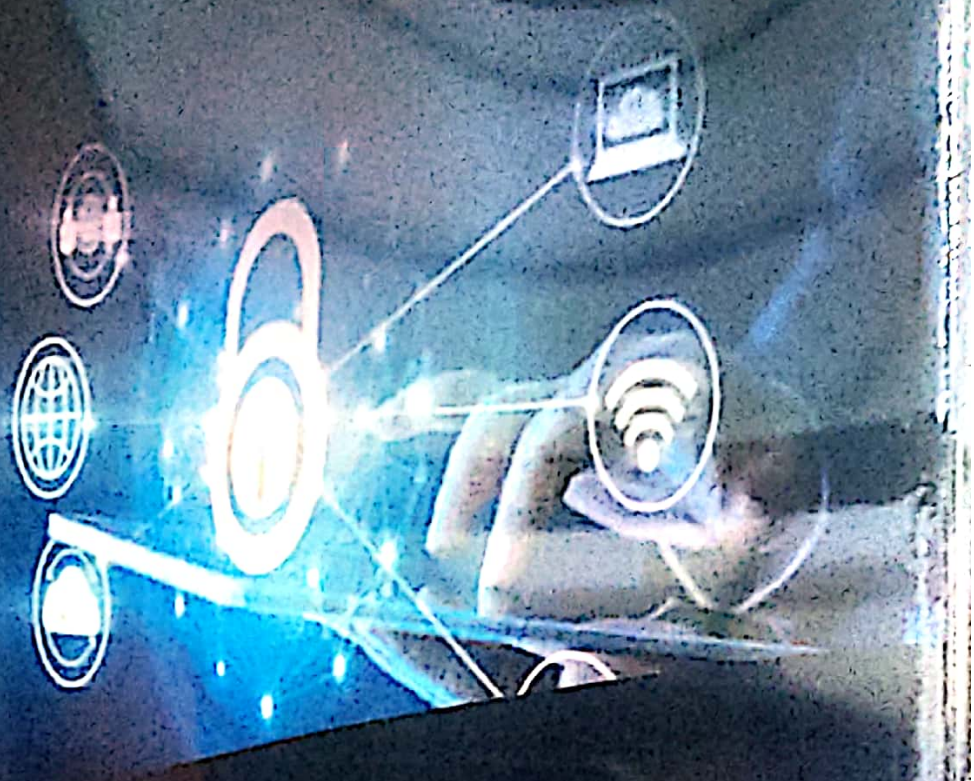
PENGANTAR HUKUM SIBER



PENULIS : IBRAHIM FIKMA EDRISY, S.H., M.H
Editor : Kamilatun, S.H., M.H

PENGANTAR
HUKUM SIBER

PENGANTAR
HUKUM SIBER

Penulis:
Ibrahim Fikma Edrisy, SH, MH

Editor :
Kamilatun S.H.,M.H

Sai Wawai
PUBLISHING

Perpustakaan Nasional RI:
Katalog Dalam Terbitan (KDT)

PENGANTAR HUKUM SIBER

Penulis:
Ibrahim Fikma Edrisy, SH, MH

Editor :
Kamilatun S.H.,M.H

Desain Cover & Layout
Team Aura Creative

Penerbit
Sai Wawai Publishing
Jl. Ashoka Blok Q7, Perumnas JSP Metro
saiwawai.publishing@gmail.com
Kerja sama dengan IAIN Metro - Lampung

x + 100 hal : 15.5 x 23 cm
Cetakan Pertama: Oktober 2019

ISBN: 978-602-60227-7-6

KATA PENGANTAR

Alhamdulillah puji syukur senantiasa penulis panjatkan kehadirat Allah Yang Maha Pengasih lagi Maha Penyayang, karena dengan pertolongan-Nya, penulis dapat menyelesaikan buku berjudul *Pengantar Hukum Siber*.

Buku ini harapannya dapat bermanfaat bagi mereka yang mempelajari ilmu hukum, baik bagi mahasiswa hukum sendiri, maupun bagi praktisi hukum atau sarjana hukum. Mengenal ilmu hukum merupakan pintu awal untuk mempelajari hukum secara lebih mudah. Buku ini juga telah berupaya untuk disesuaikan dengan perkembangan masyarakat karena hukum senantiasa berubah dan berkembang mengikuti kebutuhan masyarakat.

Pada kesempatan ini penulis menyampaikan rasa hormat dan terimakasih yang sebesar-besarnya kepada Suwardi, SH,MH Selaku Dekan Fakultas Hukum dan Ilmu Sosial Universitas Muhammadiyah Kotabumi, dan para kolega Dosen Fakultas Hukum dan Ilmu Sosial Universitas Muhammadiyah Kotabumi.

Ucapan terimakasih juga untuk keluarga penulis, ibunda, Ratnawati, S.Pd dan Ayahanda, Drs. H. Fikrie, ME, yang telah mengiringi langkah dan selalu mendoakan penulis. Kepada istri tercinta Siti Aisyah, SE., B.Econ. Kepada Ayuk dan adik-adikku, yang menemani dalam canda dan tawa.

Tidak lupa secara khusus ucapan terimakasih penulis sampaikan kepada editor yang telah berinisiatif sekaligus meluangkan waktu, pikiran dan tenaga untuk penerbitan buku ini.

Penulis menyadari bahwa dalam penulisan ini masih terdapat kekurangan untuk itu, penulis mengharapkan saran perbaikan, kritikan dari berbagai pihak yang sifatnya membangun. Akhirnya penulis berharap, semoga karya tulis ini dapat bermanfaat bagi kepentingan praktik maupun pengembangan ilmu hukum.

Kotabumi, Oktober 2019

Penulis

DAFTAR ISI

DAFTAR SINGKATAN

ATM	: Anjungan Tunai Mandiri
CERT	: *Computer Emergency Response Team*
IPTEK	: Ilmu Pengetahuan dan Teknologi
IDCERT	: *Indonesia Computer Emergency Response Team*
ISP	: *Internet Service Provider*
KUHAP	: Kitab Undang-undang Hukum Acara Pidana
KUHP	: Kitab Undang-undang Hukum Pidana
PBB	: Perserikatan Bangsa-Bangsa
PIN	: Personal Identification Number
TI	: Teknologi Informasi
UU ITE	: Undang-Undang Informasi dan Transaksi Elektronik

GLOSARI

Carding	:	Istilah yang menggambarkan perdagangan kartu kredit, rekening bank dan informasi pribadi lainnya secara online serta layanan penipuan yang terkait. Dengan kata lain carding adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet.
Cyber Crime	:	Aktivitas kejahatan di dunia maya dengan memanfaatkan jaringan komputer sebagai alat dan jaringan internet sebagai medianya.
E-commerce	:	Aktivitas penyebaran, penjualan, pembelian, pemasaran produk (barang dan jasa), dengan memanfaatkan jaringan telekomunikasi seperti internet dan jaringan komputer.

Locus delicti	:	Tempat terjadinya tindak pidana
Teknologi Informasi	:	Suatu studi perancangan, implementasi, pengembangan, dukungan atau manajemen sistem informasi berbasis komputer, khususnya perangkat keras (*hardware*) dan perangkat lunak (*software*). secara bahasa merupakan istilah dalam bidang teknologi apapun dalam kehidupan manusia yang bermanfaat untuk mengubah, membantu, mengkomunikasikan, menyimpan dan menyebarkan informasi.

BAB I
RUANG LINGKUP HUKUM SIBER

A. Pengertian Hukum Siber

Hukum Siber (*Cyber Law*) adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law of Information Techonology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual. Istilah hukum siber digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika diidentikan dengan "dunia maya" akan cukup menghadapi persoalan ketika terkait dengan pembuktian dan penegakan hukumnya. Mengingat para penegak hukum akan menghadapi kesulitan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu[1].

Cyber law sendiri adalah hukum yang khusus berlaku di dunia *cyber*. Secara luas *cyber law* bukan hanya meliputi tindak kejahatan di internet, namun juga aturan yang melindungi para pelaku *e*-commerce,*e-learning*, pemegang hak cipta, rahasia dagang, paten, *e-signature* dan masih banyak lagi. *Cyber law* erat lekatnya dengan dunia kejahatan.Hal ini juga didukung oleh

[1]Ramli, Ahmad M. *Cyber Law* dan Haki Dalam Sistem Hukum *Indonesia*, Bandung: Refika Aditama, 2006, hlm 11

globalisasi. Zaman terus berubah-ubah dan manusia mengikuti perubahan zaman itu.Perubahan itu diikuti oleh dampak positif dan dampak negatif.Ada dua unsur terpenting dalam globalisasi. *Pertama*, dengan globalisasi manusia dipengaruhi dan *kedua*, dengan globalisasi manusia saling mempengaruhi.[2]

B. Sejarah Hukum Siber

Perkembangan sejarah lahirnya Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas UndangUndang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik akan diuraikan secara singkat sebagai berikut :

1. Rekomendasi Perserikatan Bangsa-Bangsa (PBB) Tentang Kriminalisasi Cyberspace[3]

Kejahatan dunia maya antara "*virtual crime*" atau *cyber crime* sudah terjadi di Indonesia sejak tahun 1983 samapai saat ini dengan cara menyalahgunakan komputer. Komputer adalah alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmetika, dan penyimpanan. Barda Nawawi Arief mengemukakan bahwa pengertian kejahatan yang berhubungan dengan komputer sama dengan *cyber crime*. Secara terminologis, kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse*, *computer abuse*, *computer fraud*, *computer related-crime*, *computer assisted crime*, atau *computer crime*. Namun demikian, setiap negara belum tentu sama dalam menggunkan istilah tersebut, bahkan tidak konsisten.

Kejahatan siber merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para

[2]Sulaiman, Robintan. *Cyber Crimes*: *Perspektif E- Commerce Crime.* Pusat Bisnis Fakultas Hukum: Universitas Pelita Harapan, 2002, hlm 13
[3]Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Yogyakarta; Aswaja Pressindo, 2013, hlm. 101-105.

penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan komputer.Dapat disimpulkan bahwa kejahatan siber adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan.Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan.Indonesia sebagai negara hukum, selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum.

Karena hal itu, Indonesia selalu berusaha untuk melakukan pembaharuan Hukum Pidana, salah satunya dengan menerbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).Karena penyelenggaraan kegiatan dalam bidang teknologi yang berbasis komputer sangat penting bagi masyarakat dan rawan melakukan pelanggaran hak asasi manusia, maka dalam melakukan kriminalisasi, Indonesia dapat memperhatikan himbauan, anjuran, rekomendasi dari Perserikatan Bangsa-Bangsa.Berkaitan dengan kriminalisasi terhadap perbuatan yang berkategori kejahatan siber (*cyber crime*). PBB sendiri menentukan bahwa ketentuan pidana dalam perbuatan perundang-undangan setiap negara wajib melakukan perumusan ketentuan pidana secara jelas (*lex certa*).Dimana hal ini dilakukan dalam rangka memberikan perlindungan hukum bagi rakyat Indonesia, memberikan kejelasan, menjamin kepastian ketentuan hukum, agar tidak terjadi ambiguitas penafsiran.

Hal ini terungkap dalam International Review of Criminal Policy-United Nations Manual on The Prevention and Control of Computer-Related Crime sebagai berikut; The committe recommended six basic principles that should be taken into account by member States when enacting legislation in the field of computer-related criem privacy:

a) The protection of privacy against offences caused by modern computer technology is of great importance. However, this protection should be based primarily on administrative and civil law regulations. Recourse to criminal law should be made only

as a last. This means that criminal sanctions should be used only in cases of severe offences in which adequate regulation cannot be achieved by administrative or civil law measures (ultima ratio principle);

b) The respective criminal provisions must describe the forbidden acts precisely and should avoid vague general clauses. A precise description of illegal acts, without however resorting to a casuistic legislation technique, can easily be achieved, for example, for specific sensitive data;

c) The criminalized acts should be describe as clearly as possible by the respective penal law provisions;

d) Different computer-related infringements of privacy should not be criminaized im one global provision. The principle of culpability requires a differentiation according to the interests affected, the acts committed and the status of the perpetrator, as well as of his intended aims and other mental elements;

e) In principle, computer-related infringements of privacy should only be punishable if the perpetrator acts with intent;

f) Minor computer-related offences against privacy should be punished only in accordance with Council of Europe Recommendation No.(87)18 on the simplification of criminal justice, on complaint of the victim or of the Privacy Protection Commissioner or of the Privacy Protection Authority.

Berdasarkan ketentuan tersebut diketahui tentang enam prinsip dasar yang dapat digunakan untuk perancangan peraturan perundang-undangan yang mengatur kejahatan siber sebagai berikut;

a) Untuk melindungi kepentingan hukum yang berkaitan dengan teknologi informasi, hukum pidana merupakan sarana terakhir (ultimum remidium), karena pemanfaatan hukum administrasi dan hukum perdata lebih penting;

b) Ketentuan hukum pidana harus menguraikan perbuatan yang dilarang secara tepat, spesifik dan menghindari perumusan yang samar-samar. Ketentuan tersebut perlu dilakukan untuk menyeimbangkan antara perbuatan yang berkaitan dengan keleluasaan pribadi seseorang dengan kebebasan memperoleh informasi;

c) Dalam kriminalisasi perlu diuraikan secara jelas dalam ketentuan hukum pidana pada masing-masing negara. Oleh karena itu, perluasan ketentuan yang digunakan sebagai acuan yang belum jelas dan sulit dimengerti harus dihindari. Jika acuan eksplisit atau implisit digunakan untuk menerapkan hukum pidana, maka ketentuannya juga harus jelas;

d) Prinsip kesalahan pada si pembuat (asas kulpabilitas) dan tujuan suatu perbuatan kejahatan selalu dijadikan bagian dari unsur pertanggungjawaban pidana dalam kejahatan siber;

e) Kriminalisasi terhadap perbuatan yang dapat dipidana karena seseoang lalai melakukan suatu (delik omisionis), perlu didasari pada pertimbangan-pertimbangan yang mendalam;

f) Pelanggaran terhadap kebebasan pribadi merupakan delik aduan.

C. Bentuk Kejahatan Siber

1. *Unauthorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia.Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

2. *Illegal Contents*

   Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.Misalnya pemuatan suatu berita bohong atau fitnah yang mendiskreditkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan lain sebagainya.

3. *Data Forgery*

   Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

4. *Cyber Espionage*

   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized.*

5. *Cyber Sabotage and Extortion*

   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Pada beberapa kasus setelah hal tersebut terjadi, maka pelaku

kejahatan tersebut menawarkan diri kepada korban untukmemperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu.Kejahatan ini sering disebut sebagai *cyber-terrorism.*

6. *Offense Against Intellectual Property*

   Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain.

7. *Infringements of Privacy*

   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, informasi penyakit yang dirahasiakan dan sebagainya.

Cyber crime sendiri memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain: [4]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya

b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet

c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat,

[4]Deris Setiawan, *Sistem Keamanan Komputer,* PT Elex Media Komputindo, Jakarta, 2005, hlm. 40

kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional/ melintasi batas Negara

d, Pengaturan *Cyber crime* di Indonesia

Indonesia belum memiliki Undang-Undang khusus/*cyber law* yang mengatur mengenai *cyber crime* Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cyber crime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, diantaranya.[5]

a. Kitab Undang-Undang Hukum Pidana Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada cybercrime yaitu:

1. Pasal 362 KUHP yang dikenakan untuk kasus carding dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di Internet untuk melakukan transaksi di ecommerce. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.
2. Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada.Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

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

3. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.
5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet.Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luarnegeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang terlarang atau illegal.
7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus-kasus video porno para mahasiswa, pekerja atau pejabat publik.
8. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
9. Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta

Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/ software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah.Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp 20.000,00.Penjualan dengan harga sangat murah dibandingkan dengan software asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 per keping.Maraknya pembajakan software di Indonesia yang terkesan dimaklumi tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/ atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah)."

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau UndangUndang Nomor 11 Tahun 2008 jo Nomor 19 Tahun 2016Tentang Internet & Transaksi Elektronik

Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat,

tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para hacker yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: 1. Akses ke jaringan telekomunikasi 2. Akses ke jasa telekomunikasi 3. Akses ke jaringan telekomunikasi khusus Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id,11 maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)"

d. Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang Nomor 15 Tahun 2002 merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data

tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur BankIndonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan.

Di dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau digital evidence sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Dengan semakin pesatnya perkembangan teknologi informasi, maka perlu kiranya diperhatikan upaya penyempurnaan dan perbaikan Kitab Undang-Undang Hukum Pidana Nasional, yaitu:[6]

1. Semakin maraknya kejahatan-kejahatan baru yang timbul sebagai akibat dari kemajuan teknologi informasi (*cyber crime*), maka alat bukti yang diperlukan harus sesuai dengan perkembangan IPTEK, baik dengan penambahan alat bukti lain yang berbasis teknologi, seperti alat bukti berupa surat elektronik dan rekaman elektronik.
2. Salah satu ciri kejahatan di dunia maya (*cyber crime*) adalah memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. Aspek global menimbulkan kondisi seakan-akan dunia tidak ada batasnya *(borderless*) keadaan ini mengakibatkan pelaku, korban serta tempat dilakukannya

[6]Hinca IP Panjaitan dkk, *Membangun Cyber Law Indonesia yang Demokratis*, Jakarta : IMLPC, 2005,hlm 56-58

tindak pidana *(locus delicti)* terjadi dinegara yang berbeda-beda. Guna mengantisipasi hal tersebut maka pemberlakuan Kitab Undang-Undang Hukum Pidana harus diperluas, sehingga tidak hanya mengacu pada asas/ prinsip yang selama ini di anut dalam pasal 2-pasal 9 Kitab Undang-Undang Hukum Pidana yaitu asas personal, asas territorial, dan asas universal.

3. Untuk merumuskan dan menentukan perbuatan-perbuatan yang dapat dikenai sanksi pidana dalam dunia yang relative baru dan bergerak cepat, tentu bukan merupakan pekerjaan yang mudah. Oleh karena itu, untuk menjerat pelaku yang melakukan kejahatan-kejahatan di dunia maya (*cyber crime*), dapat digunakan lembaga penafsiran hukum (interpretasi). Hal ini dimaksudkan untuk menghindarkan timbulnya kekosongan hukum.

Ahmad P Ramli menjelaskan penentuan hukum yang berlaku, dikenal adanya beberapa asas yang dapat digunakan, yaitu :

a. *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum pidana ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.

b. *Objective territoriality*, yang menyatakan bahwa hukum yang berlaku adalah akibat utamanya perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.

c. *Nationality*, yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku tindak pidana.

d. *Passive nationality*, yang menekankan yurisdiksi berdasarkan kewarganegaraan dari korban kejahatan.

e. *Protective principle*, yang menyatakan bahwa berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan diluar

wilayahnya. Azas ini pada umumnya diterapkan apabila korbannya adalah negara atau pemerintah.

f. *Universality*, bahwa setiap negara berhak untuk menangkap dan menghukum pelaku kejahatan.

Munculnya kejahatan *cyber crime* merupakan suatu fenomena yang membutuhkan penanggulangan secara cepat dan akurat.Perubahan terhadap beberapa ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana merupakan salah satu cara yang dapat dipergunakan untuk mengatasi jenis kejahatan baru tersebut. Diharapkan dengan dilakukannya berbagai perubahan dalam Kitab Undang Hukum Pidana Nasional sebagai akibat dari timbulnya berbagai perubahan.

Beberapa contoh kasus siber yang terjadi Indonesia antara lain :

a. Pencurian dan penggunaan account Internet milik orang lain.Diantara kesulitan dari sebuah ISP (*Internet Service Provider*) adalah adanya account pelanggan mereka yang "dicuri" dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, "pencurian" account cukup menangkap "userid" dan "password" saja. Hanya informasi yang dicuri. Sementara orang yang kecurian tidak merasakan hilangnya "benda" yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunaan dibebani biaya penggunaan account tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.

b. Membajak situs web. Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya.

c. *Probing dan port scanning*. Salah satu langkah yang dilakukan cracker sebelum masuk ke server target yaitu melakukan pengintaian, dengan cara melakukan "port scanning" atau "probing" untuk melihat servisservis apa saja yang tersedia di server target. Misalnya, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server *Apache*, *mail server sendmail*, dan seterusnya. Analogi hal ini dengan dunia nyata yaitu dengan melihat-lihat apakah pintu rumah target terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.

d. Virus. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali sistem email seseorang yang terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat dilakukan.

e. *Denial of Service* (*DoS*) dan *Distributed DoS* (*DDos*) *attack*. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Aktifitas serangannya tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank termasuk nasabah dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan

serangan ini dengan melakukannya dari beberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

f. Kejahatan yang berhubungan dengan nama domain yang digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah *cyber squatting*. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat "domain plesetan", yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah *typo squatting*.

g. IDCERT (*Indonesia Computer Emergency Response Team*). Salah satu cara untuk mempermudah penanganan masalah keamanan dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya "sendmail worm" (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah *Computer Emergency Response Team* (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah keamanan. IDCERT merupakan CERT Indonesia .

h. Sertifikasi perangkat security. Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.

Mengingat kejahatan *e-commerce* merupakan salah satu kejahatan baru dan canggih, maka wajar dalam penegakan hukumnya masih mengalami beberapa kendala yang harus segera ditangani agar peluang pelaku kejahatan bisnis canggih dapat diatasi dan tidak dapat mengembangkan bakatkejahatannya di dunia maya khususnya kejahatan *e-commerce.* Meskipun demikian, ada kendala yang harus dipecahkan atau dicarikan solusinya diantaranya:

a. Pembuktian (bukti elektrik) Persoalan yang muncul, yaitu belum adanya kebulatan penafsiran terhadap kepastian dari alat bukti elektrik, dikarenakan alat bukti ini mudah sekali untuk di copy, digandakan atau bahkan dipalsukan, dihapus atau dipindahkan. Walaupun mengacu pada Pasal 5 Undang-Undang ITE telah jelas menyebutkan mengenai alat bukti ini, namun masih saja aparat penegak hukum mengalami kesulitan untuk mendapatkan alat bukti yang otentik.

b. Perbedaan Persepsi Perbedaan persepsi yang dimaksud yaitu bahwa terjadinya perbedaan antara penegak hukum dalam menafsirkan kejahatan yang terjadi dengan penerapan pasal-pasal dalam hukum positif yang berlaku sehingga menimbulkan ketidakpastian hukum bagi pencari keadilan.

c. Lemahnya penguasaan komputer Kurangnya kemampuan dan keterampilan aparat penegak hukum di bidang komputer yang mengakibatkan taktis, teknis penyelidikan, penuntutan dan pemeriksaan di pengadilan tidak dikuasai karena menyangkut sistem yang ada didalam komputer.

d. Sarana dan prasarana Fasilitas komputer mungkin memang ada di setiap kantor-kantor para penegak hukum, namun hanya berfungsi sebatasuntuk administrati, seperti mengetik saja, sedangkan kejahatan *e-commerce* ini dilakukan dengan menggunakan komputer yang berjaringan dan berkapasitas teknologi yang lumayan maju sehingga pihak aparat sulit untuk mengimbangi kegiatan para pelaku kejahatan tersebut.

e. Kesulitan Menghadirkan korban Terhadap kejahatan yang korbannya berasal dari luar negeri umumnya sangat sulit untuk

melakukan pemeriksaan yang mana keterangan saksi korban sangat dibutuhkan untuk membuat sebuah berita acara pemeriksaan.

Cyber crime membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Adapun langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cyber crime* adalah:[7]

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut

b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasiona

c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*

d. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya upaya pencegahan kejahatan agar tidak mudah terjadi.

e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyber space*, *Pertama* adalah pendekatan teknologi, *kedua* pendekatan sosial budaya-etika dan *ketiga* pendekatan hukum. Guna mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak.[8]

[7]http://budi.insan.co.id. *Keamanan Sistem Informasi Berbasis Internet*. Diakses 25 September 2019, pukul 15.30 WIB

[8]Ahmad Ramli, *Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, (Bandung: Fakultas Hukum Universitas Padjajaran, 2004), hlm. 2.

BAB II
ASAS TERITORIAL DAN ASAS NASIONAL AKTIF DAN PASIF

A. Latar Belakang Lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Jo Nomor 19 Tahun 2016

Kemajuan dunia elektronika berkaitan erat dengan perkembangan dunia internet. Secara harafiah, internet (kependekan dari *interconnected-networking*) ialah rangkaian komputer yang berhubungan satu sama lain.[9] Kebutuhan manusia akan informasi dan saling bertukar informasi untuk keperluan pribadi atau kelompok guna mencapai tujuan/kemajuan masing-masing. Dunia saat ini sudah semakin terkoneksi dan salah satu hal yang paling menarik dari keterkoneksian ini adalah internet sebagai dinamika dunia elektronika.[10]

Saat ini kemajuan teknologi dan informasi berjalan dengan sangat cepat.Adanya internet memungkinkan setiap orang mudah untuk mengakses informasi dan bertransaksi dengan dunia luar.Bahkan internet dapat menciptakan suatu jaringan komunikasi antar belahan dunia sekalipun.Kemajuan teknologi ini tentunya mempunyai dampak positif dan dampak negatif. Dampak positifnya antara lain mudahnya memperoleh informasi kapanpun dan dimanapun, meningkatkan perdagangan dan pertumbuhan ekonomi, menciptakan lapangan pekerjaan, dapat dimanfaatkan

[9] Darma, dkk, *Buku Pintar Menguasai Internet*, Jakarta:Mediakita, 2010, hlm.1
[10]Daryanto, *Memahami Kerja Internet*, Bandung:Rama Widya, 2004, hlm.10

sebagai mediapembelajaran dan sebagai media yang memungkinkan siapapun untuk berpartisipasi di dalamnya untuk keperluan apapun dan lain-lain.

Sedangkan dampak negatifnya yaitu membuka ruang terjadinya perdagangan gelap, penipuan dan pemalsuan, dan merusak moral bangsa melalui sitiu-situs tertentu, menurunkan rasa nasionalisme, penyalah gunaan yang tidak memandang nilai-nilai agama dan sosial budaya dapat menimbulkan perpecahan dan sebagainya.[11]

Di dalam pasal 3 UU ITE disebutkan bahwa pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik dan kebebasan memilih teknologi atau netral teknologi. Pasal 4 juga menyebutkan bahwa pemanfaatan teknologi informasi dan Elektronik dilaksanakan dengan tujuan untuk:

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
2. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
3. Meningkatkan efektivitas dan efisiensi pelayanan publik;
4. Membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi informasi seoptimal mungkin dan bertanggung jawab; dan
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.[12]

Pembangunan nasional adalah satu proses yang berkelanjutan yang harus senantiasa tanggap terhadap dinamika yang terjadi di masyarakat. Globalisasi informasi telah menempatkan Indonesia

[11] *Ibid.*
[12] *Ibid.*

sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan informasi dan transaksi elektronik di tingkat nasional, sehingga pembangunan teknologi dapat dilakukan secara optimal, merata,dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa.

Perkembangan dan kemajuan teknologi informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk perbuatan hukum baru. Penggunaan dan pemanfaatan teknologi informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan dami kepentingan nasional.

Pemanfaatan teknologi informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraanmasyarakat. Pemerintah perlu mendukung pengembangan teknologi informasi melalui instruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaan dengan memperhatikan nilai-nilai agama, sosial dan budaya masyarakat Indonesia.[13]

Berdasarkan pertimbangan di atas maka dibentuklah undang-undang tentang informasi, dan transaksi Elektronik.Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara Global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas *(borderless)* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara sigfinikan berlangsung demikian cepat teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan,

[13]lihat alasan menimbang Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

dan peradaban manusia, sekalius menjadi sarana efektif perbuatan melawan hukum.[14]

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konveregensi hukum telekomunikasi, hukum media, dan hukum informasi (*law of information technology*), hukum dunia maya (*virtual worldlaw*), dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang di lakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual.[15]

Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dua hal yang terkait dengan perbuatan hukum yang di laksanakan melalui sistem elektronik. Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik.[16]

Perangkat lunak atau program komputer adalah sekumpulan intruksi yang di wujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan merancang intruksi tersebut.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi

[14] Penjelasan atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik
[15] *Ibid*
[16] *Ibid*

informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasielektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukanya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatanya mencakup fungsi input, proses, output, storage, dan communication.[17]

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran atas dan normanya ketika menghadapi persoalan kebendaan yang tidak terwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana.Di dalam kenyataan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara yang mudah diakses kapanpun dan dari manapun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di internet.

Disamping itu, pembuktian merupakan faktor yang sangat penting mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk di rubah, disadap, dipalsukan, dan dikirim ke berbagai penjurudunia dalam waktu hitungan detik. Dengan demikian, dampak yang di akibatkannya pun bisa demikian kompleks dan rumit.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena dan transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (*electronic commerce*) telah menjadi bagian dari perniagaan nasional dan internasional.Kenyataan ini menunjukan

[17]Penjelasan atas undang-undang republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

bahwa konvergensi di bidang teknologi informasi, media, dan informarmatika (telematika) berkembang terus tanpa dapat di bendung, seiring dengan di temukannya, perkembangan baru di bidang teknologi, media, komunikasi.

Kegiatan melalui media sistem elektronik, yang di sebut juga ruang siber *(cyber space)*, meskipun bersifat virtual dapat di kategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat di dekati dengan ukuran dan kualifikasi hukum konvesional saja sebab jika cara ini di tempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual

berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain di kenal adanya dokumen elektronik yang kedudukanya di setarakan dengan dokumen yang di bauat di atas kertas.

Berkaitan dengan hal itu, perlu di perhatikan visi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agardapat berkembang secara optimal, oleh karena itu terdapat tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologika spek sosial, budaya dan etika, untuk mengatasi gangguan keamanan dalam menyelenggarakan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.[18]

Bangsa Indonesia telah memasuki babak baru dalam penggunaan teknologi dan informasi, terutama dengan di sahkanya Undang-Undang No.11 Tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) pada tanggal 21 April 2008. UU ITE mutlak diperlukan bagi Negara Indonesia, karena saat ini Indonesia

[18]Penjelasan atas UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

merupakan salah satu Negara yang telah menggunakan dan memanfaatkan teknologi secara luas dan efisien, namun belum memiliki Undang-Undang Cyber. Pelanggaran hukum dalam transaksi elektronik dan perbuatan hukum di dunia maya merupakan fenomena yang mengkhawatirkan, mengingat berbagai tindakan, seperti *carding*, *hacking*, *cracking*, *phising*, *viruses*, *cybersquating*, *pornografi*, *perjudian* (*online gambling*); *transnasional crime* yang memanfaatkan informasi teknologi sebagai ”tool” (alat), telah menjadi bagian dari aktifitas pelaku kejahatan internet.[19]

Cakupan materi UU ITE secara umum antara lain berisi: informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tanganelektronik, sertifikat elektronik, penyelenggaraan sistem elektronik, transaksi elektronik, hak atas kekayaan intelektual dan privasi. Adapun terobosan-terobosan yang penting dalam UU ITE ini adalah:

1. Tanda tangan elektronik diakui memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai)
2. Alat bukti elektronik diakui seperti alat bukti lainya yang di atur dalam KUHP maupun Hukum Acara Perdata.
3. Undang-Undang ITE, berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia.
4. Penyelesaian sengketa juga dapat di selesaikan dengan metode penyelesaian sengketa atau arbitrase.

Fakta menunjukan, masyarakat umum dan perbankan khususnya telah melakukan kegiatan transaksi yang seluruhnya menggunakan teknologi informasi sebagai alat (*tools*). Mengingat penggunaan transaksi elektronik ini terus meningkat, maka sangat diperlukan panyaring hukum untuk mengaturnya. Melalui UU ITE ini diharapkan dapat menjamin kepastian hukum bagi masyarakat yang melakukan transaksi elektronik, mendorong pertumbuhan

[19] *Ibid*

ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi.

B. Tempat dan Waktu Tindak Pidana

Locus delicti adalah tempat terjadinya tindak pidana, sedangkan yang dimaksud dengan tempus delicti adalah waktu terjadinya suatu tindak pidana.Guna menentukan *locus delicti* dan *tempus delicti* tidaklah mudah.Namun demikian, penyebutan secara tegas mengenai kedua hal ini sangat berperan penting bagi berbagai permasalahan yang terdapat dalam bidang hukum pidana.

Meskipun *locus delicti* dan *tempus delicti* ini tidak ada ketentuannya di dalam KUHP, *locus* dan *tempus delicti* tetap perlu diketahui. *Locus delicti* perlu diketahui untuk :

1) Menentukan apakah hukum pidana Indonesia tetap berlaku terhadap perbuatan pidana tersebut atau tidak, ini berhubungan dengan Pasal 2-8 KUHP
2) Menentukan kejaksaan dan pengadilan mana yang harus mengurus perkaranya, ini berhubungan dengan kompetensi relatif. [20]

Menurut Van Hamel yang dianggap sebagai locus delicti adalah:

1) Tempat di mana seorang pelaku itu telah melakukan sendiri perbuatannya.
2) Tempat di mana alat yang telah dipergunakan oleh seorang pelaku itu bekerja.
3) Tempat di mana akibat langsung dari sesuatu tindakan itu telah timbul.
4) Tempat di mana sesuatu akibat konstitutif itu telah diambil

[20]P.A.F Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, PT Citra Aditya Bakti, Bandung, 2011, hal. 180

Tempus delicti adalah penting karena berhubungan dengan:

1) Pasal 1 KUHP, untuk menentukan apakah perbuatan yang bersangkut paut pada waktu itu sudah dilarang dan diancam dengan pidana atau belum
2) Pasal 44 KUHP, untuk menentukan apakah terdakwa ketika itu mampu bertanggung jawab atau tidak
3) Pasal 45 KUHP, untuk menentukan apakah terdakwa ketika melakukan perbuatan sudah berumur 16 tahun atau belum, jika belum berumur 16 tahun, maka boleh memilih antara ketiga kemungkinan
4) Pasal 79 KUHP (verjaring atau daluarsa), dihitung mulai dari hari setelah perbuatan pidana terjadi
5) Pasal 57 HIR, diketahuinya perbuatan dalam keadaan tertangkap tangan *(opheterda)*.

C. Berlakunya Hukum Pidana Menurut Waktu

1. Asas Legalitas

Pada zaman Romawi kuno, suatu perbuatan dianggap tindak pidana dan jenis pidananya ditentukan raja, tanpa adanya aturan yang jelas perbuatan mana yang dianggap tindak pidana dan jenis pidana apa yang diterapkan. Hal ini dianggap kejam dan sangat bergantung kepada pendapat pribadi raja.

Oleh karena itu, pada saat memuncaknya reaksi terhadap kekuasaan raja yang absolut, ide asas legalitas dicetuskan oleh Montesqueau tahun 1748 (L'esprit des Lois) dan J.J. Rousseau tahun 1762 melalui karyanya (*Du Contract Social*) berupaya menghindari tindakan sewenang-wenang raja/penguasa terhadap rakyatnya. Asas ini pertama kali disebut dalam Pasal 8 *Declaration des droits de L'homme et du citoyen* (1789), sebuah undang-undang yang keluar pada tahun pecahnya Revolusi Perancis. Selanjutnya Napoelon Bonaparte memasukkan asas legalitas dalam Pasal 4 Code Penal dan berlanjut pada Pasal 1 WvS Nederland 1881 dan Pasal 1 WvSNI 1918.

Pasal 1 (1) KUHP mengatur asas legalitas tersebut sebagai berikut: "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelum perbuatan dilakukan". Anselm von Feuerbach.[21]dalam bukunya *Lehrbuch des peinlichen Recht* (1801) merumuskan asas legalitas dengan "*nullum delictum nulla poena siena praevia lege poenali*" (tidak ada tindak pidana, tidak ada pidana, tanpa undang-undang pidana yang mendahului) yang berkaitan dengan teori paksaan psikis yang dicetuskannya.

2. Konsekuensi Asas Legalitas Formil

Suatu tindak pidana harus dirumuskan/disebutkan dalam peraturan perundang-undangan agar berkonsekuensi:

a. Perbuatan seseorang yang tidak tercantum dalam undang-undang sebagai tindak pidana juga tidak dapat dipidana.

b. Ada larangan analogi untuk membuat suatu perbuatan menjadi tindak pidana. Peraturan perundang-undangan itu harus ada sebelum terjadinya tindak pidana.

Peraturan perundang-undangan itu harus ada sebelum terjadinya tindak pidana.Konsekuensi aturan pidana tidak boleh berlaku surut (retro aktif), dasar pikirannya:

a. Menjamin kebebasan individu terhadap kesewenang-wenangan penguasa.

b. Berhubungan dengan teori paksaan psikis dari Anselem von Feuerbach, bahwa si calon pelaku tindak pidana akan terpengaruhi jiwanya, motif untuk berbuat tindak pidana akan ditekan, apabila ia mengetahui bahwa perbuatannya akan mengakibatkan pemidanaan terhadapnya.

[21]PAF Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya, Bandung. 2011, hlm 12.

Di negara-negara yang menganut faham individualistis asas legalitas ini dipertahankan, sedangkan di negara yang sosialis asas ini banyak yang tidak dianut lagi.

4. Asas Legalitas Materiel

Menurut asas legalitas formil di atas, tidak ada perbuatan yang dilarang dan diancam dengan pidana kecuali telah ditentukan dengan aturan pidana.Hal ini menjadikan masalah, jika menurut hukum adat/masyarakat adat ada sebuah perbuatan yang menurut mereka kejahatan, namun menurut KUHP bukan kejahatan (dengan tidak dicantumkan di dalam KUHP).

Oleh karena itu dahulu Pasal 14 (2) UUDS 1950 telah menyebutkan aturan ini, bahwa asas legalitas meliputi juga aturan hukum tidak tertulis.Sedangkan di dalam KUHP hanya menggunakan kata-kata "...perundangundangan..." yang berarti bersifat asas legalitas formil (tertulis).[22]

Dengan tidak berlakunya lagi UUDS 1950, posisi hukum pidana adat/tidak tertulis tetap diakui. Hal ini di dasarkan pada:

a. Pasal 5 (3) sub b Undang-undang No. 1 Drt. 1951.

Bahwa suatu perbuatan menurut hukum yang hidup harus dianggap suatu perbuatan pidana, akan tetapi tiada bandingannya dalam Kitab HukumPidana Sipil, maka dianggap dengan hukuman yang tidak lebih tiga bulan penjara dan/atau denda lima ratus rupiah, yaitu sebagai hukuman pengganti bilamana hukuman adat yang dijatuhkan tidak diikuti oleh pihak yang terhukum dan penggantian yang dimaksud dianggap sepadan oleh hakim dengan dasar kesalahan si terhukum.Bahwa hukuman adat yang dijatuhkan itu menurut pikiran hakim melampaui padanya dengan hukuman kurungan atau denda yang dimaksud di atas, maka atas kesalahan terdakwa dapat dikenakan hukuman pengganti setinggi 10 tahun penjara, dengan pengertian bahwa hukuman adat yang menurut paham hakim tidak selaras lagi dengan zaman senantiasa diganti

[22]Ibid

seperti tersebut di atas. Bahwa suatu perbuatan menurut hukum yang hidup harus dianggap suatu perbuatan pidana dan yang ada bandingannya dalam Kitab Hukum Pidana Sipil, maka dianggap diancam dengan hukuman yang sama dengan hukuman bandingannya yang paling mirip kepada perbuatan pidana itu.

b. Pasal 27 ayat (1) Undang-undang No. 14 Tahun 1970 tentang Ketentuan-ketentuan Pokok Kekuasaan Kehakiman. “Hakim sebagai penegak hukum dan keadilan wajib menggali, mengikuti dan memahami nilai-nilai hukum yang hidup dalam masyarakat.”Dengan demikian, Indonesia yang mengakui hukum yang hidup yang tidak tertulis.Artinya tidak menganut asas legalitas formil secara mutlak, namun juga berdasar asas legalitas materiil, yaitu menurut hukum yang hidup/tidak tertulis/hukum adat.Artinya suatu perbuatan yang menurut hukum yang hidup/adat dianggap sebagai tindak pidana, walaupun tidak dicantumkan dalam undang-undang pidana, tetap dapat dianggap sebagai tindak pidana. Asas ini berdasar pada Pasal 5 (3) sub b Undang-undang No. 1 Drt. 1951 dan Pasal 27 (1) Undang-undang No. 14 Tahun 1970 tentang Ketentuan-ketentuan Pokok Kekuasaan Kehakiman tersebut di atas.

5. Asas Legalitas dalam Rancangan KUHP

Rancangan KUHP memperluas eksistensi hukum tak tertulis sebagai dasar patut dipidananya suatu perbuatan sepanjang perbuatan itu tidak ada persamaannya atau tidak diatur dalam perundang-undangan.Ini untuk mewujudkan asas keseimbangan antara kepentingan individu dengan kepentingan masyarakat dan antara kepastian hukum dengan keadilan. Pasal 1 (3) Konsep KUHP menyebutkan: “Ketentuan sebagaimana dimaksud dalam ayat (1) (tentang asas legalitas formil, pen.) tidak mengurangi berlakunya hukum yang hidup yang menentukan bahwa menurut adat setempat seseorang patut dipidana walaupun perbuatan tersebut tidak diatur dalam perundang-undangan.

6. Asas Temporis Delicti

Pasal 1 ayat (1) di samping mengandung asas legalitas juga mengandung asas *lex temporis delictie* yaitu tiap tindak pidana yang dilakukan seseorang harus diadili menurut ketentuan pidana yang berlaku saat itu.Jika terjadi perubahan perundangundangan pidana setelah tindak pidana itu dilakukan maka (Pasal 1 (2)) dipakailah ketentuan yang paling meringankan terdakwa.Konsep KUHP lebih memperinci perubahan undang-undang pidana tersebut.Perincian tersebut merupakan hasil perbandingan dengan KUHP Korea dan Thailand. Selengkapnya Pasal (3) Konsep KUHP menyatakan:

a. Jika terdapat perubahan undang-undangan sesudah perbuatan dilakukan atau sesudah tidak dilakukannya perbuatan, maka diterapkan peraturan perundangundangan yang paling menguntungkan.

b. Jika setelah putusan pemidanaan telah memperoleh kekuatan hukum tetap perbuatan yang dilakukan atau yang tidak dilakukan tidak lagi merupakan tindak pidana menurut peraturan perundang-undangan yang baru, maka narapidana dikeluarkan dari lembaga pemasyarakatan.

c. Jika setelah pitisan pemidanaan telah memperolejh kekuatan hukum tetap, perbuatan yang dilakukan atau yang tidak dilakukan diancam dengan pidana yang lebih ringan menurut peraturan perundang-undangan yang baru, maka putusan pemidanaan tersebut disesuaikan dengan batas-batas pidana menurut peraturan perundang-undangan yang baru

D. Asas Teritorial dan Asas Nasional Aktif dan Pasif

Pasal 1 ayat (1) dan ayat (2) KUHP mengatur berlakunya hukum pidana Indonesia menurut waktu (kapan dilakukannya tindak pidana), maka selanjutnya yang perlu diketahui adalah dimensi tempat atau dimana berlakunya hukum pidana Indonesia sekaligus juga terkait dengan bagi siapa hukum pidana itu diberlakukan.

Kekuatan berlakunya hukum pidana Indonesia menurut tempat ini diatur dalam Pasal 2 s.d. 9 KUHP yang kemudian dikelompokkan menjadi empat asas, yaitu asas teritorial, asas personal (nasional aktif), asas perlindungan (nasional pasif) dan asas universal.

1. Asas Teritorial atau Asas Wilayah

Asas teritorial mengajarkan bahwa hukum pidana suatu negara berlaku di wilayah negara itu sendiri.Asas ini merupakan asas pokok dan dianggap asas yang paling tua karena dilandaskan pada kedaulatan negara.Memang menjadi keniscayaan dan logis jika suatu ketentuan hukum suatu negara berlaku di seluruh wilayah negara itu.Asas teritorial dianut oleh Indonesia dan disebutkan dalam Pasal 2 dan 3 KUHP. Dalam Pasal 2, yang menjadi patokan adalah wilayah dan tidak mempersoalkan siapa yang melakukan tindak pidana di wilayah itu. Artinya, siapapun, baik orang Indonesia maupun orang asing, yang melakukan tindak pidana di dalam wilayah negara Indonesia maka diberlakukan hukum pidana Indonesia.

Berdasarkan Konvensi Paris 13 Oktober 1919, wilayah Indonesia meliputi tanah daratan, laut sampai 12 mil dan ruang udara di atasnya. Laut sampai 12 mil diukur dari titik pantai dari pulau-pulau terluar.Jika berbatasan langsung dengan Negara tetangga yang jaraknya kurang dari 24 mil, maka diambil titik tengah sebagai batasnya.Yang disebut sebagai wilayah Indonesia adalah wilayah Negara Indonesia sesuai dengan yang dimaksud pada waktu proklamasi kemerdekaan Indonesia yang meliputi seluruh bekas wilayah Hindia Belanda. Wilayah ini kemudian dikukuhkan dengan UU No. 7 Tahun 1976 yang memasukkan Timor Timur sebagai bagian dari wilayah Indonesia.

Pasal 3 KUHP kemudian memperluas berlakunya asas teritorial dengan memandang kendaraan air/perahu *(vaartuig)* sebagai ruang berlakunya hukum pidana.Pasal 3 ini tidak memperluas wilayah Indonesia.Arti harfiyah vaartuig adalah segala sesuatu yang dapat berlayar, yang dapat bergerak di atas air. Namun

berdasarkan hukum internasional, kendaraan air yang dapat diberlakukan asas teritorial ini adalah kapal perang dan kapal dagang Iaut terbuka yang diberlakukan *ius passagii innoxii* (ketentuan yang mengatur suatu kapal yang lewat secara damai di wilayah laut negara lain). Semula Pasal 3 KUHP tidak menyebut adanya kapal udara, karena saat KUHP dibentuk belum dikenal adanya pesawat udara. Namun dengan keluarnya UU Nomor 4 Tahun 1976 bunyi Pasal 3 ini kemudian diubah menjadi: Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang di luar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia.

2. Asas Personalitas atau Asas Nasionalitas Aktif

Asas personalitas bertumpu pada kewarganegaraan pelaku tindak pidana.Artinya, hukum pidana suatu negara mengikuti ke manapun warga negaranya. Dengan demikian, hukum pidana Indonesia akan selalu mengikuti warga Negara Indonesia ke mana pun ia berada.

Dalam KUHP, asas ini diatur dalam Pasal 5 s.d. 7. Pasal 5 ayat (1) ke-1 menentukan sejumlah pasal yang jika dilakukan oleh orang Indonesia di luar negeri maka diberlakukan hukum pidana Indonesia.Di sini tidak dipersoalkan apakah tindak pidana tersebut dianggap sebagai kejahatan menurut hukum pidana negara tempat orang Indonesia itu berada.Karena dianggap membahayakan kepentingan negara Indonesia, maka sejumlah pasal dalam Pasal 5 ayat (1) ke-1 tersebut tetap dapat diberlakukan hukum pidana Indonesia. Pasal 5 ayat (1) ke-2 menentukan bahwa hukum pidana Indonesia berlaku bagi warga negara Indonesia yang di luar Indonesia melakukan tindak pidana yang dianggap kejahatan bagi hukum pidana Indonesia dan di luar negeri tempat tindak pidana dilakukan diancam dengan pidana. Angka ke-2 ini bertujuan agar orang Indonesia yang melakukan tindak pidana kejahatan di luar negeri dan kemudian pulang ke Indonesia sebelum diadili di luar negeri tidak bebas dari pemidanaan.

Namun demikian, negara Indonesia tidak akan menyerahkan warganya diadili di luar Indonesia. Angka ke-2 ini juga membatasi bahwa yang dapat dipidana adalah yang masuk kategori kejahatan. Artinya, jika ada orang Indonesia yang melakukan tindak pidana di luar negeri kemudian pulang sebelum diadili di luar negeri, dan di Indonesia perbuatannya dianggap sebagai pelanggaran, maka tidak akan diadili di Indonesia. Ayat (2) dari Pasal 5 memperluas dalam hal penuntutan.Jadi, apabila ada orang asing yang melakukan tindak pidana di luar negeri kemudian melarikan diri ke Indonesia dan menjadi warga negara Indonesia, tidak membebaskan dia dari penuntutan pidana. Prinsip keseimbangan dalam asas ini ditunjukkan dalam Pasal 6, bahwa jika di negara tempat dilakukannya tindak pidana tidak diancam dengan pidana mati, maka ketika warga negara Indonesia itu melarikan diri ke Indonesia, di Indonesia juga tidak akan dipidana mati.

3. Asas Perlindungan atau Asas Nasional Pasif

Asas perlindungan menentukan bahwa hukum pidana suatu negara berlaku bagi perbuatan-perbuatan yang dilakukan di luar negeri, jika perbuatan tersebut melanggar kepentingan negara yang bersangkutan.Asas tersebut juga diberlakukan di Indonesia, sehingga hukum pidana Indonesia berlaku bagi tindak pidana yang menyerang kepentingan hukum negara Indonesia, baik yang dilakukan oleh warga negara Indonesia maupun bukan.

Asas perlindungan ini diatur dalam Pasal 4, 7, dan 8 KUHP, diperluas juga dengan UU Nomor 4 Tahun 1976 tentang Kejahatan Penerbangan dan UU Nomor 7 Drt Tahun 1955 tentang Tindak Pidana Ekonomi. Dalam KUHP, beberapa tindak pidana yang dikelompokkan ke dalam asas perlndungan adalah:

a. Kejahatan terhadap keamanan negara dan martabat Presiden (Pasal 104, 106, 107, 108, 110, 111 bis ke-1, 127, dan 131).
b. Kejahatan tentang merk atau materai yang dikeluarkan oleh pemerinta Indonesia.

c. Pemalsuan surat hutang atau sertifikat hutang atas beban Indonesia

d. Kejahatan jabatan (Bab XXVIII Buku II KUHP)

e. Kejahatan pelayaran (Bab XXIX Buku II KUHP).

Tindak pidana-tindak pidana tersebut dianggap menyerang kepentingan negara.Oleh karena itu, asas ini tidak berlaku jika terjadi pelanggaran terhadap kepentingan individu/pribadi warga negara di luar negeri.

4. Asas Universal

Asas ini diberlakukan demi menjaga kepentingan dunia/internasional, yaitu hukum pidana suatu negara dapat diberlakukan terhadap warga negaranya atau bukan, di wilayah negaranya atau di luar negeri.Di sini, hukum pidana diberlakukan melampaui batas kewilayahan dan personalitas.Siapapun dan di manapun tindak pidana dilakukan, hukum pidana Indonesia dapat diterapkan.

Beberapa kejahatan yang dapat diberlakukan hukum pidana Indonesia berdasarkan asas universal adalah:

a. Kejahatan mata uang yang dikeluarkan oleh negara tertentu (Pasal 4 sub ke-2 KUHP) yang didasarkan pada Konvensi Jeneva 1929.

b. Kejahatan perampokan/pembajakan di laut/udara (Pasal 4 sub 4 KUHP yang diperbaharui dengan UU Nomor 4 Tahun 1976 tentang Kejahatan Penerbangan) yang didasarkan pada Deklarasi Paris 1858, Konvensi Tokyo 1963, Konvensi The Hague 1970, dan Konvensi Montreal 1971.

Pada Pasal 9 disebutkan bahwa berlakunya Pasal 2-5, 7, dan 8 dibatasi oleh pengecualian-pengecualian yang diakui dalam hukum Internasional. KUHP tidak merinci hukum internasional mana yang membatasi pasal-pasal tersebut.Dengan demikian, aturan ini cukup luas karena dimungkinkan adanya perubahan- perubahan ketentuan berdasar pada hukum internasional.Pengecualian yang didasarkan pada hukum internasional ini adalah hak imunitas atau *exterritorialitas*. Hak imunitas adalah hak yang dimiliki oleh seseorang terhadap tuntutan pidana dari negara tempat ia melakukan tindak pidana. Hak imunitas ini didasarkan pada Perjanjian Wina 1961 yang dapat diberlakukan bagi:

a. Kepala negara asing dan keluarganya
b. Duta besar negara asing dan keluarganya
c. Anak buah kapal perang negara asing
d. Pasukan negara sahabat yang berada di wilayah negara atas persetujuan negara yang bersangkutan.

BAB III
KEJAHATAN SIBER

A. Kejahatan Teknologi Informasi

Perkembangan teknologi selain mambawa banyak manfaat dan keuntungan berupa semakin dipermudahnya hidup manusia, akan tetapi juga membawa nilainilai negatif misalnya sedemikain mudahnya para criminal melakukan tindak kejahatannya. Teknologi juga memberikan pengaruh yang cukup besar dalam pemahaman mengenai kejahatan terutama terhadap paham-paham dalam kriminologi yang menitikberatkan pada faktor manusia baik secara lahir maupun batin.Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulakan terjadinya kejahatan, sedangkan kejahatan itu sendiri telah ada dan timbul sejak kejahatan itu sendiri ada.[23]

Kejahatan sendiri merupakan perbuatan antisosial, tidak hanya terjadi dilingkungan masyarakat atau negara yang sedang berkembang, tetapi juga masyarakat atau negara yang sudah maju.Kejahatan terjadi tidak hanya terdapat dalam dunia nyata.Tetapi juga terdapat dalam dunia maya dengan formulasi yang berbeda dengan kejahatan konvensional karena semakin canggihnya teknologi.

Meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi (*cyber crime*), namun ada kesamaan pengertian universal mengenai kejahatan komputer, hal ini dapat

[23]Reda Manthovani, *Problematika & Solusi Penanganan Kejahatan Cyber di Indonesia*, Malibu,Jakarta, 2006, hlm 1

dimengerti karena kehadiran komputer yang sudah mengglobal mendorong terjadinya universalisasi aksi dan akibat yang dirasakan dari kejahatan komputer tersebut.secara umum yang dimaksud kejahatan komputer atau kejahatan didunia *cyber* adalah upaya untuk memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau diguakan tersebut.

Indra Safitri mengemukakan kejahatan dunia maya adalah jenis-jenis kejahatan yang berkaitan dengan pemanfaat sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dengan diakses oleh pelanggan internet.[24] Dengan demikian jelaslah bahwa jika seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer.

Kejahatan teknologi informasi yaitu komputer dan internet pada masa ini memang telah mewarnai pergaulan globalisasi kehidupan manusia.Kejahatan tersebut dapat timbul dari komputer maupun dari internet yang kita gunakan semagai media informasi dan kejahatan-kejahatan ini mengunakan teknologi informasi sebagai sasaran utama untuk mewujudkan niat tersebut.

B. Kejahatan Dengan Menggunakan Sarana Komputer dan Internet

Kejahatan teknologi informasi diawali dengan adanya komputer dan internet sebagai sarana manusia untuk menciptakan sesuatu inforamsi yang berguna bagi dirinya pribadi maupun orang

[24]Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime),* Refika Aditama, Bandung. 2005, hlm 40

lain. Dengan adanya komputer dan internet ini setiap orang yang menggunakan sarana ini dipaksa terus berpikir untuk menciptakan hal-hal baru untuk kesempurnaan isi dari komputer dan kemajuan serta kelengkapan materi internet tersebut dan terkadang melewati batas wajar manusia dan hal inilah yang menimbulkan kejahatan tersebut.

Istilah komputer sendiri berasal dari bahasa asing "computer" dengan kata dasar "to computer" yang berarti menhitung atau menaksir, namun dalam perkembangannya komputer memiliki fungsi yang lebih luas dari pada sekedar menghitung (*to calculate = calculator*). Sedangkan internet adalah jaringan komputer global atau jaringan yang menghubungkan jaringan komputer di seluruh dunia dengan menggunakan protokol komunikasi internet protokol.

Adanya internet dan komputer memungkinkan masyarakat untuk dapat berkomunikasi dalam bentuk yang lebih bervariasi, tidak seperti telepon yang hanya mampu menyampaikan suara, atau faksimili untuk text dan gambar saja.

Kenyataan bahwa internet adalah penting karena dapat mempermudah masyarakat untuk menemukan apa yang dicari dengan hanya memakai komputer atau internet tersebut keinginan itu terwujud. Ada berbagai definisi mengenai komputer, dari berbagai definsi tersebut setidaknya terungkap dua definisi yang dianggap paling mewakili cirri-ciri komputer:

a. Serangkaian atau kumpulan mesin elektronik yang bekerja bersama-sama dan dapat melakukan rentetan atau rangkaian pekerjaan secara otomatis melalui instruksi/program yang diberikan kepadanya.

b. Suatu rangkaian peralatan dan fasilitas yang bekerja secara elektronis, bekerja dibawah kontrol suatu operating systems melaksanakan pekerjaan berdasarkan rangkaian instruksi-instruksi yang disebut program, serta mempunyai internal storage yang digunakan untuk menyimpan system-sistem operasi, program dan data yang diolah.

C. Pengertian Penyalahgunaan Kartu Kredit

Salah satu gaya hidup global yang sedang berkembang adalah pengunaan kartu kredit. Dengan kartu kredit di tangan semua jadi mudah, gampang, dan cepat. Ketika berbelanja atau membeli tiket pesawat, membayar rekening dan tagihan, dan sebagainya, kini tidak perlu membwa uang dalam jumlah banyak. Kartu kredit merupakan sebuah gaya hidup dan bagian dari komunitas manusia untuk dapat dikatagorikan modern dalam tata kehidupan sebuah kota yang beranjak menuju metropolitan atau kosmopolitan.

Namun demikian, kehadiran kartu kredit sering disalahgunakan.Hal ini dapat ditinjau dari dua) aspek.*Pertama*, dari aspek hukum perdata dalam lingkup hukum perjanjian sebagai perbuatan wanprestasi.Misalnya, menggunkan kartu kredit secara tanpa hak dan tidak sebagaimana lazimnya, *Kedua*, dari sudut hukum pidana berupa kejahatan dengan menggunkan sarana kartu kredit, dikenal dengan istilah *carding* atau *card fraud.*

Pada perkembangannya penggunaan kartu kredit melahirkan apa yang dinamakan dengan Carding. Carding adalah kejahatan dengan menggunakan teknologi komputer untuk Carding adalah murni kejahatan lintas-negara *(trans-national crime)* karena dapat dilakukan oleh siapa saja dari belahan dunia yang berbeda dan sistem hukum yang berbeda pula. Carding sendiri merupakan penyalahgunaan kartu kredit dengan menggunakan internet dan komputer sebagai medianya dan di lakukan secara online dengan mencoba nomor-nomor yang ada dengan cara memalsukannya.[25]

Carding adalah penyalahgunaan kartu kredit menggunakan internet, carding merupakan triminologi yang biasa digunakan para hacker bagi perbuatan yang terkait penipuan menggunakan kartu kredit.Carding adalah triminologi yang digunakan hacker untuk

[25] *Ibid*

mendeskripsikan penggunaan informasi kartu kredit yang dicuri untuk membeli barang dan jasa.[26]

Jenis kejahatan ini, bila ditinjau dari segi sasarannya termasuk bentuk *cyber crime against property* atau jenis *cyber crime* yang sasaranya properti milik orang. Sedangkan dari modus operandinya, tergolong dalam *computer facilitated crime*, yaitu pola kejahatan umum menggunkaan komputer dalam aksinya.

[26]Johannes Ibrahim, *Kartu Kredit (Dilematis Antara Kontrak dan Kejahatan),* Refika Aditama, Bandung, 2004, hlm 1

BAB IV
PEMBUKTIAN HUKUM SIBER

A. Mekanisme Pembuktian Terhadap Perkara *Cyber crime*

Perkembangan internet dapat dikatakan pedang bermata dua, di satu sisi memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan sekaligus juga menjadi sarana efektif perbuatan melawan hukum. Para penekun bisnis online dari luar negeri bisa memanfaatkan kondisi ini untuk membuat target pasar ke Indonesia. Selain dampak positif, bahwa internet menimbulkan dampak negatif dengan munculnya peluang melakukan tindakan-tindakan anti sosial dan perilaku kejahatan.Kejahatan di bidang Informasi elektronik dan/atau transaksi elektronik dewasa ini sudah sangat memprihatinkan dan dampaknya sudah mengglobal.[27]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan undang-undang pertama di Indonesia yang secara khusus mengatur tentang *cyber crime* . Dua materi muatan yang cukup besar diatur didalam UU ITE ialah mengenai pengaturan transaksi elektronik dan mengenai tindak pidana siber (*cyber crime*).

Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional, yaitu UNCITRAL Model Law on Electronik Commerce, UNCITRAL Model Law on Electronik Signature, Convention on Cybercrime, EU Directives on Electronik

[27]Siwanto Sunarso, *Hukum Informasi dan Transaksi Elektronik*, PT.Asdi Mahasatya, Jakarta 2009, hlm.136

Commerce, dan EU Directives on Electronic Signature. [28]Ketentuan – ketentuan tersebut adalah instrumen internasional dan regional yang banyak diterapkan oleh negara-negara Eropa, Amerika, dan Asia.

Perkembangan teknologi telah mendorong perubahan prilaku, dan salah satunya adalah ketergantungan terhadap komputer (*computer dependency*).Disadari atau tidak, dengan teknologi yang sekarang, pengguna komputer dapat menyimpan atau mengirimkan informasi dalam berbagai bentuk dan dalam kualitas yang sangat banyak.Masyarakat tidak membutuhkan waktu yang lama untuk menerima informasi terbaru dari sanak keluarga yang berada ribuan kilometer jauhnya. Cukup dengan menggunakan email atau sms maka kabar terkinipun dapat diperoleh.[29]

Sekelumit mengenai kondisi yang terjadi dalam masyarakat ini dapat menimbulkan berbagai issu dalam menyelesaikan tindak pidana di bidang terknologi informasi. Kondisi yang seperti ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses,disimpan, atau dikirim secara elektronik. Informasi atau dokumen elektronik yang mudah diubah sering menimbulkan pertanyaan hukum mengenai keotentikan informasi atau dokumen yang dimaksud. Mudahnya seseorang menggunakan identitas apa saja untuk melakukan berbagai jenis transaksi elektronik di mana saja dapat menyulitkan aparat penegak hukum dalam menentukan identitas dan lokasi pelaku yang sebenarnya.[30]

Pertanyaan yang masih sering muncul di masyarakat umum, termasuk aparat penegak hukum ialah: apakah informasi atau dokumen elektronik dapat dijadikan alat bukti yang sah? Eksistensi alat bukti elektronik dalam sistem peradilan pidana di Indonesia dan bagaimana alat bukti elektronik tersebut dapat diterima dipersidangan sebagai alat bukti yang sah akan menjadi topik yang penting dalam penegakan hukum siber di Indonesia, terlebih setelah

[28]Josua Sitompul, *Cyberspace, Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, 2012, hlm.136
[29]Ibid, hlm.261
[30]Ibid, hlm.262

berlakunya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[31]

Secara umum, perbedaan antara informasi/dokumen elektronik dan surat/dokumen dalam bentuk konvensional terletak pada bentuk dan sifatnya. Selain itu, kemudahan memperoleh (*obtainability*), ketersediaan (*availability*), dan konten (*content*) merupakan pembeda lainnya. Informasi atau dokumen elektronik dapat dengan mudah diperoleh karena keduanya dapat dengan mudah dibuat dan dikirim secara instan dan penerima informasi atau dokumen dapat menerimanya dengan lebih cepat. Di lain pihak, informasi yang tertuang dalam kertas membutuhkan waktu yang lebih lama untuk mengirim dan memperolehnya – termasuk usaha dan biaya yang besar.[32]

Selain itu tidak seperti kertas yang membutuhkan tempat penyimpanan fisik yang lebih besar, informasi atau dokumen elektronik dapat tersimpan dalam media yang jauh lebih kecil untuk waktu yang jauh cukup lama. Pihak yang membutuhkan kertas tersebut akan memerlukan waktu yang lama untuk mencarinya, tetapi komputer yang ada saat ini telah dilengkapi dengan aplikasi pencarian file atau data.

Setiap pengguna internet dapat menggunakan mesin pencari (*search engine*) untuk memperoleh informasi yang dibutuhkan yang diperlengkapi dengan fitur-fitur untuk mencari informasi secara detail.Hal ketiga yang membedakan informasi atau dokumen elektronik dengan kertas ialah bahwa informasi atau dokumen elektronik dalam bentuk originalnya sering mengandung lebih banyak informasi yang penting yang tidak dapat ditemukan ketika informasi atau dokumen tersebut dicetak.[33]

Dalam peradilan pidana, pembuktian ialah upaya untuk menemukan kebenaran materiil (*materiel waarheid*) tentang telah terjadi suatu tindak pidana dan jelas siapa pelakunya.Untuk itu, aparat penegak hukum pada tingkat penyidikan, penuntutan,

[31] *Ibid*
[32] *Ibid,* hlm.97-99
[33] *Ibid*

maupun persidangan berusaha untuk kembali ke masa lalu untuk merekonstruksi rangkaian kejadian dan menemukan pelaku.Semua itu dilakukan berdasarkan fakta-fakta hukum yang tertanam dalam ingatan saksi-saksi, yang tertulis dalam dokumen-dokumen, yang tersimpulkan berdasarkan keterangan ahli, yang diakui oleh pelaku; fakta-fakta hukum tersebut juga dapat menjadi satu kesatuan dalam barang-barang bukti.[34]

Pembuktian dalam peradilan pidana di Indonesia, sebagaimana diatur dalam Pasal 183 KUHAP, menganut sistem pembuktian menurut Undang-Undang secara negatif (*negatief wettelijk stelsel*), maksudnya adalah bahwa kesalahan terdakwa harus dibuktikan berdasarkan Alat-alat bukti dan cara pembuktian yang diatur dalam undang-undang; dan Keyakinan hakim berdasarkan alat-alat bukti dan cara pembuktian tersebut. [35]

Kedua unsur diatas merupakan suatu kesatuan dimana seseorang tidak dapat dinyatakan bersalah hanya berdasarkan keyakinan hakim saja.Keyakinan hakim harus memiliki sumber, dan sumber itu ialah fakta-fakta hukum (peristiwa-peristiwa hukum yang terjadi mengenai atau terkait suatu tindak pidana dan pelaku tindak pidana) yang terkandung atau diberikan oleh alat bukti yang telah ditetapkan sebelumnya dalam undang-undang.Sebaliknya, walaupun alat bukti yang diajukan menunjukkan bahwa terdakwa bersalah, hakim tidak dapat menghukumnya tanpa ada keyakinan yang didasarkan pada alat bukti yang diajukan itu-fakta hukum yang direkayasa dan saksi dapat lupa peristiwa hukum yang terjadi, misalnya.[36]

Sistem pembuktian menurut Undang-Undang secara negatif (*negatief wettelijk stelsel*), mempunyai maksud sebagai berikut:

1. Untuk mempersalahkan seorang terdakwa (tertuduh) diperlukan suatu minimum pembuktian, yang ditetapkan dengan undang-undang;

[34]Josua Sitompul, *Op.Cit,* hlm.264-265
[35]R.Subekti, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, 2010, hlm 117
[36]*Ibid*

2. Namun demikian, biarpun bukti bertumpuk-tumpuk, melebihi minimum yang ditetapkan dalam undang-undang tadi, jikalau hakim tidak berkeyakinan tentang kesalahan terdakwa ia tidak boleh mempersalahkan dan menghukum terdakwa tersebut.[37]

Dengan demikian didalam sistem tadi, yang pada akhirnya menentukan nasibnya si terdakwa adalah keyakinan hakim. Jika, biarpun bukti bertumpuk-tumpuk hakim tidak yakin akan kesalahan terdakwa itu, ia harus membebaskannya. Karena itu, maka dalam tiap-tiap putusan hakim pidana, yang menjatuhkan hukuman, dapat kitabaca pertimbangan, "bahwa hakim, berdasarkan bukti-bukti yang sah, berkeyakinan akan kesalahan terdakwa.

Kitab Undang-Undang Hukum Pidana (KUHAP) sendiri mengatur secara limitatif mengenai alat bukti, yaitu: keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Semua alat bukti dinyatakan sah apabila telah memenuhi persyaratan formil dan materiil.Ketentuan dan persyaratan mengenai alat bukti yang diatur dalam KUHAP seperti yang dijelaskan di atas dimaksudkan agar alat bukti yang diajukan dipersidangan adalah alat bukti yang sah sehingga dapat digunakan di persidangan.[38]

Meski demikian KUHAP belum mengatur secara tegas mengenai alat bukti yang sah.Akan tetapi perkembangan peraturan perundangundangan setelah KUHAP menunjukkan adanya kebutuhan untuk mengatur alat bukti elektronik.Sampai saat ini ada beberapa peraturan perundang-undangan yang secara parsial telah mengatur eksistensi alat bukti elektronik. Pengaturan alat bukti pada peraturan perundang-undangan tersebut menunjukkan keberagaman, tetapi keberagaman tersebut telah diselesaikan dengan dikeluarkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.[39]

Pengaturan alat bukti elektronik dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[37] *Ibid*
[38] Josua Sitompul, *Op.Cit,* hlm.26
[39] *Ibid,* hlm.271

diatur dalam bab III tentang informasi, dokumen, dan tanda tangan elektronik, serta Pasal 44 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 5 ayat (1) UU ITE mengatur secara tegas bahwa informasi atau dokumen elektronik dan/hasilcetaknya merupakan alat bukti hukum yang sah. Lebih lanjut, Pasal 5 ayat (2) Undang-Undang ITE menegaskan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.[40]

Seperti yang telah dijelaskan sebelumnya bahwa dalam system pembuktian di Indonesia, kesalahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan keyakinan hakim.Keabsahan alat bukti didasarkan pada pemenuhan syarat dan ketentuan baik segi formil dan materiil. Prinsip ini juga berlaku terhadap pengumpulan dan penyajian alat bukti elektronik baik yang dalam bentuk original maupun hasil cetaknya, yang diperoleh baik melalui penyitaan maupun hasil cetaknya, yang diperoleh baik melalui penyitaan maupun intersepsi.

KUHAP telah memberikan pengaturan yang jelas mengenai upaya paksa penggeledahan dan penyitaan secaraumum, tetapi belum terhadap sistem elektronik.Akan tetapi, KUHAP belum mengatur mengenai intersepsi atau penyadapan, hal ini diatur dalam berbagai Undang-Undang yang lebih spesifik.Oleh karena itu, ketentuan dan persyaratan formil dan materiil mengenai alat bukti elektronik harus mengacu kepada KUHAP, UU ITE, dan undang-undang lain yang mengatur secara spesifik mengenai alat bukti elektronik tersebut.[41]

Sementara yang dimaksud dengan persyaratan materiil ialah ketentuan dan persyaratan yang dimaksudkan untuk menjamin keutuhan data (*integrity*), ketersediaan (*availability*), keamanan (*security*), keotentikan (*authenticity*), dan keteraksesan (*accessibility*). Informasi atau dokumen elektronik dalam proses

[40]Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime),*Rajawali Pers, Jakarta, 2012, hlm.100
[41]*Ibid*

pengumpulan dan penyimpanan dalam proses penyidikan dan penuntutan, serta penyampaiannya di siding pengadilan. Dalam hal ini dibutuhkan suatu cabang disiplin ilmu di bidang forensic komputer (*computer forensic*) atau forensik digital (digital forensic) yaitu : "*a branch of forensic science pertaining to legal evidence found in computers and digital storage media.* Cabang ilmu ini penting mengingat:

> Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.[42]

Persyaratan materiil alat bukti elektronik diatur dalam Pasal 5 ayat (3) UU ITE, yaitu informasi atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU Ite.Lebih lanjut sistem elektronik diatur dalam pasal 15 sampai dengan pasal 16 UU ITE dan dari kedua pasal ini, dapat diperoleh persyaratan yang lebih rinci yaitu bahwa sistem elektronik.[43]

a. andal,aman, dan bertanggung jawab;
b. dapat menampilkan kembali informasi atau dokumen elektronik secara utuh;
c. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik;
d. dilengkapi dengan prosedur atau petunjuk dan dapat beroperasi sesuai prosedur atau petunjuk yang telah ditetapkan tersebut.

[42] *Ibid*
[43] *Ibid*

Selain itu, pasal 6 UU ITE juga memberikan persyaratan materiil mengenai keabsahan alat bukti elektronik, yaitu bahwa informasi atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. UU ITE tidak mengatur perihal cara atau metode yang digunakan untuk mengumpulkan, mengamankan, menampilkan, atau menjamin keutuhan informasi alat bukti elektronik karena pada dasarnya, UU ITE menganut asas netral teknologi. Maksudnya, cara atau metode pengumpulan dan pengamanan alat bukti elektronik dapat menggunakan teknologi yang tersedia sepanjang dapat memenuhi persyaratan keabsahan alat bukti elektronik.

Sedangkan persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 UU ITE, yaitu:

1. Informasi atau dokumen elektronik tersebut bukanlah[44] :
    a. Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis;
    b. Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.
2. Penggeledahan atau penyitaan terhadap sistem elektronik harus dilakukan atas izin ketua Pengadilan Negeri setempat. [45]
3. Penggeledahan atau penyitaan tetap menjaga terpeliharanya kepentingan pelayanan umum.[46]

B. Keabsahan Alat Bukti Elektronik Dalam Perkara *Cyber crime*

Di dalam sistem elektronik yang digunakan telah memenuhi persyaratan tersebut, maka kualitas alat bukti elektronik dalam bentuk originalnya (informasi elektronik atau dokumen elektronik)

[44]Pasal 5 ayat (4) Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
[45]Pasal 43 ayat (3) Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
[46]Pasal 43 ayat (4) Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

dan hasil cetak dari informasi atau dokumen elektronik adalah sama. Dengan kata lain, polisi, jaksa, dan hakim dapat menggunakan keduanya atau salah satunya. Akan tetapi, perlu diingat pula bahwa dalam kasus-kasus tertentu ada kalanya penggunaan alat bukti elektronik lebih tepat dibandingkan penggunaan hasil cetak dari informasi atau dokumen elektronik karena informasi atau dokumen elektronik tersebut dapat memberikan informasi yang tidak dapat diberikan apabila informasi atau dokumen elektronik tersebut dicetak.[47]

Alat bukti elektronik yang mana yang digunakan?Apakah yang dalam bentuk originalnya ataukah yang telah dicetak?Hal ini tentunya dapat dilihat kasus per kasus. Salah satu contoh adalah dalam kasus perampokan yang terekam dalam kamera *cctv* maka dokumen elektronik yang terekam oleh cctv sebaiknya disajikan dalam bentuk originalnya. Video dapat berisi gambar bergerak dan bersuara. Penggunaan alat bukti dalam bentuk originalnya ini akan memudahkan aparat penegak hukum dalam memahami fakta hukum yang terekam dalam video tersebut. Aparat penegak hukum juga dapat mencetak setiap gerakan pelaku waktu melakukan aksi perampokan yang terekam, tetapi ini tentunya akan membutuhkan kertas yang sangat banyak sehingga tidak efektif.[48]

Akan tetapi, dalam kasus-kasus tertentu penggunaan hasil cetak dari informasi atau dokumen elektronik lebih memudahkan aparat penegak hukum dalam menyajikannya di persidangan.Salah satu contohnya adalah dalam tindak pidana pemerasan yang dikirimkan lewat SMS atau email.Dalam kasus seperti ini, penggunaan dan penyajian hasil cetak dari SMS atau email yang diperoleh dari suatu telepon genggam atau computer lebih memudahkan aparat penegak hukum dalam menilai fakta hukum.

Pada prinsipnya SMS atau email sama dengan tulisan, tetapi dalam bentuk elektronik. Oleh karena itu sepanjang SMS dalam handphone yang dimaksud sudah diperiksa integritas, ketersediaan, dan keotentikan atau keoriginalan serta relevansinya dengan kasus

[47]Josua Sitompul, *Op.cit,* hlm.285
[48]*Ibid,* hlm.286

yang diperkarakan, maka hasil cetak SMS itupun sudah cukup sebagai alat bukti. Polisi atau jaksa tidak perlu membawa, memperagakan serta menunjukkan SMS dalam handphone tersebut di persidangan karena akan membutuhkan waktu dan biaya yang lebih besar.

BAB V
UPAYA PENANGGULANGAN KEJAHATAN SIBER

A. Penegakan Hukum *Cyber Crime* dengan Sarana Penal

Kebijakan Penal adalah salah satu kebijakan dalam penanggulangan kejahatan dengan menggunakan hukum pidana. Kebijakan tersebut dioperasikan dengan cara menerapkan hukum pidana, yaitu pidana materiil, hukum formil dan penitentier dalam masyarakat.

Pada Kongres PBB ke-4 yang berlangsung di Kyoto disepakati bahwa usaha pencegahan kejahatan, termasuk penerapan hukum pidana merupakan bagian integral dari rencana pembangunan nasional. Kebijakan hukum pidana pada hakikatnya merupakan usaha untuk mewujudkan peraturan perundang-undangan pidana agar sesuai dengan keadaan pada waktu tertentu (ius constitutum) dan masa yang akan datang (ius constituendum).[49]Di dalam upaya menanggulangi kejahatan siber, resolusi Kongres PBB VIII/1990 mengenai *computer related crimes* mengajukan beberapa kebijakan antara lain:

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut;
   a) Melakukan modernisasi hukum pidana meateriil dan hukum acara pidana

[49]Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, 2013, Yogyakarta, hlm 188

b) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer

c) Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat penegak hukum, dan pengadilan terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer

d) Melakukan upaya-upaya pelatihan bagi para hakim, penegak hukum, pejabat mengenai kejahatan dibidang ekonomi dan kejahatan siber

e) Memperluas *rules of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika

f) Mengadopsi kebijakan perlindungan korban sesuai deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya kejahatan siber.

2. Menghimbau agar negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan kejahatan siber,

3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan PBB untuk;

   a) Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi kejahatan siber ditingkat nasional, ragional dan internasional,

   b) Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi permasalahan kejahatan siber dimasa mendatang,

   c) Mempertimbangkan kejahatan siber sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama dibidang penangulangan kejahatan.[50]

[50]Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, *Op.cit*, hlm. 3.

B. Penegakan Hukum *Cyber Crime* dengan Sarana Non-Penal

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut dikemukakan oleh Barda Nawawi Arief sebagai berikut:[51]

a. Sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana.

b. Hukum pidana hanya merupakan bagian kecil (subsistem) dari sarana control social yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemayarakatan yang sangat kompleks (sebagai masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya).

c. Penggunaan hukum pidana dalam menanggulangi kejahatan hanya merupakan "kurieren am symptom", oleh karena itu hukum pidana hanya merupakan "pengobatan simptomatik" dan bukan "pengobatan kausatif".

d. Sanksi hukum pidana merupakan "remedium" yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif.

e. Sistem pemidanaan bersifat fragmentair dan individual/ personal, tidak bersifat struktural/fungsional.

f. Keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif.

g. Bekerjanya/berfungsingnya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan memerlukan "biaya tinggi".

[51]Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, PT Citra Aditya Bakti, Bandung, 1998, hlm. 46-47.

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya.Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya.Untuk itu, pencegahan kejahatan tidak melulu harus menggunakan hukum pidana.Agar penegakan hukum *cyber crime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non-penal.

Resolusi Kongres PBB VIII/1990 mengenai *computer-related crimes* sebagaimana dikutip dari Barda Nawawi Arief menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:[52]

a. Melakukan Modernisasi hukum pidana material dan hukum acara pidana
b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
c. Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
d. Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime*
e. Memperluas *rule of ethics* dalam penggunaan computer dan mengajarkannya melalui kurikulum informatika
f. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime* .

[52]Barda Nawawi Arief,*Op. Cit.,* hlm. 238-239.

BAB VI
URGENSI PENGATURAN TEKNOLOGI INFORMASI

A. Faktor Perkembangan Teknologi dan Internet yang Cepat

Kemajuan teknologi dan internet yang merupakan hasil budaya manusia di samping membawa dampak positif, juga menimbulkan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif ini berkaitan dengan dunia kejahatan.Salah satu kejahatan yang ditimbulkan adalah kejahatan yang berkaitan dengan dunia internet, dalam istilah asing disebut dengan *Cyber crime* (kejahatan siber).[53]

Di Indonesia perkembangan kejahatan siber sudah mencapai tingkat yang memprihatinkan. Akibatnya, Indonesia dijuluki dunia sebagai negara kriminal internet. Pada tahun 2002, pihak Kepolisian Indonesia telah mengungkap 109 kasus tindak pidana Teknologi Informasi (TI) yang dilakukan oleh 124 orang tersangka yang notabene merupakan Warga Negara Indonesia yang melakukan aksinya di berbagai kota di Indonesia.

Secara garis besar, kejahatan yang berkaitan dengan teknologi informasi ini dibagi menjadi dua.*Pertama*, kejahatan yang bertujuan untuk merusak atau menyerang sistem atau jaringan komputer. *Kedua*, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan. Di dalam

[53]Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT RajaGrafindo Persada, 2012 , hlm. 3.

beberapa literatur dan siitus-situs yang mengetengahkan kejahatan siber, berpuluh jenis kejahatan siber yang terjadi. Sementara yang termasuk dalam kategori kejahatan umum yang difasilitasi teknologi antara lain penipuan kartu kredit, penipuan bursa efek, penipuan perbankan, pornografi anak, perdagangan narkoba, serta terorisme. Sedangkan kejahatan yang menggunakan teknologi informasi adalah *defacing*, *cracking*, ataupun *phreaking*.

B. Faktor Sosial dan Ekonomi

Kehadiran teknologi dan internet meskipun masih merupakan industri baru dan masih dalam fase pertumbuhan telah mengokohkan keyakinan tentang pentingnya teknologi dalam pencapaian tujuan finansial. Teknologi dan internet dapat dimanfaatkan untuk melakukan transaksi perdagangan, dan banyak situs di internet yang menawarkan jasa pemasangan iklan. Disamping manfaat yang diperoleh atas penggunaan teknologi dan internet ada kenyataan bahwa para pengusaha baru mulai membuat *net companies* setelah terinspirasi dari keberhasilan yang diraih oleh para pengusaha digital di berbagai negara maju.

Perkembangan teknologi dan internet ini terjadi diberbagai bidang kehidupan manusia terutama dibidang sosial dan ekonomi. Pergaulan hidup masyarakat modern saat ini lebih banyak di dunia virtual/maya dibandingkan dengan berinteraksi secara langsung dengan manusia lain. Pergeseran ini membuat masyarakat perlahan mulai meninggalkan dunia nyata dan menghabiskan waktu dengan berinteraksi dengan orang lain melalui internet dimana manusia lintas negara dapat saling terhubung. Dibidang ekonomi, saat ini di Indonesia sudah banyak berkembang berbagai transaksi melalui jaringan internet yang lebih memudahkan suatu transaksi tanpa bertemu secara langsung.[54]

Banyak aktifitas bisnis yang berkembang pada decade 2000-an dimana dinamika perdagangan dan bisnis industri perbankan

[54]Mansur, Dikdik M. Arif & Elisatris Gultom, *Cyber Law (Aspek Hukum Teknologi Informasi),* PT Refika Aditama, Bandung, 2005, hlm 143

melahirkan model transaksi yang eksistensinya lahir karena kemajuan teknologi dan internet di era globalisasi, yaitu *electronic commerce transaction* (*e-commerce*). E-commerce sendiri merupakan model bisnis modern yang *non-face* dan *non-sign* yang melakukan pertukaran data melalui internet dimana kedua belah pihak yaitu penjual dan pembeli melakukan transaksi. Saat ini, ecommerce sudah seperti gaya hidup di mana-mana termasuk di Indonesia.

Berkembangnya *e-commerce* diikuti pula dengan berkembangnya kejahatan teknologi canggih . Seiring waktu dikenallah istilah *cybank crime*, internet *banking crime*, *online business crime*, *cyber/electronic money laundering*, dan lain-lain.Kejahatan *e-commerce* tidak hanya ditujukan pada pencurian data, tetapi juga pada penggunaan, pengungkapan, penghapusan, perusakan data, atau bertujuan untuk menggangu atau merusak sistem transfer.Kejahatan yang terjadi pada transaksi ini tentu sangat merugikan baik dari aspek ekonomi, perbankan, politik dan keamanan nasional.[55]

C. Faktor Penegakan Hukum

Rasa aman tentu akan dirasakan oleh pelaku kejahatan siber saat melakukan aksinya.Hal ini terjadi karena internet lazim dipergunakan ditempat tertutup seperti rumah, kamar, tempat kerja, perpustakaan dan lain-lain. Aktivitas ini akan membuat orang lain sulit untuk diketahui oleh orang lain, sehingga orang lain jarang mengetahui bahwa seseorang itu sedang melakukan suatu tindak pidana kejahatan siber.

Hal ini tentu berbeda dengan kejahatan yang bersifat konvensional yang mana pelaku dapat diketahui karena melakukan aksinya secara fisik. Disamping itu, pelaku juga dapat menghapus jejak kejahatan yang telah dilakukannya mengingat internet menyediakan fasilitas untuk menghapus data/file yang ada.

[55]Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: PT Raja Grafindo Persada, 2006. hlm. 52.

Akibatnya pelaku sulit untuk ditangkap karena aparat penegak hukum sulit untuk menemukan alat bukti.

Faktor penegak hukum juga sering menjadi penyebab dari berkembangnya kejahatan siber itu. Hal ini dilatarbelakangi oleh sedikitnya aparat penegak hukum yang memahami tentang seluk beluk teknologi informasi, sehingga saat pelaku ditangkap mereka kesulitan untuk mencari bukti-bukti untuk menjerat pelaku. Terlebih bila kejahatan siber yang dilakukan memiliki sstem pengoperasian yang sulit untuk dimengerti. Dengan demikian peningkatan kualitas dari aparat penegak hukum sangat diperlukan untuk dapat menangani berbagai kejahatan siber yang saat ini marak terjadi dan berkembang.[56]

[56] *Ibid*

DAFTAR PUSTAKA

Buku :

Abdul Wahib, dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung.

Ahmad Ramli, 2004, *Prinsip-prinsip Cyber Law dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran, Bandung,

Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT Raja Grafindo Persada, Jakarta,

Barda Nawawi Arief, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, PT Citra Aditya Bakti, Bandung

Budi Suhariyanto,2012,*Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, PT RajaGrafindo Persada, Jakarta

Deris Setiawan, 2005, *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta,

Darma, dkk, 2010, *Buku Pintar Menguasai Internet*, Mediakita, Jakarta,

Daryanto, 2004, *Memahami Kerja Internet*, Rama Widya, Bandung,

Hinca IP Panjaitan dkk,2005, *Membangun Cyber Law Indonesia yang demokratis*, IMLPC, Jakarta

Mansur, Dikdik M. Arif & Elisatris Gultom, 2005, *Cyber Law* (*Aspek Hukum Teknologi Informasi*), PT Refika Aditama, Bandung

Johannes Ibrahim, 2004 *Kartu Kredit (Dilematis Antara Kontrak dan Kejahatan)*, Refika Aditama, Bandung,

Ramli, Ahmad M, 2006 *Cyber Law* dan Haki Dalam Sistem Hukum *Indonesia*, Refika Aditama, Bandung

R.Subekti, 2010, *Hukum Pembuktian*, Pradnya Paramita, Jakarta,

Reda Manthovani, 2006, *Problematika & Solusi Penanganan Kejahatan Cyber di Indonesia*, Malibu, Jakarta

Sulaiman, Robintan, 2002, *Cyber Crimes*: *Perspektif E- Commerce Crime*. Pusat Bisnis Fakultas Hukum: Universitas Pelita Harapan, Jakarta

Siwanto Sunarso, 2009, *Hukum Informasi dan Transaksi Elektronik*, PT.Asdi Mahasatya, Jakarta

Josua Sitompul,2012, *Cyberspace*, *Cybercrime Cyberlaw Tinjauan Aspek*

Hukum Pidana, Tatanusa, Jakarta

P.A.F Lamintang, 2011, *Dasar-Dasar Hukum Pidana Indonesia*, PT Citra Aditya Bakti, Bandung

Widodo,2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta

Undang-Undang :

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang No 19 Tahun 2002 tentang Hak Cipta

Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Internet :

http://budi.insan.co.id. Keamanan Sistem Informasi Berbasis Internet. Diakses 25 September 2019, pukul15.30 WIB

INDEKS

TENTANG PENULIS

Ibrahim Fikma Edrisy, SH, MH, lahir di Kotabumi, 25 Oktober 1992. Menyelesaikan Sarjana Hukum dari STIH Muhammadiyah Kotabumi Lampung (2010) dan Magister Hukum diperoleh dari Universitas Lampung (2014). Sebelumnya ia pernah menjadi Kasubbag UKA (Umum, Kemahasiswaan, dan Alumi) (2017), Kasubbag Keuangan (2018). Dan Sekretaris Unit Penelitian Pengabdian Masyarakat (UPPM) (2019). Pada program S1 mengasuh mata kuliah Hukum Siber, Kriminologi, dan Pengantar Sosiologi. Jabatan Akademik penulis saat ini adalah Asisten Ahli