Dr. Sahat Maruli T. Situmeang, S.H., M.H.

CYBER LAW

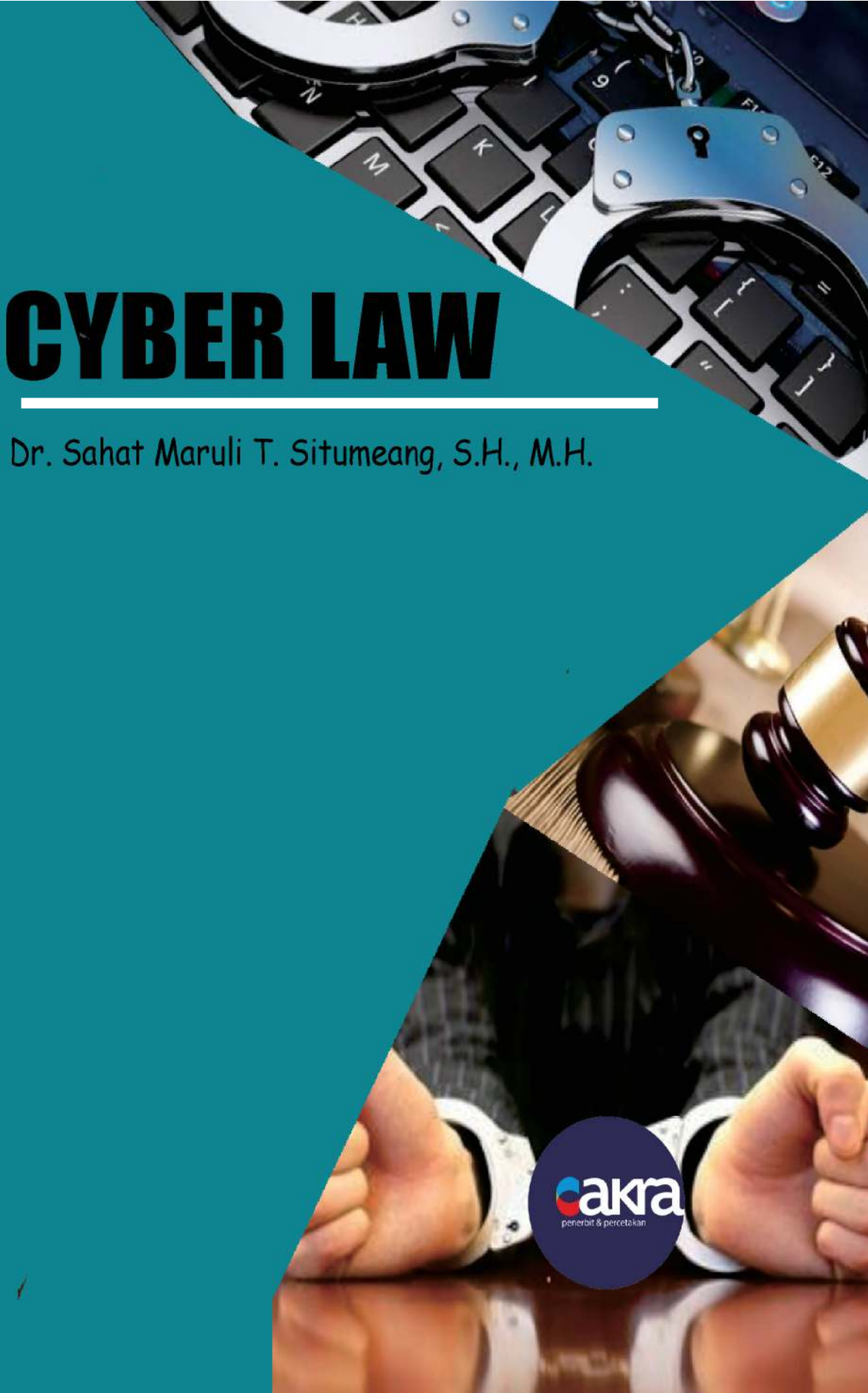
Buku ini menjelaskan tentang cyber law yaitu kejahatan didunia maya melalui jaringan internet .pada mata kuliah ini diberikan pengetahuan terkait cyber law, dengan begitu mahasiswa dapat memperoleh pengetauan tentang cyber law secara garis besar dan melalui mata kuliah ini mahasiswa dapat memperoleh manfaat teoritis dan praktis.

akra
penerbit & percetakan

ISBN 978-623-6868-06-5
9 786236 868065

Dr. Sahat Maruli T. Situmeang, S.H., M.H. CYBER LAW

akra



CYBER LAW

Dr. Sahat Maruli T. Situmeang, S.H., M.H.

akra
penerbit & percetakan

CYBER LAW

Dr. Sahat Maruli T. Situmeang, S.H., M.H.

CYBER LAW

PENERBIT CAKRA

Katalog dalam terbitan

CYBER LAW

Dr. Sahat Maruli T. Situmeang, S.H., M.H

-Ed. I. –Cet, 1
-Bandung : Penerbit Cakra 2020

1 jil., xx + 112 hlm.: 17 cm x 25 cm

ANGGOTA IKAPI

ISBN 978-623-6868-06-3

Cetak pertama

November 2020

Diterbitkan Oleh:
CV.Cakra

KANTOR BOJONG MALAKA INDAH

D4 NO 90
Percetakan jalan jati mekar No.01
Telp./Faks. 022-85934522
081221122.073
Penerbit.cakra@gmail.com
cakrabooks90@yahoo.com
www.cakraoffset.co.id

CYBER LAW
Dr. Sahat Maruli T. Situmeang, S.H., M.H

DAFTAR ISI

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadapan Tuhan Yang Maha Esa karena atas berkat rahmat-Nya, penyusun dapat menyelesaikan bahar ajar mata kuliah *Cyber Law* ditengah-tengah kesibukan menjalankan aktifitas sebagai dosen maupun sebagai lawyer. Rampungnya penulisan buku ajar ini diharapkan dapat membantu pemahamam mahasiswa tentang *cyber law* baik pada program ilmu hukum maupun di luar disiplin ilmu hukum. Penulisan buku ajar ini diharapkan dapat membantu ketersediaan akan bahan ajar dan menambah bahan referensi agar mahasiswa dapat memahami ruang lingkup *cyber law* yang memiliki karakteristik khusus. Penyusun menyadari bahwa penyusun memiliki keterbatasan-keterbatasan, baik itu menyangkut keterbasan akan materi maupun hal-hal lainnya yang dapat menunjang penyusunan buku ajar ini. Maka untuk kesempurnaan buku ajar ini, besar harapan penyusun kepada semua pihak agar dapat memberikan masukkan, kritik dan saran. Akhir kata, bagi semua pihak yang telah membantu dan memberikan dorongan moril dalam penyusunan buku ini, dengan kerendahan dan ketulusan hati, penyusun menyampaikan ucapan terima kasih yang sebesar-besarnya

Bandung, Juni 2020

Penyusun,

Dr. Sahat Maruli T. Situmeang, SH., MH.

PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi yang dihasilkan peradaban manusia senantiasa selalu berubah dan meningkat sehingga berdampak pada perilaku masyarakat modern yang tidak terlepas dari teknologi yang dapat meningkatkan kesejahteraan masyarakat dengan tetap memperhatikan kepastian, keadilan dan kemanfaatan hukum.

Perkembangan ilmu pengetahuan dan teknologi yang pesat ini diikuti pula dengan penyalahgunaan teknologi informasi, sehingga diperlukan upaya pencegahan dan penindakan pelaku kejahatan *cyber*. Berbagai implikasi kompleks dalam kehidupan manusia seiring perkembangan ilmu pengetahauan serta adanya beberapa kasus *cyber crime* tersebut seperti pencurian kartu kredit, *hacking, e*-commerce, pencurian data pribadi dan lain-lain memerlukan penanganan yang serius. Berdasarkan hal tersebut, penegakan hukum merupakan hal yang tidak dapat diremehkan, karena dapat berakibat pula terhadap stabilitas negara. oleh karenanya, penciptaan terhadap rasa aman merupakan tanggungjawab semua pihak, yaitu Pemerintah, penegak hukum dan masyarakat (baik konsumen maupun pelaku usaha atau baik individu maupun korporasi).

Bahwa *cyber crime* memiliki karakteristik khusus dibandingkan dengan kejahatan konvensional lainnya, yaitu mengenai ruang lingkup kejahatan, sifat kejahatan, pelaku kejahatan, modus kejahatan dan jenis kerugian yang ditimbulkannya. Pembahasan mengenai ruang lingkup *cyber law* dimaksudkan sebagai inventarisasi terhadap aspek-aspek hukum yang berkaitan dengan dunia maya melalui pemanfaatan internet.

Secara umum, setelah mempelajari buku ajar ini, mahasiswa diharapkan dapat menjelaskan ruang lingkup *cyber law*, diantaranya mahasiswa mampu menjeleskan tentang :

1. Istilah dan pengertian *cyber law;*
2. Sejarah keberadaan *cyber law;*
3. Perkembangan *cyber law* di Indonesia;
4. Sumber hukum *cyber law;*
5. Karakteristik *cyber law;*
6. Jenis-jenis *cyber law;*
7. Faktor pendorong terjadinya *cyber crime;*
8. *Cyber crime* sebagai kejahatan transnasional;
9. Penegakan hukum tindak pidana *cyber crime;*
10. Pembuktian dalam *cyber crime;*
11. Hubungan perlindungan konsumen dengan *cyber law* meliputi pengertian, dasar hukum, asas dan tujuan;
12. *E-commerce.*

Selain istilah *cyber law* ada juga yang menggunakan istilah hukum telematika. Dalam buku ajar ini, istilah yang digunakan adalah *cyber law.*

PENDAHULUAN

BUKU AJAR CYBER LAW

I. IDENTITAS MATA KULIAH

Nama Mata Kuliah	: *Cyber Law*
Kode Mata Kuliah	: 16119
SKS	: 3 (Tiga) SKS
Prasyarat	: Hukum Pidana
Semester	: VII (Tujuh)
Status	: Wajib Fakultas

II. DESKRIPSI SUBSTANSI PERKULIAHAN

Mata kuliah *Cyber law* merupakan mata kuliah unggulan di Fakultas Hukum Universitas Komputer Indonesia karena memiliki dosen tetap yang merupakan dosen yang ahli dan spesialisasi di bidang *cyber crime*. Pada mata kuliah ini diberikan pengetahuan-pengetahuan terkait istilah dan pengertian *cyber law*, sejarah keberadaan *cyber law*, perkembangan *cyber law* di Indonesia, sumber hukum *cyber law*, karakteristik *cyber law*, jenis-jenis *cyber law*, faktor-faktor pendorong terjadinya *cyber crime, Cyber crime* sebagai kejahatan transnasional, penegakan hukum tindak pidana *cyber crime*, pembuktian dala *cyber crime*, hubungan perlindungan konsumen dengan *cyber law* meliputi : pengertian, dasar hukum, asas dan tujuan dan *e-commerce.*

III. CAPAIAN PEMBELAJARAN

Dengan konsep dan pemahaman substansi mata kuliah *Cyber Law* mahasiswa memperoleh pengetahuan mengenai *Cyber Law* secara garis besar. Konsep pembelajaran *cyber law* telah disesuaikan dengan Rencana Pembelajaran Semester (RPS). Adapun dengan mempelajari dan memahami buku ajar ini diharapkan materi yang diberikan dapat dikuasai oleh mahasiswa mengenai *cyber law* secara umum baik

mengenai perkembangan hukum *cyber law*, penegakan hukum *cyber law* serta hubungannya dengan ilmu hukum lainnya.

IV. MANFAAT MATA KULIAH

Melalui mata kuliah ini mahasiswa dapat memperolah manfaat teoritis dan praktis. Manfaat teoritis, mahasiswa dapat mengetahui dan mendalami materi-materi dalam *cyber law*, khususnya mengenai : istilah dan pengertian *cyber law*, sejarah keberadaan *cyber law*, sumber hukum *cyber law*, asas-asas *cyber law*, *cyber crime, Cyber Crime* sebagai kejahatan transnasional, pemberantasan dan penangangan cyber crime melalui perluasan alat bukti, kaitan antara Hak Kekayaan Intelektual dengan *cyber law*, perlindungan konsumen dalam transaksi e-commerce. Cyber Law merupakan salah satu kuliah yang sangat penting dalam dunia saat ini, sehingga sevara teoritis mahasiswa dapat memperoleh pemahaman yang luas mengenai *cyber law*. Secara praktis, dengan pemahaman mengenai *cyber law* mahasiswa akan mampu menganalisa dan memcahkan permasalahan atau kasusu-kasus yang terdapat dalam ruang lingkup *cyber law* khususnya *cyber crime* yang terjadi di dalam lingkungan masyarakat.

V. ORGANISASI MATERI

Materi kuliah terdiri dari beberapa pokok bahasan, yang dapat digambarkan sebagai berikut :

Pendahuluan :

- Istilah dan Pengertian *Cyberlaw*
- Sejarah Keberadaan *Cyberlaw*
- Sejarah Perkembangan *Cyberlaw* di Indonesia

Sumber Hukum *Cyberlaw* :

- Konvensi atau Perjanjian Internasional
- Hukum Positif di Indonesia

***Cybercrime* :**

- Pengertian dan Karakteristik *Cyber Crime*
- Jenis-Jenis *Cyber Crime*
- Faktor Pendorong Terjadinya *Cyber Crime*

Cyber Crime Sebagai Kejahatan Transnasional :

- Pengertian Kejahatan Transnasional
- Yurisdiksi Suatu Negara dalam Kejahatan Transnasional
- Hukum Pidana Indonesia dalam *Cyber Crime*
- Penegakan Hukum Tindak Pidana *Cyber Crime*

Pemberantasan Dan Penanganan Cybercrime Melalui Perluasan Alat Bukti

- Alat Bukti dalam Sistem Hukum Pembuktian di Indonesia
- Asas-Asas dalam Pembuktian
- Alat Bukti Elektronik dalam *Cyber Crime*

Kaitan Antara Haki Dengan *Cyber Law*

- Pengertian Hak Kekayaan Intelektual
- Pengaturan Hak Kekayaan Intelektual
- Ruang Lingkup Hak Kekayaan Intelektual
- Perlindunagn HaKI dalam *Cyber Law*

Perlindungan Konsumen Dalam Transaksi E-Commerce

- Pengertian Perlindungan Konsumen
- Dasar Hukum Perlindungan Konsumen
- Asas-Asas dan Tujuan Perlindungan Konsumen
- Pengertian Transaksi E-Commerc
- Undang-Undang Perlindungan Konsumen dalam Mengakomodasi Transaksi E-Commerce

-

VI. METODE, STRATEGI, DAN PELAKSANAAN PROSES PEMBELAJARAN

1. Metode Pembelajaran

Metode pembelajaran adalah *Problem Based Learning* (PBL), pusat pembelajaran ada pada mahasiswa. Metode yang diterapkan adalah "belajar" bukan "mengajar". Dosen memfasilitasi mahasiswa untuk belajar.

2. Strategi Pembelajaran

Kombinasi perkuliahan 50% (6 kali perkuliahan) dan Tutorial (6 kali pertemuan tutorial). Satu kali pertemuan untuk Ujian Tengah semester (UTS) dan satu kali pertemuan untuk Ujian Akhir Semester (UAS).

3. Pelaksanaan Perkuliahan dan Tutorial

a. Strategi dan Teknik Perkuliahan

Perkuliahan tentang sub-sub pokok bahasan dipaparkan dengan alat bantu media papan tulis, power point slide, serta penyiapan bahan bacaan tertentu yang dipandang sulit diakses oleh mahasiswa. Sebelum mengikuti perkuliahan mahasiswa sudah mempersipakan diri, mencari bahan yang akan dibahas pada saat perkuliahan sesuai dengan arahan dalam Rencana Pembelajaran Semester. Teknik perkuliahan : pemaparan materi, tanya-jawab dan diskusi (proses pembelajaran dua arah).

b. Strategi Tutorial

- Mahasiswa mengerjakan tugas-tugas (*Discussion task; Study Task dan Problem Task*) sebagai bagian dari self study, kemudian berdiskusi di kelas, tutorial, presentasi power point, dan diskusi.
- Dalam tutorial dikelas, mahasiswa diwajibkan :

- Menyetor karya tulis berupa paper dan/atau tugas-tugas lain sesuai dengan topik;
- Mempresentasikan tugas dalam bentuk power point.

VII. TUGAS-TUGAS

Mahasiswa diwajibkan untuk mengerjakan, mempersiapkan, dan membahas tugas-tugas yang ditentukan di dalam buku ajar. Tugas-tugas terdiri dari tugas mandiri dan tugas kelompok yang dikerjakan di luar jam perkuliahan, tugas yang harus dikumpulkan dan tugas yang harus dipresentasikan.

VIII. UJIAN-UJIAN DAN PENILAIAN

a. Ujian

Ujian dilaksanakan dua kali dalam bentuk tertulis yaitu Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS).

b. Penilaian

Penilaian akhir dalam mata kuliah mengikuti ketentuan sebagaimana yang telah diatur dalam Buku Panduan Akademik UNIKOM 2017-2018, yang menjelaskan mengenai bobot penilaian dari serangkaian kegiatan yang harus dilakukan/ditempuh oleh mahasiswa, yaitu sebagai berikut :

Komponen Penilaian	Bobot/ Persentase Penilaian
Tugas/Quiz	30%
Nilai UTS	30%
Nilai UAS	40%

Indeks penilaian akhir :

Predikat	Indeks	Bobot Nilai	Angka Mutu	Deskripsi Penilaian
Lulus, Sangat Baik	A	80 - 100	4	Mahasiswa memenuhi semua komponen penilaian dan menyelesaikan tugas dengan sangat baik serta mampu menganalisis materi dan tugas sesuai dengan topik yang telah ditentukan dengan sangat baik
Lulus, Baik	B	68 - 79	3	Mahasiswa memenuhi semua komponen penilaian dan menyelesaikan tugas dengan baik serta mampu menganalisis materi dan tugas sesuai dengan topik yang telah ditentukan dengan baik
Lulus, Cukup	C	56 - 67	2	Mahasiswa memenuhi beberapa komponen penilaian dan menyelesaikan tugas serta mampu menganalisis materi dan tugas sesuai

				dengan topik yang telah ditentukan dengan cukup baik
Lulus, Kurang	D	45 - 55	1	Mahasiswa tidak memenuhi beberapa komponen penilaian dan tidak menyelesaikan tugas dengan cukup baik serta tidak dapat menganalisis materi dan tugas sesuai dengan topik yang telah ditentukan.
Tidak Lulus	E	<44	0	Mahasiswa tidak memenuhi semua komponen penilaian tidak dapat menganalisis materi dan tugas sesuai dengan topik yang telah ditentukan.

BAB I

PENDAHULUAN

A. Istilah dan Pengertian

Cyber Law yaitu Hukum yang mengatur aktivitas di dunia maya (kejahatan dunia maya melalui jaringan internet).[1] Istilah *cyber law* telah membentuk rezim hukum baru di Indonesia, khususnya dalam kegiatan teknologi dan informasi. Rezim hukum *cyber law* di Indonesia ditandai dengan lahirnya Undang-undang

Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang diundangkan oleh Presiden RI tanggal 21 april 2008.

Cyber Law adalah aspek hukumyang istilahnya berasal dari *cyberspace law* yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai *online* dan memasuki *cyber space* atau dunia maya.

Istilah hukum *cyber* berasal dari *cyberlaw,* yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan Teknologi Informasi. Istilah lain yang juga digunakan adalah Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Secara akademis, terminology *cyber law* belum menjadi terminologi yang umum. Terminologi lain untuk tujuan yang sama seperti *The Law of The Internet, Law and the Information Superhighway, Information Technology Law, The Law of Information, Lex Informatica* dan sebagainya. Di Indonesia sendiri tampaknya belum ada satu istilah yang disepakati. Istilah yang dimaksudkan sebagai terjemahan dari *cyber law*, misalnya, Hukum Sistem

[1] Widodo, *Hukum Pidana di Bidang teknologi Informasi (cybercrime law) : Telaah Teoritik dan Bedah Kampus,* Yogyakarta, 2013, hlm.15.

Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika).

Cyber Law diperlukan karena kegiatan *Cyber* dengan berbasis internet saat ini tidak bisa dibatasi oleh teritori Negara dan dapat dilakukan kapanpun. Meskipun alat buktinya berbentuk *virtual* (maya) dan bersifat elektronik kegiatan *cyber* adalah kegiatan virtual yang berdampak nyata. [2]

B. Sejarah Keberadaan Cyberlaw

1. Sejarah *Cyberlaw* di Dunia

Pada tahun 1980-an khusunya Negara-negara di Eropa dan Amerika Utara mulai melakukan kriminalisasi terhadap perbuatan baru seiring dengan penggunaan teknologi komputer dalam melakukan tindak pidana konvensional. Pada tahun 1990-an beberapa Negara di berbagai belahan dunia sudah mulai mengatur tindak pidana siber seperti memasuki sistem komputer secara illegal, merusak data dalam sistem komputer dan menyebarkan virus. Pelaku tindak pidana siber mempunyai kemampuan dan kesempatan untuk melakukan tindakpidana dari suatu Negara yang akan mengakibatkan kerugian terhadap seseorang di beberapa tempat di Negara lain.

Untuk mengahdapi ancaman tindak pidana siber beberapa organisasi internasional telah melakukan kajian-kajian dan pertemuan-pertemuan ilmiah yang membahas tindak pidana siber, kerjasama internasional untuk mendorong pembentukan hukum internasional tentang tindak pidana siber. Beberapa organisasi internasional yang telah melakukan usaha-usaha tersebut antara lain :[3]

---

[2] Ahmad ramli, *Cyber Law dan Haki dalam Sistem Hukum Indonesia,* Bandung, Refika Aditama, 2010, hlm.2-3.

[3] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* Bandung, Refika Aditama, 2012, hlm. 102-124

a. Organisation for Economic Co-operation and Development (OECD)

Usaha internasional pertama dalam memerangi tindak pidana penyalahgunaan komputer dilakukan oleh OECD antara tahun 1983dan tahun 1985. Pada tahun 1985 negara-negara anggota OEDC direkomendasikan mempertimbangkan untuk melakukan kriminalisasi terhadap kejahatan dengan penyalahgunaan komputer dan mengaturnya dalam hukum pidana nasional. Tahun 1986 OECD mengeluarkan laporan tentang *Computer-Related-Crime*: *Analysis of Legal Policy*. Berdasarkan hasil kajian tersebut OECD menganjurkan beberapa perbuatan untuk dikriminalisasi dalam hukum pidana nasional, yaitu :

1) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/program komputer dengan maksud untuk melakukan transfer dana atau sesuatu yang bernilai lainnya secara illegal.
2) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/program komputer dengan maksud untuk melakukan pemalsuan.
3) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/program komputer dengan maksud untuk mengganggu sistem komputer atau sistem telekomunikasi lainnya.
4) Pelanggaran hak eksklusif atas program komputer yang dilindungi yang dilakukan dengan sengaja untuk kepentingan komersial.
5) Mengakses atau mengintersep sistem komputer/telekomunikasi tanpa seizing pihak yang bertanggungjawab atas sistem tersebut baik dengan cara pelanggaran atas sistem pengamanan, atau untuk tujuan maksud jahat lain.

Usaha lain yang dilakukan OECD adalah kontribusinnya mengenai pedoman tentang kebijakan keamanan komputer internasional yang saat ini menjadi *Guidelines for the Security of Information System and Networks.*

b. United Nations (UN)

Perserikatan Bangsa-Bangsa (PBB) melakukan monitoring terhadap *Computer related crime,* dimulai pada tahun 1990 dengan *Eight UN Congress on the Prevention of Crime and Treatment of Offender.* Dalam resolusi kongres PBB tersebut Negara-negara dihimbau untuk mengintensifkan usaha-usaha memerangi *computer related crime* dengan melakukan tindakan-tindakan berikut :

1) Modernisasi hukum pidana materiil dan hukum acara pidana nasional untuk menjamin dan memadai dalam menindak tindak pidana siber.
2) Meningkatkan upaya-upaya pengamanan komputer dan upaya-upaya preventif, dengan memperhitungkan masalah-masalah terkait perlindungan privasi, penghormatan hak asasi manusia dan kebebasan-kebebasan fundamental serta setiap mekanisme pengaturan penggunaan/pemanfaatan komputer.
3) Mengadopsi upaya-upaya agar masyarakat, aparat pengadilan dan penegak hukum peka terhadap masalah *computer-related crimes* dan pentingnya mencegah tindak pidana tersebut.
4) Mengadopsi pelatihan-pelatihan yang memadai untuk hakim, pejabat dan aparat yang bertanggungjawab atas pencegahan, penyidikan, penuntutan dan pengadilan mengenai tindak pidana ekonomi dan *computer-related crimes*
5) Mengelaborasi -- dalam kolaborasi dengan organisasi-organisasi yang berkepentingan—*rules of ethics* dalam penggunaan komputer

dan mengajarkannya sebagai bagian dari kurikulum dan training informatika.

6) Mengadopsi kebijakan-kebijakan untuk korban *computer-related crimes* yang konsisten dengan *United Nations Declarartion of Basic Principles of Justice for Victims of Crime and Abuse of Power,* termasuk pengembalian aset yang diperoleh dari kejahatan, dan upaya-upaya mendorong korban agar mau melaporkan kejahatan kepada penguasa yang berwenang.

c. The Group of Eight (G8)

G8 adalah kelompok Negara-negara industry yang terdiri dari Kanada, Jerman, Perancis, Itali, Jepang, Inggris, Amerika Serikat, dan Rusia. Menurut G8 setidaknya ada 2 bentuk ancaman dari perkembangan *high-tech crime/*tindak pidana teknologi tinggi yaitu ; (1) para pelaku kejahatan yang canggih menjadikan komputer dan sistem telekomunikasi sebagai target untuk memperoleh atau mengalihkan informasi yang berharga tanpa izin dan mencoba mengganggu sistem-sistem perdagangan penting dan sistem-sistem public lainnya, (2) para pelaku kejahatan termasuk kelompok dari anggota kejahatan terorganisir dan para teroris, menggunakan teknologi baru ini sebagai alat kejahatan tradisional yang merupakan ancaman terhadap keamanan umum. G8 menyetujui 10 prinsip memerangi *high-tech crimes* tersebut adalah :

1) Tidak boleh ada tempat berlindung bagi mereka yang menyalahgunakan teknologi informasi.
2) Penyidikan dan penuntutan atas pelaku kejahatan *high-tech* internasional harus dilaksanakan dengan berkoordinasi dengan seluruh Negara yang berkepentingan, terlepas dari wilayah hukum mana kerugian ditimbulkan.

3) Aparat penegak hukum harus terlatih dan diperlengkapi/dipersiapkan untuk menangani kejahatn *high-tech*.
4) Sistem hukum harus melindungi kerahasiaan, keutuhan dan ketersediaan data dan sistem dari kerusakan yang diakibatkan oleh adanya perbuatan melawan hukum dan menajmin adanya penghukuman terhadap penyalahgunaan serius.
5) Sistem hukum harus memungkinkan pengamanan data elektronik dan akses yang cepat terhadap data elektronik, yang kerap sangat penting bagi keberhasilan investigasi kejahatan.
6) Rezim bantuan timbal balik harus dapat menjamin perolehan dan pertukaran alat bukti yang cepat dalam kasus yang melibatkan kejahatan *high-tech* internasional.
7) Akses elektronik lintas batas oleh penegak hukum terhadap informasi yang dapat diakses oleh umum tidak memerlukan pengesahan/izin dari Negara dimana data itu diperoleh atau berada.
8) Harus dikembangkan dan diterapkan standar forensic untuk memperoleh dan mensahkan data elektronik dalam proses investigasi dan penuntutan.
9) Sistem informasi dan telekomunikasi harus dirancang untuk membantu pencegahan dan mengetahui penyalahgunaan jaringan, dan juga harus dapat digunakan menelusuri dan menemukan para penjahat dan mengumpulkan alat bukti.
10) Kegiatan dibidang ini harus dikoordinasikan dengan kegiatan dalam for a internasional lainnya yang relevan untuk memastikan tidak adanya upaya yang tumpang tindih.

d. Council of Erope (CoE)

Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*)2001 yang digagas oleh Uni Eropa.konvensi ini dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapundi Dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber. *Convention on Cyber Crime* 2001 merupakan puncak dari usaha-usaha yang telah dimulai lebih dari 20 tahun lalu oleh OECD, kemudian juga dilakukan PBB dan organisasi internasional lainnya yang telah mengkaji dan menyelenggarakan berbagai penemuan internasional dalam menghadapi perkembangan tindak pidana siber. *Convention on Cyber Crime* 2001 merupakan regulasi internasional pertama yang mengatur tindak pidana Siber dan menjadi pedoman dalam regulasi tindak pidana siber dalam hukum nasional.

Convention on Cyber Crime 2001 terdiri dari 48 pasal dan dibagi dalam 4 bab,ketentuan yang berkaitan dengan kriminalisasi tindak pidana siber adalh Bab II Hukum Pidana Materil Bagian 1 hukum pidana materil (Pasal2-Pasal 13) mengatur ketentuan-ketentuan tentang hukum pidana materiil, kriminalisasi, dan ketentuan lainnyab yang berkaitan dengan tindak pidana siber. Tindak pidana siber terdapat 9 jenis tindak pidana siber yang dikelompokan dalam empat kategori tindak pidana, yaitu :

1) Kelompok pertama : tindak pidana terhadap kerahasiaan (*confidentiality)*, integritas (*integrity),* dan ketersediaan data (*availability)* data dan sistem komputer terdiri dari : *illegal access* (pasal 2)*, illegal interception* (pasal 3)*, data interference* (pasal 4)*, system interference* (pasal 5)*,* dan *misuse of device* (pasal 6).

2) Kelompok kedua : tindak pidana yang berkaitan dengan komputer, terdiri dari pemalsuan yang berkaitan dengan komputer (*computer related forgery* (pasal 7)), dan penipuan yang berkaitan dengan komputer (*computer related fraud* (pasal 8)).
3) Kelompok ketiga : tindak pidana yang berkaitan dengan konten yang berisi ketentuan tentang tindak pidana yang berkaitan dengan pornografi anak (*offens related to child pornography* (pasal 9)).
4) Kelompok keempat : tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait (pasal 10).

Disamping empat kelompok tindak pidana siber, dalam Bab I hukum pidana materil juga mengatur kewajiban tambahan dan sanksi terdiri dari :

1) Pasal 11, perbuatan yang dikriminalisasi adalah dengan sengaja (1) membantu atau menghasut, (2) mencoba untuk melakukan tindak pidana yang diatur dalam PAsal 2-Pasal 10.
2) Pasal 12, mengatur tentang badan-badan hukum dapat diminta pertanggungjawaban atas tindak pidana yang telah ditetapkan sesuai dengan konvensi ini,yang dilakukan untuk keuntungan mereka oleh orang perseorangan, baik secara individual, maupun sebagai bagian dari organ badan hukum, yang memegang posisi pimpinan didalamnya berdasarkan:
    a) Kuasa perwakilan badan hukum tersebut,
    b) Wewenang untuk mengambil keputusan atas nama badan hukum tersebut,
    c) Wewenang untuk mengendalikan dalam badan hukum tersebut.

3) Pasal 13, mengatur mengenai adanya jaminan bahwa tindak pidana dari pasal 2-pasal 10 dipidana denga sanksi yang efektif, proporsional, dan dissuasive, termasuk sanksi pidana perampasan kemerdekaan untuk orang atau sanksi non-penal atau tindakan, termasuk juga sanksi pidana denda utnuk badan hukum.

C. Sejarah *Cyberlaw* di Indonesia

Perkembangan teknologi informasi dan komunikasi saat ini diawali dengan perkembangan teknologi komputer sejak tahun 1990-an sudah menjadi perhatian masyarakat dan pemerintah indonesia. Pada tahun 2000 pemerintah mulai menggagas untuk mengatur berbagai aktivitas di *cyberspace.* Usaha untuk melakukan regulasi terhadap aktivitas manusia di *cyberspace* termasuyk aspek hukum pidananya telah dilakukan sejakm tahun 2000, yaitu pertama dengan disusunnya RUU Pemanfaatan Teknologi Informasi yang diprakarsai Direktorat Jendral Pos dan Telekomunikasi Departemen Perhubungan. RUU Pemanfaatan Teknologi Informasi disusun oleh Tim Fakultas Hukum UNPAD dan ITB. Kedua, RUU Tanda Tangan Digital diprakarsai oleh Departemen Perindustrian dan Perdagangan dan disusun oleh Tin Fakultas Hukum UI, khususnya Lembaga Kajian Hukum dan Teknologi (LKTH).[4]

RUU tersebut akhirnya digabung menjadi, RUU Informasi, Komunikasi, dan Transaksi Elektronik (RUU IKTE) yang diprakarsai oleh Direktorat Jendral Pos dan Telekomunikasi Departemen Perhubungan dan Departemen Perindustrian dan Perdagangan, dengan penyusun berasa dari Tim Fakultas Hukum UNPAD dan Tim Asistensi ITB serta Lembaga Kajian Hukum dan Teknologi (LKTH)

[4] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* Bandung, Refika Aditama, 2012, hlm.125.

UI. Seiring dengan dibentuknya Kementrian Negara Komunikasi dan Informasi (KOMINFO), sejak maret 2003 pembentukan RUU IKTE selanjutnya dilakukan olehKementrian Kominfo dan menjadi RUU Informasi Elektronik dan Transaksi Elektronik (RUU IETE). Pada tahun2005 Kementrian Komunikasi dan Informasi berdasarkan Peraturean Pemerintah RI No.9 Thaun 2005 berubah menjadi Departemen Komunikasi dan Informatika (DEPKOMINFO) dan penyusunan RUU IETE yang kemudian berubah menjadi RUU Informasi dan Transaksi Elektronik (RUU ITE) dilakukan oleh Departemen Komunikasi dan Informatika. [5]

Melalui pembahasan di DPR pada tanggal 25 maret 2008 rapat paripurna DPR menyetujui RUU ITE ditetapkan menjadi Undang-undang dan kemudian pada tanggal 21 April 2008 oleh Presiden Republik Indonesia diundangkan dengan Undang-undang No.11 tahun2008 tentang Informasi dan Transaksi Elektronik Lembaran Negara tahun 2008 No.58.[6]

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pemebentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejaqhatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi. UU ITE terdiri dari 54 pasal yang terbagi dalam 13 Bab. Ketentuan-ketentuan yang mengatur kriminalisasi perbuatan yang termasuk kategori tindak pidana siber adalah Bab VII tentang perbuatan yang dilarang pasal 27-

[5] *Ibid.,*
[6] *Ibid.*

pasal37. Sanksi pidana atas perbuatan-perbuatan tersebut dirumuskan dalam Bab XI tentang ketentuan pidana Pasal 45-Pasal52.

Dalam perjalanannya, kriminalisasi tinak pidana siber dalam UU ITE yang mengatur penyalahgunaan teknologi informasi dan komunikasi dalam aktifitas di dunia siber belum memadai. Saat ini hukum internasional yang banyak digunakan negara-negara di dunbia sebagai pedoman dalam pengaturan tindak pidana siber adalah *Convention on Cybercrime 2001*. Sehubungan dengan itu pemerintah Indonesia bermaksud untuk melakukan aksesi terhadap *Convention on Cybercrine 2001* dan melakukjan harmonisasi hukum nasional indonesia dengan *Convention on Cybercrime 2001*. Berdaarkan hasilmkajian dan juga hasil *Workshop on Cybercrime Legislation in Indonesia* dengan *Council of Europe Expert,* ketentuan-ketenrtuan UU ITE belum sesuai dengan ketentuan tindak pidana siber dalam konvensi. Untuk itu pemerintah telah menyusun draf RUU Tindak Pidana Teknologi Informasi (RUU TIPITI) yang akan menhgatur beberapa terminologi dan norma-norma dalam konvensi yang belum sesuai atau belum diatur dalam UU ITE.[7]

RUU TIPITI yang terdiri dari 10 Bab dan 27 pasal merumuskan beberapa pengertian baru yang dirumuskan adalah sistem komputer, data komputer dan data trafik. Perbuatan-perbuatan yang dikriminalisasi dalam dalam RUU TIPITI pada dasarnya mengatur 5 jenis tindak pidana yaitu : penipuan, pelanggaran hak cipta dan hak-hak terkait, menghambat atau mengahalangi proses peradilan, pembantuan dan penghasutan serta pelanggaran kewajiban oleh penyelenggara sistem.[8]

[7] *Ibid.,*
[8] *Ibid.*

D. ASAS-ASAS CYBERLAW

Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :[9]

1. ***Subjective territoriality***, dalam perspektif ini hukum berlaku berdasarkan tempat *cybercrime* dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
2. ***Objective territoriality***, dalam perspektif ini hukum berlaku berdasarkan dimana akibat utama kejahatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
3. ***Nationality*** dalam perspektif ini negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
4. ***Passive nationality*** yang menekankan jurisdiksi berdasarkan kewarganegaraan korban.
5. ***Protective principle***, dalam perspektif ini hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah,
6. ***Universality***. Asas ini selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini disebut juga sebagai "*universal interest jurisdiction*". Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan (*crimes against humanity*), misalnya penyiksaan, genosida, pembajakan udara dan lain-lain. Meskipun di masa mendatang asas jurisdiksi universal ini mungkin dikembangkan

[9] Widodo, , *Hukum Pidana di Bidang teknologi Informasi (cybercrime law) : Telaah Teoritik dan Bedah Kampus,* Yogyakarta, 2013, hlm.40.

untuk internet piracy, seperti computer, cracking, carding, hacking and viruses, namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional. Oleh karena itu, untuk ruang cyber dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah. Ruang cyber dapat diibaratkan sebagai suatu tempat yang hanya dibatasi oleh screens and passwords. Secara radikal, ruang cyber telah mengubah hubungan antara legally significant (online) phenomena and physical location.

BAB II
SUMBER HUKUM CYBER LAW

A. Konvensi atau Perjanjian Internasional

Cyber Crime, merupakan sebuah fenomena kejahatan baru dalam tatanan hukum internasional. *Cyber crime* sebelumnya tidak mendapat perhatian Negara-negara sebagai subjek hukum Internasional. Munculnya kejahatan baru yang bersifat transnasional dan dalam bentuk tindakan-tindakan yang dilakukan dalam dunia maya ttelah menyadarkan masyarakat Internasional tentang perlunya perangkat Hukum Internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *cybercrime.*

Instrument Hukum Internasional public yang mengatur kejahatan siber adalah Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*)2001 yang digagas oleh Uni Eropa.konvensi ini dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapundi Dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber.

Konvensi ini dibentuk dengan pertimbangan-pertimbangan (dalam pembukaan *EU Convention On Cyber Crime*) antara lain sebagai berikut :

1) Masyarakat internasional menyadari perlunya kerjasama antar Negara dan industry dalam memerangi kejahatan siber dan adanya kepentingan untuk melindungi kepentingan yang sah di dalam penggunaan serta pengembangan teknologi informasi.

2) Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan criminal. Dengan demikian perlunya adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestic melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.
3) Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegak hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Konvenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat.

Konvensi ini telah disepakati oleh Masyarakat Uni Eropa sebagai Konvensi yang terbuka untuk diaksesi oleh Negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrument Hukum Internasional dalam mengatasi kejahatan siber, tanpa mengurangi kesempatan setipa individu untuk tetap mengemabngakan kreativitasnya dalam mengembangkan teknologi informasi.

B. Hukum Positif di Indonesia

1. Kitab Undang-undang Hukum Pidana

Sebelum UU-ITE berlaku, dalam mengadili *cybercrime* pengadilan menggunakan ketentuan KUHP dan ketentuan dalam Undang-undang di luar KUHP yang mengatur tindak pidana. Ketentuan yang digunakan untuk menangani *cybercrime* dalam KUHP adalah tentang pemalsuan (pasal 263-276), pencurian (pasal 362-372), penipuan

(pasal 378-395), perusakan barang (pasal 407-412). 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: [10]

a) **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.
b) **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.
c) **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.

[10] H. Sofwan Jannah, dkk., *Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif dan Hukum Islam*, Jurnal Al-Mawarid,Vol. XII, Nomor 1, Februari-Agusutus, 2012, hlm. 74-75.

d) **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.

e) **Pasal 303 KUHP** dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.

f) **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.

g) **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.

h) **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.

i) **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.

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang ITE merupakan ketentuan yang mengatur bagi setiap orang yang melakukan perbuatan hukum serta memiliki akibat hukum dan merugikan kepentingan negara Indonesia, baik setiap orang yang berada di wilayah hukum negara Indonesia maupun yang berada di luar wilayah hukum Indonesia. Berikut diuaraikan penegrtiannya dalam UU ITE :

a. Informasi Elektronik

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pemebentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejaqhatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi.

Beberapa materi perbuatan yang dilarang (*cybercrimes*) yang diatur dalam UU ITE, antara lain: [11]

a. Perbuatan yang dikriminalisasi dalam pasal 27 meiputi Dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan atau membuat informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dapat diakses, memiliki muatan perudian dapat diakses, memiliki muatan penghinaan

[11] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* Bandung, Refika Aditama, 2012, hlm.127-130

dan/atau pencemaran nama baik dapat diakses, memiliki muatan pemerasan atau pengancaman dapat diakses.

b. Pasal 28 Perbuatan yang dikriminalisasi dalam pasal 28 meliputi perbuatan yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dan dengan sengaja dan tanpa hak menyebarkan informasi untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyaraat tertentu berdasarkan SARA.

c. Perbuatan yang dikriminalsisasi dalam pasal 29 adalah dengan sengaja serta tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang didalamnya memuat ancaman berupa kekerasan atau menakuti yang ditujukan kepada pribadi atau seseorang.

d. Perbuatan yang dikriminaslisasi dalam pasal 30 meliputi, dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik atau dokumen eektronik, dan dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

e. Perbuatan yang dikriminalisasi dalam pasal 31 meliputi, yaitu dengan sengaja dan tanpa hak atau melawan hukum melakukan penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer atau sistem elektronik tertentu milik orang lain dan dengan melakukan penyadapan suatu transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik dari, ke dan

didalam suatu komputer atau sistem elektronik tertentu milik orang lain, baik yang tiak menyebabkan perubahan, penghilangan, atau penghentian informasi elektronik atau dokumen elektronik yang sedang di transmisikan.

f. Perbuatan yang dikriminalisasi dalam pasal 32 sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik atau dokumen elektronik milik orang lain atau milik publik dan yang tidak berhak.

g. Perbuatan yang dikriminalisasi dalam pasal 33 adalah dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektroni atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

h. Perbuatan yang dikriminalisasi dalam pasal 34 adalah dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau meniliki, Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusu dikembangkan untuk memfasilitasi perbuatan sebagaiman dimaksud dalam pasal 27 sampai dengan pasal 33, Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33.

i. Perbuatan yang dikriminalisasi dalam pasal 35 adalah dengan sengaja dan tanpa hak atau melawan hukum, melakukan manipulasi, penciptaan, perubahan, penghilangan, pengeruskan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersbut dianggap seolah-olah data yang otentik.
j. Perbuatan yang dikriminalisasi dalam pasal 36 adalah dengan senagaja dan tanpa haka tau melawan hukum perbuatan sebagaimana dimaksud dalam Pasal 27 s/d Pasal 34 yang dapat mengakibtkan kerugian bagi orang lain.
k. Ketentuan pasal 37 tidak mengatur perbuatan yang dilarang tetapi mengatur mengenai yurisdiksi atas perbuatan yang dilakuakn di luar wilayah Indonesian terhadap sasaran atau objek yang ada di wilayah indonesia.

Berdasarkan rumusan perbuatan yang dikriminalisasi sebagai tindak pidana siber dalam UU ITE terdapat unsur delik yang dirumuskan, yaitu unsur "dengan sengaja" dan "tanpa hak". Dalam beberapa pasal unsur "tanpa hak" dirumuskan alternatif dengan "melawan hukum", yaitu Pasal 30 sampai dengan Pasal 36. Penggunaan kata "dengan sengaja" menagndung arti bahwa tindak pidana Siber sebagaimana diatur dalam UU ITE diancam dengan pidana apanila dilakukanb dentgan sengaja. Perbuatan yang dilakukan dengan kelalaian atau kebetulan bukan merupakan tindak pidana dan tidak diancam dengan pidana.[12]

[12] *Ibid.* Hlm.130.

BAB III

CYBERCRIME

A. Pengertian dan Karakteristik *Cybercrime*

Secara terminologis, kejahatan di bidang teknologi informasi dengan basis 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.*[13]

Istilah *cyberspace* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung (online) ke internet oleh Jhon Perry Barlow pada tahun 1990. Secara etimologis, istilah *cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir *Cambridge Advanced Learner's Dictionary* memberikan definisi *cyberspace* sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject"*. Yakni pertimbangan internet sebagai suatu area imajiner tanpa batas,dimana anda bisa bertemu dengan banyak orang dan mendapatkan informasi tentang berbagai hal. Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime*. [14]

---

[13] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara,* Yogyakarta, Aswaja Pressindo, 2013, hlm.5

[14] Yadi, *Cybersoace, Cybercrune dan Cyberlaw, http://yandi-sage./cyberspace-cybercrime-dan-cyberlaw.html,* diakses Pada hari Minggu, tanggal 14 Juni 2020, Pukul 10.30 WIB.

Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *Cyber crime*, yaitu *cyber crime* dan *computer related crime*. Dalam back ground paper untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, cyber crime dalam arti sempit (*in a narrow sense*) disebut computer crime. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:[15]

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them.*
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possess Pion, offering or distributing information by means of a computer system or network.*

Istilah *cybercrime* saat ini merujuk pada suatu aktivitas kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai media utama untuk melangsungkan kejahatan.[16]. Secara umum pengertian *Cybercrime* adalah perbuatan tanpa ijin dan melawan hukum dengan menggunakan komputer sebagai fasilitas

[15] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Predana Media Group, Jakarta, 2007, hlm. 24.
[16] Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi,* Bandung, Refika Aditama, 2009, hlm.8.

utama atau target untuk melakukan kejahatan, dengan atau tanpa merubah dan atau merusak sistem komputer yang digunakan.[17]

Perlu kita ketahui pelaku cybercrime adalah mereka yang memiliki keahlian tinggi dalam ilmu computer, pelaku cybercrime umumnya menguasai algoritma dan pemrograman computer unutk membuat script/kode malware, mereka dapat menganalisa cara kerja system computer dan jaringan, dan mampu menemukan celah pasa system yang kemudian akan menggunakan kelemahan tersebut untuk dapat masuk sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan.

Karakteristik khusus dari kejahatan siber antara lain menyangkut 5 hal sebagai berikut :[18]

1. Ruang lingkup kejahatan

Sesuai sifat global *internet,* ruang lingkup kejahatan ini juga bersifat global.Cybercrime sering kali dilakukan secara transnasional, melintasi batas antarnegara sehingga sulit dipastikan yuridiksi hukum Negara mana yang berlaku terhadapnya.

2. Sifat Kejahatan

Sifat kejahatan di dunia maya yang non-violence, atau tidak menimbulkan kekacauan yang mudah terlihat. Jika kejahatan konvensional sering kali menimbulkan kekacauan maka kejahatan di *internet*bersifat sebaliknya.Oleh karena itu, ketakutan atas kejahatan tersebut tidak mudah timbul meskipun bias saja kerusakan yang diakibatkan oleh kejahatan cyber dapat lebih dahsyat dari pada kejahatan – kejahatan lain.

---

[17] *Ibid.,* hlm.8.

[18] NN., *Karakteristik Cyber Crime,* http://eptikkel/2013/05/karakteristik-cyber-crime.html, diakses pada Hari Selasa, Tanggal 16 Juni 2020, Pukul 21.46 WIB.

3. Pelaku Kejahatan

Jika pelaku kejahatan konvensional mudah diidentifikasi dan memiliki tipe tertentu maka pelaku*cybercrime* bersifat lebih universal meski memiliki ciri khusus yaitu kejahatan dilakukan oleh orang – orang yang menguasai penggunaan *internet* beserta aplikasinya. Pelaku kejahatan tersebut tidak terbatas pada usia dan stereotip tertentu.

4. Modus Kejahatan

Dalam hal ini, keunikan kejahatan ini adalah penggunaan tekhnologi informasi dalam modus operandi. Itulah sebabnya mengapa modus operandi dalam dunia *cyber* tersebut sulit dimengerti oleh orang – orang yang tidak menguasai pengetahuan tentang komputer, tekhnik pemrogramannya dan seluk beluk dunia cyber.

5. Jenis Kerugian yang ditimbulkan

Kerugian yang ditimbulkan dari kejahatan ini dapat bersifat material maupun non-material. Cybercrime berpotensi menimbulkan kerugian pada banyak bidang seperti politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan berintensitas tinggi lainnya.

B. Jenis-jenis *Cyber Crime*

Beberapa jenis *cybercrime,* dalam beberapa literature dan praktiknya dikelompokan dalam beberapa bentuk, antara lain :[19]

1. Unauthorized Access Merupakan kejahatan yang terjadi ketika seseorang emasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

[19] Dikdik, Elisatris,*Op., Cit.,* hlm.9.

2. Illegal Contents Merupakan kejahatn yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

3. Penyebaran virus secara sengaja**,** Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. Data Forgery**,** Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

5. Cyber Espionage, Sabotage, and Extortion, Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. Cyberstalking Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut

menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7. Carding, Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. Hacking dan Cracker, Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

9. Cybersquatting and Typosquatting**,** Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain

plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

10. Hijacking**,** Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

11. Cyber Terorism Suatu tindakan *cybercrime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.

C. Faktor Pendorong Terjadinya *Cyber Crime*

Kemajuan teknologi informasi dapat ditandai dengan meningkatnya penggunaan internet, meningkatnya penggunaan internet dapat memberikan dampak positif namun dampak negatif akibat kemajuan teknologi sangat banyak dan sering kali menjadi pidana.. Menurut Didik M. Arief Mansur dan Elisatris Gultom, bahwa *cyber crime* lahir disebabkan karena faktor kurangnya kemampuan atau pengetahuan dari aparat penegak hukum dalam menangani kasus siber.[20]

Antara teknologi informasi dengan operator yang mengawaki mempunyai hubungan yang erat sekali, keduanya tidak dapat dipisahkan. Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali dari sebuah alat. Apakah alat itu digunakan sebagai sarana kebajikan untuk mencapai kesejahteraan umat manusia, ataukah alat itu akan dikriminalisasikan

[20] Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya Cetakan I,* Laksbang Pressindo, Yogyakarta, 2007, hlm. 64.

sehingga dapat merusak kepentingan negara dan masyarakat. Teknologi sebagai hasil temuan dan pengembangan manusia kemudian dimanfaatkan, untuk perbaikan umat, namun di sisi lain dapat membawa petaka bagi umat manusia sebagai akibat adanya penyimpangan. Di Indonesia sumber daya pengelola teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan teknologi ini masih kurang. Penyebabnya ada berbagai hal, di antaranya kurangnya tenaga peneliti dan kurangnya biaya penelitian atau mungkin kurangnya perhatian dan apresiasi terhadap penelitian. sehingga sumber daya manusia di Indonesia lebih banyak sebagai pengguna saja dan jumlahnya cukup banyak.[21]

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologi terbentuklah sebuah komunitas baru di dunia maya yakni komunitas para pecandu internet yang saling berkomunikasi, bertukar pikiran berdasarkan prinsip kebebasan dan keseim– bangan di antara para pecandu atau maniak dunia maya tersebut. Komunitas ini adalah sebuah populasi gaya baru sebagai gejala sosial, dan sangat setrategis untuk diperhitungkan, sebab dari media ini banyak hikmah yang bisa didapat. Dari hal yng tidak tahu menjadi tahu, yang tahu jadi semakin pintar, sementara yang pintar semakin canggih. Terjadinya perkembangan teknologi dan laju perkembangan masyarakat diketahui dengan cepat dan akurat, dan mereka saling bertukar pikiran serta dapat melakukan rechecking di antara mereka sendiri.

Secara emosional, mereka melekatkan dirinya kepada teman di dunia maya. salah satu bentuk komunitasa itu adalah mailing list. Di yahoo terdapat komunitas dan kemudian difasilitasi oleh yahoo dalam

[21] Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya Cetakan 1*, LaksBang Pressindo, Yogyakarta, 2007, hlm. 88-89.

bentuk group.yahoo.com. Dalam mailing list mereka dapat berdiskusi tentang suatau masalah, namun mereka tidak harus menghidupkan komputer dan internet secara bersamaan, sedangkan chatting, di antara mereka harus sama-sama menghidupkan komputer.[22]

Selain tiga faktor diatas, ada juga beberapa hal yang menyebabkan makin maraknya kejahatan komputer diantaranya :[23]

Akses internet yang tidak terbatas, Di zaman sekarang ini internet bukanlah hal yang langka lagi, karena semua orang telah memanfaatkan fasilitas internet. Dengan menggunakan internet kita diberikan kenyamanan kemudahan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyaman itu lah yang merupakan faktor utama bagi sebagian oknum untuk melakukan tindak kejahatan Cybercrime dengan mudahnya. Kelalaian pengguna computer, Hal ini merupakan salah satu penyebab utama kejahatan komputer. Seperti kita ketahui orang-orang menggunakan fasilitas internet selalu memasukan semua data-data penting ke dalam internet. Sehingga memberikan kemudahan bagi sbagian oknum untuk melakukan kejahatan.

Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern, Inilah yang merupakan faktor pendorong terjadinya kejahatan di dunia maya. Karena seperti kita bahwa internet merupakan sebuah alat yang dengan mudahnya kita gunakan tanpa memerlukan alat-alat khusus dalam mengunakannya. Namunpendorong utama tindak kejahatan di internet yaitu susahnya melacak orang yang menyalahgunakan fasilitas dari internet tersebut.

---

[22] *Ibid.,* hlm. 90.

[23] NN, *Penyebab Terjadinya Cybercrime Dan Upaya Penanggulangannya Di Indonesia*, http://rutinitasinformatika//html., diakses pada Hari Minggu, Tanggal 14 Juni 2020, Pukul 22.34 WIB.

Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer, Hal ini merupakan faktor yang sulit untuk di hindari, karena kelebihan atau kecerdasan dalam mengakses internet yang di miliki seseorang di zaman sekarang ini banyak yang di salah gunakan demi mendapatkan keuntungan semata. Sehingga sulit untuk di hindari.

Sistem keamanan jaringan yang lemah, Seperti kita ketahui bahwa orang-orang dalam menggunakan fasilitas internet kebanyakan lebih mementingkan desain yang di milikinya dengan menyepelekan tingkat keamanannya. Sehingga dengan lemahnya sistem keamanan jaringan tersebut menjadi celah besar sebagian oknum untuk melakukan tindak kejahatan.

Kurangnya perhatian masyarakat, Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvensional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya. Hal ini disebabkan karena rendahnya faktor pengetahuan tentang penggunaan internet yang lebih dalam pada masyarakat.

BAB IV

CYBER CRIME SEBAGAI KEJAHATAN TRANSNASIONAL

A. Pengertian Kejahatan Transnasional

Cyber crime merupakan suatu kejahatan yang dapat dikatakan sebagai kerjahatan baru, karena kejahatan siber memiliki karakteristik yang sangat khusus jika dibandigkan dengan kejahatan-kejahatan konvensional. *Cyber Crime* muncul bersamaan dengan lahirnya kemajuan teknologi informasi. R. Nitibaskara mengatakan bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial yang berupa kejahatan (*crime*), akan menyesuaikan bentuknya dengan karakter baru tersebut." Ringkasnya, sesuai dengan ungkapan "kejahatan merupakan produk dari masyarakatnya sendiri" (*crime is a product of society its self*), "habitat" baru ini, dengan segala bentuk pola interaksi yang ada di dalamnya, akan menghasilkan jenis-jenis kejahatan yang berbeda dengan kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah "*cyber crime".* [24]

Dengan memperhatikan jenis-jenis *cyber crime* yang dibahas pada bab sebelumnya dapat digambarkan bahwa *cyber crime* memiliki cirri-ciri khusus, yaitu (1) tanpa kekerasan, (2) sedikit melibatkan kontak fisik, (3) menggunakan peralatan, (4) memanfaatkan jaringan telematika (telekomunikasi, media, dan informatika) global.[25] Melihat cirri ke 3 dan 4, terlihat jelas *cyber crime* dapat dilakukan dimana saja, kapan saja, serta berdampak kemana saja, seperti tanpa batas (*borderless*). Kondisi ini mengakibatkan tempat terjadinya *cyber crime*, pelaku, korban, serta akibat yang timbul bisa terjadi di

[24] Dikdik, Elisatris,*Op., Cit.,* hlm.25.
[25] *Ibid.,* hlm. 27.

beberapa Negara, disinilah terlihat aspek dari transnasional *cyber crime.*

Dari penjelasan diatas kemudian dapat didefinisikan bahwa kejahatan transnasional atau transnational crime adalah kejahatan dengan akibat yang ditimbulkan terjadi di lebih dari satu negara, dengan melibatkan warga negara lebih dari satu negara, sarana dan prasarana serta metoda-metoda yang dipergunakan melampaui batas-batas teritorial suatu negara.

Jadi istilah kejahatan transnasional dimaksudkan untuk menunjukkan adanya kejahatan-kejahatan yang sebenarnya nasional (di dalam batas wilayah negara), tetapi dalam beberapa hal terkait kepentingan negara-negara lain. Sehingga lebih dari satu negara yang berkepentingan atau yang terkait dengan kejahatan itu. Kejahatan transnasional jelas menunjukkan perbedaannya dengan kejahatan atau tindak pidana dalam pengertian nasional semata-mata. Sifatnya yang transnasional yang meliputi hampir semua aspek nasional maupun internasional, baik privat maupun publik, politik maupun bukan politik. Oleh karena itu, dalam memberantas *cyber crime* diperlukan penanganan yang serius serta melibatkan kerjasama internasional baik yang sifatnya regional maupun multilateral.

B. Yurisdiksi Suatu Negara dalam Kejahatan Transnasional

Cyber space merupakan dunia virtual atau biasa disebut dengan dunia maya dimana dunia virtual tersebut tidak mengenal batas wilayah, sehingga dapat menimbulkan masalah tersendiri yang berkaitan dengan yurisdksi, Yurisdiksi merupakan suatu wilayah dalam hal berlakunya suatu peraturan perundang-undangan dalam kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Mengacu kepada asas umum dalam hukum internasional, bahwasannya setiap negara itu memiliki kedaulatan

dalam wilayahnya, sehingga suatu negara tidak dapat malampui kedaulatannya dalam melaksanakan suatu tindakan yang berada dalam wilayah negara lain.[26]

Penerapan yurisdiksi criminal suatu Negara berdaulat berdasarkan hukum internasional dilaksanakan berdasarkan beberpa prinsip yurisdiksi antara lain :

1. Prinsip Teritorial**,** Dapat menerapkan yuriskdiksi nasionalnya terhadap semua orang (baik warga negara atau asing), badan hukum dan semua benda yang berada di dalamnya. Prinsip territorial merupakan prinsip yurisdiksi yang utama yang dilaksankan dalam melaksanakan yurisdiksi Negara
2. Prinsip Nasional Aktif**,** Prinsip berdasarkan pada nasionalitas atau kewarganegaraan. Dalam hal ini nasionalitas pelaku kejahatan. Di sini kewarganegaraan pelaku menjadi titik taut diberlakukannya yurisdiksi negara asal. Berdasarkan prinsip ini Negara mempunyai yurisdiksi terhadap warga negaranya yang melakukan tindak pidana di dalam yurisdiksi Negara lain.
3. Prinsip Nasional Pasif**,** Prinsip yang didasarkan pada kewarganegaraan dari korban kejahatan. Berdasarkan prinsip ini sutau Negara memiliki yurisdiksi untuk mengadili pelaku tindak pidana di luar negeri yang merugikan warga negaranya.
4. Prinsip Perlindungan Hukum internasional menyatakan bahwasannya suatu negara dapat menerapkan hukum nasionalnya kepada pelaku kejahatan walupun kejahatan itu dilakukan di luar wilayah negara tersebut, yang mana tindak

[26] *Ibid.*, hlm.30.

pidana kejahatan yang dilakukan merupakan suatu tindakan yang dapat mengacam kepentingan negara yang bersangkutan.

5. Prinsip Universal pada dasarnya tidak mensyaratkan adanya suatu hubungan, sehingga dapat disimpulkan bahwa suatu hukum pidana dapat diberlakukan apabila dalam suatu tindak pidana yang telah dilakukan oleh seseorang itu bertentangan dengan nilai-nilai universal dalam suatu negara dan bertentngan dengan kepentingan masyarakat secara luas.

Secara garis besar, yurisdiksi dapat dibedakan menjadi dua yaitu pertama adalah yurisdiksi perdata dimana kewenangan hukum suatu negaraterdapat obyek perkara dalam yang di dalamnya dalam lingkup hukum privat yang memikiki unsur asing maupun unsur nasional, yang kedua adalah yurisdiksi pidana dimana kewenangan hukum suatu negara terdapat obyek perkara yang dalam ketentuannya telah melanggar hukum publik dan memiliki unsur asing.

Asas *au dedere au Judicare* merupakan salah satu pedoman yang dapat dijadikan tolak ukur dalam hal penanggulangan tindak pidana internasional, asas ini secara tersurat menyebutkan bahwa setiap negara berkwajiban untuk berkolaborasi dengan negara lain untuk dapat menunutu serta mengadili setiap orang yang patut di duga telah melakukan suatu tindak pidana internasional. Tentang masalah yurisdiksi di internet/cyber space, Darrel Menthe mengemukakan suatu teori bahwa dalam hal berinteraksi dalam dunia virtual terdapat dua hal yang mendasari yaitu memberikan informasi dan mengambil informasi kedalam serta keluar dunia virtual atau dalam hal ini adalah dunia cyber.

Dalam hal ini ada dua peran yang berbeda secara nyata yaitu ***the uploader*** yang memberi informasi ke dalam dunia cyber dan ***the***

downloader sebagai pengambil informasi di kemudian hari; dengan tidak memperhatikan identitas keduanya (baik the uploader maupun the downloader). Teori yang dikemukakan oleh Darrel Menthe ini disebut sebagai ***The Theory of the Uploader and the Downloader.***

Johnson dan Post berpendapat bahwa penerapan prinsip-prinsip tradisional dari *"Due Process and personal jurisdiction"* tidak sesuai dan mengacaukan apabila diterapkan pada cyberspace. Menurut Johnson dan Post, cyberspace harus diperlakukan sebagai suatu ruang yang terpisah dari dunia nyata dengan menerapkan hukum yang berbeda untuk cyberspace (*cyberspace should be treated as a separate "space" from the "real world" by applying distinct law to cyberspace*).

Selanjutnya menurut Barda Nawawi Arief, bahwa sistem hukum dan jurisdiksi nasional/teritorial memang mempunyai keterbatasan karena tidaklah mudah menjangkau pelaku tindak pidana di ruang cyber yang tidak berbatas. Namun tidak berarti ruang cyber dibiarkan bebas tanpa hukum. Ruang cyber merupakan bagian atau perluasan dari "lingkungan" ("*environment*") dan "lingkungan hidup" *("life environment")* yang perlu dipelihara dan dijaga kualitasnya; jadi merupakan suatu "kepentingan hukum" yang harus dilindungi. Oleh karena itu, jurisdiksi legislatif atau *"jurisdiction to prescribe"* , tetap dapat dan harus difungsikan untuk menanggulangi *"cybercrime"* yang merupakan dimensi baru dari *"environmental crime"*. Masalah yurisdiksi yang timbul lebih banyak sebagai yurisdiksi horisontal, artinya negara manakah yang berhak untuk memutuskan atau melaksanakan yurisidiksi di dunia mayantara (*cyberspace*); hal ini muncul karena sulitnya untuk menetapkan diwilayah mana dunia mayantara (*cyberspace*) dapat dikenai jurisdiksi.

Menghadapi masalah jurisdiksi di dunia mayantara ini serta memperhatikan ketentuan dalam Convention on Cybercrime, Barda Nawawi Arief mengemukakan ,digunakannya asas universal atau prinsip ubikuitas (***the principle of ubiquity***) untuk menanggulangi masalah kejahatan cyber. Prinsip ubikuitas adalah prinsip yang menyatakan bahwa delik-delik yang dilakukan/terjadi sebagian wilayah teritorial negara dan sebagian di luar teritorial suatu negara, harus dapat dibawa ke dalam jurisdiksi setiap negara yang terkait. Prinsip ubikuitas ini pernah direkomendasikan dalam *"International Meeting of Experts on The Use of Criminal Sanction in The Protection of Environment, Internationally, Domestic and Regionally* di Portland, Oregon, Amerika Serikat, tanggal 19-23 Maret 1994.[27]

C. Yurisdiksi Hukum Pidana Indonesia dalam *Cybercrime*

Tindak pidana siber merupakan salah satu kejahatan tarnsnasional dimana kejahatan ini terjadi tanpa batas, dalam hal ini akan terdapat permasalahan terkait dengan yurisdiksi suatu negara dalam hal menegakan hukum apabila terjadi kejahatan siber. Negara Indonesia telah memiliki paying hukum terkiat peraturan perundang-undangan yang khusus mengatur mengenai kejahatan siber dan didalamnya termuat aturan mengenai yurisdiksi yang telah memiliki asas universal yaitu Undnag-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE) Hal ini dapat dilihat dalam Pasal 2 Undang-Undang ITE yang menyebutkan bahwa :

"Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum

[27] Barda Nawawi Arief, (IV), halaman 267.

Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Undang-undang ini memiliki jangkauan yurisdiksi yang sangat luas, pada pokoknya menjelaskan mengenai bahwa Undang-Undang ITE mengatur mengenai perbuatan hukum yang dilakukan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga dapat berlaku untuk perbuatan hukum yang dilakukan diluar wilayah negara Indonesia dan/atau dilkukan oleh warga negara Indonesia maupun warga negara asing yang memiliki akibat hukum di wilayah negara Indonesia dengan menimbulkan kerugian. Yang dimaksud dengan "merugikan" meliputi tetapi tidak terbatas pada kepentingan ekonomi nasioanl, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamnan negara, kedaulatan negara, warga negara serta badan hukum Indonesia.

Di dalam tindak pidana yang tidak bersifat lintas batas negara dikenal tiga macam yurisdiksi:

1. Yurisdiksi legislatif (*jurisdiction to prescribe*), yaitu kekuasaan membuat peraturan atau perundang-undangan yang mengatur hubungan atau status hukum orang atau peristiwa-peristiwa hukum di dalam wilayahnya. Kewenangan seperti ini biasanya dilaksanakan oleh badan legislatif sehingga seringkali disebut pula sebagai yurisdiksi legislatif atau preskriptif.

2. Yurisdiksi yudikatif (*jurisdiction to adjudicate*), yaitu kekuasaan pengadilan untuk mengadili orang (subyek hukum) yang melanggar peraturan atau perundang-undangan.

3. Yurisdiksi eksekutif (*jurisdiction to enforce*), yaitu kekuasaan negara untuk memaksakan atau menegakkan (*enforce*) agar subyek hukum menaati hukum. Tindakan pemaksaan ini dilakukan oleh badan eksekutif negara yang umumnya tampak pada bidang-bidang ekonomi, misalnya kekuasaan untuk menolak atau memberi izin, kontrak-kontrak, dan lain- lain.

Berdasarkan ketiga kategori yurisdiksi di atas, perbuatan yang dapat menimbulkan masalah dalam Undang-Undang ITE adalah ketika Warga Negara Indonesia melakukan tindak pidana di luar wilayah negara Indonesia dan akibatnya tidak timbul di wilayah negara Indonesia. Hal tesebut berkaitan erat dengan masalah yurisdiksi dimana kewenangan mengadili dan penerapan hukum serta kewenangan melaksanakan putusan, karena hal tersebut berkaitan pula dengan keadualayan suatu wilayah dan kedaualatan hukum suatu negara. Karena konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, sehingga dibutuhkan kesepakatan Internasional dan kerjasama dengan negara-negara lain dalam menanggulangi tindak pidana teknologi informasi.

D. Penegekan Hukum Tindak Pidama *Cybercrim*e

Penegakan hukum merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya menjadi pikiran badan pembuat undang-undang yang dirumuskan dalam peraturan-peraturan hukum. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan. Pada kenyataannya proses penegakan hukum memuncak pada

pelaksanaannya oleh para pejabat penegak hukum.[28] Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim adalah salah satu aparat penegak hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutus perkara dengan seadil-adilnya.

Hakim adalah pejabat yang melakukan kekuasaan kehakiman yang diatur dalam Undang-undang Nomor 48 Tahun 2009 tentang kekuasaan kehakiman. Dalam rangka penegakan hukum di Indonesia tugas hakim adalah menegakkan hukum dan keadilan melalui perkara-perkara yang dihadapkan kepadanya. Jaksa adalah aparat penegak hukum yang merupakan pejabat fungsional yang diberikan wewenang oleh undangundang dan pelasanaan putusan pengadilan. Selanjutnya adalah Polisi, polisi sebagai penegak hukum dituntut melaksanakan profesinya secara baik dengan dilandasi etika profesi. Etika profesi tersebut berpokok pangkal pada ketentuan yang menentukan peranan polisi sebagai penegak hukum. Polisi dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketenteraman. Penegakan hukum selalu akan melibatkan manusia di dalamnya dan dengan demikian hal tersebut tingkah laku manusia terlibat di dalamnya. Hukum tidak bias tegak dengan sendirinya sehingga melibatkan aparat penegak hukum, dan aparat dalam mewujudkan tegaknya hukum harus dengan undang-undang, sarana , dan kultur, sehingga hukum dapat ditegakkan dengan seadil-adilnya sesuai dengan cita hukum itu sendiri.

Hal ini menunjukan bahwa tanntangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam

[28] Satjipto Rahardjo,*Penegakan Hukum Suatu Tinjauan Sosiologis*, Genta Publishing, Cetakan 1, Yigyakarta, 2009, hlm. 24.

menerapkan normannya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang dipengaruhi oleh rangsangan dari prilaku masyrakat untuk sama-sama menjadi pelanggar hukum. Pendapat Soerjono Soekanto mengatakan bahwa pokok penegakan hukum terletak pada faktor-faktor yang mempengaruhinya. Faktor-faktor tersebut, adalah sebagai berikut:[29]

1. Faktor hukumnya sendiri, yaitu peraturan perundang-undangan yang berlaku di Indonesia.
2. Faktor penegk hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

Dari kelima faktor tersebut saling berkaitan dengan eratnya karena antara yang satu dengan yang lainnya saling mempengaruhi. Kelima faktor tersebut dapat dikatakan esensi dari penegakan hukum, dan dapat dijadikan tolok ukur daripada keefektifitasan penegak hukum di Indonesia.

Kejahatan teknologi informasi atau cybercrime memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum

[29] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Rajawali Pers, Cetakan 13, Jakarta, 2014, hlm. 8.

Acara Pidana (KUHAP). Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenis-jenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.[30]

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana cybercrime yakni dalam penyelesaian tindak pidana tersebut , kondisi yang paperless (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik. mendasar penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkap tindak pidana tersebut baik pelaku, dan kejahtan yang sering sekali sulit untuk dibuktikan sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana cybercrime.

---

[30] NN, *Tindak Pidana Cybercrime, Repository* Universitas Muhammadiyah Yogyakarta, http://repository.umy.ac.id/
Diakses pada Hari Senin, Tanggal 16 Juni 2020, Pukul 20.59 WIB.

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan tugasnya. Dalam penanganan tindak pidana cybercrime, hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-undan Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undang-undan Nomor 11 tahun 2008. Dalam Pasal 42 UU Undang-undan Nomor 11 tahun 2008 disebutkan : "Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-undang ini." Hal tersebut juga ditegaskan dalam UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 43.

Berdasarkan pasal tersebut sehingga dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan lex genaralis, sedangkan ketentuan acara dalam UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan lex specialis. Dengan demikian sepanjang tidak terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentran yang diatur lain dalam UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE. Pelaksanaan penyelidikan tindak pidana cybercrime agak sedikit berbeda dengan penyelidikan tindak pidana lainya, pejabat dalam hal ini adalah pejabat polisi

Negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan (Pasal 1 angka 4 KUHAP) dihadapkan pada masalah dari mana dan dimana penyelidikan harus dimulai. Akibat perbuatan tindak pidana cybercrime seperti cyber porno, cyber terrorism, hacking , dll baik yang diketahui pertama kali oleh penyelidik yang sedang melukan cyber-patroling maupun berdasarkan laporan dari korban tindak pidana cybercrime, diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringan melalui koneksi internet, ataupun terjun langsung ke warnet-warnet. Proses awal penyelidikan harus melibatkan komputer, alat elektronik seperti handphone maupun android, tablet, dan jaringannya yang terkoneksi dengan suatu jaringan dan terkoneksi melalui internet. Bukti-bukti dalam suatu tindak pidan cybercrime biasanya sealu dapat tersimpan di dalam sistem alat alat elektronik tersebut ataupun sistem komputer.

Dengan Demikian inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita alat alat atau barang elektronik maupun komputer milik tersangka. Dari komputer tersebutlah penyelidikan dapat menentukan apakah ada bukti-bukti tindak pidana. Karakteristik tindak pidana cybercrime berbeda dengan tindak pidana yang lain , karakteristik bentuk tindak pidana cybercrime antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus operandi yang digunakan berbeda. Sehingga dengan demikian dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus. Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-undang Nomor 11 Tahun 2008, yang telah dirubah oleh Undang-undang Nomor 19 Tahun 2016

tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik adalah sebagai berikut;

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana cybercrime.
2. Adanya wewenang khusus yang diberiakan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik.
3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.
4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Upaya penegakan hukum terhadap tindak pidana cybercrime selain dengan aturan-aturan tersebut seharusnya juga diimbangi dengan skill dan kemampuan penegak hukumnya dalam pemberantasan tindak pidana cybercrime. Hal ini dikarenakan modus-modus tindak pidana cybercrime semakin hari semakin berkembang

dikhawatirkan kejahatan tersebut akan merajalela dan pelaku-pelaku sulit untuk dilacak dan ditangkap, sehingga dapat merugikan masyarakat dan Negara dan bahkan dunia luas.

BAB V

PEMBERANTASAN DAN PENANGANAN CYBERCRIME MELALUI PERLUASAN ALAT BUKTI

A. Alat Bukti dalam Sistem Hukum Pembuktian di Indonesia

Dalam sistem hukum pembuktian di Indonesia, terdapat beberapa doktrin pengelompokan alat bukti, yang membagi alat bukti ke dalam kategori *oral evidence, documentary evidence, material evidence, dan electronic evidence.* Berikut pembagian pada masing-masing kategori:

1. *Oral Evidence*
    a. Perdata (keterangan saksi, pengakuan, dan sumpah)
    b. Pidana (keterangan saksi, keterangan ahli, dan keterangan terdakwa)
2. *Documentary Evidence*
    a. Perdata (surat dan pesangkaan)
    b. Pidana (surat dan petunjuk)
3. *Material Evidence*
    a. Perdata (tidak dikenal)
    b. Pidana (barang yang digunakan untuk melakukan tindak pidana, barang yang digunakan untuk membantu tindak pidana, barang yang merupakan hasil dari suatu tindak pidana, barang yang diperoleh dari suatu tindak pidana, dan informasi dalam arti khusus)
4. *Electronic Evidence*
    a. Konsep pengelompokan alat bukti menjadi alat bukti tertulis dan elektronik. Tidak dikenal di Indonesia
    b. Konsep tersebut terutama berkembang di Negara-negara common law.

c. Pengaturannya tidak melahirkan alat nukti baru, tetapi memperluas alat bukti yang masuk kategori *documentary evidence.*

KUHAP telah mengatur mengenai alat bukti yang sah yang dapat diajukan dalam sidang peradilan, pembuktian tidak dirumuskan dalam KUHAP dapat dianggap bahwa alat bukti tersebut tidak memiliki kekuatan hukum yang mngikat. Adapun alat bukti yang sah menurut Pasal 184 KUHAP adalah sebagai berikut :

1. Keterangan Saksi

Keterangan saksi merupakan salah satu alat bukti yang sah sebagaimna disebutkan dalam Pasal 184 KUHAP, pembuktian dalam perkara pidana akan selalu merujuk pada keterangan saksi. Pengertian saksi menurut KUHAP adalah orang yang mengetahui tentang suatu peristiwa hukum pidana yang ia dengar, ia lihat dan ia alami sendiri, sehingga dapat membuat terang suatu peristiwa hukum pidana dalam proses penyidikan, penuntutan serta peradilan

Dalam Pasal 185 KUHAP menjelaskan bahwa, keterangan saksi dapat dinyatakan sebagai alat bukti adalah apabila saksi menyatakan di hadapan pengadilan, keterangan satu orang saksi tidak cukup menjadikan keterangan tersebut sebagai bukti, karena satu orang saksi tidak bisa dianggap sebagai bukti sehingga harus disertai dengn suatu alat bukti yang sah lainnya. Keterangan beberapa saksi yang berdiri sendiri-sendiri tentang suatu kejadian atau keadaan dapat digunakan sebagai suatu alat bukti yang sah apabila keterangan saksi itu ada hubungannya satu dengan yang lain sedemikian rupa, sehingga dapat membenarkan adanya suatu kejadian atau keadaan tertentu. Dalam hal ini jika keterangan yang diberikan oleh saksi merupakan suatu hasil pemikiran saja biak itu merupakan suatu pendapat atau rekaan maka hal tersebut tidak dapat dikatakan sebagai sketerangan saksi.

Dalam menilai kebenaran keterangan seorang saksi, Hakim harus dengan sungguh-sungguh memperhatikan terkait hal-hal beriku, yaitu persamaan keterangan saksi yang satu dengan saksi yang lainnya, persamaan antara keterangan saksi dengan alat bukti lainnya yang berhubungan dengan peristiwa hukum tersebut, dasar yang digunakan oleh saksi dalam hal memberikan keterangan tertentu.

Keterangan dari saksi yang tidak disumpah meskipun sesuai dengan yang lain, tidak merupakan alat bukti, namun apabila keterangan dari saksi yang disumpah dapat dipergunakan sebagai tambahan alat bukti sah yang lain.

Pada umumnya semua orang dapat menjadi seorang saksi, namun demikian ada pengecualian khusus yang menjadikan mereka tidak dapat bersaksi. Hal ini sebagaimana yang tercantum dalam Pasal 168 KUHAP yang pada pooknya menyebutkan bahwa Keluarga sedarah atau semenda dalam garis lurus keatas atau kebawah sampai derajat ketiga dari terdakwa atau bersama-sama sebagai sebagai terdakwa, saudara dari terdakwa atau yang bersama-sama sebagai terdakwa, saudara ibu atau saudara bapak, juga mereka yang mempunyai hubungan karena perkawinan dan anak-anak saudara terdakwa samapai derajat ketiga, dan suami atau istri terdakwa meskipun sudah bercerai atau yang bersama-sama sebagai terdakwa.

Selanjutnya dalam pasal 171 KUHAP juga menambahkan pengecualian untuk memberikan kesaksiaan dibawah sumpah, yakni berbunyi :

a. Anak yang umurnya belum cukup lima belas tahun dan belum pernah kawin;
b. Orang yang sakit ingatan atau sakit jiwa meskipun kadang-kadang ingatannya baik kembali.

Sebagaimana yang telah dijelaskan diatas bahwa keterangan saksi yang dinyatakan dimuka sidang mengenai apa yang ia lihat, ia rasakan, ia alami adalah keterangan sebagai alat bukti (pasal 185 ayat (1)), bagaimana terhadap keterangan saksi yang diperoleh dari pihak ketiga? Misalnya, pihak ketiga menceritakan suatu hal kepada saksi bahwa telah terjadi pembunuhan. Kesaksian demikian adalah disebut *testimonium de auditu*. Sesuai dengan penjelasan KUHAP yang mengatakan kesaksian *de auditu* tidak diperkenankan sebagai alat bukti. Selaras pula dengan tujuan hukum acara pidana yang mencari kebenaran material, dan pula untuk perlindungan terhadap hak-hak asasi manusia dimana keterangan seorang saksi yang hanya mendengar dari orang lain tidak terjamin kebenarannya, maka kesaksian *de auditu* atau *hearsay evidence* patut tidak dipakai di Indonesia pula.

Namun demikian, kesaksian *de auditu* perlu pula didengar oleh hakim. Walaupun tidak mempunyai nilai sebagai bukti kesaksian, tetapi dapat memperkuat keyakinan hakim bersumber pada dua alat bukti yang lain. Dalam hal lain juga dalam KUHAP tentang prinsip minimum pembuktian. Hal ini terdapat dalam pasal 183 yang berbunyi:

"Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia peroleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya".

Dalam pasal 185 ayat (2) juga menyebutkan sebagai berikut: "Keterangan seorang saksi saja tidak cukup membuktikan bahwa terdakwa bersalah terhadap terhadap dakwaan yang didakwakan kepadanya".

M. Yahya Harahap megungkapkan bahwa bertitik tolak dari ketentuan pasal 185 ayat (2), keterangan seorang saksi saja belum dianggap

sebagai suatu alat bukti yang cukup untuk membuktikan kesalahan terdakwa (*unus testis nullus testis*). Ini berarti jika alat bukti yang dikemukakan penuntut umum yang terdiri dari seorang saksi saja tanpa ditambah dengan keterangan saksi yang lain atau alat bukti yang lain, kesaksian tunggal seperti ini tidak dapat dinilai sebagai alat bukti yang cukup untuk membuktikan kesalahan terdakwa sehubungan dengan tindak pidana yang didakwakan kepadanya.

Namun apabila disuatu pesidangan seorang terdakwa mangaku kesalahan yang didakwakan kepadanya, dalam hal ini seorang saksi saja sudah dapat membuktikan kesalahan terdakwa. Karena selain keterangan seorang saksi tadi, juga telah dicukupi dengan alat bukti keterangan terdakwa. Akhirnya telah terpenuhi ketentuan minimum pembuktian yakni keterangan saksi dan keterangan terdakwa.

2. Keterangan ahli

Pengertian keterangan ahli sebagai alat bukti hanya bisa didapat dengan melakukan pencarian dan menghubungkan dari beberapa ketentuan yang terpencar dalam pasal KUHAP, mulai dari Pasal 1 angka 28, Pasal 120, Pasal 133, dan Pasal 179 dengan jalan merangkai pasal-pasal tersebut maka akan memperjelas pengertian ahli sebagai alat bukti :

a. Pasal 1 angka 28

Pasal ini memberi pengertian apa yang dimaksud dengan keterangan ahli, yaitu keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperluakan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan.

b. Pasal 120 ayat (1) KUHAP

Dalam hal penyidik menganggap perlu, ia dapat minta pendapat orang ahli atau orang yang memiliki keahlian khusus. Dalam pasal ini kembali ditegaskan yang dimaksud dengan keterangan ahli ialah orang yang memiliki keahlian khusus yang akan memberi keterangan menurut pengetahuannya dengan sebaik-baiknya.

c. Pasal 133 (1) KUHAP

Dalam hal penyidikan untuk kepentingan peradilan mengenai seorang korban baik luka, keracunan ataupun mati yang diduga karena peristiwa yang merupakan tindak pidana, ia berwenang mengajukan permintaan keterangan ahli kepada ahli kedokteran kehakiman atau dokter dan atau ahli lainnya.

d. Pasal 179 KUHAP menyatakan:

1) Setiap orang diminta pendapatnya sebagai ahli kedokteran kehakiman atau dokter atau ahli lainnya wajib memberi keterangan ahli demi keadilan.
2) Semua ketentuan tersebut diatas untuk saksi berlaku juga bagi mereka yang memberikan keterangan ahli, dengan ketentuan bahwa mereka mengucapkan sumpah atau janji akan memberikan keterangan yang sebaik-baiknya dan yang sebenarnya menurut pengetahuan dalam bidang keahliannya.

Sebenarnya apabila kita hubungkan Pasal 133 dan Pasal 186 KUHAP, maka dapat dilihat bahwa ternyata keterangan saksi tidak hanya diberikan di depan persidangan tetapi juga diberikan dalam rangka pemeriksaan penyidikan.

3. Surat

Alat bukti surat harus dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, diantaranya adalah sebagai berikut :

a. Berita acara atau surat resmi yang telah dibuat oleh pejabat yang berwenang atau yang dibuat dihadapannya, yang di dalamnya memuat mengenai fakta-fakta suatu kejadian baik yang didengar, dilihat atau yang dialaminya sendiri hatus disertai dengan alasan yang jelas dan tegas;
b. Surat yang dibuat menurut ketentuan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksanan yang menjadi tanggungjawabnya dan diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau sesuatu keadaan yang diminta secara resmi dari padanya;
d. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

4. Petunjuk

Dalam KUHAP, alat bukti petunjuk dapat dilihat dalam Pasal 188, Petunjuk adalah perbuatan, kejadian atau keadaan yang karena persamaannya, Keternagan saksi

a. Surat;
b. Keterangan Terdakwa.

Peniaian atas kekuatan pembuktian dari suatu petunjuk atas kekupayan suatu pembuktian dilakukan oleh hakim dengan pemeriksaan yang cermat dan harus berdasarkan hati nuraninya.

Dari penjelasan pasal diatas, maka dapat disimpulkan bahwa petunuk adalah meruapkah salah satu alat bukti yang tidak langsung karena dalam prosesnya hakim haruslah dapat menghubungkan suatu alat bukti dengan alat bukti lainnya dan haruslah memiliih yang ada persamaannya antara yang satu dengan yang lainnya.

5. Keterangan terdakwa

Mengenai keterangan terdakwa diatur dalam KUHAP pada Pasal 189 yang berbunyi sebagai berikut : keterangan terdakwa adalah apa yang ia nyatakan dalam persidangan mengenai perbuatan yang ia ketahui dan ia alami sendiri, keterangan terdakwa yang diberikan diluar persidangan hanya dapat digunakan untuk menemukan bukti yang lainnya dan keterangan terdakwa hanya dapat digunakan terhadap dirinya sendiri, keterangan terdakwa saja tidak cukup untuk mealat bukti lainnya yang mendukung dan sah.

Keterangan terdakwa sebagai alat bukti tidak perlu sama atau terbentur pengakuan. Semua keterangan terdakwa hendaknya didengar, apakah itu berupa penyangkalan, pengakuan ataupun pengakuan sebagaian dari perbuatan atau keadaan.

B. Asas – Asas dalam Pembuktian

Hukum pembuktian dalam *cyber crime* adalah bersifat khusus. Akan tetapi atasnya tetap diharuskan mengacu kepada asas-asas pembuktian yang umum. Beberapa asas dalam hukum acara perdata mengenai pembuktian, yaitu :

1. Asas *Audi Et Alteram Partem*; adalah asas kesamaan proses dan para pihak yang berperkara. Berdasarkan asas ini, hakim tidak boleh menjatuhkan putusan sebelum memberi kesempatan untuk mendengarkan kedua pihak. Hakim harus adil dalam memberikan beban pembuktian pada pihak yang berperkara agar kesempatan untuk kalah atau menang bagi kedua pihak tetap sama.
2. Asas *Actori Incumbit Probatio*; bahwa asas ini terkait dengan beban pembuktian. Asas ini berarti bahwa barangsiapa yang mempunyai suatu hak atau menyangkali adanya hak orang lain, harus membuktikannya. Hal ini berarti bahwa dalam hal pembuktian yang diajukan penggugat dan tergugat sama-sama kuat, maka baik penggugat maupun tergugat ada kemungkinan dibebani dengan pembuktian oleh hakim.
3. Gugatan harus diajukan pada pengadilan dimana tergugat bertempat tinggal atau dikenal dengan "*Actor sequitor forum rei"*

Hukum acara pidana mengenal beberapa macam teori pembuktian yang menjadi pegangan bagi hakim dalam melakukan pemeriksaan terhadap di sidang pengadilan. Sejalan dengan perkembangan waktu, teori atau sistem pembuktian mengalami perkembangan dan perubahan. Demikian pula penerapan sistem pembuktian di suatu negara dengan negara lain dapat berbeda. Adapun sistem atau teori pembuktian yang dikenal dalam dunia hukum pidana yaitu *conviction intime* atau teori pembuktian berdasarkan keyakinan hakim semata-mata, *conviction rasionnee* atau teori pembuktian berdasarkan keyakinan hakim dalam batas-batas tertentu atas alasan yang logis, *positif wettelijk bewijstheorie* atau teori Pembuktian yang hanya

berdasarkan kepada alat-alat pembuktian yang disebut oleh undang-undang secara positif, dan *negatief wettelijk bewijstheorie* atau teori pembuktian berdasarkan keyakinan hakim yang timbul dari alat-alat bukti dalam undang-undang secara negatif, berikut penjelasannya :

1. *Conviction intime* atau Teori pembuktian berdasaran keyakinan hakim semata-mata

   Conviction intime diartikan sebagai pembuktian berdasarkan keyakinan hakim belaka. Teori pembuktian ini lebih memberikan kebebasan kepada hakim untuk menjatuhkan suatu putusan berdasarkan keyakinan hakim, artinya bahwa jika dalam pertimbangan putusan hakim telah menganggap terbukti suatu perbuatan sesuai dengan keyakinan yang timbul dari hati nurani, terdakwa yang diajukan kepadanya dapat dijatuhkan putusan.

   Keyakinan hakim pada teori ini adalah menetukan dan mengabaikan hal-hal lainnya jika sekiranya tidak sesuai atau bertentangan dengan keyakinan hakim tersebut .Sistem ini mengandung kelemahan yang besar, karena sebagai manusia biasa, hakim bisa salah keyakinan yang telah dibentuknya, berhubung tidak ada kriteria, alat-alat bukti tertentu yang harus dipergunakan dan syarat serta cara-cara hakim dalam membentuk keyakinannya itu. Di samping itu, pada sistem ini terbuka peluang yang besar untuk terjadi praktik penegakan hukum yang sewenang-wenang, dengan bertumpa pada alasan keyakinan hakim.

2. *Conviction Rasionnee* atau Teori pembuktian berdasarkan keyakinan hakim dalam batas-batas tertentu atas alasan yang logis Sistem pembuktian *conviction rasionnee* adalah sistem pembuktian yang tetap menggunakan keyakinan hakim, tetapi keyakinan hakim didasarkan pada alasan-alasan (*reasoning)* yang rasional. Dalam sistem ini hakim tidak dapat lagi memiliki kebebasan untuk menentukan keyakinannya, tetapi keyakinannya harus diikuti dengan alasan-alasan yang *reasonable* yakni alasan yang dapat diterima oleh akal pikiran yang menjadi dasar keyakinannya itu.
3. Teori Pembuktian yang hanya berdasarkan kepada alat-alat pembuktian yang disebut oleh undang-undang secara positif
   Sistem pembuktian berdasarkan alat bukti menurut undang-undang secara positif atau pembuktian dengan menggunakan alat-alat bukti yang sebelumnya telah ditentukan dalam undang-undang. Dengan kata lain, keyakinan hakim tidak diberi kesempatan dalam menentukan ada tidaknya kesalahan seseorang, keyakinan hakim harus dihindari dan tidak dapat dijadikan sebagai pertimbangan dalam menentukan kesalahan seseorang.
4. Teori pembuktian berdasarkan keyakinan hakim yang timbul dari alat-alat bukti dalam undang-undang secara negatif
   Pembuktian pembuktian berdasarkan undang-undang secara negatif adalah pembuktian yang selain menggunakan alat-alat bukti yang dicantumkan di dalam undang-undang, juga menggunakan keyakinan hakim. Sekalipun menggunakan keyakinan hakim, namun keyakinan hakim terbatas pada alat-alat bukti yang ditentukan dalam undang-undang. Sistem pembuktian ini menggabungkan antara sistem pembuktian

menurut undang-undang secara positif dan sistem pembuktian menurut keyakinan hakim sehingga sistem pembuktian ini disebut pembuktian berganda (*doubelen grondslag)*.

Dengan demikian, maksud dilakukannya kegiatan pembuktian sebagaimana diatur dalam Pasal 183 KUHAP adalah untuk menjatuhkan atau mengambil putusan *in casu* menarik amar putusan oleh majelis hakim. Pembuktian dilakukan terlebih dahulu dalam usaha mencapai derajat keadilan dan kepastian hukum yang setinggi-tingginya dalam putusan hakim. Sehigga pembuktian tidak hanya ditujukan untuk menjatuhkan pidana saja berdasarkan syarat minimal dua alat bukti yang harus dipenuhi dalam hal pembuktian untuk menjatuhkan pidana.

C. Alat Bukti Elektronik dalam *Cyber Crime*

Berbicara mengenai pembuktian secara elektronik, tidak terlepas dari alat-alat elekrtonik itu sendiri. Proses pembuktian secara elektronik sebagaimana telah dibahas pada bagian sebelumnya, merupakan pembuktian yang melibatkan berbagai hal terkait teknologi informasi seperti informasi dan atau dokumen elektronik dalam perkara Cyber Crime namun tetap mendasarkan pada ketentuan pembuktian sebagaimana diatur dalam Kitab UndangUndang Hukum Acara Pidana serta peraturan perundang-undangan lainnya seperti Undang-Undang Nomor 11 Tahun 2008.

Proses pembuktian secara elektronik, tentu harus didukung oleh berbagai alat-alat bukti secara elektronik pula, dalam hal ini tetap melihat pada ketentuan tentang alat bukti yang sah dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana yang menyebutkan alatalat bukti yang sah terdiri dari : (1) Keterangan saksi; (2) Keterangan ahli; (3) Surat; (4) Petunjuk; (5) Keterangan terdakwa.

Proses pembuktian pada kasus cybercrime pada dasarnya tidak berbeda dengan pembuktian pada kasus pidana konvensional, tetapi dalam kasus cybercrime terdapat ada beberapa hal yang bersifat elektronik yang menjadi hal utama dalam pembuktian, antara lain adanya informasi elektronik atau dokumen elektronik. Ketentuan hukum mengenai pembuktian atas kasus cybercrime telah diatur dalam Pasal 5 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008, yang menyatakan bahwa informasi dan atau dokumen elektronik dianggap sebagai alat bukti yang sah dalam proses pembuktian kasus cybercrime dan alat bukti elektronik tersebut dianggap pula sebagai perluasan dari alat bukti yang berlaku dalam hukum acara pidana yang berlaku di Indonesia, dalam hal ini alat-alat bukti yang terdapat dalam Pasal 184 KUHAP. Minimal, kesalahan pelaku dapat terbukti dengan sekurang-kurangnya 2 (dua) alat bukti yang sah. Alat-alat bukti ini harus mampu membuktikan telah terjadi suatu perbuatan dan membuktikan adanyab akibat dari perbuatan *cybercrime.*\

1. **Keterangan Saksi**

   Sehubungan dengan sifat *cybercrime* yang virtual, sehingga pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung melainkan hanya dapat berupa hasil pembicaraan atau mendengar dari orang lain (*testimonium de auditum*). Meskipun kesaksian jenis ini dianggap tidak sah sebagai alat bukti, dalam praktik tetap dapat dipergunakan sebagai bahan pertimbangan hakim untuk memperkuat keyakinannya dalam menjatuhkan putusan. Yang dapat dijadikan keterangan saksi dalam dunia *cyber,* seperti *chatting* dan *e-mail* antara pengguna internet.

2. Keterangan Ahli

Peran keterangan ahli disini adalah untuk memberikan suatu penjelasan dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum. Saksi ahlimelibatkan ahli-ahli dalam berbagai bidang antara lain, ahli dalam teknologi informasi, mendesain internet, program-program jaringan komputer, serta ahli dalam bidang enskripsi/*password* atau pengamanan jaringan komputer. Pentingnya kedudukan seorang ahli yaitu untuk memberikan keyakinan kepada hakim.

3. Alat Bukti Surat

Surat merupakan alat bukti yang penting dalam proses penyelidikan dan penyidikan kasus *cybercrime*. Surat menajdi alat bukti yang sah dengan didukung oleh keterangan saksi. Secara terminology surat dalam kasus *cybercrime* mengalami perubahan dari bentuk yang tertulis,emjadi tidak tertulis dan bersifat *on-line.* Alat bukti surat dalam sistem komputer ada dua kategori :

a. Bila sebuah sistem komputer yang telah disertifiksi oleh badan yang berwenang maka hasil prin out komputer dapat dipercaya hasil keotentikannya.
b. Bukti sertifikasi dari badan yang berwenang tersebut dapat dikategorikan sebagai alat bukti surat, karena dibuat oleh pejabat yang berwenang.

4. Petunjuk

Pengumpulan data secara fisik dalam *cyber crime* akan sulit dipenuhi, lebih mudah mencari petunjuk-petunjuk yang mengindikasikan telah adanya suatu niat jahat berupa akses

secara tidak sah antara lain dengan melihat dan mendengarkan keterangan saksi di pengadilan atau hasil *print out* data, atau juga dari keterangan terdakwa di pengadilan. Petunjuk yang diajukan di persidangan adalah bukti elektronik (yang disertai dengan keterangan ahli) maka petunjuk ini bersifat lebih kuat dan memberatkan terdakwa.

5. Keterangan Terdakwa

Pasal 189 ayat 1 KUHAP menentukan bahwa keterangan terdakwa adalah ap yang terdakwa lakukan, ketahui dan alam sendiri. Dalam kasus *cybercrime,* keterangan terdakwa yang dibutuhkan terutama mengenai cara-cara pelaku melakukan perbuatannya, akibat yang ditimbulkan, informasi jaringan serta motivasinya. Sifat keterangan terdakwa adalah memberatkan terdakwa.

Sistem hukum pembuktian sampai saat ini masih menggunakan ketentuan hukum yang lama, yang belum mampu menjangkau pembuktian atas kejahatan-kejahatan yang berlaku di *cyberspace*. Namun demikian keberadaan Undang-undang No. 8 tahun 1997 tentang dokumen perusahaan telah mulai menjangkau kea rah pembuktian data elektronik. Walaupun tidak mengatur masalah pembuktian, namun melalui undang-undang ini, pemerintah berusaha mengatur pengakuan atas *microfilm,* dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dpat dialihkan atau ditansformasikan) misalnya Compact Disk-Read Only Memory (CD-ROM) dan Write-One-Read-many (WORM), yang diatur dalam pasal 12 Undang-Undang Dokumen Perusahaan sebagai alat bukti yang sah.

Pasal 12 Undang-undang Dokumen Perusahaan tersebut berbunyi sebagai berikut :

(1) Dokumen perusahaan dapat dialihkan ke dalam *microfilm* atau media lainnya.
(2) Pengalihan dokumen perusahaan ke dalam *microfilm* atau media lainnya sebagaimana dimaksud dalam ayat 1 dapat dilakukan sejak dokumen tersebut dibuat atau diterima perusahaan yang bersangkutan.
(3) Dalam mengalihkan dokumen perusahaan sebagaiman dimaksud dalam ayat 1, pimpinan perusahaan wajib mempertimbangkan kegunaan naskah asli dokumen yang perlu tetap disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau demi kepentingan nasional.
(4) Dalam hal dokumen perusahaan yang dialihkan ke dalam *microfilm* atau sarana lainnya adalah naskah asli yang mempunyai kekuatan hukum pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut.

Kemudian pasal 3 Undang-undang Dokumen Perusahaan member pemahaman secara luas atas alat bukti, yaitu : "*dokumen keuangan terdiri dari catatan, bukti pembukuan dan data pendukuung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan."*

Selanjutnya, pasal 4 menyatakan "*dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen perusahaan"*

Sebuah dokumen perusahaan baru mempunyai kekuatan sebagai alat bukti setelah dilakukan proses pengalihan yang kemudian dilanjutkan dengan proses legalisasi, yang diatur dalam pasal 13 dan 14 Undang-undang Dokumen Perusahaan. Setelah proses pengalihan dan legalisasi, dokumen perusahaan tersebut dinyatakan sebagai alat bukti yang sah sebagaimana disebutkan dalam pasal 15 Undang-undang Dokumen Perusahaan.

a) Pasal 13 : *"Setiap pengalihan dokumen perusahaan sebagaimana dimaksud dalam Pasal 12 ayat (1) wajib dilegalisasi"*

b) Pasal 14 :

   (1) Legalisasi sebagaimana dimaksud dalam Pasal 13 dilakukan oleh pimpinan perusahaan atau pejabat yang ditunjuk di lingkungan perusahaan yang bersangkutan, dengan dibuatkan berita acara.

   (2) Berita acara sebagaimana dimaksud dalam ayat (1) sekurang-kurangnya memuat :

      a. keterangan tempat, hari, tanggal, bulan, dan tahun dilakukannya legalisasi;

      b. keterangan bahwa pengalihan dokumen perusahaan yang dibuat di atas kertas ke dalam mikrofilm atau media lainnya telah dilakukan sesuai dengan aslinya; dan

      c. tanda tangan dan nama jelas pejabat yang bersangkutan.

c) Pasal 15 :

   (1) Dokumen perusahaan yang telah dimuat dalam mikrofilm atau media lainnya sebagaimana dimaksud

dalam Pasal 12 ayat (1) dan atau hasil cetaknya merupakan alat bukti yang sah.

(2) Apabila dianggap perlu dalam hal tertentu dan untuk keperluan tertentu dapat dilakukan legalisasi terhadap hasil cetak dokumen perusahaan yang telah dimuat dalam mikrofilm atau media lainnya.

Pengakuan catatan transaksi elektronik sebagai alat bukti yang sah di pengadilan sudah dirintis oleh *United Nation Commission on Internasional Trade* (UNCITRAL) yang mencantumkan dalam *e-commerce model law* ketentuan mengenai transaksi elektronik diakui sederjat dengan "tulisan" diatas kertas sehingga tidak dapat ditolak sebagai bukti pengadilan. Pasal 5 dan Pasal 6 peraturan ini menyatakan bahwa transaksi yang dilakukan dengan memanfaatkan media elektronik memiliki nilai yang sama dengan tulisan atau akta yang dibuat secara konvensional, sehingga pada praktiknya tidak dapat ditolak suatu bukti transaksi yang dilakukan secara elektronik.

Kemudian peraturan peundang-undangan lain yang memberikan pengakuan terhadap dokumen elektronik adalah Undang-undang Nomor 7 tahun 1971 tetntang Sistem Kearsipan yang menyatakan bahwa suatu informasi elektronik tetap diakui, karena definisi kearsipan tidak pernah menyatakan arsip harus dalam bentuk tertulis dalam media kertas saja tapi dimungkinkan juga untuk disimpan dalam media lainnya. Dalam UU tersebut yang dimaksud dengan arsip ialah :

a. Naskah-naskah yang dibuat dan diterima oleh lembaga-lembaga Negara dan badan-badan pemerintahan dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan tugas pemerintah.

b. Naskah-naskah yang dibuat dan diterima oleh badan-badan swasta dan/atau perorangan, dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kehidupan kebangsaan.

Dalam Rancangan Undang-undang Teknologi Informasi memuat hal yang baru mengenai data elektronik yaitu dengan mengakui data elektronik yang terdapat pada ruang maya. Hal ini dapat dilihat pada BAB I mengenai ketentuan Umum, Pasal 1 angka 16, yaitu :

> "Dokumen Elektronik adalah setiap informasi yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam media magnetic, optikal, memori komputer atau media elektronik"

Berdasarkan ketentuan diatas, maka berkenaan dengan dokumen elektronik sebagai alat bukti pada *cybercrime* harus juga dibarengi oleh alat bukti lainnya sehingga sesuai dengan ketentuan alat bukti minimum dalam KUHAP. Keabsahan dokumen elektronik harus mendapatkan keyakinan dari hakim bahwa dokumen tersebut memang benar digunakan untuk melakukan *cybercrime.*

BAB VI
KAITAN ANTARA HAKI DENGAN *CYBER LAW*

A. Pengertian HaKI

Hak Kekayaan Intelektual (HaKI), merupakan hak eksklusif yang diberikan negara kepada seseorang, sekelompok orang, maupun lembaga untuk memegang kuasa dalam menggunakan dan mendapatkan manfaat dari kekayaan intelektual yang dimiliki atau diciptakan. Istilah HAKI merupakan terjemahan dari *Intellectual Property Right (IPR)*, sebagaimana diatur dalam undang-undang Nomor 7 Tahun 1994 tentang pengesahan WTO (Agreement Establishing The World Trade Organization). Pengertian Intellectual Property Right sendiri adalah pemahaman mengenai hak atas kekayaan yang timbul dari kemampuan intelektual manusia, yang mempunyai hubungan dengan hak seseorang secara pribadi yaitu hak asasi manusia (human right).[31]

Jadi HaKI pada umumnya berhubungan dengan perlindungan penerapan ide dan informasi yang memiliki nilai jual. HakI merupakan kekayaan pribadi yang dpat dimiliki dan diperlakukan sama dengan bentuk-bentuk kekayaan lainnya.[32] Hak Kekayaan Intelektual dipergunakan untuk mewadahi hak-hak yang timbul dari hasil kreasi intelektual manusia yang mempunyai nilai ekonomi bagi pencipta, perancang, penemu atau pemiliknya. Oleh karenanya Hak Kekayaan Intelektual masuk dalam bidang hukum harta benda (benda tak berwujud).

---

[31] Tomi Suryo, *Hak Kekayaan Intelektual (HKI) di Era Globalisasi, Sebuah Kajian Kontemporer*, Graha Ilmu, Yogyakarta, 2010, hlm. 1.

[32] Tim Lindsey, dkk, *Hak Kekayaan Intelektual Suatu Pengantar,*Bandung, PT Alumni, 2013, hlm.3.

Karya cipta berwujud dalam bahasan bidang kekayaan intelektual yang dapat didaftarkan untuk memperoleh perlindungan hukum, yaitu seperti karya kesusastraan, artistik, ilmu pengetahuan (scientific), pertunjukan, kaset, penyiaran audio visual, penemuan ilmiah, desain industri, paten, merek dagang, nama usaha, dan lain sebagainya. Jadi pada prinsipnya HKI merupakan suatu hak kekayaan yang berada dalam ruang lingkup kehidupan manusia di bidang teknologi, ilmu pengetahuan, maupun seni dan sastra, sehingga pemilikannya bukan terhadap barangnya melainkan terhadap hasil kemampuan intelektual manusianya dan tentu harus berwujud. Pemerintah mempunyai kewajiban untuk melindungi secara hukum dari ide, gagasan dan informasi yang mempunyai nilai komersial atau nilai ekonomi yang telah dihasilkan oleh seseorang maupun kelompok tersebut.Hak kekayaan Intelektual (HKI) memberikan hak monopoli kepada pemilik hak dengan tetap menjujung tinggi pembatasan-pembatasan yang mungkin diberlakukan berdasarkan peraturan perundang-undangan yang berlaku.

Direktorat Jenderal Hak Kekayaan Intelektual di dalam buku panduan HKI menjelaskan bahwa Hak Kekayaan Intelektual atau yang disingkat "HKI" atau akronim "HaKI", adalah padanan kata yang biasa digunakan untuk Intellectual Property Rights (IPR), yakni hak yang timbul bagi hasil olah pikir otak yang menghasilkan suatu produk atau proses yang berguna untuk manusia. Pada intinya HKI adalah hak untuk untuk menikmati secara ekonomis hasil dari suatu kreatifitas intelektual. Objek yang diatur dalam HKI adalah karya-karya yang timbul atau lahir karena kemampuan intelektual manusia.[33]

[33] Buku Panduan Hak Kekayaan Intelektual (Direktorat Jenderal Hak Kekayaan Intelektual, 2013)

Dasar dari Hak Kekayaan Intelektual didasarkan pada suatu pandangan bahwa hak tersebut lahir dari karya-karya intelektual yang dihasilakan oleh manusia, dalam proses pembuatan suatu karya intelektual sudah barang tentu memerlakukan sauatu keahlian khusus, ketekunan dan juga pengorbanan baik waktu, tenaga maupun pemikiran yang dituangkan dalam karya tersebut. Pada hakikatnya kepemilikan hak atas karya intelektual merupakan suatu hal yang sangat abstrak jika dibandingkan dengan kepemilikan hak benda yang dapat terlihat namun keduanya meiliki sifat mutlak. Selanjutnya, terdapat analogi bahwa setelah benda yang tak berwujud itu keluar dari pikiran manusia, menjelma dalam suatu ciptaan kesusastraan, ilmu pengetahuan, kesenian atau dalam bentuk pendapat. Jadi, berupa berwujud (lichamelijke zaak) yang dalam pemanfaatannya (exploit) dan reproduksinya dapat merupakan sumber keuntungan uang. Inilah yang membenarkan penggolongan hak tersebut ke dalam hukum harta benda yang ada.[34]

B. Pengaturan Hak Kekayaan Intelektual

1. Pengaturan Hukum Hak Kekayaan Intelektual dalam Hukum Internasional

Seiringa dengan berkembangnya zaman dan dunia teknologi informasi, bekremabnganya pula mengenai hukum yang berkaitan dengan Hak Kekayaan Intelektual yang pada umumnya bersifat melintasi batas negara. Negara berperan aktif dalan hal penegakan hukum melalui sistem hukumnya sebagai salah satu bentuk perlindungan Hak Kekayaan Inteletual Negara akan menindak tegas siapa saja yang melanggar perraturan mengabi Hak Kekyaan Intelektual,

[34] Muhammad Djumhana & R. Djubaedillah, *Hak Milik Intelektual (Sejarah, Teori dan Prakteknya di Indonesia)*, Bandung, Citra Aditya Bakti, 1997, hlm. 18.

karena perdagangan internasional sudah sedemikian meluas maka produk tidak hanya dinikmati oleh nagara asalnya saja, namun juga dinikmati di seluruh dunia. Ketentuan hukum mengenai Hak Kekayaan Intelektual untuk pertama kalinya dilakukan di Venesia, yakni aturan Paten yang mulai berlaku pada tahun 1470. Upaya harmonisasi (penyelarasan aturan secara internasional) tentang Hak Kekayaan Intelektual pertama kali terjadi pada tahun 1883 dengan lahirnya Paris Convention[35]

Di dalam tatanan internasional, Hak Kekayaan Intelektual berkembang cukup pesat dan menjadi salah satu identitas yang menunjukkan suatu era globalisasi sekarang. Aspek-Aspek Hak Kekayaan Intelektual dalam Perdagangan Internasional World Trade Organization (WTO)diratifikasi oleh lebih dari 150 negara berisi norma dan standar perlindungan bagi karya-karya intelektual. Berikut ini berbagai instrumen hukum internasional yang mengatur tentang Hak Kekayaan Intelektual.

a. *Convention Establishing The World Intellectual Property Organization (WIPO)* diadakan di Stockholm tahun 1967, yang kemudian diratifikasi Indonesia melalui Keputusan Presiden Nomor 24 Tahun 1979 yang telah dirubah dengan Keputusan Presiden Nomor 15 Tahun 1997. WIPO adalah perjanjian khusus di bawah Konvensi Bern. Setiap Pihak harus mematuhi ketentuan-ketentuan substantif tentang Perlindungan Karya Sastra dan Seni (1886).

[35] Haris Munandar dan Sally Sitanggang, *Mengenal Hak Kekayaan Intelektual, Hak Cipta, Paten,Merek, dan Seluk-Beluknya*, Erlangga,Jakarta, 2008, hlm.6.

b. *Paris Convention for The Protection of Industrial Property Rights* (Paris Convention) di bidang hak milik perindustrian ditandatangani di Paris pada tanggal 20 Maret 1883. Konvensi ini diratifikasi dengan Keputusan Presiden Nomor 15 Tahun 1997, membahas mengenai perlindungan terhadap industrialpropertyuntuk membantu rakyat satu negara mendapatkan perlindungan di negara-negara lain untuk kreasi intelektual mereka dalam bentuk hak kekayaan industri, dikenal sebagai: Penemuan (paten), Merek dagang, Desain industri.

c. *Berne Convention for The Protection of Literary and Artistic Works (Berne Convention)* di bidang Hak Cipta, ditandatangani di Berne, 9 September 1986. Indonesia meratifikasi dengan dengan Keputusan Presiden Nomor 18 Tahun 1997.Konvensi Bern mewajibkan penandatangan mengakui hak cipta dari karya-karya penulis dari negara-negara penandatangan lain.

d. *Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs)* yang mulai berlaku pada tanggal 1 Januari 1995. Perjanjian ini membahas perdagangan barang palsu untuk, meningkatkan perlindungan terhadap hak atas kekayaan intelektual dari produk-produk yang diperdagangkan, Menjamin prosedur pelaksanaan hak atas kekayaan intelektual yang tidak menghambat kegiatan perdagangan;, merumuskan aturan serta disiplin mengenai pelaksanaan perlindungan terhadap hak atas kekayaan intelektual, dan

mengembangkan prinsip, aturan dan mekanisme kerjasama internasional

e. *Agreement Establishing World Trade Organization (WTO)* yang diratifikasi dengan Undang-Undang Nomor 7 Tahun 1994. World Trade Organization (WTO) atau Organisasi Perdagangan Dunia merupakan satu-satunya badan internasional. Sistem perdagangan multilateral WTO diatur melalui suatu persetujuan yang berisi aturan-aturan dasar perdagangan internasional sebagai hasil perundingan yang telah ditandatangani oleh negara-negara anggota.

f. *Trademark Law Treaty*, mengatur perlindungan terhadap Merek, disahkan di Genewa pada tanggal 27 Oktober 1997, diratifikasi Indonesia melalui Keputusan Presiden Nomor 17 Tahun 1997. Perjanjian ini membahasperjanjian dari praktek merek dagang untuk menyelaraskan mencakup, antara jangka waktu pendaftaran dan pembaharuan pendaftaran merek dagang akan sepuluh tahun dan layanan tanda diberi perlindungan yang sama.

g. *Patent Cooperation Treaty (PCT)*, yaitu perjanjian kerjasama di bidang Paten. Indonesia meratifikasinya dengan Keputusan Presiden Nomor 16 Tahun 1997. Perjanjian ini membahas mengenai para negara pihak :

   1) Ingin memberi kontribusi pada kemajuan ilmu pengetahuan dan teknologi;
   2) Penyempurnaan perlindungan hukum terhadap penemuan;

3) Penyederhanaan dan membuat lebih ekonomis dalam memperoleh perlindungan penemuan;
4) Mempermudah dan mempercepat akses oleh masyarakat dengan informasi teknis yang terkandung dalam dokumen yang menjelaskan penemuan baru.[36]

2. Pengaturan Hukum Hak Kekayaan Intelektual dalam Hukum Positif di Indonesia

Sejarah lahirnya pertauran mengenai Hak Kekayaan Inteletual di Indonesia di mulai pada tahun 1953, dimana ada suatu Rancangan pearuran perundang-undanagn di bidang Hak Kekayaan Inteltual yang memuat mengenai Paten dan kemudian pemerintah Indonesia melalui Menteri Kehakiman Republik Indonesia menerbitkan surat edaran Nomor : J. S. 5/41 tanggal 12 Agustus 1954 dan Nomor J.G. 1/2/17 tanggal 29 Oktober 1953 tentang Pendaftaran Sementara Paten, hal ini dilakukan agar tidak adanya kekosangan hukum karena Undang-Undang Paten masih dalam proses pembuatan. Kemudian pada tahun 1989 awal mula disahkannya Undang-Undang Nomor 6 Tahun 1989 tentang Paten, kemudian dilakukan amandemen pada tahun 1997 yang di ubah menjadi Undang-Undnag Nomor 13 Tahun 1997 Tentang Paten, hal ini lah yang menjadi tonggak lahirnya pertauran hukum nasional yang terkiat dengan Hak Kekayaan Intelektual.

Setelah mengalami beberapa perkembangan, maka peraturan perundang-undangan yang terkait dengan Hak Kekayaan Intelektual adalah sebagai berikut :

[36] *Ibid.,* hlm. 9.

a. Undang-Undang Nomor 29 Tahun 2000 tentang Perlindungan Varietas Tanaman;
b. Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang;
c. Undang-Undang Nomor 31 Tahun 2000 tentang Desain Industri;
d. Undang-Undang Nomor 32 Tahun 2000 tentang Desain Tata Letak Sirkuit Terpadu;
e. Undang-Undang Nomor 14 Tahun 2001 tentang Paten;
f. Undang-Undang Nomor 8 Tahun 2014 tentang Hak Cipta;
g. Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis.

Penegakan hukum dalam tindak pidana yang berkaitan dengan Hak Kekayaan Intelektual memiliki pengaruh yang cukup signifikan dalam perkembangan ilmu pengetahuan dan teknologi di wilayah negara Indonesia. Hak Kekayaan Intelektual hadir sebagai bentuk keseimbnagan untuk mencegah timbulnya suatu konflik yang dapat merugikan orang lain bahkan negara. Dengan hadirnya payung hukum yang mengatur mengenai Hak Kekyaan Intelektual diharapkan dapat saling melengkapi sehingga tidak akan terjadi keksongan hukum.

C. Ruang Lingkup Hak Kekayaan Intelektual

Istilah Hak Kekayaan Intelektual sebagai hak milik intelektual dan hak tak berwujud, pengertian Hak Kekayaan Intelektual merujuk pada hubungan proses berfikir manusia yang rasional bahwa kenyataan itu membutuhkan sebuah usaha. Di dalam ketentuan Pasal 2 Ayat 8

Konvensi Pendirian WIPO yang cakupan Hak Kekayaan Intelektual didefinisikan sebagai berikut:[37]

"Intellectual property shall incude the rights relating to :

a. *Literary, artistic and scientific works,*
b. *Performance of performing artists, phonograms, and broadcastas,*
c. *Inventions in all fields of human endeavour,*
d. *Scientific discoveries,*
e. *Industrial designs,*
f. *Trademarks, service marks, and commercial names and designations, 7) Protection against unfair competition,*
g. *And all other rights resulting from intel*

Secara umum, Hak Kekayaan Intelektual terbagi menjadi 2 (dua) bagian, yaitu:

1. Hak Cipta (*copyright*)

   Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta: "Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan"

   Hak Cipta. adalah hak eksklusif bagi pencipta atau penerima hak untuk mengumumkan atau memperbanyak ciptaannya atau memberi izin untuk itu dengan tidak mengurangi pembatasan menurut Peraturan Perundang-undangan yang berlaku.

[37] Muhammad Akham Subroto dan Suprapedi, *Pengenalan Hak Kekayaan Intelektual*, Indeks, Jakrta, 2008, hlm. 15.

Pencipta, adalah seorang atau bebetapa orang yang secara bersama-sama yang atas inspirasinya melahirkan suatu ciptaan berdasarkan kemampuan pikiran, imajinasi, kecekatan, keterampilan, dan keahlian yang dituangkan dalam bentuk yang khas dan bersifat pribadi.

Perlindungan Hak Cipta. Perlindungan terhadap suatu ciptaan timbul secara otomatis sejak ciptaan itu diwujudkan dalam bentuk nyata. Pendaftaran ciptaan tidak merupakan suatu kewajiban untuk mendapatkan hak cipta. Namun demikian, pencipta maupun pemegang hak cipta yang mendaftarkan ciptaannya akan mendapat surat pendaftaran ciptaan yang dapat dijadikan sebagai alat bukti awal di Pengadilan apabila timbul sengketa di kemudian hari terhadap ciptaan tersebut

2. Hak Milik Perindustrian, yang terdiri dari:
   a. Paten (Patent)

      Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 14 Tahun 2001 tentang Paten: "Paten adalah hak eksklusif yang diberikan negara kepada inventor atas hasil invensinya di bidang teknologi, yang untuk selama waktu tertentu melaksanakan sendiri invensinya tersebut atau memberikan persetujuannya kepada pihak lain untuk melaksanakannya."
   b. Merek (Trademark)

      Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis: "Merek adalah tanda yang dapat ditampilkan secara grafis berupa gambar, logo, nama, kata, huruf, angka,

susunan warna, dalam bentuk 2 (dua) dimensi dan/atau 3 (tiga) dimensi, suara, hologram, atau kombinasi dari 2 (dua) atau lebih unsur tersebut untuk membedakan barang dan/atau jasa yang diproduksi oleh orang atau badan hukum dalam kegiatan perdagangan barang dan/atau jasa."

c. Desain Industri (Industrial Design)

Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 31 Tahun 2000 tentang Desain Industri: "Desain industri adalah suatu kreasi tentang bentuk, konfigurasi, atau komposisigaris atau warna, atau berbentuk tiga dimensi atau dua dimensi yang memberikan kesan estetis dan dapat diwujudkan dalam pola tiga dimensi atau dua dimensi serta dapat dipakai untuk menghasilkan suatu produk, barang komoditas industri, atau kerajinan tangan."

d. Desain Tata Letak Sirkuit Terpadu

Berdasarkan Pasal 1 Angka 1 dan 2 Undang-Undang Nomor 32 Tahun 2000 Tentang Desain Tata Letak Sirkuit Terpadu: "Sirkuit terpadu adalah suatu produk dalam bentuk jadi atau setengah jadi, yang di dalamnya terdapat berbagai elemen, dan sekurang-kurangnya satu dari elemen tersebut adalah elemen aktif, yang sebagian atau seluruhnya saling berkaitan serta dibentuk secara terpadu di dalam sebuah bahan semi konduktor yang dimaksudkan untuk menghasilkan fungsi elektronik."

e. Perlindungan Varietas Tanaman

Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 29 Tahun 2000 tentang Perlindungan Varietas Tanaman: "Perlindungan Varietas Tanaman yang selanjutnya disingkat PVT adalah suatu perlindungan khusus yang diberikan negara, yang dalam hal ini diwakili oleh Pemerintah dan pelaksanaannya dilakukan oleh Kantor Perlindungan Varietas Tanaman, terhadap Varietas Tanaman yang dihasilkan oleh pemulia tanaman melalui kegiatan pemuliaan tanaman"

f. Rahasia Dagang

Menurut Pasal 1 Angka 1 Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang: "Rahasia dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang".

Ruang linkup dari Hak Kekayaan Intelektual mencakup didalamnya yaitu hak milik dalam lingkup kehidupan manusia seperti teknologi, ilmu pengentahuan, ataupun sebuah seni dan juga sastra. Kepemilikan Hak Kekyaan Inteltual bukan tertelatk pada sebuah barang yang dihasilan melainkan terhadap hasil intelektual berupa ide atau pemikiran yang memiliki kekhasan. Menurut W.R. Cornish, milik intelektual melindungi pemakaian ide dan informasi yang mempunyai nilai komersial atau nilai ekonomi.[38] Hak Kekayaan Intelektual baru ada jika kemampuan intelektual manusia itu membentuk sesuatu, baik itu yang bisa

[38] Muhammad Djumhana R. Djubaedillah, *Op. Cit.,* hlm. 17.

dilihat, didengar, dibaca, maupun digunakan dengan praktis. David I. Bainbridge mengatakan:

> *"Intellectual property is the collective name given to legal rights which protects the product of human intellect. The term intellectual property seem tobe the best available to cover the body of legal rights which arise from mental and artistic endeavour."*

Dari uraian di atas maka dapat diketahui bahwa bentuk nyata dari karya intelektual tersebut bisa di bidang tata teknologi, ilmu pengetahuan ataupun seni dan sastra.Sebagai suatu hak milik yang timbul dari karya, karsa, cipta manusia atau dapat pula dikatakan sebagai hak yang timbul karena lahir dari kemampuan intelektualitas manusia, maka harus diakui bahwa yang telah menciptakan tersebut boleh menguasainya untuk tujuan yang menguntungkannya. Kreasi sebagai milik berdasarkan postulat hak milik dalam arti seluasluasnya yang juga meliputi milik yang tidak berwujud. Esensi terpenting dari setiap bagian Hak Kekayaan Intelektual yaitu adanya suatu ciptaan tertentu (*creation*).

Hak Kekayaan Intelektual, sebagai bagian dari hukum benda (hukum kekayaan), maka pada prinsipnya adalah pemiliknya bebas dalam berbuat apa saja sesuai dengan kehendaknya dan memberikan isi yang dikehendakinya sendiri pada hubungan hukumnya. Hanya di dalam perkembangan selanjutnya kebebasan itu mengalami perubahan. Misalnya terkait dengan adanya suatu pembatasan berupa adanya lisensi wajib, pengambilalihan oleh negara, ataupun kreasi dan penciptaan tidak boleh bertentangan dengan kesusilaan dan ketertiban umum.

Perubahan pengaturan tersebut masih bertumpu pada sifat asli yang ada pada Hak Kekayaan Intelektual itu sendiri, di antaranya:

a. Mempunyai jangka waktu terbatas

   Setelah habis masa perlindungannya, ciptaan (penemuan) tersebut akan menjadi milik umum. Namun, ada pula yang setelah habis masa perlindungannya bisa diperpanjang terus, misalnya, Hak Merek. Jangka waktu perlindungan Hak Kekayaan Intelektual ini ditentukan secara jelas dan pasti dalam undang-undangnya.

b. Bersifat eksklusif dan mutlak

   Hak tersebut dapat dipertahankan terhadap siapapun. Pemiliknya dapat menuntut pelanggarnya. PemilikHak Kekayaan Intelektual mempunyai suatu hak monopoli, yaitu dia dapat mempergunakan haknya dengan melarang siapapun tanpa persetujuannya membuat ciptaan/penemuan ataupun menggunakannya.

c. Bersifat hak mutlak yang bukan kebendaan

   Di dalam hal pemanfaatannya, berdasarkan ketentuan Pasal 50 Kitab Undang-Undang Hukum Perdata disebutkan bahwa hak milik adalah hak untuk menikmati kegunaan suatu benda dengan leluasa dan untuk berbuat bebas terhadap kebendaan itu dengan kedaulatan sepenuhnya asal tidak bersalahan dengan undang-undang atau peraturan umum yang ditetapkan oleh suatu kekuasaan yang berhak menetapkannya dan tidak mengganggu hak orang lain.

D. Perlindungan HaKI dalam *Cyber Law*

Salah satu keterkaitan teknologi informasi yang saat ini mejadi perhatian adalah pengaruhnya terhadap eksistensi Hak Atas Kekayaan Intelektual (HAKI), di samping terhadap bidang-bidang lain seperti transaksi bisnis (eletronik), kegiatan *e-government*, dan lain-lain. Kasus-kasus terkait dengan pelanggaran Hak Cipta dan Merek melalui sarana internet dan media komunikasi lainnya adalah contoh yang marak terjadi saat ini. Di samping itu pelanggaran hukum dalam transaksi eletronik juga merupakan fenomena yang sangat mengkhawatirkan mengingat tindakan *carding, hacking, cracking,* dan *cybersquating* telah menjadi bagian dari aktivitas internet yang telah menjadikan Indonesia disorot dunia Interntional. *Cyber Crime* dilakukan oleh subjek yang menggunakan sarana teknologi canggih dan sulit dilacak keberadaannya bahkan seringkali dilakukan dari luar teritori Indonesia atau sebaliknya, Sehingga menjadi persoalan yang seringkali sulit terpecahkan.

Dalam *Cyber Law,* Hak Kekayaan Intelektual memiliki kedudukan yang sangat khusus mengingat kegiatan dalam *cyber crime* sangat lekat dengan pemanfaatan teknologi informasi berbasis pada perlindungan rezim hukum Hak Cipta, Merek, Paten, Rahasia Dagang, Desain Industri dll. Seiring dengan perkembangan zaman yang ditandai dengan lahirnya aktivitas virtual dan internet, hukum mengenai Hak Kekayaan Intelektual mendapatkan tantangan baru. Permasalahan yang timbul saat ini mengenai perlindungan terhadap program computer, dan objek hak cipta lainnya yang ada dalam aktivitas siber.

Berdasarkan teori negara hukum yang demokratis, pengaturan terkait *cybersquatting* ditujukan tidak hanya untuk memberikan perlidungan dan keadilan bagi pemilk merek, melainkan juga

menguoayakan tercapainya suatu peningkatan kesejahteraan melalui penggunaan merek sebagai nama domain. Keadilan bagi pemilik merek tetap dapat ditegakan meskipun penggunaan merek oleh para *cybersqutter* merupakan bentuk baru penggunaan merek yang memang belum diatur dalam Undang-Undang Nomor 15 Tahun 2001 Tentang Merek (untuk selanjutnya disebut sebagai Undnag-Undang Merek). Penggunaan merek sebagai nama domain oleh pihak lain secara tabpa hak dapat terjadi karena ketiadaan pemeriksaan terhadap keniripan dalam proses pendaftaran nama domain. *Cybersquatter* memanfaatkan celah atau kelemahan dalam prinsip pendaftaran nama domain yang dilakukan berdasarjab prinsip pendaftaran nama domain yang dilakukan berdasarkan prinsip pendaftar pertama. [39]

Risiko penyalahgunaan merek dalam dunia Teknologi Informasi sebagai nama domain dalam prakti *cybersquatting* menjadi bukti bahwa risiko yang dihadapi pemilik merek tidak hanya dapat terjadi di dunai nyata dalam bentuk pelanggaran merek konvensional berupa pemasaran merek atau penggunaan merek unrtuk produk palsu, melainkan pula risiko dalam dunia maya dalam bentuk *cybersquatting* sebagai bentuk baru pelanggaran merek di internet. Menurut Eric H. Smith manfaat Hak Kekayaan Intelektual tidak terkecuali di dalamnya termasuk merek sangat erat kaitannya engan ekonomi dan investasi. Pelaksanaan Hak Kekayaan Intelektual akan membawa manfaat bagi sebuah negara, antara lain meningkatkan pertumbuhan ekonomi domestik.[40]

Dalam praktik *cybersquatting,* merek menjadi obyek pelanggaran hak yang dilakukan oleh para *cybersquatter*, di Indonesia gugatan

[39] Muhammad Amirulloh, *Cyber Law Perlindnungan Merek Dalam Cyber Space (Cybersquatting terhadap Merek)*, Refika Aditama, Bandung, 2017, hlm. 80.
[40] Eric H. Smith, dikutip dalam *Ibid.,* hlm. 82.

ganti rugi terhadap warga negara Indonesia (WNI) atau badan hukum Indonesia yang melakukan pelanggaran terhadap merek terdaftar sebagai nama domain tanpa hak dapat dilakukan dengan berdasarkan pada Undang-Undang Merek. Pengertian merek diatur dalam Pasal 1 Angka 1 Undang-Undang Merek, yang menyatakan :

> "Merek adalah tanda yang dapat ditampilkan secara grafis berupa gambar, logo, nama, kata, huruf, angka, susunan warna, dalam bentuk 2 (dua) dimensi dan/atau 3 (tiga) dimensi, suara, hologram, ataui kombinasi, dari 2 (dua) atau lebih unsur tersebut untuk membedakan barang dan/atau jasa yang diproduksi oleh orang atau badan hukum dalam kegiatan perdagangan barang dan/atau jasa."

Kata tanda dapat diartikan secara luas melalui penafsiran yang luas sehingga juga meliputi nama domain itu sendiri, mengingat nama domain juga merupakan tanda yang berfungsi sebagai penunjuk alamat dalam aktivitas di internet. Unsur diguakan dalam perdagangan barang/jasa dalam pengertian merek, harus pula diartikan bahwa nama domain dalam internet sebagai tempat melakukan *e-commerce* juga merupakan sarana perdagangan barang/jasa. Nama domain dalam hal ini dapat diibaratkan sebagai took virtual tempat melakukan kegiatan jual beli, penawaran, bahkan tanda tangan kontrak dalam suatu proses transaksi jual beli barang/jasa.

Penggunaan merek terdaftar milik orang lain sebagai suatu nama domain tanpa izin juga harus dikualifikasikan sebagai perbuatan yang dilakukan drngan itikad buruk sebagaiman diatur dalam Pasal 21 ayat (3) Undang-Undang Merek mengingat bahwa dengan perbuatan tersebut dimaksudkan untuk memperoleh keuntungan secara tidak jujur dengan memanfaatkan reputasi merek orang lain dengan

melakukan penyesatan terhadap kinsumen. Adanya upaya untuk mendaftarkan suatu merek dari suatu nama domain yang dilakukan setelah suatu nama domain terdaftar lebih dahulu, membuat ketentuan tentang itikad baik ini sangat relevan untuk dikaji agar pendaftaran merek dari suatu nama domain hasil *cybersquatting* dapat ditolak karena melanggar prinsip itikad baik.

Terkait hal tersebut bagi yang merasa dirugikan dapat menempuh upaya hukum melalui gugatan ganti rugi perdata, hak untuk melakukan gugatan ganti rugi perdata terhadap pelanggaran merek diatur dalam Pasal 83 ayat (1) Undang-Undang Merek yang pada pokoknya menyebutkan bahwa pemilik merek terdaftar dan/atau penerima Lisensi Merek terdaftar dapat mengajukan gugatan terhadap pihak lain yang secara tanpa hak menggunakan Merek yang mempunyai persamaan pada pokoknya atau keseluruhannya untuk barang dan/atau jasa yang sejenis, berupa gugatan ganti rugi dan/atau pengehentian semua perbuatan yang berkaitan dengan penggunaan merek tersebut. Dengan rumusan yang jelas tersebut, maka rumusan dalam Pasal 83 ayat (1) Undang-Undang Merek menjadi dapat diharmonisasikan dengan Pasal 38 ayat (1) Undnag-Undang ITE yang pada pokoknya menyebutkan bahwa setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan system elektronik dan/atau menggunakan teknologi informasi yang menimbulkan kerugian., sehingga maksud pengaturan dalam Undang-Undang ITE dapat secara nyata dirumuskan oleh Undang-Undnag Merek.[41]

[41] *Ibid.,* hlm. 104.

BAB VII
PERLINDUNGAN KONSUMEN DALAM TRANSAKSI E-COMMERCE

A. Pengertian Perlindungan Konsumen

Undang-undang Nomor 8 Tahun 1999 tentang perlindungan konsumen telah mengatur mengenai pengertian perlindungan konsumen yakni terdapat di pasal 1 angka 1 yang berbunyi "Perlindungan Konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada Konsumen." Pengertian perlindungan Konsumen terdapat dalam pasal tersebut, dirasa cukup memadai. Kalimat yang menyatakan "segala upaya yang menjamin adanya kepastian hukum", menjadi harapan untuk dapat meniadakan tindakan sewenang-wenang yang justru dapat merugikan pelaku usaha hanya demi untuk kepentingan perlindungan Konsumen, begitu pula sebaliknya menjamin kepastian hukum bagi konsumen. [42]

Kepastian hukum dilakukan guna melindungi hak-hak konsumen, yang diperkuat melalui undang-undang khusus tersendiri, memberikan harapan agar pelaku usaha tidak dapat bertindak sewenang-wenang yang selalu merugikan hak konsumen. Dengan dibentuknya Undang-undang perlindungan konsumen beserta perangkat hukum lainnya, konsumen memiliki hak dan posisi yang sama serta berimbang, mereka pun bisa menggugat maupun menuntut jika suatu saat ternyata hak-hak konsumen telah dirugikan atau dilanggar oleh pelaku usaha.

Berbicara mengenai konsumen, Undang-undang Nomor 8 Tahun 1999 tentang perlindungan konsumen telah mencantumkan pengertian konsumen yakni setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri,

[42] Ahamadi Miru dan Sutarman Yodo, *Hukum Perlindungan Konsumen,* Jakarta, PT. Raja Grafindo Persada, 2004, hlm. 1.

keluarga, orang lain, maupun makhluk hidup lain dan tidak untuk diperdagangkan. Karena posisi konsumen yang lemah maka ia harus diberikan perlindungan oleh hukum.

Prinsip kedudukan konsumen dalam hubungan dengan pelaku usaha antara lain prinsip *let the buyer beware*, kedudukan pelaku usaha berada di posisi seimbang dengan konsumen. Prinsip *the due care theory*, pelaku usaha mempunyai kewajiban untuk berhati-hati dalam memasarkan suatu produk, baik berupa barang maupun jasa. Selama berhati-hati dengan produknya, pelaku usaha tidak dapat dipersalahkan. Prinsip *the privity of contract* pelaku usaha mempunyai kewajiban melindungi konsumen, namun hal tersebut dilakukan bila diantara mereka terjadi suatu hubungan kontraktual.

Az. Nasution mendefinisikan Perlindungan Konsumen adalah suatu bagian dari hukum yang memuat asas-asas atau kaidah-kaidah yang bersifat mengatur dan juga mengandung sifat yang melindungi kepentingan Konsumen. Adapun hukum Konsumen diartikan sebagai keseluruhan asas-asas dan kaidah-kaidah hukum yang mengatur hubungan dan masalah antara berbagai pihak satu sama lain yang berkaitan dengan barang dan/atau jasa Konsumen dalam pergaulan hidup.

Perlindungan konsumen merupakan hal yang sangat perlu untuk terus dikembangkan karena berkaitan dengan upaya mensejahterakan masyarakat dalam kaitan dengan semakin berkembangnya transaksi perdagangan di era serba modern saat ini. Perhatian mengenai perlindungan konsumen ini bukan hanya di Indonesia namun telah menjadi perhatian dunia.

Hukum Perlindungan Konsumen secara umum bertujuan untuk memberikan perlindungan bagi konsumen baik dalam bidang hukum privat maupun bidang hukum publik. Kedudukan Hukum

Perlindungan Konsumen berada dalam kajian Hukum Ekonomi. Berdasarkan ketentuan Pasal 1 angka (1) UUPK, perlindungan konsumen adalah "Segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan hukum kepada konsumen" Kalimat yang menyatakan "segala upaya yang menjamin adanya kepastian hukum", diharapkan menjadi benteng untuk meniadakan tindakan sewenang-wenang yang merugikan pelaku usaha hanya demi untuk kepentingan perlindungan konsumen.

Berdasarkan pemahaman bahwa perlindungan konsumen mempersoalkan perlindungan hukum yang diberikan kepada konsumen dalam usahanya untuk memperoleh barang atau jasa dari adanya kemungkinan kerugian, maka. Hukum perlindungan konsumen dapat dikatakan sebagai hukum yang mengatur tentang pemberian perlindungan terhadap konsumen sebagai pemenuhan kebutuhannya terhadap konsumen Dengan demikian, hukum perlindungan konsumen mengatur hak dan kewajiban produsen, serta cara-cara untuk mempertahankan hak dan kewajiban itu.[43] Dalam berbagai litelatur ditemukan sekurang-kurangnya dua istilah mengenai hukum yang mempersoalkan konsumen, yaitu hukum konsumen dan hukum perlindungan konsumen. Az. Nasution berpendapat bahwa kedua istilah itu berbeda, yaitu bahwa hukum perlindungan konsumen adalah bagian dari konsumen. Hukum Konsumen menurutnya adalah "Keseluruhan asas-asas dan kaidah-kaidah hukum yang mengatur hubungan dan masalah antara berbagai pihak satu sama lain berkaitan dengan barang dan/atau jasa konsumen, didalam pergaulan hidup".

Makna dari kata "keseluruhan" bermaksud untuk menggambarkan bahwa didalamnya termasuk seluruh pembedaan hukum menurut

[43] Janus Sidabolok, *Hukum Perlindungan Konsumen di Indonesia*, Citra Aditya Bakti, Bandung, 2010, hlm. 45.

jenisnya. Jadi termasuk didalamnya, baik aturan hukum pidana, perdata, administrasi negara hingga aturan hukum internasional. Sedangkan cakupannya adalah ”hak dan kewajiban serta cara-cara pemenuhannya dalam usahanya untuk memenuhi kebutuhannya”, yaitu bagi konsumen mulai dari usaha untuk mendapatkan kebutuhannya dari produsen, meliputi : hak atas informasi yang diterima, memilih harga, hingga akibat-akibat yang timbul karena penggunaan kebutuhan itu, misalnya untuk mendapatkan penggantian kerugian. Sedangkan bagi produsen meliputi kewajiban yang berkaitan dengan produksi, penyimpanan, peredaran dan perdagangan produk, serta akibat dari pemakaian produk itu. Dengan demikian, jika perlindungan konsumen diartikan sebagai segala upaya yang menjamin adanya kepastian pemenuhan hak-hak konsumen sebagai wujud perlindungan kepada konsumen, maka hukum perlindungan konsumen tidak lain adalah hukum yang mengatur upaya-upaya untuk menjamin terwujudnya perlindungan hukum terhadap kepentingan konsumen.

B. Dasar Hukum Perlindungan Konsumen

Pada dasarnya, terdapat dua instrumen hukum penting yang menjadi landasan kebijakan perlindungan konsumen di Indonesia, yakni:

Pertama, Undang-Undang Dasar 1945, sebagai sumber dari segala sumber hukum di Indonesia, mengamanatkan bahwa pembangunan nasional bertujuan untuk mewujudkan masyarakat adil dan makmur. Tujuan pembangunan nasional diwujudkan melalui sistem pembangunan ekonomi yang demokratis sehingga mampu menumbuhkan dan mengembangkan dunia yang memproduksi barang dan jasa yang layak dikonsumsi oleh masyarakat.

Kedua, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). Lahirnya Undang-undang ini memberikan harapan bagi seluruh masyarakat Indonesia, untuk memperoleh perlindungan atas kerugian yang diderita atas transaksi suatu barang dan jasa. UUPK menjamin adanya kepastian hukum bagi konsumen.

C. Asas-asas dan Tujuan Perlindungan Konsumen

Asas hukum menurut Paul Scholten adalah kecenderungan yang memberikan suatu penilaian yang bersifat etis terhadap hukum. Begitu pula menurut H.J. Hommes, asas hukum bukanlah norma hukum yang konkrit, melainkan sebagai dasar umum atau petunjuk bagi hukum yang berlaku. Sepakat dengan pendapat tersebut, menurut Satjipto Rahardjo asas hukum mengandung tuntutan etis, merupakan jembatan antara peraturan dan cita-cita sosial dan pandangan etis masyarakat.[44] Terdapat lima asas penting yang diatur dalam Undang-undang perlindungan konsumen Pasal 2 UUPK dan dijabarkan lebih lanjut dalam penjelasan atas pasal 2 UUPK , yaitu:

1. Asas manfaat;
2. Asas keadilan;
3. Asas keseimbangan;
4. Asas keamanan dan keselamatan;
5. Asas kepastian hukum.

Asas manfaat dimaksudkan dalam penyelenggaraan perlindungan konsumen harus memberikan manfaat bagi kepentingan konsumen serta pelaku usaha secara keseluruhan. Artinya asas ini mengharapkan bahwa pengaturan dan penegakkan hukum perlindungan konsumen tidak bermaksud untuk menempatkan salah satu pihak konsumen maupun pelaku usaha diatas pihak lainnya atau sebaliknya, tetapi

[44] Wahyu Sasongko, *Ketentuan-Ketentuan Pokok Hukum Perlindungan Konsumen,* Universitas Lampung, 2007, hlm. 36.

untuk memberikan kepada para pihak yakni, pelaku usaha dan konsumen, tentang hak apa saja yang diperoleh kedua pihak. Dengan demikian, diharapkan bahwa pengaturan dan penegakkan hukum perlindungan konsumen dapat bermanfaat bagi seluruh lapisan masyarakat dan pada gilirannya bermanfaat bagi kehidupan berbangsa. Asas keadilan dimaksudkan agar partisipasi atau keterlibatan seluruh rakyat dapat diwujudkan semaksimal mungkin dan memberikan kesempatan kepada konsumen dan pelaku usaha untuk memperoleh haknya dan melaksanakan kewajibannya secara adil. Asas ini menghendaki bahwa melalui pengaturan dan penegakkan hukum perlindungan konsumen indonesia, konsumen dan pelaku usaha dapat berlaku adil melalui perolehan hak dan kewajiban yang berimbang. Karena itu, undang-undang ini mengatur sejumlah hak dan kewajiban konsumen dan pelaku usaha (produsen).[45]

Asas keseimbangan dimaksudkan untuk memberikan keseimbangan antara kepentingan konsumen, pelaku usaha, dan pemerintah dalam arti materiil dan spiritual. Asas ini menghendaki agar konsumen, pelaku usaha, dan pemerintah mampu memperoleh manfaat yang sama imbangnya sesuai hak dan kewajibannya.

Asas keamanan dan keselamatan konsumen dimaksudkan untuk memberikan jaminan atas keamanan dan keselamatan kepada konsumen dalam penggunaan, pemakaian dan pemanfaaatan barang atau jasa yang dikonsumsi atau digunakan. Asas ini mengharapkan bahwa adanya jaminan hukum terhadap konsumen yang akan mendapatkan berbagai macam manfaat dari produk yang dipakai atau dikonsumsi oleh konsumen, begitu pula sebaliknya produk yang

[45] Janus Sidabalok, *Op., Cit.,* hlm. 31-32.

dipakai atau dikonsumsi tidak akan mengancam keselamatan harta bendanya.

Asas kepastian hukum dimaksudkan agar baik pelaku usaha maupun konsumen menaati hukum dan memperoleh keadilan dalam penyelenggaraan perlindungan konsumen serta negara menjamin kepastian hukum. Artinya asas ini mengharapkan aturan-aturan tentang hak dan kewajiban yang terdapat di undang-undang perlindungan konsumen harus diterapkan dalam kehidupan sehari-hari sehingga masing-masing pihak mendapatkan keadilan.

Guna menjamin terlaksananya undang-undang ini setiap peraturan perundang-undangan yang mengatur hubungan antara pelaku usaha dan konsumen harus mengikuti dan mengacu mengacu dan mengikuti kelima asas tersebut, karena dijunjung tinggi dalam penyelenggaraan perlindungan konsumen.

Berdasarkan isi Pasal 2 UUPK, terlihat bahwa rumusannya merujuk pada filosofi pembangunan nasional yakni pembangunan manusia Indonesia seutuhnya yang berlandaskan falsafah NKRI. Kelima asas yang disebutkan dalam pasal tersebut, bila diperhatikan substansinya dapat dibagi menjadi 3 (tiga) asas, yaitu :[46]

1. Asas kemanfaatan yang didalamnya meliputi asas keamanan dan keselamatan konsumen;
2. Asas keadilan yang didalamnya meliputi asas keseimbangan;
3. Asas kepastian hukum.

Menurut Radbruch Friedman menerangkan ketiga macam asas tersebut yakni keadilan, kemanfaatan, dan kepastian hukum sebagai

[46] *Ibid.,*

"tiga ide dasar hukum" atau "tiga nilai dasar hukum",[47] artinya dapat disamakan dengan asas hukum. Dari ketiga macam asas yang disebutkan sering menjadi sorotan utama adalah masalah keadilan, dimana Friedman menyebutkan bahwa: *"In terms of law, justice will be judget as how law treats people and how it distributes its benefits and cost," dan dalam hubungan ini Friedman juga menyatakan bahwa "every function of law, general or specific, is allocative".*[48]

Sebagai asas hukum, secara langsung menempatkan asas ini menjadi awal rujukan, baik dalam pengaturan perundang-undangan maupun dalam berbagai kegiatan yang berhubungan dengan perlindungan konsumen. Asas keadilan, kemanfaatan, dan kepastian hukum oleh banyak ahli hukum disebut juga sebagai tujuan hukum. Permasalahannya, sebagai tujuan hukum, baik Radbruch Friedman maupun Achmad Ali mengemukakan adanya kesulitan untuk mewujudkannya secara bersamaan. Achmad Ali berpendapat, bila dikatakan tujuan hukum sekaligus mewujudkan keadilan, kemanfaatan dan kepastian hukum, apakah hal itu tidak menimbulkan masalah? Pada kenyataannya tujuan yang satu dan tujuan lainnya sering berbenturan satu sama lain. Sebagai contoh, dalam suatu kasus hukum tertentu bila hakim menginginkan putusannya "adil" menurut pandangannya, maka akibatnya sering merugikan kemanfaatan bagi masyarakat luas, demikian pula sebaliknya.[49]

Tujuan Hukum Perlindungan Konsumen

Tujuan perlindungan konsumen mencakup aktivitas-aktivitas penciptaan dan penyelenggaraan perlindungan konsumen. Dalam Pasal 3 UUPK telah dijelaskan mengenai tujuan konsumen, yakni :

[47] Ahmad Miru dan Sutarman Yudo, *Op. Cit.,* hlm. 26.
[48] *Ibid.,*
[49] *Ibid.,*

1. Meningkatkan kesadaran, kemampuan dan kemandirian konsumen untuk melindungi diri;
2. Mengangkat harkat dan martabat konsumen dengan cara menghindarkannya dari ekses negatif pemakaian barang dan/atau jasa;
3. Meningkatkan pemberdayaan konsumen dalam memilih, menentukan dan menuntut hak-haknya sebagai konsumen;
4. Menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi;
5. Menumbuhkan kesadaran pelaku usaha mengenai pentingnya perlindungan konsumen sehingga tumbuh sikap yang jujur dan bertanggung jawab dalam berusaha;
6. Meningkatkan kualitas barang dan/atau jasa yang menjamin kelangsungan usaha produksi barang dan/atau jasa, kesehatan, kenyamanan, keamanan, dan keselamatan konsumen.

Tujuan dari perlindungan konsumen tersebut seakan-akan disusun secara bertahap, mulai dari kesadaran hingga pemberdayaaan kualitas barang atau jasa. Akan tetapi, untuk mencapai tujuan perlindungan konsumen tidak harus melalui tahapan-tahapan berdasarkan susunan dalam pasal 3 UUPK tersebut. Namun melihat pada urgensinya. Sebagai contoh, tujuan yang tercantum dalam nomor enam yakni, tujuan untuk meningkatkan kualitas barang atau jasa, untuk mencapainya tidak harus menunggu tujuan yang tercantum dalam nomor pertama tercapai terlebih dahulu. Idealnya, pencapaian tujuan perlindungan konsumen dilakukan secara simultan atau serempak.[50]

[50] Wahyu Sasongko, *Op., Cit.,* hlm. 41.

D. Pengertian Transaksi E-Commerce

E-Commerce atau *Electronic Commerce* juga biasa diterjemahkan dalam bahasa indonesia sebagai "perdagangan elektronik" adalah kegiatan yang berkaitan dengan pembelian, penjualan, pemasaran barang atau jasa dengan menggunakan sistem elektronik seperti internet atau jaringan komputer. *E-commerce* juga melibatkan aktivitas yang berkaitan dengan proses transaksi elektronik seperti transfer dana elektronik, pertukaran data elektronik, data persediaan sistem pengolahan dilakukan oleh sistem komputer atau jaringan komputer, dan lain sebagainya.

Kegiatan perdagangan di masyarakat telah berkembang sangat pesat. Hal tersebut dipengaruhi beberapa faktor salah satunya dengan berkembangnya teknologi yang berbasis internet yang dikenal dengan nama *E-commerce*. Perkembangan *E-commerce* tidak terlepas dari laju pertumbuhan dunia maya/internet karena *E-commerce* berjalan melalui jaringan internet. Pertumbuhan pengguna internet yang sedemikian pesatnya merupakan suatu kenyataan yang membuat internet menjadi media yang efektif baik untuk perseorangan maupun perusahaan untuk mempromosikan atau menjual barang dan atau jasa kepada konsumen yang berada diseluruh dunia. *E-Commerce* merupakan jenis bisnis modern yang tidak menghadirkan pelaku bisnis secara fisik (*non-fice*) dan tidak memakai tanda tangan asli (*non-sign*).

Sebagai suatu perdagangan dengan basis teknologi caggih, *E-commerce* telah mereformasi perdagangan konvensional di mana interaksi antara konsumen dengan perusahaan yang sebelumnya dilakukan secara langsung (*face to face*) menjadi interaksi tidak langsung. *E-commerce* telah merubah pandangan bisnis klasik dengan cara menumbuhkan macam-macam cara interaksi antara produsen dan

konsumen di dunia maya. Sistem perdagangan yang digunakan dalam *E–commerce* dirancang guna penandatanganan secara elektronik. Penandatanganan elektronik ini dirancang dimulai dari saat proses jual-beli, pemeriksaan hingga pengiriman.[51] Oleh karena itu ketersediaan informasi yang benar dan akurat mengenai konsumen dengan perusahaan dalam *E-commerce* merupakan suatu persyaratan mutlak. Permasalahan akibat liberalisasi perdagangan melalui internet diwujudkan dalam bentuk pengaduan/komplain dari konsumen atas barang atau jasa yang dikonsumsinya.

E-commerce dapat diartikan sebagai segala bentuk transaksi perdagangan atau perniagaan barang atau jasa *(trade of goods and services)* dengan menggunakan media elektronik. Adapun ruang lingkup *E-commerce* meliputi tiga sisi yakni segmentasi bisnis ke bisnis, bisnis ke konsumen dan konsumen ke konsumen.[52]

E. Undang-Undang Perlindungan Konsumen dalam Mengakomodasi Transaksi *E-commerce*

UUPK belum dapat melindungi konsumen dalam transaksi *E-commerce* karena ketentuan–ketentuan yang tercantum dalam UUPK belum mengakomodir hak–hak konsumen dalam transaksi *E-commerce*. Hal ini dikarenakan *E-commerce* memiliki ciri khas/karakteristik tersendiri dibandingkan dengan transaksi konvensional. Karakteristik tersebut adalah : tidak bertemunya penjual dan pembeli, media yang digunakan adalah internet, transaksi dapat terjadi melintasi batas–batas yuridis suatu negara, barang yang diperjualbelikan dapat berupa barang/jasa atau produk digital seperti software. Dalam hukum positif Indonesia, hak –

---

[51] Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis E-commerce*, Pustaka Pelajar, Yogyakarta, 2005, hlm. 7.

[52] Riyeke Ustadianto, *Frameworks E-commerce*, Penerbit Andi, Yogyakarta, 2001, hlm. 139-143.

hak konsumen diakomodir dalam Pasal 4 UUPK yang terdiri dari. Hak atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang maupun jasa. Hak untuk memilih barang maupun jasa serta mendapatkan barang atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan. Hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang maupun jasa. Hak untuk didengar pendapat dan keluhannya atas barang atau jasa yang digunakan. Hak untuk mendapatkan advokasi perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut. Hak untuk mendapatkan pembinaan dan pendidikan konsumen. Hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif. Hak untuk mendapatkan kompensasi, ganti rugi penggantian, apabila barang atau jasa yang diterima tidak dengan perjanjian atau tidak sebagaimana mestinya. Hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.

Mengenai transaksi *E-commerce* terutama dalam pemenuhan hak–hak konsumen sangat riskan sekali untuk dilanggar, dalam hal ini konsumen tidak mendapatkan hak–haknya secara penuh dalam transaksi *E-commerce*. Hak–hak tersebut antara lain hak atas kenyamanan, hak atas informasi, hak untuk didengar pendapat, serta hak untuk mendapatkan advokasi.

Beraneka ragam kasus yang muncul berkenaan dengan tumbuh kembangnya metode-metode transaksi secara elektronik terutama faktor keamanan dalam *E-commerce* tentunya sangat merugikan konsumen. Padahal dengan adanya jaminan dalam transaksi *E-commerce* ini sangat diperlukan untuk menumbuhkan tingkat kepercayaan konsumen. Dengan tidak diperhatikannya jaminan keamanan dikhawatirkan akan mengakibatkan pergeseran substansi

yang terkandung dalam transaksi *E-commerce* menuju ke arah ketidakpastian yang akan menghambat perkembangan *E-commerce.*[53]

Apabila diperhatikan, hak–hak konsumen yang secara normatif diatur oleh UUPK seakan-akan terbatas pada kegiatan perdagangan yang bersifat konvensional. Di sisi lain perlindungan difokuskan hanya pada posisi konsumen serta posisi produk yang diperdagangkan sedangkan perlindungan dari posisi pelaku usaha seperti informasi-informasi umum mengenai identitas perusahaan pelaku usaha dan jaminan kerahasiaan data-data milik konsumen belum diakomodir oleh UUPK, padahal hak–hak tersebut sangat penting untuk diatur untuk keamanan konsumen dalam bertransaksi

[53] Yudha Sri Wulandari, *Perlindungan Hukum bagi Konsumen terhadap Transaksi Jual Beli E-Commerce*, Jurnal Ilmu Hukum, Vol. 2, No 2, Desember 2018, hlm. 205.

DAFTAR PUSTAKA

Buku

Abdul Hakim Barkatullah dan Teguh Prasetyo, *Bisnis E-commerce*, Pustaka Pelajar, Yogyakarta, 2005.

Agus Raharjo, Cyber Crime, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, 2002.

Ahamadi Miru dan Sutarman Yodo, *Hukum Perlindungan Konsumen,* Jakarta, PT. Raja Grafindo Persada, 2004.

Ahmad ramli, *Cyber Law dan Haki dalam Sistem Hukum Indonesia,* Bandung, Refika Aditama, 2010.

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Predana Media Group, Jakarta, 2007.

Buku Panduan Hak Kekayaan Intelektual (Direktorat Jenderal Hak Kekayaan Intelektual, 2013)

Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya Cetakan I,* Laksbang Pressindo, Yogyakarta, 2007.

Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi,* Bandung, Refika Aditama, 2009.

H. Sofwan Jannah, dkk., *Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif dan Hukum Islam*, Jurnal Al-Mawarid,Vol. XII, Nomor 1, Februari-Agusutus, 2012.

Haris Munandar dan Sally Sitanggang, *Mengenal Hak Kekayaan Intelektual, Hak Cipta, Paten,Merek, dan Seluk-Beluknya*, Erlangga,Jakarta, 2008.

Janus Sidabolok, *Hukum Perlindungan Konsumen di Indonesia*, Citra Aditya Bakti, Bandung, 2010, hlm. 45.

M. Sadar, Moh. Taufik Makarao, Habloel Mawadi, *Hukum Perlindungan Konsumen di Indonesia*, Akademia, Jakarta, 2012.

Muhammad Amirulloh, *Cyber Law Perlindnungan Merek Dalam Cyber Space (Cybersquatting terhadap Merek)*, Refika Aditama, Bandung, 2017.

Muhammad Djumhana & R. Djubaedillah, *Hak Milik Intelektual (Sejarah, Teori dan Prakteknya di Indonesia)*, Bandung, Citra Aditya Bakti, 1997.

Riyeke Ustadianto, *Frameworks E-commerce*, Penerbit Andi, Yogyakarta, 2001.

Satjipto Rahardjo,*Penegakan Hukum Suatu Tinjauan Sosiologis*, Genta Publishing, Cetakan 1, Yigyakarta, 2009.

Sigid Suseno, *Yurisdiksi Tindak Pidana Siber,* Bandung, Refika Aditama, 2012.

Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Rajawali Pers, Cetakan 13, Jakarta, 2014.

Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya Cetakan 1*, LaksBang Pressindo, Yogyakarta, 2007.

Tim Lindsey, dkk, *Hak Kekayaan Intelektual Suatu Pengantar,* Bandung, PT Alumni, 2013.

Tomi Suryo, *Hak Kekayaan Intelektual (HKI) di Era Globalisasi, Sebuah Kajian Kontemporer*, Graha Ilmu, Yogyakarta, 2010.

Wahyu Sasongko, *Ketentuan-Ketentuan Pokok Hukum Perlindungan Konsumen,* Universitas Lampung, 2007.

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

----------, *Hukum Pidana di Bidang teknologi Informasi (cybercrime law) : Telaah Teoritik dan Bedah Kampus,* Yogyakarta, 2013.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Acara Pidana

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman

Website

NN, *Tindak Pidana Cybercrime, Repository* Universitas Muhammadiyah Yogyakarta, http://repository.umy.ac.id/, Diakses pada Hari Senin, Tanggal 16 Juni 2020, Pukul 20.59 WIB.

NN., *Karakteristik Cyber Crime,* http://eptikkel/2013/05/karakteristik-cyber-crime.html, diakses pada Hari Selasa, Tanggal 16 Juni 2020, Pukul 21.46 WIB.

Yadi, *Cybersoace, Cybercrune dan Cyberlaw, http://yandi-sage./cyberspace-cybercrime-dan-cyberlaw.html,* diakses Pada hari Minggu, tanggal 14 Juni 2020, Pukul 10.30 WIB

Dr. SAHAT MARULI TUA SITUMEANG, S.H., M.H.

Adalah seorang Advokat dan juga dosen Fakultas Hukum UNIKOM, dilahirkan pada tahun 1961. Saat ini beliau menjabat sebagai Ketua Prodi Ilmu Hukum. Dikenal oleh banyak orang, sebagai *seorang praktisi yang gigih, berani dan berpihak kepada keadilan*, dalam bidang ilmu hukum sudah tidak diragukan lagi keilmuannya, terbukti dengan terbitnya buku "**Penahanan Tersangka"**. Buku tersebut mendapatkan tempat yang luar biasa dan sambutan yang hangat di antara para Doktor Ilmu Hukum. Dalam kesehariannya banyak mengikuti berbagai seminar dan menulis, baik artikel maupun makalah. Saat ini beliau sedang menyiapkan beberapa buku yang merupakan hasil dari pemikirannya dalam bergelut di bidang hukum, di antaranya: **Mengupas Tuntas Kejahatan *Cyberlaw***; **Praktik Beracara di Pengadilan: Antara *Das Solen* dan *Das Sein*;** serta buku yang sangat dinanti oleh para ahli ilmu hukum yakni **Perkembangan Aliran filsafat Hukum Kontemporer.**