhadap teori pidanaan yang mengintegrasikan beberapa fungsi sekaligus, yang secara terpadu diarahkan untuk mengatasi dampak individual dan sosial yang ditimbulkan oleh tindak pidana atas dasar kemanusiaan dalam sistem Pancasila. Kombinasi tersebut mencakup seperangkat tujuan pidanaan yang harus dipenuhi oleh setiap penjatuhan sanksi pidana. Ini selaras dengan kondisi filosofis, sosiologis, dan ideologis masyarakat Indonesia (Muladi, 1992: 11).

Uraian berikut akan menjelaskan relevansi pidana kerja sosial dengan 4 tujuan pidanaan dalam teori pidanaan integratif: *Pertama*, Memberikan Perlindungan Masyarakat. Pengertian perlindungan masyarakat mengarah pada semua keadaan yang mendukung agar masyarakat terlindung dari bahaya pengulangan tindak pidana. Tujuan ini merupakan tujuan setiap pidanaan. Melalui penjatuhan pidana kerja sosial pada pelaku *cybercrime*, masyarakat dapat terlindung dari

pengulangan tindak pidana. Hal ini didasarkan pada rasionalitas berikut. Jumlah durasi pidana kerja sosial paling lama 180 jam orang yang belum berusia 18 tahun, dan 200 jam bagi orang yang berusia di atas 18 tahun. Waktu pelaksanaan kerja sosial relatif lama, yaitu paling lama 2 tahun. Pidana kerja sosial yang dilakukan dalam waktu relatif lama dan dilaksanakan di luar Lembaga Pemasyarakatan tersebut selalu dikendalikan di bawah binaan dan pengawasan pihak-pihak yang kompeten sehingga memungkinkan terpidana dibimbing ke arah tingkah laku yang baik. Selain itu, narapidana yang bergaul dengan orang-orang nonkriminal akan dapat mendukung upaya perbaikan tingkah laku narapidana (aspek pencegahan khusus). Aspek pencegahan umum juga terkandung dalam pidana kerja sosial, yaitu membuat jera orang lain yang berpotensi melakukan kejahatan. Jika tingkah laku terpidana baik, anggota masyarakat tidak melakukan tindak pidana, maka masyarakat akan terlindung karena tidak akan ada lagi *cybercrime*; *Kedua*, Pemeliharaan Solidaritas Masyarakat. Pemeliharaan solidaritas mengarah pada upaya penegakan adat istiadat atau kebiasaan masyarakat dan pencegahan balas dendam perseorang atau balas dendam tidak resmi (*private revenge or unofficial retaliation*) terhadap penjahat. Selain itu, solidaritas masyarakat seringkali dikaitkan dengan kompensasi terhadap korban kejahatan berupa ganti kerugian. Melalui pidana kerja sosial, masyarakat termasuk korban *cybercrime* akan mengetahui bahwa pelaku tindak pidana sudah dijatuhi pidana berdasarkan hukum yang berlaku, sehingga dapat memperkecil atau bahkan meniadakan kemungkinan balas dendam masyarakat atau korban terhadap pelaku tindak pidana. Melalui penjatuhan pidana, juga ada langkah konkret penegakan hukum pidana, yaitu mengarah pada prinsip bahwa siapa yang melakukan tindak pidana secara bersalah akan dijatuhi pidana sesuai dengan hukum. Dalam pidana kerja sosial juga terkandung solidaritas sosial, yaitu peran serta masyarakat dalam rangka ikut membina narapidana; Sarana Pencegahan Umum dan Pencegahan Khusus. Pencegahan umum ditujukan kepada masyarakat agar tidak melakukan tindak pidana. Sedangkan pencegahan khusus ditujukan agar pelaku tindak pidana yang sudah dijatuhi pidana tidak melakukan tindak pidana lagi di kemudian hari. Melalui pidana kerja sosial, warga masyarakat khususnya para komunitas underground akan mengetahui bahwa siapapun yang

melakukan tindak pidana akan dipidana. Ini untuk menunjukkan kepada masyarakat bahwa anggapan yang menyatakan bahwa aktivitas dan *cybercrime* tidak dapat diatur dengan hukum sebagaimana didoktrinkan melalui Manifesto *Hacker*. Buktinya, semua aktivitas tersebut dapat diatur, bahkan pidana dapat dijatuhkan berdasarkan hukum pidana. Pidana tersebut dilakukan di luar Lembaga Pemasyarakatan sehingga dapat menyebabkan rasa malu kepada terpidana karena diketahui oleh banyak orang. Rasa malu tersebut diharapkan menjadi salah satu sarana pencegahan agar terpidana tidak melakukan tindak pidana. Selain itu, melalui pidana kerja sosial narapidana dapat memperoleh kepercayaan diri dan pembinaan mental agar tidak mengulangi kejahatannya. Muladi menyebutkan, bahwa dalam pencegahan khusus mencakup 3 faktor, *Pertama*, yaitu tipologi kejahatan, karakter pelaku, kepastian dan kecepatan pidana. Berdasarkan hasil penelitian ini, tipologi kejahatan *cybercrime* adalah kejahatan lintas negara (*trans-nationalcrimes*), *cybercrime* bukan hanya menggunakan komputer konvensional, *cybercrime* tergolong *white collar crime* dan bukan *white collar crime*, *cybercrime* bukan merupakan kejahatan terorganisasi, dan *cybercrime* merupakan kejahatan korporasi dan bukan kejahatan korporasi. Karakter pelaku *cybercrime* adalah mempunyai keterampilan sangat memadai dalam mengoperasikan komputer, internet beserta program aplikasinya; berpendidikan relatif tinggi (termasuk mahasiswa); tinggal di kota-kota besar, yaitu ibukota kabupaten, provinsi, dan ibukota negara; menyukai tantangan di bidang teknologi informasi yang berbasis komputer; mayoritas berjenis kelamin laki-laki; mempunyai kreativitas yang tinggi dan ulet; pandai memanfaatkan peluang yang ada untuk dalam melakukan kejahatan; mayoritas tergabung dalam komunitas *underground*. Selama ini, proses penjatuhannya sanksi pidana di Indonesia relatif cepat. Diketuinya ketiga tipologi tersebut secara empiris dapat menopang pencapaian tujuan pemidanaan, karena dapat digunakan sebagai dasar penentuan langkah-langkah pencegahan kejahatan. Berdasarkan hasil tipologi tersebut, pidana kerja sosial lebih relevan dijatuhkan terhadap pelaku *cybercrime* daripada penjatuhannya pidana penjara, karena kejahatan dilakukan oleh orang-orang yang berpendidikan, termasuk orang-orang terhormat. Jika terdakwa dijatuhi pidana penjara, justru dikhawatirkan terjadi prisonisasi dan stigmatisasi sehingga tujuan pemidanaan tidak berhasil; *Ketiga*,

Pengimbangan atau Pengimbangan. Pengertian pengimbangan atau pengimbangan adalah perlunya keseimbangan antara perbuatan pidana dengan pidana yang dijatuhkan. Hal ini perlu diperhatikan dalam setiap tahap pembinaan. Pidana kerja sosial dapat mengarah pada upaya membalas keseimbangan antara tindak pidana dan pidana yang dijatuhkan. Hal ini didasarkan pada alasan bahwa orang-orang yang mempunyai karakter terdidik, terhormat tidak sesuai jika dijatuhi pidana penjara, karena fasilitas dan proses pembinaan di LAPAS Indonesia selama ini belum mendukung upaya rehabilitasi pelaku *cybercrime*.

Pidana Kerja Sosial dapat digunakan sebagai sarana pencapaian tujuan pemidanaan sebagaimana Diatur dalam RUU KUHP. Dalam Bagian Ke Satu Paragraf 1 Pasal 51 ditentukan tentang tujuan pemidanaan, yaitu mencegah dilakukannya tindak pidana dengan menegakkan norma hukum demi pengayoman masyarakat atau memasyarakatkan terpidana dengan mengadakan pembinaan sehingga menjadi orang yang baik dan berguna; menyelesaikan konflik yang ditimbulkan oleh tindak pidana, memulihkan keseimbangan, dan mendatangkan rasa damai dalam masyarakat; dan membebaskan rasa bersalah pada terpidana.

Selain itu Pemidanaan tidak dimaksudkan untuk menderitakan dan merendahkan martabat manusia. Pidana kerja sosial dapat mencegah tindak pidana, karena dalam pelaksanaan tersebut tercakup aspek pembinaan, pendidikan, pengawasan, dan evaluasi narapidana dan hasil pekerjaannya. Pidana kerja sosial mempunyai beberapa keunggulan dibandingkan dengan pidana penjara, sehingga akan lebih efektif dalam mencapai tujuan. Dalam pidana kerja sosial terkandung juga aspek perlindungan baik bagi masyarakat maupun narapidana sehingga terpidana dapat menjadi lebih baik, dan masyarakat merasa aman dari terulangnya tindak pidana. Pidana kerja sosial dilaksanakan di masyarakat sehingga masyarakat mengetahui bahwa pelaku kejahatan sudah dijatuhi pidana dan dibina. Melalui pidana kerja sosial, terpidana dapat merasakan penderitaan dan sekaligus pembinaan oleh masyarakat dan petugas khusus. Berdasarkan uraian penulis tentang tahap-tahap pelaksanaannya dan pelaksanaan pidana kerja sosial di Indonesia, tampak bahwa pidana kerja sosial tidak mendatangkan penderitaan yang berlebihan dan tidak merendahkan martabat manusia.

PENUTUP

Di Indonesia, persoalan kejahatan dalam hukum telematika atau lebih khususnya mengenai *cybercrime* sebenarnya bukan hal baru, akan tetapi aturan untuk mengkriminalisasi pelaku *cybercrime* dengan perangkat aturan khusus berupa cyberlaw (Undang-Undang ITE) adalah persoalan yang baru, karena baru pada tahun 2008 Indonesia benar-benar mempunyai kebijakan hukum khusus dalam persoalan *cybercrime*. Persoalan pidana tersebut timbul karena di hadapan masyarakat terdapat perbuatan yang berdimensi baru, sehingga di masyarakat banyak muncul pertanyaan adakah hukumnya untuk perbuatan tersebut. Kesan yang muncul kemudian adalah terjadinya kekosongan hukum yang akhirnya mendorong kriminalisasi terhadap perbuatan tersebut. Hal tersebut sesuai dengan apa yang dikemukakan oleh von Savigny bahwa hukum tumbuh, hidup dan berkembang karena menyesuaikan kebutuhan masyarakat. Salah satu kunci agar sistem hukum tidak tertinggal dengan perkembangan telematika yang semakin pesat maka aturan yang dibuat harus bisa holistik, fleksibel dan antisipatif terhadap perubahan zaman. Undang-Undang ITE mengandung pendekatan *futuristic* karena pada masa yang akan datang teknologi semakin berkembang sehingga hukum harus mengatur tentang perubahan yang ada di masyarakat termasuk perubahan dalam bidang teknologi supaya tercapai kepastian hukum dalam Undang-Undang ITE tercemin kaidah-kaidah bahwa hukum dapat menjangkau perkembangan zaman sehingga Undang-Undang ITE ini bersifat fleksibel sepanjang tidak bertentangan dengan Undang-Undang yang lain. Akan tetapi walaupun hukum dibuat antisipatif atau preventif dan seholistik mungkin agar dapat memayungi setiap kegiatan khususnya bidang telematika akan tetapi Undang-Undang ITE ini tetap memiliki kendala-kendala antara lain kendala yuridis dan kendala dalam penanganan tersangka. Banyak ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang-Undang Informasi dan Transaksi Elektronik seperti hal-hal yang di atur dalam buku I KUHP tidak ada dalam Undang-Undang ITE. Seperti Kelalaian atau khilaf, lalai atau khilaf adalah kalimat yang sering dilakukan oleh manusia dalam melakukan kegiatannya. Selain itu kendala lain terkait proses penanganan tersangka, di mana Penindakan kasus *cybercrime* sering

mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti.

Untuk kendala-kendala yuridis yang ada maka untuk mengatasinya perlu dilakukan revisi atas undang undang tersebut seperti melakukan redefinisi mengenai pengertian atau peristilahan dalam peraturan perundang-undangan ITE sehingga terdapat batasan dan kejelasan makna serta tidak menimbulkan celah hukum (*loopholes*). Selain itu Berkaitan dengan kebijakan hukum pidana yang tidak hanya memikirkan ke-butuhan hukum saat ini tetapi juga yang akan datang, maka untuk memberikan alternatif pemidanaan bagi pelaku *cybercrime*, rumusan dalam RUU KUHP mengenai pidana kerja sosial bisa memberikan alternatif penjeratan bagi pelaku pidana. Perlunya alternatif pidana kerja sosial seperti yang diatur dalam RUU KUHP dikarenakan hal tersebut sesuai dengan dasar filosofis dan teoritis hukum yang berlaku

DAFTAR PUSTAKA

- Anonim, 2001, *Seluk Beluk Telematika*, (<http://www.beritanet.com/Technology/Communication/seluk-beluk-telematika.htm>)
- Arief, Barda Nawawi, 1996, *Bunga Rampai Kebijakan Pidana*, Bandung: PT. Citra Aditya Bakti.
- _____, 2005, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*, Bandung: Citra Aditya.
- Friedmann, W., 1993, *Teori dan Filsafat Hukum (Susunan I)*, Jakarta: Raja Grafindo Persada.
- Golose, Petrus Reinhard, 2006, *Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri, Makalah disampaikan dalam Seminar Nasional Mengenai "Penanganan Cybercrime di Indonesia ke arah Pengembangan Kebijakan yang Menyeluruh dan Terpadu"*, diselenggarakan di Menara Sjafruddin Prawiranegara Kompleks Perkantoran Bank Indonesia Jakarta
- Hamzah, Andi, 1993, *Sistem Pidana dan Pemidanaan di Indonesia*, Jakarta: Pradnja Paramita.
- Kiswanto, Muslim Heri, 2009, *Cyber crime dan Transaksi Elektronik dalam UU No. 11 Tahun 2008 tentang ITE*, Diunduh dari <http://www.scribd.com/doc/24106593/Smtr-Sejarah-Hukum>.
- Lamintang, PAF, 1984, *Hukum Penitensier Indonesia*, Bandung: Amico.\