BAB IV

PENGATURAN CYBER CRIME DALAM RUU KUHP SEBAGAI PEMBAHARUAN HUKUM PIDANA

Pada negara-negara yang menganut sistem hukum *Civil Law* seperti di Indonesia respon yang dilakukan terhadap suatu fenomena yang mengganggu keseimbangan antara kepentingan-kepentingan yang telah ada pada masyarakat menggunakan pendekatan peraturan. Hal ini merupakan konsekuensi dari sistem hukum *Civil Law* yang mendasarkan pada hukum tertulis. Kitab Undang-undang adalh merupakan sebbuah kitab yang hendaknya dapat dipergunakan dalam waktu yang lama dan dapat mengikuti perkembangan jaman.

4.1. RESPON HUKUM DI INDONESIA TERHADAP PERKEMBANGAN TEKNOLOGI INFORMASI

Perkembangan hukum memang akan selalu tertinggal dalam rangka merespon perkembangan-perkembangan sosial, ekonomi, dan teknologi di masyarakat. KUHP yang berlaku di Indonesia saat ini merupakan produk Belanda akibat pendudukannya di Indonesia yang mulai berlaku sejak 1918 dan merupakan pencerminan dari Wetboek van Strafrecht tahun 1886. Usia dan perjalanan KUHP Indonesia yang telah cukup lama maka sudah sewajarnya diadakan pembaharuan agar lebih sesuai dengan kondisi dan perkembangan jaman dan masyarakat Indonesia saat ini. Pembaharuan hukum pidana yang menyeluruh harus meliputi hukum pidana materiil, hukum pidana formil, dan hukum pelaksanaan pidana.[120] Ketiganya harus bersama-sama diperbaharui, karena apabila tidak maka akan timbul kesulitan dalam penerapannya dan tentu saja tujuan pembaharuan hukum tidak akan tercapai.

Salah satu upaya pemerintah untuk merespon perubahan sosial akibat perkembangan teknologi informasi tersebut adalah dengan menyusun Rancangan KUHP. Sejak tahun 1993 Indonesia telah mempunyai Rancangan Kitab Undang-Undang Hukum Pidana (RUU

[120] Sudarto, Loc cit

KUHP). Sejak tahun 1993 RUU KUHP telah mengalami beberapa perubahan hingga yang terakhir pada tahun 2005.

RUU KUHP tahun 2005 telah memuat ketentuan mengenai tindak pidana informatika. Ketentuan ini diatur dalam bagian Kelima mengenai "Tindak Pidana terhadap Informatika dan Telematika" yang terdiri dari tujuh pasal, yaitu Paragraf 1 mengenai Penggunaan dan Perusakan Informasi Elektronik dan Domain yang berisi tiga pasal, dari pasal 373 sampai dengan pasal 375. Kemudian diatur dalam paragraf 2 mengenai Tanpa hak Mengakses Komputer dan Sistem Elektronik, yang terdiri dari tiga pasal, yaitu pasal 376 sampai dengan pasal 378 . Paragraf tiga mengatur mengenai Pornografi anak melalui komputer, yaitu pasal 379.

Selain ketentuan pasal-pasal pada bagian kelima tersebut, pada ketentuan umum buku 1 RUU KUHP juga terdapat ketentuan mengenai perluasan istilah yang dipergunakan dalam RUU tersebut. Perluasan tersebut diantaranya adalah menganai anak kunci (pasal 158) dan barang (pasal 165).

Model yang digunakan dalam RUU KUHP tersebut adalah dengan cara menambah pasal-pasal baru yang mengatur mengenai kejahatan komputer dengan ditambah perluasan istilah umum.

4.2. KRIMINALISASI KEJAHATAN KOMPUTER DALAM RANCANGAN UNDANG-UNDANG KITAB UNDANG-UNDANG HUKUM PIDANA.

Pada pembahasan RUU KUHP tahun 1993 mengenai kejahatan komputer terdapat 4 kategori yang dibahas, 3 diantaranya adalah:

1) Pencurian data komputer (mengenai data).
2) Merusak/memasuki komputer (hardware).
3) Permasalahan mengenai privasi.

Permasalahan-permasalahan tersebut merupakan gambaran apa yang menjadi perhatian terhadap perkembangan teknologi informasi. Seperti yang telah penulis kemukakan pada Bab III, terhadap aspek-aspek tersebut di atas saat ini peristiwa tersebut telah terjadi. Pada pembahasan kasus-

kasus diatas, berdasarkan motif (maksud) dari pelaku penyimpangan dapat dikategorikan menjadi dua bagian yaitu:

- Motif hanya untuk membuktikan bahwa ia dapat membobol sebuah situs karena ketrampilannya yang lebih dari yang lain dan agar mendapat pengakuan dari komunitasnya atau yang lain.
- Motif selain tersebut di atas yaitu diantaranya untuk mencari keuntungan secara materi seperti pada kasus-kasus pembelian barang dengan menggunakan kartu kredit milik orang lain lewat online shop serta motif lainnya seperti untuk mempermalukan orang lain.

4.2.1. Pencurian data komputer (mengenai data)

Hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan yang belum tertampung di dalam peraturan yang ada, seperti dalam kasus pencurian listrik yang sulit dikategorikan sebagai delik pencurian karena definisi benda dalam hukum itu sendiri tetapi akhirnya dapat diterima sebagai perbuatan pidana.

Dari delik-delik yang telah dibahas pada Bab III di atas dimana kasus yang sering terjadi adalah penggunaan kartu kredit milik orang lain untuk membeli barang. Pelaku mendapat nomor-nomor kartu kredit tersebut dengan cara mengambil atau membeli lewat situs internet. Setelah mendapatkan nomor kartu kredit milik orang lain tersebut pelaku membeli barang melalui online shop. Sehingga dapat disimpulkan bahwa perbuatan yang dikriminalisasi dalam KUHP adalah perbuatan melawan hukum terhadap **barang atau benda**.

Pada peristiwa tersebut di atas terdapat dua peristiwa yaitu:

- Pencurian identitas kartu kredit dan,
- pencurian barang dengan menggunakan kartu kredit tersebut.

Pada kasus-kasus di atas yang menjadi masalah adalah pelaku tidak dapat dibuktikan perbuatan pokoknya yang menimbulkan kerugian berupa materi bagi orang lain. Dari dua kasus yang menjadi contoh salah satunya hanya dapat dibuktikan pasal 263 ayat (2) KUHP yaitu

menggunakan identitas palsu. Pada RUU KUHP terdapat beberapa pasal untuk merespon peristiwa tersebut.

Terhadap pelaku yang mendapatkan identitas kartu kredit secara melawan hukum dapat dijerat dengan pasal-pasal:

Pasal 373

Dipidana dengan pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik.

Pasal 378

Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI, setiap orang yang :

a. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;

Pasal 373 tersebut mengkriminalisasi perbuatan seseorang yang memasuki/mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dan yang dimaksud komputer dan sistem elektronik adalah termasuk jaringan komputer dan internet. Sedangkan maksud dari pelaku menurut pasal tersebut dapat berupa memperoleh, mengubah, merusak, atau menghilangkan informasi. Memperoleh informasi disini dapat ditafsirkan termasuk juga data mengenai identitas dan rekening kartu kredit. Pasal ini merupakan sebuah delik materiil karena terdapat kata-kata "dengan maksud untuk..."

Pada perkara yang telah di bahas pada Bab III bahwa pelaku menggunakan identitas kartu kredit milik orang lain tersebut untuk membeli barang. Pembelian barang dengan menggunakan kartu kredit milik orang lain tersebut ditampung di dalam pasal 378 huruf b:

Pasal 378

Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI, setiap orang yang :

b. Menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan;

Berdasarkan pasal-pasal tersebut, sebuah peristiwa pembelian barang melalui internet dengan menggunakan kartu kredit milik orang lain dapat dikenakan dua pasal yaitu memperoleh identitas kartu kreditnya itu sendiri yang diancam hukuman 4 tahun pada pasal 373 serta diancam hukuman selama 10 tahun pada pasal 378 huruf a. Sedangkan perbuatan menggunakan kartu kredit milik orang lain tersebut diancam tersendiri di dalam pasal 378 huruf b dengan ancaman 10 tahun.

Perumusan tentang delik kejahatan komputer di dalam RUU KUHAP tidak efektif,karena selain terdapat rumusan delik kejahatan komputer tersendiri juga terdapat perluasan istilah-istilah yang digunakan dalam delik-delik konvensional. Hal ini dapat dilihat pada ketentuan umum buku 1 RUU KUHP dimana terdapat perluasan istilah-istilah yang digunakan dalam delik-delik konvensional seperti pencurian, penipuan, penggelapan, pengrusakan barang, dan lain-lain. Perluasan tersebut diantaranya adalah menganai anak kunci (pasal 158) yang berbunyi:

Pasal 158

Anak Kunci adalah alat yang digunakan untuk membuka kunci, termasuk kode rahasia, kunci masuk komputer, kartu

magnetik, atau signal yang telah diprogram yang dapat digunakan untuk membuka sesuatu oleh orang yang diberi hak untuk itu.

Serta pengertian barang pada pasal 165 yang berbunyi:

Pasal 165

Barang adalah benda berwujud termasuk air dan uang giral, dan benda tidak berwujud termasuk aliran listrik, gas, data dan program komputer, jasa termasuk jasa telepon, jasa telekomunikasi, atau jasa komputer.

Perluasan pengertian barang pada pasal 165 tersebut dapat dikaitkan dengan pasal:

Pasal 593

Setiap orang yang mengambil suatu barang yang sebagian atau seluruhnya milik orang lain, dengan maksud untuk memiliki barang tersebut secara melawan hukum, dipidana karena pencurian, dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Kategori IV.

Pasal 593 tersebut merupakan delik pencurian,dimana obyek pencurian adalah berupa barang, sedangkan menurut pasal 165 yang dimaksud dengan barang adalah termasuk data dan program komputer.

Sesuai dengan uraian di atas, bahwa terhadap pelaku yang mendapatkan identitas/nomor kartu kredit milik orang lain terdapat beberapa pasal yang dapat diterapkan yaitu:

- Pasal 373 dengan ancaman **pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV.**
- Pasal 378 huruf a dengan ancaman **pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI.**

- Pasal 593 dengan ancaman **pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Kategori IV**

Perbuatan-perbuatan yang dikriminalisasi tersebut pada intinya melarang pelaku untuk memperoleh data informasi mengani kartu kredit orang lain secara melawan hukum dengan sarana mengakses jaringan komputer secara tidak sah. Namun terhadap perbuatan tersebut terdapat beberapa pasal yang dapat digunakan untuk menjerat pelaku dengan ancaman hukuman yang berbeda.

Selain itu juga terdapat ayat lain yang serupa yang mengkriminalisasi penyebaran data atau informasi mengenai kartu kredit dan/atau menggunakannya yaitu pada pasal yang sama huruf d:

Pasal 378

Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI, setiap orang yang :

d. Menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

Pasal ini mengkriminalisasi dua hal yaitu:

- Menyebarkan, memperdagangkan, kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik.
- Memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik.

Perbuatan tersebut dilarang apabila dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di

dalam dan luar negeri. "Mempengaruhi" disini dapat diartikan luas termasuk merugikan secara finanisal.

Dengan adanya perbedaan pada ancaman pasal-pasal tersebut maka perumusan pasal-pasal di dalam RUU KUHP menjadi berlebihan karena sebuah perbuatan yang seharusnya sudah dapat dijerat dengan sebuah pasal dengan perluasan-perluasan istilah saja namun dibagian lainnya dibuat pasal yang mengkriminalisasi perbuatan serupa dalam sebuah pasal tersendiri. Selain perumusannya tidak efektif juga dapat menimbulkan akibat negatif yaitu tidak adanya kepastian hukum terhadap perbuatan tersebut. Hal ini berhubungan dengan salah satu unsur asas legalitas yaitu *lex certa* dimana sebuah peraturan haruslah jelas dan tidak menimbulkan ambigu[121]. Asas ini mengharuskan adanya peraturan yang tegas sehingga menjamin adanya kepastian (*requirement of certainty*). Terhadap pelaku dalam hal ini akan mengalami ketidakpastian yaitu aturan mana yang akan dikenakan kepadanya apabila ia melakukan perbuatan tersebut.

Apabila kita melihat dari motif pelakunya maka jelas bahwa pada kasus-kasus tersebut di atas pelaku menghendaki untuk memiliki barang milik orang lain secara melawan hukum. Sementara itu modus operandi pelaku akan berkembang seiring dengan perkembangan teknologi dan penyesuaian pelaku terhadap kondisi yang ada. Seperti data yang ada pada Mabes Polri bahwa sampai saat ini Mabes Polri telah menerima laporan dari korban yang berada di luar negeri karena mereka merasa ditipu karena membeli barang melalui situs di Indonesia. Pelaku membuka sebuah situs online shoping berbagai macam barang. Korban telah membeli barang-barang melalui situs tersebut dan memberikan identitas kartu kredit mereka dan ternyata barang tersebut tidak pernah dikirim kepada pembeli tersebut. Pelaku mendapatkan identitas kartu kredit milik pembeli tersebut untuk digunakan kembali membeli barang di tempat lain.

[121] Marjane Termorshizen-Arts, *Same Root, Different Development*, ceramah hukum pidana FHUI Depok, 3-4 April 2006.

Pada peristiwa tersebut pelaku tidak dapat dijerat dengan pasal 378 huruf a RUU KUHP karena pada pasal tersebut mensyaratkan pelaku harus aktif mengakses jaringan komputer untuk mendapatkan informasi data kartu kredit milik orang lain sedangkan dalam peristiwa tersebut di atas pelaku bersikap pasif dan menunggu korban untuk mendapatkan identitas kartu kredit tersebut.

Menurut Soerjono Soekanto salah satu unsur penegakan hukum adalah "Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum". Penegak hukum mempunyai peranan yang sangat penting karena mereka yang akan mengaplikasikan peraturan-peraturan tersebut di lapangan. Apabila aturan dalam pasal-pasal RUU KUHP seperti telah penulis kemukakan di atas yaitu sebuah perbuatan dapat dijerat oleh beberapa pasal yang berbeda ancaman hukumannya maka terdapat kemungkinan penegak hukum yang satu dan lainnya akan berbeda dalam menerapkan peraturan tersebut.

4.2.2. Merusak/memasuki komputer.

Merusak atau memasuki komputer pihak lain adalah persoalan mengenai kejahatan yang ditujukan kepada perangkat keras komputer (hardware). Selama ini terdapat beberapa kasus yng dilaporkan kepada penyidik Polri. Kasus yang menjadi perhatian publik adalah kasus *cracking* website Komisi Pemilihan Umum yang terjadi pada masa Pemilu tahun 2004 serta *cracking* terhadap website Partai Golkar pada tahun 2006.

Perbuatan memasuki jaringan komputer pihak lain merupakan perbuatan yang dianggap sebagai perbuatan menyimpang oleh korban. Sesuai dengan kasus-kasus yang dibahas belum terdapat aturan yang memadai untuk menjerat pelaku. Korban dalam hal ini pihak yang merasa daerah yang terbatas telah dimasuki oleh pihak yang tidak berhak untuk memasuki daerah tersebut.

Dalam kejahatan komputer (cyber crime), perbuatan perusakan, penghancuran barang mempunyai pengertian suatu

perbuatan yang dilakukan dengan suatu kesengajaan untuk merusak / menghancurkan sesuatu yaitu data atau program komputer yang disimpan dalam suatu media penyimpanan data elektronik sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak dapat dipergunakan lagi. Selain data elektronik suatu web site ataupun hompe page juga dapat menjadi sasaran perusakan tersebut.

Pada RUU KUHP pasal yang dapat digunakan untuk menjerat pelaku yang memasuki jaringan komputer milik orang lain dan atau merusaknya adalah pasal 373:

Pasal 373

> Dipidana dengan pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik.

Pasal 373 tersebut mengkriminalisasi perbuatan mengakses komputer dan/atau sistem elektronik tanpa hak, dan perbuatan tersebut dengan maksud untuk melakukan sesuatu terhadap data/informasi di dalamnya. Delik ini merupakan delik materiil sehingga menghendaki adanya perubahan dalam data/informasi di dalamnya. Pasal ini dapat diterapkan terhadap kasus memasuki jaringan komputer atau elektronik tanpa hak yang mengakibatkan perubahan/perusakan.

Pada kasus pembobolan website KPU dan partai Golkar motif pelaku hanya untuk membuktikan bahwa ia dapat membobol sebuah situs karena ketrampilannya yang lebih dari yang lain dan agar mendapat pengakuan dari komunitasnya atau pihak lain. Pada peristiwa ini terdapat dua kepentingan yang bersinggungan yaitu pemilik jaringan komputer atau elektronik yang merasa hak-haknya telah dilanggar dengan para pelaku yang hendak membuktikan eksistentinya dengan cara memasuki jaringan komputer orang lain.

Pada kasus pembobolan situs KPU dimana situs tersebut berisi data penghitungan suara pemilihan Presiden adalah berisi informasi yang sangat penting. Namun pelaku hanya merubah nama-nama partai tanpa merubah angka-angka di dalamnya. Sehingga jelas dalam peristiwa ini pelaku tidak mempunyai motif selain untuk membuktikan kepada KPU bahwa keamanan situsnya kurang dan dapat diterobos oleh pelaku. Pelaku-pelaku dalam kasus hacking ini dapat dikatakan pelaku yang "baru". Dikatakan baru karena pelaku tersebut tergiur dengan adanya karakteristik kejahatan komputer yang sulit terdeteksi[122].

Selain itu karakteristik pelaku kejahatan komputer lainnya adalah memiliki ketrampilan khusus, sehingga dapat dikatakan pelaku dalam kasus-kasus ini dari kalangan terdidik. Pelaku dalam kasus-kasus ini seperti yang dijelaskan pada Bab III mempunyai komunitas tersendiri bahkan cenderung mempunyai budaya tersendiri dengan *conduct norms* yang tersendiri pula. Dengan adanya ancaman pidana yaitu pada pasal 373 tersebut adalah pidana penjara paling lama 4 (empat) tahun dan denda paling banyak kategori IV akan mengakibatkan dua kemungkinan yaitu pertama, pelaku akan jera dan pelaku-pelaku lainnya akan takut untuk melakukan atau kedua, pelaku-pelaku lainnya akan membentuk sebuah solidaritas untuk mendukung anggota komunitasnya hingga peristiwa-peristiwa lainnya akan terus terjadi dan peraturan tersebut tidak akan efektif untuk menanggulanginya.

Terhadap karakteristik kejahatan komputer yaitu sulit terdeteksi tersebut mengakibatkan adanya pelaku "baru" yang tergoda untuk melakukannya. Pelaku-pelaku baru tersebut adalah pelaku yang mempunyai keahlian lebih dari yang lainnya. Keahlian tersebut digunakan untuk tujuan yang merugikan orang lain. Apabila seluruh pelaku akan dijerat dengan pasal tersebut dan akhirnya dihukum, maka akan banyak sumber daya manusia terdidik yang akan tidak

[122] John T Soma, Loc Cit.

berguna. Hal ini terjadi karena jenis pidana pada pasal ini mulai dari pidana penjara sehingga seluruh pelaku yang terbukti bersalah akan dijatuhi hukuman pidana penjara.

Mantan napi mempunyai sebuah konsekuensi sosiologis dan yuridis. Tidak semua lapangan kerja akan dapat menerima seseorang mantan narapidana. *The unspoken premise is that a person who is convicted of a crime has a "criminal mind", should be quarantined like a person with a communicable disease-people with "criminal mind" should not be allowed to infect respectable businesses, their employees or customer*[123]. (terjemahan bebas penulis; sebuah premis yang tidak terungkapkan bahwa seseorang yang melakukan perbuatan kriminal mempunyai "pikiran kriminal", seharusnya dikarantina seperti seseorang yang berpenyakit tidak dapat berkomunikasi dengan "pemikiran kriminal" yang seharusnya tidak menulari bisnis mereka yang terhormat, pegawai serta pelanggan mereka).

Hampir semua lapangan pekerjaan di Indonesia mensyaratkan adanya sebuah surat yang dikeluarkan oleh pihak Kepolisian bahwa mereka tidak pernah terlibat dalam tindak pidana. Sedangkan para pelaku yang dinyatakan bersalah oleh hakim tidak dapat mendapatkan surat dimaksud. Hal ini akan menjadikan keadaan menjadi semakin tidak terkendali yang akhirnya terdapat banyak pengangguran terdidik.

Untuk meminimalkan dampak dari kriminalisasi tersebut dapat dilakukan beberapah hal diantaranya membuat pasal 373 menjadi delik aduan mutlak dimana pelaku tidak dapat dituntut kecuali dengan adanya pengaduan dari korban. Dengan adanya syarat aduan tersebut dapat meminimalkan pelaku yang menjalani proses dan masuk dalam koridor sistem peradilan pidana yang mempunyai efek samping yang besar. Selain itu tindakan lain yang dapat dilakukan adalah memperbesar rentang pidananya dari pidana penjara dan denda menjadi pidana penjara atau denda, sehingga penegak hukum dapat

[123] Bahan mata kuliah Sistem Peradilan Pidana, Whitney North Seymour, *The Correction System : Unwritting Partner in Crime,* Pusat Dokumentasi Hukum Universitas Indonesia, 1983 hal 448.

mempunyai pilihan untuk memberikan hukuman yang sesuai dengan pelaku terutama pelaku pertama (*first offender*).

4.2.3. Kejahatan terhadap privasi.

Pada suatu saat nanti seluruh informasi dan data akan disimpan dan ditransfer melalui jaringan komputer. Informasi tersebut meliputi seluruh aspek kehidupan manusia, diantaranya informasi mengenai identitas pribadi seseorang dan informasi lainnya yang bersifat pribadi. Jika hal tersebut terjadi maka privasi menjadi sebuah hal yang memerlukan perhatian lebih. Privasi tersebut merupakan hak setiap orang dimana didalamnya terkandung beberapa aspek seperti terhadap kepribadian, data dan komunikasi. Terhadap aspek-apek tersebut hendaknya dapat dilindungi dengan hukum.

Seperti yang dikatakan oleh *Thomas J. Imedinghaff* yang dikutip oleh Edmon Makarim yang telah penulis kemukakan pada Bab II di atas bahwa aspek-aspek dalam privasi yaitu:

a. *Privacy of a Person's Persona* (privasi terhadap kepribadian seseorang).
b. *Privacy of Data About Person* (privasi terhadap data/informasi seseorang).
c. *Privacy of a Person's Communications* (privasi terhadap komunikasi seseorang).

Hak atas privacy tersebut juga mencakup komunikasi secara *online*. Dalam hal-hal tertentu, pengawasan dan penyingkapan isi dari komunikasi elektronik oleh orang lain bukan oleh pengirim atau orang yang dikirim dapat merupakan pelanggaran dari privasi seseorang.

Informasi yang memuat privasi seseorang saat ini banyak terdapat lembaga-lembaga pemerintah maupun organisasi-organisasi lainnya untuk berbagai keperluan. Pihak pemerintah mengumpulkan identitas dalam jumlah besar seperti kartu tanda penduduk sedangkan lembaga lain seperti perbankan mengumpulkan data-data mengeni nasabahnya. Dengan adanya teknologi informasi maka data-data tersebut dapat diakses oleh berbagai pihak baik pihak yang berwenang

menerima informasi maupun pihak-pihak lain yang tidak berwenang yang mungkin menyalahgunakan informasi tersebut.

Pada contoh kasus yang telah penulis kemukakan pada Bab III yaitu kasus foto-foto milik orang lain yang tidak seharusnya disebarkan dengan media internet. Pada kasus tersebut terhadap tersangka penyidik menggunakan pasal 282 ayat (1) KUHP dan pasal 335 KUHP. Pasal 282 ayat (1) KUHP mengkriminalisasi setiap orang yang menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan yang diancam pidana penjara paling lama satu tahun enam bulan atau pidana denda paling tinggi empat ribu lima ratus rupiah. Pasal ini tidak dimaksudkan untuk mengkriminalisasi seseorang yang menyebarkan gambar yang melanggar kesusilaan untuk mencemarkan nama baik seseorang.

Pada RUU KUHP BAB VIII "TINDAK PIDANA YANG MEMBAHAYAKAN KEAMANAN UMUM BAGI ORANG, KESEHATAN, BARANG, DAN LINGKUNGAN HIDUP", bagian kelima yaitu Tindak Pidana terhadap Informatika dan Telematika belum terdapat aturan yang mengkriminalisasi hal tersebut, yang ada adalah pasal yang serupa dengan yang dengan pasal 282 KUHP yaitu pasal 468 ayat (1)RUU KUHP yang berbunyi:

(1). Setiap orang yang menyiarkan, memperdengarkan, mempertontonkan, atau menempelkan tulisan, suara, atau rekaman suara, film atau yang dapat disamakan dengan film, syair lagu, puisi, gambar, foto, dan/atau lukisan melalui media massa cetak, media massa elektronik dan/atau alat komunikasi medio yang mengeksploitasi daya tarik seksual pada bagian tubuh, aktivitas seksual, hubungan seksual antara laki-laki dengan perempuan atau sesama jenis, atau aktivitas atau hubungan seksual dengan binatang atau dengan jenazah, dipidana karena pornografi dengan ancaman pidana penjara

paling lama 5 (lima) tahun atau pidana denda paling banyak Kategori IV.

Pasal 468 ayat (1)RUU KUHP tersebut pada intinya sama dengan pasal 282 KUHP yaitu mengkriminalisasi setiap orang yang menyebarluaskan sesuatu yang mengandung unsur asusila. Penyebaran sesuatu yang mengandung unsur asusila tersebut tidak disyaratkan siapa obyek yang ada pada gambar/foto/tulisan tersebut.

Untuk peristiwa seperti kasus yang telah disebutkan di atas yaitu seseorang yang menyebarkan gambar/foto dan hal tersebut dimaksudkan untuk mengganggu privasi seseorang, belum terdapat aturan/delik yang mengatur mengenai hal tersebut di dalam RUU KUHP.

Selain peristiwa yang dijadikan contoh kasus di atas, secara umum terdapat kepentingan-kepentingan yang perlu dilindungi seperti yang telah dikemukakan pada Bab III diantaranya adalah:

1. Informasi mengenai seseorang yang sebenarnya merupakan informasi rahasia(privacy). Dengan dapat diaksesnya data-data tersebut maka tidak menutup kemungkinan akan terjadi penggunaan identitas atau data-lainnya secara melawan hukum yang dapat dilakukan oleh siapapun juga termasuk pemerintah.
2. Dunia bisnis yang mempunyai informasi yang perlu dilindungi.

RUU KUHP bagian Tindak Pidana terhadap Informatika dan Telematika hanya terdapat peraturan yang melindungi kepentingan-kepentingan beberapa pihak yaitu:

- Jaringan komputer.
- Nama domain perusahaan.
- Informasi keuangan dari bank sentral dan lembaga keuangan lainnya.

Jaringan komputer yang dilindungi dalam RUU KUHP tersebut merupakan jaringan komputer secara umum. Dalam pasal tersebut terhadap perbuatan masuk ke dalam jaringan komputer yang memuat data-data atau informasi secara umum. Sedangkan terhadap dunia

bisnis juga terdapat kepentingan-kepentingan yang harus dilindungi yaitu informasi-informasi dunia bisnis yang apabila diambil oleh pihak lain secara melawan hukum akan merugikan yang bersangkutan sehingga merupakan delik materiil.

4.2.4. Undang-undang Informasi dan Transaksi Elektronik.

Pada tanggal 21 April 2008 telah disahkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut memuat kriminalisasi beberapa perbuatan yang berhubungan dengan informasi dan transaksi elektronik pada Bab VII dari pasal 27 hingga pasal 37.

Pada pasal-pasal tersebut dapat dibagi menjadi beberapa bagian:

1. Pasal-pasal yang memuat delik yang sudah ada di dalam KUHP dengan sarana teknologi informasi.
2. Pasal-pasal yang memuat delik yang mengkriminalisasi perbuatan yang belum pernah diatur sebelumnya.

Pasal-pasal yang memuat delik yang sudah ada di dalam KUHP contohnya pornografi, perjudian, penghinaan/pencemaran nama baik dan pemerasan/pengancaman. Terhadap pasal-pasal tersebut dapat terjadi dualisme peraturan walaupun dapat digunakan asas bahwa Undang-undang No. 11 tahun 2008 lebih khusus dan dikeluarkan belakangan dibandingkan dengan KUHP.

Pada undang-undan No. 11 tahun 2008 terdapat pasal-pasal yang mengkriminalisasi perbuatan yang belum pernah diatur sebelumnya, diantaranya pasal 30 yang berbunyi:

(1). Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.(ancaman maksimal 6 (enam) tahun penjara dan denda).

(2). Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh

informasielektronik dan/atau dokumen elektronik (ancaman maksimal 7 (tujuh) tahun penjara dan denda).

(3). Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan. (Ancaman maksimal 8 (delapan) tahun penjara dan denda).

Pasal tersebut melindungi kepentingan seseorang terhadap jaringan elektronik/komputer miliknya. Pasal ini serupa dengan pasal 373 RUU KUHP. Dalam pasal ini dibagi menjadi tiga ayat dimana ayat (1) dan (3) merupakan delik formil dan ayat (2) merupakan delik materiil. Seperti yang telah penulis sampaikan pada poin 4.2.2 bahwa karena karakteristik kejahatan komputer yaitu sulit terdeteksi tersebut mengakibatkan adanya pelaku "baru" yang tergoda untuk melakukannya.

Terhadap pasal tersebut hendaknya menjadi delik aduan mutlak dimana pelaku tidak dapat dituntut kecuali dengan adanya pengaduan dari korban atau dengan memperbesar rentang pidananya dari pidana penjara dan denda menjadi pidana penjara atau denda untuk menekan efek yang tidak diinginkan dari sistem peradilan pidana ini.

Pada undang-undang No. 11 tahun 2008 ini telah melindungi kepentingan-kepentingan pihak-pihak yaitu terhadap akses jaringan komputer yang tidak sah dan data/informasi, sedangkan terhadap privasi belum diatur seperti privasi yang telah penulis kemukakan pada poin 4.2.3.

Rumusan delik di dalam undang-undang nomor 18 tahun 2008 tersebut serupa dengan rumusan delik kejahatan komputer di dalam RUU KUHP. Rumusan-rumusan delik di dalam UU no. 18 tahun 2008 tersebut tidak membedakan mana yang termasuk kejahatan konvensional namun menggunakan sarana komputer dan mana yang termasuk dengan kejahatan komputer. Sebagai contoh pada pasal 27

ayat (2) UU no. 18 tahun 2008 yang sebenarnya mengkriminalisasi perjudian dengan menggunakan sarana komputer, sedangkan di dalam KUHP yang sekarang berlaku perjudian tidak diatur secara limitatif sarana yang dipergunakan. Sehingga terhadap undang-undang No. 18 tahun 2008 tersebut juga terjadi tumpang tindih aturan dengan aturan yang telah ada. Hal ini apabila dihubungkan dengan asas *lex specialis derograt legi generali,* maka kedua delik tersebut tidak dapat dikatakan salah satu lebih khusus dari lainnya karena hanya menyangkut sarana dalam melakukan kejahatan saja dan bukan inti dari apa yang dilarang.

4.3. SINGKRONISASI KRIMINALISASI KEJAHATAN KOMPUTER DENGAN RUU KUHAP

Dalam kasus-kasus *cyber crime*, alat bukti bukti elektronik merupakan alat bukti yang sangat penting karena peristiwa kejahatan komputer biasanya hanya sedikit melibatkan manusia secara langsung dan dapat dilakukan dimana saja bahkan dari jarak yang jauh. Dengan karakteristik tersebut maka sangat kecil kemungkinan untuk mendapatkan alat bukti berupa saksi dimana disyaratkan harus melihat atau mendengar sendiri peristiwa tersebut.

Pada Rancangan Undang-undang Kitab Hukum Acara Pidana (RUU KUHAP) terdapat pasal yang mengatur mengenai jenis-jenis alat bukti yaitu pasal 177 yang berbunyi:

(1). Alat bukti yang sah mencakup:
   a. barang bukti ;
   b. surat-surat;
   c. bukti elektronik;
   d. keterangan seorang ahli;
   e. keterangan seorang saksi;
   f. keterangan terdakwa; dan.
   g. pengamatan Hakim.

(2). Alat bukti yang sah sebagaimana dimaksud pada ayat (1) harus diperoleh secara tidak melawan hukum.

(3). Hal yang secara umum sudah diketahui tidak perlu dibuktikan.

Pasal-pasal dalam RUU KUHAP menambah beberapa alat bukti baru yang sebelumnya telah ada dan diatur dalam KUHAP yang saat ini berlaku. Tambahan tersebut adalah dimasukkannya barang bukti, bukti elektronik dan pengamatan hakim menjadi alat bukti. Bukti elektronik tersebut mempunyai karakteristik yang berbeda dengan bukti yang berbasis kertas, dimana bukti elektronik tersebut mudah diubah atau berubah.

Untuk memperoleh alat bukti penyidik dapat melakukannya dengan beberapa cara. Sesuai dengan RUU KUHAP bahwa penyidik dapat melakukan penggeledahan dan penyitaan untuk menemukan barang bukti yang dapat menjadi bukti awal untuk menentukan tersangka dan nantinya akan diserahkan kepada penuntut umum.

Seperti yang telah penulis kemukakan pada Bab III bahwa penyidik Polri dalam melakukan penyidikan mempunyai "Pedoman penyitaan&penanganan barang bukti elektronik". Mabes Polri saat melakukan penyidikan kejahatan komputer selama ini memperoleh bukti permulaan terhadap dugaan tindak pidana komputer selain dari keterangan saksi juga didapat dari *log file* dan beberapa contoh bukti digital lainnya yaitu:

- E-mail dan alamat e-mail.
- Word processor.
- Pesan dari chat room di internet.
- Source code dari software.
- Voice mail.
- File image digital.
- Web browser, book marks, cookies, dll.

Pada penjelasan pasal 117 ayat (1) huruf c RUU KUHAP yang dimaksud dengan bukti elektronik adalah:

> Informasi yang diucapkan, dikirim, diterima atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu,

termasuk setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan/atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana baik yang tertuang di atas kertas, benda fisik apapun selain kertas maupun yang terekam secara elektronik yang berupa tulisan, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Permasalahan yang timbul adalah sampai di mana bukti elektronik tersebut keabsahannya dapat dipertanggungjawabkan. alat bukti elektronik tersebut seringkali mendapatkan keberatan dari pihak-pihak yang beracara di pengadilan karena mereka mengalami keragu-raguan apakah alat bukti tersebut layak untuk dijadikan dasar dalam menuntut dan memutus sebuah perkara. Untuk menghindari keragu-raguan tersebut penyidik Polri telah mempunyai forensik komputer yang dapat menjelaskan asal dan keabsahan alat bukti elektronik tersebut.

Pada contoh kasus atas nama tersangka Joko (Bab III) dimana Penuntut Umum memberikan petunjuk (P-19) yang diberikan kepada penyidik terhadap permasalahan alat bukti yang dipergunakan antara lain:

(1) Agar ditambahkan ahli dari external Polri (Perguruan Tinggi atau profesional pada teknologi informatika).

(2) Agar ditanyakan kepada ahli tentang kegunaan dan cara kerja software komputer forensik EnCase versi 4 dan Forensik Tool Kit (FTK), Hardware Write Blocker, sebagaimana penjelasan ahli pada nomor 5.

Dari petunjuk yang diberikan oleh Penuntut Umum tersebut terlihat bahwa Penuntut Umum mengalami keragu-raguan akan keabsahan alat bukti elektronik yang diperoleh penyidik walaupun telah dilakukan audit forensik oleh Mabes Polri. Hal tersebut karena tidak adanya prosedur yang baku dalam menggunakan alat bukti elektronik. Pihak yang melakukan audit forensik harus merupakan lembaga yang telah terakreditasi sehingga hasil auditnya dapat dipercaya dan terdapat standarisasi yang jelas dan Saat ini belum ada aturan yang jelas yang mengatur hal tersebut.

Alat bukti yang berasal dari output komputer dapat dibagi dalam dua variasi yaitu pertama peraturan yang tidak mensyaratkan formalitas berkenaan dengan bukti dan kedua undang-udang mengadopsi beberapa macam bentuk pembuktian dalam menerima output komputer. Kelompok pertama tersebut terbagi dalam 3 kelompok yaitu pertana sistem yang meminta adanya suatu dokumen tertulis. Kedua sistem yang membuat daftar bentuk-bentuk bukti yang diterima dan yang ketiga adalah dalam praktek negara-negara *Common Law* yaitu *Hearsay evidence* dan *Best Evidence Rule* sebagai aturan untuk mengatur tentang penerimaan output komputer di Pengadilan. Untuk kelompok yang pertama adalah menggunakan pendekatan menyediakan seluruh jalan bagi penerimaan bukti dari *output* komputer di pengadilan.Pendekatan ini dilakkukan oleh Belanda, Jerman, Portugal dan Denmark.

Alat bukti elektronik (dalam perkara kejahatan komputer) adalah sebuah alat bukti yang tidak dapat dibaca atau dipahami oleh semua orang dan hanya oieh kalangan tertentu yang mempunyai keahlian khusus. Dengan demikian diperlukan keterangan ahli yang menerangkan perihal otentitaksi alat bukti tersebut sehingga dapat mendukung keabsahan bukti sebagai dasar dalam menuntut dan menjatuhkan putusan.

Rancangan KUHAP pada pasal 177 hanya menyebutkan jenis-jenis alat bukti dimana didalamnya terdapat tambahan alat bukti elektronik. Sedangkan pada penjelasan pasal tersebut juga hanya menyebutkan apa yang dimaksud dengan bukti elektronik. Pasal-pasal selanjutnya pada RUU KUHAP tidak menjelaskan bagaimana prosedur penggunaan alat bukti elektronik tersebut. Hal ini yang akan menyebabkan penggunaan alat bukti elektronik menjadi belum jelas dan tidak ada standarisasi untuk digunakan sebagai alat bukti. Dengan demikian pada RUU KUHAP belum terdapat peraturan yang mengatur tentang proses-proses yang harus dilakukan pada penggunaan sebuah bukti elektronik tersebut untuk dapat digunakan sebagai alat bukti di pengadilan.